Stable Natural Language Understanding via Invariant Causal Constraint

Anonymous ACL submission

Abstract

Natural Language Understanding (NLU) task requires the model to understand the underlying semantics of input text. However, recent analyses demonstrate that NLU models tend to utilize dataset biases to achieve high dataset-specific performances, which always leads to performance degradation on out-of-distribution (OOD) samples. To increase the performance stability, previous debiasing methods empirically capture bias features from data to prevent model from corresponding biases. However, we argue that, the semantic information can form a causal relationship with the target labels of the NLU task, while the biases information is only correlational to the target labels. Such difference between the semantic information and dataset biases still remains not fully addressed, which limits the effectiveness of debiasing. To address this issue, we analyze the debiasing process under a causal perspective, and present a causal invariance based stable NLU framework (CI-sNLU). Experimental results show that CI-sNLU can consistently improve the stability of model performance on OOD datasets.

1 Introduction

State-of-the-art Natural Language Understanding (NLU) models such as BERT have demonstrated promising performance on various tasks (Devlin et al., 2019; Liu et al., 2019). These NLU models are generally first pretrained to learn universal language representations, then finetuned to adapt to specific downstream tasks. However, recent analyses demonstrate that these models tend to exploit the dataset biases spuriously associated with the target labels, rather than learn the underlying semantic information (McCoy et al., 2019; Clark et al., 2019; Sanh et al., 2020). This leads to performance degradation on out-of-distribution (OOD) samples.

To mitigate the impact of dataset biases and obtain NLU models that have stable performance on both in-distribution samples and OOD samples, a number of debiasing methods have been proposed. These methods work by first identifying the potential dataset biases within the dataset, then regularizing NLU model prevent it from capturing the bias information. To identify the potential biases, one line of debiasing works depends on the intuitions of researchers to design features characterizing the distribution of dataset biases (Schuster et al., 2019; Clark et al., 2019; He et al., 2019). However, the assumption that the types of bias should be known a-priori limits their application to many NLU tasks and datasets. Hence, automatic debiasing methods are proposed to move beyond the reliance on prior knowledge. These works usually train a biased model to to automatically capture the dataset bias and obtain a set of bias features. Then based on the identified biases information, model regularization methods such as Product-of-Expert (Hinton, 2002) or Confidence Regularization (Hinton et al., 2015) can be employed to prompt model to focus on learning the semantic information.

While promising, previous debiasing methods work by empirically inducing bias features from data. However, we argue that, the semantic information of text is causal to the target label, while the bias information has only correlational relationship. This drives to the essential difference between the bias information and semantic information. Present debiasing methods are still unaware of knowledge about causal invariance. Hence, the effectiveness of bias feature identification could be rather limited, influencing the efficiency of debiasing.

Figure 1 provides an example for illustrating the difference between semantic information and bias information in the causal perspective. In specific, it is the similar semantics between the Premise: A cat caught a mouse. and Hypothesis: A mouse was caught by a cat., that causes the label to be “entailment”. Therefore, the semantic information forms a causal relationship with the label. Fur-
We first analyze the stable NLU process under a causal perspective. The natural language understanding (NLU) task requires a model to understand the semantic of input text and then predict the target label. Formally, it can be characterized by a projection \( X \rightarrow Y \), where \( X \) and \( Y \) denote the input text and the label, respectively. A NLU model \( M \) is trained to capture the predictive informations within \( X \), and get a representation of input text \( h_M \in \mathbb{R}^d \). For brevity, in the following sections, we call \( h_M \in \mathbb{R}^d \) as model representation. Then the label can be predicted based on \( h_M \). Hence, concerning \( h_M \), the NLU process can be reformulated as: \( M : X \rightarrow h_M \rightarrow Y \).

However, the predictive information within \( X \) is actually composed of two components: the semantic information \( S \) that decides the value of label, and the dataset biases \( B \) that only correlative to the value of label (Tsipras et al., 2018; McCoy et al., 2019; Pearl, 2009). The dataset biases could range from simple lexical overlap (Gururangan et al., 2018; Poliak et al., 2018), to complex language stylistic patterns (Zellers et al., 2019; Nie et al., 2020). As Figure 2 (a) shows, since the semantic information decides the value of labels, there is a causal relationship between \( S \) and \( Y \). Furthermore, such relationship would keep valid upon different instances across different datasets (Pearl et al., 2000; Pearl, 2009). Formally, such invariance can be characterized as:

\[
P(Y_{D_i}|S_{D_i}) = P(Y_{D_j}|S_{D_j}),
\]

where \( D_i = \{X_{D_i}, Y_{D_i}\} \) and \( D_j = \{X_{D_j}, Y_{D_j}\} \) are arbitrary two NLU datasets, \( S_{D_i} \) denotes the semantic information within \( X_{D_i} \).

