Unveiling Project-Specific Bias in Neural Code Models

Zhiming Li¹, Yanzhou Li², Tianlin Li¹, Mengnan Du³ Bozhi Wu¹, Yushi Cao¹, Xiaofei Xie⁴, Yi Li¹, Yang Liu¹,

¹Nanyang Technological University

²University of Edinburgh

³Texas A&M University

⁴Singapore Management University

{zhiming001, tianlin001, bozhi001, yushi002}@e.ntu.edu.sg, y.li-353@sms.ed.ac.uk, dumengnan@tamu.edu, xiaofei.xfxie@gmail.com, {yi_li, yangliu}@ntu.edu.sg,

Abstract

Neural code models have introduced significant improvements over many software analysis tasks like type inference, vulnerability detection, etc. Despite the good performance of such models under the common intra-project independent and identically distributed (IID) training and validation setting, we observe that they usually fail to generalize to realworld inter-project out-of-distribution (OOD) setting. In this work, we show that such phenomenon is caused by model heavily relying on projectspecific, ungeneralizable tokens like self-defined variable and function names for downstream prediction, and we formulate it as the project-specific bias learning behavior. We propose a measurement to interpret such behavior, termed as Cond-Idf, which combines co-occurrence probability and inverse document frequency to measure the level of relatedness of token with label and its projectspecificness. The approximation indicates that without proper regularization with prior knowledge, model tends to leverage spurious statistical cues for prediction. Equipped with these observations, we propose a bias mitigation mechanism Batch Partition Regularization (BPR) that regularizes model to infer based on proper behavior by leveraging latent logic relations among samples. Experimental results on two deep code benchmarks indicate that BPR can improve both interproject OOD generalization and adversarial robustness while not sacrificing accuracy on IID data.

1 Introduction

Neural network models have revolutionized the software engineering community by achieving significant improvements on many benchmarks, while not requiring much domain expert knowledge and manual efforts. In particular, the CodeBert[Feng et al., 2020] model and its variants have surpassed many delicately designed model architectures without much inductive bias thanks to the power of the 'pre-training and fine-tuning' training paradigm.

Figure 1: Illustrative examples of attribution vectors using integrated gradient for cases in type inference and vulnerability detection. The shades of the green color indicate value of weight of respective token in the attribution vector.

Despite the success reported in the literature, we notice that almost all of them evaluate the model merely under the intra-project independent identically distributed (IID) datasplit scheme[Zhou et al., 2019; Hellendoorn et al., 2018; Jesse et al., 2021], i.e. randomly shuffle and split the dataset for training and validation. However, in real-world scenario, deep code models should be trained and validated under the inter-project setting for the majority of cases, i.e. trained on a set of projects while test on previously unseen projects. It is obvious that the *inter-project* setting is much more challenging since the vocabulary within different projects varies considerably because the naming conventions among developers differs. In particular, we observe that neural code models that have a decent performance on intra-project data will have a significant performance drop on inter-project data even though the co-domain of the prediction remains unchanged. In addition, previous empirical analysis indicates that deep code models are sensitive to semantic-preserving adversarial attacks like variable renaming and dead code insertion[Yefet et al., 2020; Bielik and Vechev, 2020].

In this work, we target to explore the reason of why neural code models have low generalization ability on *inter-project* settings and why they are vulnerable to naive adversarial attacks. Towards this end, we probe the model behavior with a DNN model explanation algorithm: integrated gradient[Sundararajan *et al.*, 2017], and notice that model heavily relies on

ungeneralizable project-specific tokens for prediction when trained without regularization. We formulate it as the projectspecific bias learning behavior. As shown in the examples in Figure 1 (refer to Section 3.1 for description of the two tasks), for the visualization of the type inference sample, CodeBert fails to infer the user-defined variable is Test Watch as boolean, it is obvious that model attributes its prediction utterly to uninformative subwords like Watch, works in the snippet. In contrast, human developers usually infer based on === and 's' in the declaration statement. Similarly, in the case of vulnerability detection, to predict whether the snippet contains vulnerability, model distributes almost all its weights to userdefined function names and variable names while ignoring the relevant memory allocation API malloc. Whereas the vulnerability can be easily identified by noticing that the malloc API is not paired with a deallocation operation. This learning behavior is problematic when applying the model under the inter-project setting since the semantics of these user-defined variable/function names are inconsistent and they may even not exist across different projects. We further show such spurious project-specific bias learning behavior can be interpreted with the Cond-Idf distribution, i.e. without appropriate regularization with prior knowledge, model would rely heavily on the tokens that frequently co-occur with label yet highly semantically inconsistent and ungeneralizable for prediction.