On the contrary, the correlation relationship between the dataset biases with the label would vary across different datasets, i.e.:

\[
P(Y_{D_i}|B_{D_i}) \neq P(Y_{D_j}|B_{D_j}),
\]

where \( B_{D_i} \) is the dataset biases within \( X_{D_i} \). Therefore, having or not causal invariance forms the essential difference between semantic information and bias information.

In order for \( M \) to capturing the necessary semantic information within \( X \) without involving the bias information, \( h_M \) should satisfy a causal invariant constraint:

\[
\forall X_i \in \mathcal{T} : P_{do(X=X_i)}(Y|h_M) = P_{do(X=X_i)}(Y|X)
\]

\[
P(Y_{D_i}|h_{D_i}^M) = P(Y_{D_j}|h_{D_j}^M)
\]

where \( \mathcal{T} \) denotes the training set, \( P_{do(X=X_i)} \) denotes the distribution arising from assigning \( X \) to
be a certain instance \( X_i \) (Pearl, 2009). This means, (1) \( h^M \) contains the semantic information that decides the value of label \( Y \). (2) Such causal relationship exist in every instance \( X_i \in \mathcal{T} \), and keep valid for arbitrary OOD datasets. Hence, training a model \( \mathcal{M} \) satisfying the causal invariant constraint is the goal of stable NLU, as shown in Figure 2 (b).

However, for models that only have access to the input text-target label pairs, they have no information to distinguish the causal relationship from the correlative relationship. Hence, with the existence of the bias in the dataset, such models would inevitably capture the dataset bias correlative to the target label (Figure 2 (c)). Which makes \( h^M \) contain both the semantic information \( S \) and the biases \( B \) and leads to the instability. Debiasing methods have been proposed to mitigate the influence of biases. However, due to the absence of causal mechanism in these debiasing methods, their ability for distinguishing the bias information from the semantic information would still be limited.

To address this issue, we propose a Causal Invariance based stable NLU (CI-sNLU) framework. CI-sNLU employs criteria deduced from the causal invariant constraint to identify the bias information that the model captured, and regularizes model to exclude the identified bias information by enforcing \( h^M \) to obey the constraint.

3 Methodology

3.1 Causal Invariance Based Biases Identification

The causal invariance bias feature identification algorithm dynamically identifies the biases captured by the model during the training process. The core assumption of the algorithm is that the semantic representation of instances will obey the causal invariance constraint, while the bias features correlate relative to the label does not. Hence, if we can discover the instances on which the causal invariance constraint is violated, then it could be probable to identify the bias features from the model representations of these instances.

In specific, as described in the causal invariance constraint (Eq. 3), if the model can capture the semantic information causal to the label and obtain representation \( h^M \), then for two instances \( X_i \) and \( X_j \), if their representation \( h^M_i \) and \( h^M_j \) are rather similar, then \( P(Y_i | M_i) \) should be rather close to \( P(Y_j | M_j) \). Therefore, if we can find instance pairs \( (X_i, X_j) \), on which \( h^M_i \) is rather close to \( h^M_j \), whereas \( Y_i \neq Y_j \), then these examples can be regarded as counter instances that violates the causal invariance constraint, and can be utilized for detecting the bias information \( M \) utilizes. For clarity, we define such instance pairs \( (X_i, X_j) \) as a counter instance pair:

Definition 1 (Counter Instance Pair):

\[
\forall \{X_i, Y_i\}, \{X_j, Y_j\} \in \mathcal{T}, i \neq j, \text{ if:}
\]

\[
S(h^M_i, h^M_j) > \tau, \text{ s.t. } Y_i \neq Y_j \wedge (Y_i = Y_j \lor Y_i = Y_j)
\]

where \( S(\cdot) \) is a score function measuring the similarity between \( h^M_i \) and \( h^M_j \), \( \tau \) is a threshold controlling the confidence that \( h^M_i \) and \( h^M_j \) can be deemed as the representation of the same semantic information. \( Y_i, Y_j \) are model prediction of \( Y_i \) and \( Y_j \), respectively. Note that, the additional condition \( Y_i = Y_i \lor Y_j = Y_j \) requires that model should make a correct prediction for \( X_i \) or \( X_j \). This is because, if \( M \) fails to correctly predict the label on both \( X_i \) and \( X_j \), then it is more likely that \( M \) has not captured the predictive information in \( X_i \) and \( X_j \), rather than using the bias information.