We then evaluate four representative bias mitigation methods proposed by previous literature, including reweighting[Schuster et al., 2019], product-of-expert[Clark et al., 2019], adversarial training[Madry et al., 2017; Goodfellow et al., 2014] and gradient reversal[Stacey et al., 2020]. We observe that though such methods manage to mitigate model from using observed shortcuts¹ [Geirhos et al., 2020], there is no guarantee that the post mitigated model would infer based on the expected behavior instead of falling to leverage other unexpected bias. To handle such concerns, we propose a novel bias mitigation mechanism, termed as BPR (Batch Partition Regularization). The proposed regularization is based on the principle of invariant risk minimization (IRM)[Arjovsky et al., 2019], which explicitly regularizes the learning process of model by identifying common logic properties among samples. Concisely, BPR unshuffles and sorts samples according to metric that embeds prior knowledge about logic relations. Then the dataset is divided into batches of *environments* in which samples are most closely correlated. The in-batch representations would be regularized during gradient update such that logically correlated samples would share similar representation instead of falling to embed other unknown shortcuts after debiasing the known ones. The major contributions of our work are summarized as follows:

- We unveil and indicate that the poor inter-project OOD generalization and adversarial robustness of deep code models can be interpreted by the Cond-Idf feature distribution.
- We propose a novel mitigation method, called BPR, which explicitly regularizes the model's behavior using logic relations among samples.
- Experimental results on two representative benchmarks

validate that BPR can effectively improve OOD generalization and adversarial robustness by learning more robust representation.

2 Methodology

In this section, we first analyze the *project-specific bias learning behavior* of neural code model, and then we propose the bias mitigation mechanism, called batch partition regularization (BPR), to alleviate the bias of neural code model.

2.1 Behavior Analysis and Interpretation

We consider two typical software analysis tasks: vulnerability detection and type inference (refer to Section 3.1 for detailed description of the two tasks). The underlying model we analyze is the pre-trained CodeBert [Feng et al., 2020]. Even though CodeBert is reported to achieve the state-of-theart performance on these software analysis tasks[Feng et al., 2020; Guo et al., 2020; Jesse et al., 2021], we find that the performance only holds for IID test data. In contrast, the generalization performance would drop dramatically if we test CodeBert on inter-project OOD set and adversarial set.

In order to robustly infer, model should learn to embed abstract, high-level code semantics, instead of using merely low-level self-defined variable or function names. Whereas in the following sections, we will unveil that CodeBert would spuriously use these uninformative tokens as shortcut for prediction since they co-occur frequently with some labels due to developer's idiosyncrasies.

Model Behavior Analysis. We analyze the model's behavior using a post-hoc DNN model explanation algorithm: Integrated Gradient[Sundararajan et~al., 2017]. Intuitively, the algorithm attributes the prediction to all inputs by giving each input an importance score[Montavon et~al., 2018] indicating its contribution to the output. Formally, given an input sequence $x_i = (x_i^1, x_i^2, ..., x_i^T) \in R^T$, a baseline reference input $x' \in R^T$, a neural model $f: R^T \to [0, 1]$. The integrated gradient importance vector of the prediction $f_y(x_i)$ is computed as the combination of gradients of m intermediate samples along the straightline path from reference x_i' to input x_i , which is as follows:

$$IGs(x_i) = (x_i - x_i') \cdot \frac{1}{m} \sum_{k=1}^m \frac{\partial f_y\left(x_i' + \frac{k}{m}(x_i - x_i')\right)}{\partial x_i}. (1)$$

We use zero word embedding as the baseline reference input vector. To summarize attributions of each token in the sequence, we take the L1 norm of each importance vector w.r.t to each token $x_i^t \in x_i$ and normalize the final importance vector w.r.t to the sequence x_i with its L2 norm. Eventually, we obtain a feature importance vector $\mathrm{IGs}(x_i) \in R^T$ with each scalar (weight) within indicates the contribution of each token for the model's prediction $f_u(x_i)$.

Skewed Dataset Distribution. To reflect the project-specific bias learning behavior, we propose a metric called conditional inverse document frequency (Cond-Idf), which measures the correlation between a word w and a label l, and its occurrence frequency across corpus of projects Π , denoted

¹we use bias and shortcut interchangeably in the following paper.

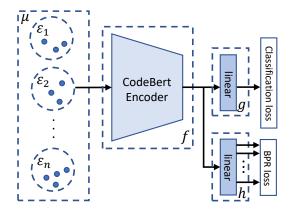


Figure 2: Overview of the proposed bias mitigation method. Training samples $x \in \mathcal{X}$ are first embedded with μ and sorted in terms of similarity measure κ , then they are batchified and partitioned into multiple *environments* $\varepsilon \in \mathcal{E}$ according to their labels and similarity scores. Based upon which, the batch partition regularization (BPR) loss is computed along with the classification loss.

as follows:

Cond-Idf
$$(w, l, \Pi) = p(l \mid w) \operatorname{Idf}(w, \Pi)$$

= $p(l \mid w) \log \frac{N}{|\{\pi \in \Pi : w \in \pi\}|},$ (2)

where the conditional probability is calculated as $p(l|w) = \frac{count(w,l)}{count(w)}$, and N is the total number of projects in the corpus $N = |\Pi|$. For each label l, we obtain a distribution of all words in the vocabulary. Words with high Cond-Idf weights denote that they frequently co-occur with the label while are also highly project-specific. We observe that this part of words majorly consists of user-defined variable name, function name, macro definition, etc. Though these words strongly correlate with the label in the training set, their semantics are inconsistent and would not generalize to interproject OOD or adversarial settings. This is because developers have different idiosyncrasies in naming and those user-defined tokens existing in the projects of training set might be absent or represent different meanings in other projects.

To validate the root cause of model's bias learning behavior, we evaluate the alignment between the model's learning behavior and theimn, proposed Cond-Idf that quantifies the biased dataset distribution. We first calculate the integrated gradients importance vector for every sample in the IID test set, and base upon it, we calculate the mean integrated gradient for all the words in the test set vocabulary and sort the vocabulary in descending order. Then we use polynomial regression to approximate its corresponding Cond-Idf distribution. Besides, we measure the ratio of samples in the IID test set whose top-n ($n \in \{1, 2, 3\}$) highest integrated gradient tokens lies in the defined class of biased vocabulary. Our experiments reveal that the regression results positively correlate with the distribution of integrated gradients, thus indicate that the neural code model is superficial learners that rely heavily on project-specific and semantically inconsistent features for prediction.

Algorithm 1: Batch Partition Regularization

```
Data: Training set \mathcal{X}, similarity measure \kappa, embedding
                function \mu, encoder f, classification head g,
                partitioning head h
     // calculate similarity matrix
1 \mathcal{X}_{\mu} \leftarrow ();
2 for (x_i, x_j) \in \mathcal{X} \times \mathcal{X} do
      \lambda_{ij} \leftarrow \kappa(\mu(x_i), \mu(x_j)), \lambda \in \mathbb{R}^{|\mathcal{X}| \times |\mathcal{X}|}
     // training set unshuffling
4 for \lambda_{ij} \in sorted(vec(\lambda \setminus \{\lambda_{ij} | i = j\})) do
            for k \in \{x_i, x_i\} do
5
                   if k \notin \mathcal{X}_{\mu} then
 6
                         \mathcal{X}_{\mu} \leftarrow \mathcal{X}_{\mu} || k;
     // train with BPR loss
s for B \in batches(\mathcal{X}_{\mu}) do
            \mathcal{L}_{BPR} \leftarrow \mathbb{E}_{(x_i, x_j) \sim B \times B} \mathbb{1}^{ij} \kappa(\mu(x_i), \mu(x_j)) \cdot S_{c}(h \circ f(x_i; \theta), h \circ f(x_j; \theta))
9
10
            \mathcal{L} \leftarrow \mathcal{L}_{\text{DEBIAS}} + \gamma_p \cdot \mathcal{L}_{\text{BPR}}
            // update model weights
           \theta \leftarrow \theta - \eta \nabla_{\Theta} \mathcal{L}
12
```