To dynamically detect counter instance pairs within \( \mathcal{T} \) during the training process, as Figure 2 (d)
shows, we divide the training process into two alternate stages: a parameter optimization stage and a retrospect stage. In the parameter optimization stage, we train \( \mathcal{M} \) to find new predictive features from data, meanwhile regularize \( \mathcal{M} \) to exclude the known biases using a causal invariance based regularizer (which is described in the following section). In the retrospect stage, CI-sNLU finds the counter instance pairs using the model representations, to discover the bias features that model temporarily captures and update the bias features.

Parameter Optimization Given training dataset \( \mathcal{T} = \{X_i, Y_i\} \), we update the parameters of the NLU model \( \mathcal{M} \) through maximizing the likelihood. Meanwhile \( \mathcal{M} \) is regularized using a regularizer \( \mathcal{R}(\mathcal{M}, h^b_t) \) to exclude the bias components from fitting the bias information, where \( h^b_t = \{h^b_{i,t}\} \) is a \( d \)-dimension random variable, characterizing the distribution of the dataset biases on the training set \( \mathcal{T} \), \( h^b_{i,t} \) is the temporal bias feature of sample \( i \) at \( t \)th step. \( h^b_0 \) is initialized using the previous automatic debiasing methods (e.g., the method of Utama et al. (2020b)), and updated in the retrospect stage of the training process.

Retrospect After \( t \) steps of parameter optimization, we examine whether all model representation of each instance \( \{X_i, Y_i\} \in \mathcal{T} \) satisfy the causal invariance constraint, to find the representation of instances that may contains bias information, and update \( h^b \). In specific, for each instance \( \{X_i, Y_i\} \in \mathcal{T} \), we utilize \( \mathcal{M} \) to obtain corresponding temporal model representations \( h^M_{i,t} \), and predictions of the label \( \hat{Y}_{i,t} \), together with a probability \( \hat{p}_{i,t} = P(Y_{i,t}|h^M_{i,t}) \).

Then We traverse \( \mathcal{T} \) to find all the counter instance pairs according to the definition described in Eq.4. In practice, we implement \( S(\cdot) \) using the cosine similarity function, and introduce two more conditions to enhance the confidence of counter instance pairs detection, i.e., for \( X_i, X_j \in \mathcal{T} \), to be the counter instance pairs, we further require that:

\[
\hat{p}_{i,t} > \tau_p, \quad \hat{p}_{j,t} > \tau_p
\]

where \( \tau_p \) is a threshold for filtering out the predictions that have low confidence. With this additional threshold, we can further control the confidence on the discovered bias feature. Note that, the counter instance pairs are found at the \( t \)th parameter optimization step. Hence, we can dynamically detect the bias feature temporarily captured by the model for updating the bias feature distribution, rather than only relying on fixed bias features.

Hence, for each sample \( X_i \in \mathcal{T} \), at the \( t \)th step, its bias features \( h^b_{i,t} \) can be updated using the representation of corresponding counter instances as:

\[
h^b_{i,t} = h^b_{i,t_0} + \alpha \frac{1}{|\mathcal{N}_{C_i}|} \sum_{j \in \mathcal{N}_{C_i}} h^M_{j,t}
\]

where \( h^b_{i,t_0} \) is the bias feature of the \( i \) th sample previously obtained after the \( t_0 \)th parameter optimization step, \( \mathcal{N}_{C_i} \) is a set composed by all counter instances of \( X_i \), \( |\mathcal{N}_{C_i}| \) is the size of \( \mathcal{N}_{C_i} \), \( \alpha \) is a coefficient controlling the proportion of bias feature update.

After the retrospect stage, following parameter stage is conducted with \( \mathcal{M} \) regularized using the updated bias features \( h^b_{i,t} \).

3.2 Causal Invariance Based Model Regularization

In the parameter optimization stage, we employ an causal invariance based regularizer to exclude the bias information model captured by forcing the model \( \mathcal{M} \) to fulfilling the causal invariance constraint. As described in Eq. 3, the prediction should keep invariant under different kinds of bias features. A sufficient condition is that the information model representation \( h^M \) contains keeps invariant under different biases. In other words, manipulating the value of bias feature does not influence information contained within \( h^M \). The information within \( h^M \) can be characterized using its information entropy \( H(h^M) \). Hence, formally,

\[
\forall h^b_i, h^b_j \in h^b; \forall X_i \in X, \\
H^{\mathcal{D}(h^M=h^b_i)}(h^M_i|X_i) = H^{\mathcal{D}(h^M=h^b_j)}(h^M_j|X_i)
\]

One way to ensure such invariance is making the model representation \( h^M \) independent to the bias feature \( h^b \), i.e., \( h^M \perp \| h^b \). The independence makes the mutual information between \( h^b \) and \( h^M \) becomes 0, i.e., \( I(h^M, h^b) = 0 \). Hence, \( H(h^M|h^b) = H(h^M) - I(h^M, h^b) = H(h^M) \). In other words, the value of bias will not influence the information contained in \( h^M \).

Therefore, at an arbitrary parameter optimization step \( t \), if we can calculate the temporal mutual information \( I(h^M_t, h^b_t) \) and encourage it to be zero, then we can reduce the proportion of bias information contained in model representation \( h^M \) to increase the stability of model. However, in general, the precise value of mutual information \( I(h^M_t, h^b_t) \) for two random variables with complex
distribution are hard to calculate. To address this issue, we resort to approximations.

With information theory and the Law of Large Numbers (Cramér, 2016; Rao, 1992), we find that, in the training process, by predicting the label as:

\[
\hat{Y}_t = \sigma(W^2 h^2_{i,t}); \quad (8)
\]

\[
h_{i,t}^h = (h_{i,t}^M + h_{i,t}^b) \quad (9)
\]

where \(\hat{Y}_t\) is the predicted label of sample \(i\), \(\sigma(\cdot)\) is a sigmoid function, \(W \in \mathbb{R}^{d \times d}\) is a weight matrix, and then training \(\hat{Y}_t\) to close to the ground truth label \(Y_t\), theoretically, we can approximately make \(I(h_t^M, h_t^b)\) achieving its lower bound \(0\). We show the specific proving process in the Appendix. For clarity, we denote this regularizer as ADD.

4 Experiments

4.1 Evaluation Tasks

We evaluate our approach on three NLU tasks: natural language inference (NLI), fact verification, and paraphrase identification. We compare the in-distribution performance on the test set of each task.

Then examine the stability of model on OOD samples by comparing the zero-shot performance on the corresponding challenge dataset. On the NLI and fact verification task, model performance is evaluated using prediction accuracy. Following Devlin et al. (2019) and Radford et al. (2018), on the Paraphrase Identification task, we evaluate model performance using the F1 score.

Natural Language Inference This task requires the model to predict the semantic entailment relationship between a premise and a hypothesis. We use the MNLI dataset (Williams et al., 2018) as the benchmark, and use corresponding challenge HANS McCoy et al. (2019) to test the stability on OOD samples. Since HANS is built by removing the lexical overlap bias that extensively exists in the MNLI dataset, models trained on MNLI often perform close to a random baseline on HANS.

Fact Verification This task requires a model to predict whether a claim can be supported or refuted by corresponding evidences. We train model on the Fever dataset (Thorne et al., 2018), and evaluate the stability of models on the FeverSymmetric V 0.1 (Schuster et al., 2019) dataset, which is collected to remove the claim-only biases (i.e., the biases within the claims which make models able to make predictions without evidence).

Paraphrase Identification We conduct experiments on the QQP dataset\(^1\), which consists of 362K questions pairs annotated as either duplicate or non-duplicate, together with the corresponding challenge dataset PAWS (Zhang et al., 2019b), which is constructed by removing the lexical overlap biases within the QQP dataset.

4.2 Experimental Details

On all three tasks, we implement the main model \(M\) using the BERT-base model (Devlin et al., 2019), and regularize \(M\) with the ADD regularizer. The biased feature of each example \(h_b^i\) is initialized using the automatic debiasing method of (Utama et al., 2020b), which employs a BERT-base model trained upon a tiny subset of the original training set to capture the biased information.

During the training process, the biased feature detecting algorithm detects and updates the biased features at the start of the 2nd to last epoch. Before fed into the model, each example is pre-processed into a [CLS] premise [SEP] hypothesis / [CLS] claim [SEP] evidence form, where [CLS] and [SEP] are two special tokens (Devlin et al., 2019). Then we employ the embedding vector of the [CLS] token at the top transformer layer as the model representation \(h^M_{i,t}\) of each instance for finding the counter instances pairs. To increase the confidence of detected biased feature, on all three datasets, we set \(\tau_p = 0.95\), and \(\tau = 0.9\). The information update coefficient is set as \(\alpha = 0.5\). We report the average result across 5 runs. More details about the hyperparameter selection and time-costing are provided in the Appendix.

4.3 Baseline Methods

We make comparisons with:

(i) BERT (Devlin et al., 2019) refers to the BERT-base model trained upon each NLU dataset without debiasing process.

Prior-knowledge-depended Debiasing Methods

These methods rely on prior knowledge about the distribution of dataset biases to detect the biased instances, then regularize model by down-weighting the biased instances, so that the main model can focus on learning from harder examples. The major difference resides in how the main model is regularized.