2.2 Proposed Mitigation Mechanism

From our empirical observations, it is shown that though prevalent bias mitigation baselines manage to improve generalization on the OOD data and robustness on adversarial data by removing the known bias, there is no guarantee that the debiased model would infer based on expected behavior of developers instead of falling back to using other unknown bias. Motivated by this concern, we propose a novel mitigation mechanism called *batch partition regularization* (BPR) to regularize the behavior of neural code models (see Figure 2). BPR follows the *invariant-risk-minimization* (IRM)[Arjovsky *et al.*, 2019] philosophy and aims to constrain neural code representation such that model's learning behavior is invariant when handling samples with similar syntactic and semantic evidence, *i.e.* invariant stable evidence is utilized instead of spurious project-specific shortcuts.

Details of the BPR algorithm are shown in Algorithm 1. Given a training set \mathcal{X} , we first obtain a similarity matrix $\lambda \in \mathbb{R}^{|\mathcal{X}| \times |\mathcal{X}|}$ based on similarity measure κ in terms of embedding μ which is positively correlated with the level of logic closeness (similarity) of syntactic or semantic invariance (see line 1-3). For type inference, we focus on variables with assignment, we use bag-of-words vector that consists of one-hop neighborhood based on the abstract syntax tree that the target token belongs to as embedding and use cosine similarity S_c to calculate logic closeness: $\kappa(\mu(\cdot), \mu(\cdot)) =$ $S_c(BoW(N_{AST}(\cdot)), BoW(N_{AST}(\cdot)))$ since the neighborhood contains information that is most related to the type of the variable. For vulnerability detection, we use all-pairsshortest-path[Floyd, 1962] based on control flow graph as embedding. Then given an embedded sample $\mu(x_i)$, we obtain a vector \mathbf{u}^{ij} that contains the similarity score between each path and its most similar path in another sample x_i : $\mathbf{u}_m^{ij} = \max_{n \in [1,N]} \langle \mu(x_i), \mu(x_j) \rangle_{mn}, m \in [1,M], \text{ where}$ M, N are the number of paths in $\mu(x_i)$ and $\mu(x_i)$. And the

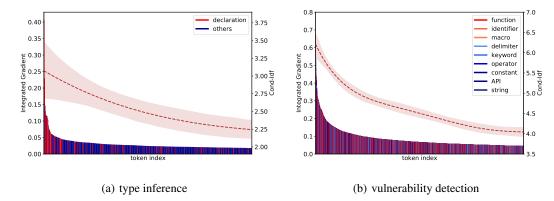


Figure 3: The discrete distribution is the sorted distribution of integrated gradient of the test set vocabulary. The red dashed line is the polynomial regression approximation of the corresponding Cond-Idf distribution.

similarity score between x_i and x_j is: $\lambda_{ij} = \frac{\|\mathbf{u}^{ij}\|_1}{M}$. Then, training samples are unshuffled and sorted given the vectorized similarity matrix $sorted(vec(\lambda \setminus \{\lambda_{ij} | i = j\}))$ (see line 4-7). In this way, after batchifying, each mini-batch $B \in batches(\mathcal{X}_{\mu})$ would consist of samples with closest logic relations. Finally, during training, within each mini-batch, we use cosine embedding loss $\mathbb{I}^{ij}\mathrm{S}_{c}(h\circ f(x_i;\theta),h\circ f(x_j;\theta))$ to constrain model into using similar representation when embedding samples with the same label and similar syntactic or semantic evidence. Here f is the backbone CodeBert encoder, g,h are the classification head and partitioning head layer respectively, \mathbb{I}^{ij} is a Boolean operator that selects samples with the same label. We weigh the loss of each pair with the corresponding similarity score $\lambda_{ij} = \kappa(\mu(x_i), \mu(x_j))$ to prevent misalignment. Detailed BPR loss is as below:

$$\mathcal{L}_{BPR} = \mathbb{E}_{(x_i, x_j) \sim B \times B} \mathbb{1}^{ij} \kappa(\mu(x_i), \mu(x_j))$$

$$\cdot S_c(h \circ f(x_i; \theta), h \circ f(x_j; \theta))$$
(3)