(ii) Known-biasReweighting (Clark et al., 2019; Schuster et al., 2019) weights the importance of a instance using the probability that the instance exhibits a bias. (iii) Known-biasPoE (Clark et al.,

\(^1\)https://data.quora.com
2019) forces the main model to focus on learning from examples that are not predicted well by the biased model. (iv) **Known-bias**\textsubscript{Conf-reg} (Utama et al., 2020a) regularizes the main model by decreasing model confidence on biased examples.

### Auto-Debiasing Methods

(v) **Shallow Model Debiasing** (Utama et al., 2020b) trains a BERT-base model on a small subset of the training set to obtain biased features characterizing dataset biases distribution. (vi) **Weak Learner Debiasing** (Sanh et al., 2020) employs a Tiny-BERT model (Turc et al., 2019) as a weak learner to obtain the biased features. (vii) **LTGR** (Du et al., 2021) employs a teacher model to regularize the main model from capturing bias and encourage it to learn long-tailed features.

In this paper, all the baseline debiasing methods take the BERT-base model as the main model.

#### 4.4 Main Results

From Table 1 we observe that:

1. Comparing the automatic debiasing methods with the prior knowledge based debiasing methods show that, in general, there is still a performance gap between automatic and prior-knowledge based debiasing methods. This is because the distribution of dataset bias can be rather complex, which leads to challenges in precisely and comprehensively detecting the potential biases, and makes automatic debiasing still remaining a challenging problem. However, comparing with the prior-knowledge based debiasing methods, our approach can have better or comparable performance on all three challenge datasets and can have comparable in-distribution performance. This indicates the effectiveness of our approach.

2. Comparing to the Shallow Model Debiasing and the Weak Learner Debiasing which rely on pre-detected fixed bias features, CI-sNLU can consistently improve model performance on all three challenge datasets. This indicates that, by dynamically detecting the bias information and regularizing model to follow the causal invariance constraint, our approach can effectively increase the stability of model performance.

(3) In general, improvements on the challenge datasets come with the expense of the in-distribution performance. This is because, the bias provides additional clues that leak the label information (Zhang et al., 2019a; Tsipras et al., 2018; Sanh et al., 2020). Hence, omit of the bias would naturally lead to a performance decrease on in-distribution samples. Different from previous methods, as described in Eq.(8-9), CI-sNLU can also combine the bias features to make predictions, to accommodate the situation where only in-distribution performance is desired.

### 4.5 Ablation Study

We conduct ablation study by training CI-sNLU without the causal invariance based feature identification (denoted as CI-sNLU -w/o iden) and substituting the ADD regularizer by a POE regularizer (denoted as CI-sNLU -w POE), as POE regularizer show strong performance across multiple datasets and hence can be a strong baseline. The results are shown in Table 2, where -iden + POE represents the combination of -w/o iden and -w POE.

We have the following observations: (1) Compared to CI-sNLU -w/o iden, the vanilla CI-sNLU has better performance on the challenge set. This indicates that based on the causal invariance constraint, our approach can effectively detect the bias...
We further examine the stability of our approach, to enhance the effectiveness of debiasing. (2) Compared to CI-sNLU -w POE, CI-sNLU has better performance. This is because, the causal invariant based regularizer can minimize the mutual information between the bias features and model representations to zero, while POE cannot precisely control the amount of mutual information between $h^M$ and $h^b$, so that the model representation may still contain bias information. (3) The large performance gap between CI-sNLU and CI-sNLU -iden + POE indicates the synergetic relationship between bias feature identification and model regularizing.

4.6 Transferability Analysis

We further examine the stability of our approach through a transferability analysis. In specific, we train CI-sNLU on the MNLI dataset, then evaluate its zero-shot performance on three challenge sets ANLI R1-R3 (Nie et al., 2020). ANLI R1-R3 contains instances designed to fool the model to make wrong predictions by human edition on input text. Hence, to make correct predictions, models have to understand the semantic of input. Models utilizing bias information always have a zero-shot performance close to 0. The reason for not adopting other NLI datasets is that, different NLI datasets could probably share similar dataset bias patterns (McCoy et al., 2019; Geva et al., 2019; Du et al., 2021). Hence, it would be hard to distinguish the performance improvement brought by utilizing the same bias pattern, or by promotion in the understanding of the semantic information. Two baselines are involved for comparison: BERT-base, and Shallow Model Debiasing.