 $\mathcal{L}_{\mathrm{BPR}}$ can be trained together with existing mitigation methods and our final loss function is: $\mathcal{L} = \mathcal{L}_{\mathrm{DEBIAS}} + \gamma_p \cdot \mathcal{L}_{\mathrm{BPR}}$. In this work, we combine BPR with adversarial training/gradient reversal methods since they are empirically found to be more effective. $\mathcal{L}_{\mathrm{DEBIAS}}$ denotes loss function for adversarial training/gradient reversal (refer to Section 3.1 and Appendix A). The hyperparamter γ_p is a regulatory coefficient, and we use delay update[Ganin *et al.*, 2016]. In particular, γ_p is set as $\gamma_p = \frac{2}{1+\exp(-10 \cdot p)} - 1$, where $p \in [0,1]$ is the training progress. The key reason to use delay update is that the representations would fail to be updated if they are unsuitably penalized during the early stage of training.

3 Experiments

3.1 Experimental Setup

Tasks & Datasets. We analyze, interpret and mitigate the bias learning behavior of the neural code model on two tasks:

• *Type Inference*: The goal of this task is to predict type for variables/parameters/functions in a code snippet written in

	Ту	pe Infere	ıce	Vulnerability Detect			
#Words	Top1	Top2	Top3	Top1	Top2	Top3	
Ratio	12.8%	61.7%	74.8%	69.1%	58.6%	48.1%	

Table 1: The ratio of samples whose top-integrated gradient token belongs to the project-specific bias.

optionally-typed language. In this work, we use the Type-Script dataset[Hellendoorn *et al.*, 2018]. During testing, we constrain to only predict variable with and only with the data type that exists in the training set such that the co-domain remains consistent. The dataset is then split into 162 projects for IID training and testing (randomly shuffled and split by 80% and 20%), 27 and 44 projects for interproject OOD/adversarial validation and test set. We perform a single non-targeted Breadth-First Search step[Yefet *et al.*, 2020] on the inter-project samples to form the adversarial set (same for vulnerability detection).

• Vulnerability Detection: Previous works formulate vulnerability detection as a sequence/graph classification task, in which given a code snippet, the neural model should learn to predict whether it contains vulnerability or not. In this work, we collect 1,000 projects from GitHub which contains vulnerabilities via keyword mapping in commit message. The dataset is split into 700 projects for IID training and testing (randomly shuffled and split by 80% and 20%), 100 projects and 200 projects for inter-project OOD/adversarial validation and test set respectively. Notice that we have balanced the number of vulnerable and non-vulnerable samples in the dataset such that model would not be affected by the data imbalance problem.

Mitigation Baselines. We evaluate BPR along with four representative bias mitigation baselines. The first baseline is re-weighting[Schuster et al., 2019; Clark et al., 2019], it first obtains a biased model by training the model only on selected biased features, then the output probability of the bias-only model p_b is used to adjust the weights of training samples for training the debaised model such that the contribution of sam-