The results are shown in Table 3. We observe that: (1) The BERT-base model has poor performance on all three target tasks, especially on the ANLI R1 dataset, as it is specifically designed to fool the BERT model to make its performance close to 0. This suggests that BERT may utilize a large amount of bias features for making predictions. (2) Shallow Model Debiassing and CI-sNLU can enhance model performance on all three target datasets, indicating the effectiveness of automatic debiasing methods in mitigating the influence of dataset bias to improve model stability. (3) Compared to Shallow Model Debiassing, our approach can further increase the model performance on all three target datasets, and has more consistent performance. This suggests that by introducing the causal invariance constraint, CI-SNLU can better detect the bias information model used and regularize model to further increase the stability.

4.7 Sensitivity Analysis

In the bias feature identification process, we employ two hyperparameters $\tau_p$ and $\tau$ to control the confidence of the identified bias feature, and a hyperparameter $\alpha$ to control the proportion of bias feature update. We investigate the sensitivity of model performance upon these hyperparameters by changing the value of one hyperparameter and fixing the value of the other three hyperparameters, then observe the model performance. Experiments are conducted on MNLI and HANS. The results are shown in Figure 3.

From which we observe that: (1) Empirically, the performance of CI-sNLU keep relative stable with a wide range of hyperparameter values, for example, when $\tau_p > 0.8$, $\tau > 0.9$ and $\alpha \in [0.3, 0.7]$. This indicates the robustness of our approach on hyperparameter settings. (2) The change of hyperparameters can lead to a trade-off between the performance on in-distribution samples and OOD samples. This is because, with lower $\tau_p$, more examples can find corresponding counter instances. With lower $\tau$, a given example can match up with more counter instances. Hence, more abundant potential bias features can be identified. However, with a lower confidence on identified bias feature, some of the semantic information would be mistaken as bias information. This would lead to a performance decrease on the in-distribution samples. On the contrary, with $\tau$ and $\tau_p$ close to 1, the identification of new bias features would be strictly controlled, which impact the effectiveness of debiasing and influence the performance on the challenge set. On the other hand, too much or less bias feature updates would both harm the perfor-

<table>
<thead>
<tr>
<th>Model</th>
<th>R1</th>
<th>R2</th>
<th>R3</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT-base</td>
<td>0</td>
<td>28.9</td>
<td>28.8</td>
</tr>
<tr>
<td>Shallow Model Debiasing</td>
<td>26.4</td>
<td>29.5</td>
<td>29.3</td>
</tr>
<tr>
<td>CI-sNLU</td>
<td>27.2</td>
<td>29.5</td>
<td>31.5</td>
</tr>
</tbody>
</table>

Table 3: Zero-shot performance on target datasets.

![Image](image-url)
The NLU task requires model to understand the underlying semantic information. However, the existence of dataset biases allows model to complete the task without learning the intended reasoning skill (Gururangan et al., 2018; McCoy et al., 2019; Belinkov et al., 2019). This phenomenon exist in various different tasks, such as reading comprehension (Kaushik et al., 2019), question answering (Mudrakarta et al., 2018), and fact verification (Schuster et al., 2019). To better evaluate the reasoning ability of models, researchers constructed challenge datasets composed of “counterexamples” to the biases that models may adopt (McCoy et al., 2019; Schuster et al., 2019; Naik et al., 2018). Model performances always have a significant decline on these challenge sets.

One line of debiasing methods mitigates the dataset biases based on human prior knowledge. Based on the human intuitions on task-specific biases, Schuster et al. (2019); Clark et al. (2019); He et al. (2019) detect the biased examples and down-weight these samples, while Min et al. (2020); Belinkov et al. (2018) explicitly modify the dataset distribution by data augmentation. However, these methods are limited by their assumption that the task-specific biases should be available a priori. To address this issue, automatic debiasing methods are proposed to detect the dataset biases without dependency on prior knowledge. For example, Utama et al. (2020b) automatically capture the dataset bias by training a shallow model on a tiny training set, while Sanh et al. (2020) capture the dataset bias using a learner with limited capacity. However, researches indicate the difference between the biases shallow model or weaker learner captured, and that the main NLU model captured (Kaushik et al., 2019). More crucially, without the incorporation of causal assumptions, the debiasing methods still cannot distinguish the causation with correlation, which limits the effectiveness of debiasing.

In this paper, we propose a Causal Invariance based stable NLU framework. With the causal invariance constraint, CI-sNLU can effectively detect the bias feature model utilized and regularize model to exclude the correlative component to increase the stability of model performance.

6 Conclusion

In this paper, we propose a Causal Invariance based stable NLU framework. By introducing a causal invariance constraint into the debiasing process, we can dynamically detect the bias information model captured, then regularize the model to exclude the bias components temporarily captured by the model to enhance the stability. Experimental results show that our approach can significantly increase stability on out-of-distribution samples compared to previous methods.
References


Divyansh Kaushik, Eduard Hovy, and Zachary Lipton. 2019. Learning the difference that makes a difference with counterfactually-augmented data. In International Conference on Learning Representations.


7.1 Theoretical analysis of the regularizer

During the parameter optimization stage, we devise a causal invariance based ADD regularizer to exclude the bias information model captured. We argue that, theoretically, this regularizer can approximately minimize the mutual information between the model representation $h^M$ and the bias feature distribution $h^b$ to lower bound 0 at each training step. Here is the specific proof process.

Let $I(h^M_i, h^b_i)$ denote the mutual information between $h^M_i$ and $h^b_i$ at the $i$th parameter optimization step. We notice that, to make $I(h^M_i, h^b_i) = 0$, a sufficient condition is that, for each instance $i \in T$, $I(h^M_i, h^b_i) = 0$, where $h^M_i$ and $h^b_i$ is the model representation and bias feature for sample $i$. Note that, here we regard $h^M_i$ and $h^b_i$ as two random variables, as both $h^M_i$ and $h^b_i$ are estimated from data, hence are not certain values and with uncertainty.

However, in general, the precise value of mutual information $I(h^M_i, h^b_i) = 0$ for two random variables with complex distribution is hard to calculate. To address this issue, we resort to approximations.

We start from modeling the distribution of $h^M_i$ and $h^b_i$. Cramér (2016) and (Rao, 1992) have proved that, under specific regularity conditions, if a random variable is estimated through maximizing the likelihood function, then it should asymptotically converge to a normal distribution. In this paper, since we initialize $h^b_i$ from the methods of Utama et al. (2020b) which captures bias features by maximizing the likelihood, and the model representation $h^M$ is optimized using maximizing the likelihood function, hence both the bias feature distribution $h^b_i$ and the model representation $h^M_i$ would asymptotically converge to normal distribution:

$$h^M_i \rightarrow N(\mu_i, \Sigma_i), \ h^b_i \rightarrow N(\mu_i, \Sigma_i)$$

where $\mu_i, \Sigma_i \in \mathbb{R}^d$ is the mean of the corresponding distributions, $\Sigma_i \in \mathbb{R}^{d \times d}$ is the covariance matrix of corresponding distributions.
Furthermore, for arbitrary two normal distributed random variables \( a_1 \) and \( a_2 \), their mutual information has a close form:

\[
I(a_1, a_2) = -\frac{1}{2} \ln \left( \frac{\text{Det}(\Sigma_z)}{\text{Det}(\Sigma_{a_1}) \text{Det}(\Sigma_{a_2})} \right) \quad (11)
\]

where \( z = p(a_1, a_2) \) is the joint distribution of \( a_1 \) and \( a_2 \); \( \text{Det} \) is the determinant operator.

Hence, if we can: (1) derive the joint distribution of \( h_{i,t}^b \) and \( h_{i,t}^M \), which we denote as \( h_{i,t}^z = p(h_{i,t}^b, h_{i,t}^M) \); (2) obtain \( \Sigma_{i,t}^z, \Sigma_{i,t}^M, \) and \( \Sigma_{i,t}^b \), then we can calculate the mutual information \( I(h_{i,t}^M, h_{i,t}^b) \).

For the first problem, notice that the joint distribution \( h_{i,t}^z \) is a combination of the information of \( h_{i,t}^b \) and \( h_{i,t}^M \). Hence, we can get an approximation of \( h_{i,t}^z \) by integrating \( h_{i,t}^b \) and \( h_{i,t}^M \) in various ways. For example, integrating \( h_{i,t}^b \) and \( h_{i,t}^M \) using a neural network as \( h_{i,t}^z = NN(h_{i,t}^b, h_{i,t}^M) \), or by directly adding \( h_{i,t}^b \) and \( h_{i,t}^M \) as \( h_{i,t}^z = (h_{i,t}^b + h_{i,t}^M) \).

To calculate the covariance matrices, interestingly, Cramér (2016) and Rao (1992) have also proven that, during the training process, if a group of parameters \( h \) is estimated by maximizing the likelihood, as the value of \( h \) converges to its expectation \( E(h) \), the covariance matrix of \( h \) asymptotically converge to the expectation of the square of the partial derivative, i.e.:

\[
\Sigma_h \rightarrow \mathbb{E} \frac{\partial Y}{\partial h}^2 \quad (12)
\]

where \( Y \) is the model output.