Type. I. (Acc(%))				Vul. D. (Acc(%))				
INTRA	INTER	ADV	Δ	INTRA	INTER	ADV	Δ	
62.88	51.20	39.78	-	81.66	64.01	61.5	-	
63.17	53.10	41.47	+1.690	80.34	61.99	58.64	-2.860	
60.11	25.30	17.46	-22.32	81.24	63.09	58.12	-3.380	
61.11	51.33	39.93	+0.150	81.84	64.52	63.21	+1.710	
62.97	51.35	41.89	+2.110	82.28	64.57	64.56	+3.060	
63.10 63.36	54.00 53.48	54.56 55.74	+14.78 + 15.96	82.12 82.76	64.53 64.72	63.31 64.83	+1.810 +3.330	
	62.88 63.17 60.11 61.11 62.97 63.10	INTRA INTER 62.88 51.20 63.17 53.10 60.11 25.30 61.11 51.33 62.97 51.35 63.10 54.00	INTRA INTER ADV 62.88 51.20 39.78 63.17 53.10 41.47 60.11 25.30 17.46 61.11 51.33 39.93 62.97 51.35 41.89 63.10 54.00 54.56	INTRA INTER ADV Δ 62.88 51.20 39.78 - 63.17 53.10 41.47 +1.690 60.11 25.30 17.46 -22.32 61.11 51.33 39.93 +0.150 62.97 51.35 41.89 +2.110 63.10 54.00 54.56 +14.78	INTRA INTER ADV Δ INTRA 62.88 51.20 39.78 - 81.66 63.17 53.10 41.47 +1.690 80.34 60.11 25.30 17.46 -22.32 81.24 61.11 51.33 39.93 +0.150 81.84 62.97 51.35 41.89 +2.110 82.28 63.10 54.00 54.56 +14.78 82.12	INTRA INTER ADV Δ INTRA INTER 62.88 51.20 39.78 - 81.66 64.01 63.17 53.10 41.47 +1.690 80.34 61.99 60.11 25.30 17.46 -22.32 81.24 63.09 61.11 51.33 39.93 +0.150 81.84 64.52 62.97 51.35 41.89 +2.110 82.28 64.57 63.10 54.00 54.56 +14.78 82.12 64.53	INTRA INTER ADV Δ INTRA INTER ADV 62.88 51.20 39.78 - 81.66 64.01 61.5 63.17 53.10 41.47 +1.690 80.34 61.99 58.64 60.11 25.30 17.46 -22.32 81.24 63.09 58.12 61.11 51.33 39.93 +0.150 81.84 64.52 63.21 62.97 51.35 41.89 +2.110 82.28 64.57 64.56 63.10 54.00 54.56 +14.78 82.12 64.53 63.31	

Table 2: Generalization and robustness performance evaluation of the base CodeBert model and different bias mitigation baselines on the type inference and vulnerability detection benchmarks.

ples which the biased model assigns high prediction probability are lower-weighted. The second baseline is *product-of*expert[He et al., 2019; Clark et al., 2019], which also requires a trained biased model, the debiased model is trained by ensembling its output probability with that of the biased model. The third baseline is adversarial training [Madry et al., 2017; Yefet et al., 2020], which optimizes the model based on both the original samples and adversarial samples such that the cooccurrence of spurious data cues and label are down-weighted and the model is expected to focus less on known bias and behave more robustly after training. We follow the implementation of Yefet et al. [Yefet et al., 2020] and use a single Breadth-First Search step to generate non-targeted adversarial attacked counterpart for each sample in the training set. The forth baseline is gradient reversal[Stacey et al., 2020; Kim et al., 2019; Minervini and Riedel, 2018], which unlearns the bias in a minimax game by predicting the target bias using model's representation and reverse its gradient during back propagation. Please refer to Appendix A and B for more details about the baselines and related works.

Implementation Details We focus on the analysis of the pretrained CodeBert model. We use the open-sourced checkpoint from Feng *et al.* [Feng *et al.*, 2020], and use 256-dimensional linear layers as classification and partitioning head g, h. For both benchmarks, we fine-tune the model for 10 epochs, which all models could converge. We use Adam optimizer for the update and the learning rate is set as $2*10^{-5}$. The training batch size is set as 32. For gradient reversal, the regulatory coefficient of bias classification loss is set as 0.1. Parameter m in Equation 1 is fixed as 50 for all experiments.

3.2 Project-Specific Bias Analysis & Interpretation

In this section, we quantitatively analyze and interpret the project-specific bias learning behavior of neural code model.

Bias Behavior Analysis We calculate the mean integrated gradient for each token in the IID test set vocabulary and rank them in descending order to obtain the sorted distribution. Then, we perform a lexical analysis and categorize tokens into different lexical items. For type inference, we categorize tokens into user-defined declaration variable (including variable, parameter and function names) which are the set of tokens awaiting for prediction and others. As shown in Figure 3(a), we denote the bar that represents the numeric value