Hence, we can get the expectation of \( \Sigma_{i,t}^z \), \( \Sigma_{i,t}^M \), and \( \Sigma_{i,t}^b \) based on the partial gradients on \( h_{i,t}^z \), \( h_{i,t}^M \), and \( h_{i,t}^b \) at the \( t \)th parameter optimization step, i.e.:

\[
\Sigma_{i,t}^z = \mathbb{E} \left( \frac{\partial Y_i}{\partial h_{i,t}^z} \right)^2 \quad (13)
\]

\[
\Sigma_{i,t}^M = \mathbb{E} \left( \frac{\partial Y_i}{\partial h_{i,t}^M} \right)^2 \quad (14)
\]

\[
\Sigma_{i,t}^b = \mathbb{E} \left( \frac{\partial Y_i}{\partial h_{i,t}^b} \right)^2 \quad (15)
\]

In practical, we use the sample partial gradient to estimate the expectation of covariance matrix as:

\[
\hat{\Sigma}_{i,t}^z = \left( \frac{\partial Y_i}{\partial h_{i,t}^z} \right)^2 \quad (16)
\]

\[
\hat{\Sigma}_{i,t}^M = \left( \frac{\partial Y_i}{\partial h_{i,t}^M} \right)^2 \quad (17)
\]

\[
\hat{\Sigma}_{i,t}^b = \left( \frac{\partial Y_i}{\partial h_{i,t}^b} \right)^2 \quad (18)
\]

where \( \hat{\Sigma}_{i,t}^z, \Sigma_{i,t}^M, \) and \( \Sigma_{i,t}^b \) is the expectation of \( \Sigma_{i,t}^z, \Sigma_{i,t}^M, \) and \( \Sigma_{i,t}^b \), respectively.

By substituting Eq. 16 17 18 into Eq. 11, we can get the estimation of \( I(h_{i,t}^M, h_{i,t}^b) \).

Furthermore, we prove that, by training model using the ADD regularizer which is formulated as:

\[
\hat{Y}_i = \sigma(W h_{i,t}^z);
\]

\[
h_{i,t}^z = (h_{i,t}^M + h_{i,t}^b) \quad (19)
\]

where \( \sigma(\cdot) \) is a sigmoid function, \( W \in \mathbb{R}^{d \times d} \) is a weight matrix. Then we can make \( I(h_{i,t}^M, h_{i,t}^b) \) achieving its lower bound 0.

In specific, under the formalization in Eq. 19, the partial derivatives upon \( h_{i,t}^z, h_{i,t}^M \), and \( h_{i,t}^b \) equal:

\[
\hat{\Sigma}_{i,t}^z = \left( \frac{\partial Y_i}{\partial h_{i,t}^z} \right)^2 = (\hat{Y}_{i,t} - Y)^TW \quad (20)
\]

\[
\hat{\Sigma}_{i,t}^M = \left( \frac{\partial Y_i}{\partial h_{i,t}^M} \right)^2 = (\hat{Y}_{i,t} - Y)^TW \quad (21)
\]

\[
\hat{\Sigma}_{i,t}^b = \left( \frac{\partial Y_i}{\partial h_{i,t}^b} \right)^2 = (\hat{Y}_{i,t} - Y)^TW \quad (22)
\]

By substituting Eq. 20 21 22 into Eq. 11, we can have \( I(h_{i,t}^M, h_{i,t}^b) = 0 \).

By employing the ADD regularizer, we can gradually exclude the bias components within \( h_{i,t}^M \) to increase the model stability. Furthermore, \( I(h_{i,t}^M, h_{i,t}^b) \) is calculated based on the partial gradients, and the partial gradients can reflect the sensitivity of model prediction \( \hat{Y} \) upon \( h_{i,t}^z, h_{i,t}^M \), and \( h_{i,t}^b \). Hence, our regularizer is built upon the actual contribution of model representation and bias feature on model prediction at each parameter optimization step, rather than using fixed weights to regularize \( M \) as previous researches adopts.

### 7.2 Experimental Details

**MNLI**

- batch size: 32
- number of epochs: 3
- learning rate: 5e-5
- Optimizer: Adam

Time Costing: 1 Geforce rtx_2080_ti with 4 CPUs: \(\sim8h\)

Fever
- batch size: 32
- number of epochs: 3
- learning rate: 2e-5
- Optimizer: Adam

Time Costing: 1 Geforce rtx_2080_ti with 4 CPUs: \(\sim4h\)

QQP
- batch size: 32
- number of epochs: 3
- learning rate: 2e-5
- Optimizer: Adam

Time Costing: 1 Geforce rtx_2080_ti with 4 CPUs: \(\sim5.5h\)