of integrated gradient of these two categories using reddish and purplish colors respectively. For vulnerability detection, we categorize the vocabulary into nine categories, including: function name, identifier (variable) name, macro definition, delimiter, etc. As shown in Figure 3(b), we denote the bar of project-specific lexemes (function name, identifier name, macro definition) with reddish colors and others using purplish colors. As shown in the distribution, we observe that area under the head of the distribution are heavily reddish for both two tasks, meaning that model focuses heavily on user-defined components. Quantitatively, we take the top 1% of tokens as the head. For type inference, while the declaration variable only takes up 12.3% of the vocabulary, 50.0% of tokens within the head falls in these categories. For vulnerability detection, 51.8% of the vocabulary belongs to userdefined components (function name, variable name, macro definition), and 86.9% of tokens within the head falls in these categories. Furthermore, we measure the extent of bias learning behavior from sample-level. For each sample in the IID test set, we generate the integrated gradient attribution vector for the prediction. Specifically, for vulnerability detection, we take the attribution vector of the [CLS] token that lies at the head of every sample, upon which the prediction is performed; for type inference, we use the attributions of the tokens that require prediction. We then rank the integrated gradient of the tokens within each sample, for type inference, we calculate the ratio of samples whose top-n ($n \in \{1, 2, 3\}$) integrated gradient tokens contain self-defined components; for vulnerability detection, we calculate the ratio of samples that contain and only contain self-defined components within its top-n (previous works observe that model mainly relies on a few top-*n* attribution words for prediction[Du *et al.*, 2021]). The results are shown in Table 1, for type inference, 74.8% of samples whose top-3 interpretation words contain declaration variables; for vulnerability detection, 48.1% of samples merely use self-defined variables for prediction (top-3) while ignoring the vulnerability related APIs. The results indicate that CodeBert model heavily biases towards using spurious project-specific shortcuts for prediction.

Bias Behavior Interpretation Given the integrated gradient distribution, we calculate the Cond-Idf distribution in terms of the integrated gradient ranked token index and approximate the distribution with polynomial regression (order=10). As shown in Figure 3, the fitted curve of Cond-Idf

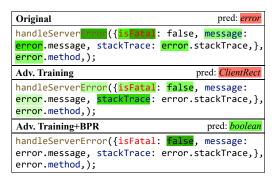


Figure 4: Mitigation example of applying *BPR* on type inference sample compared with original model and model trained with mere non-targeted adversarial training. The color on tokens represents attribution vector for the prediction of variable *isFatal*.

positively correlates with the distribution of integrated gradient for both two tasks. We can thus conclude from the result that without proper regularization, the frequent co-occurrence between project-specific bias and the label can elicit spurious project-specific bias learning behavior and cause the model performs poorly on OOD or adversarial data.

3.3 Bias Mitigation Effectiveness

We present the intra-project IID test set accuracy, interproject OOD generalization and adversarial robustness accuracy of the two tasks in Table 2. Note that all the results are average of 5 runs with different seeds.

We observe that: (1) With the standard IID training-test split, CodeBert model achieves decent performance on intraproject IID test set, whereas it generalizes poorly on the interproject OOD and adversarial set, e.g. it achieves 62.88% accuracy on intra-project test set of type inference and drops to 51.20% on the inter-project OOD and further decreases to 39.78% on the adversarial data. The results indicate that the project-specific bias learning behavior seriously undermines CodeBert's generalizability and robustness by leveraging spurious shortcuts. (2) Among the four evaluated mitigation baselines, model-agnostic mitigation approaches (Reweighting and PoE) are less helpful or even counterproductive compared with representation-based mitigation methods (Adversarial training and Gradient reversal). E.g. for vulnerability detection, adversarial training increases adversarial robustness accuracy by +1.81%, while reweighting and PoE decrease the original baseline by -2.86% and -3.38% respectively. Similarly, for type inference, adversarial training increases adversarial robustness accuracy by +14.78% while PoE decreases it by -22.32%. We think this is because there is not a clear boundary for defining biased and unbiased samples since every code sample requires the usage of user-defined lexemes like variable or function names, thus representationbased mitigation methods are more effective. (3) BPR is effective in improving generalization and robustness by learning more robust representation. Specifically, for vulnerability detection, BPR improves adversarial training and gradient reversal by +1.52%, +1.35% respectively; for type inference, BPR improves them by +1.18%, +1.96%. Besides, we also notice that BPR can further improve IID performance

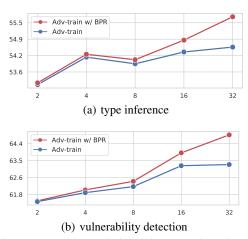


Figure 5: Hyperparamter analysis on the two tasks. The x axis denotes different batch size and y axis represents the corresponding robustness accuracy on the adversarial data.

(Please refer to Appendix D for further discussion). To better understand the source of improvement, we conduct a case study as shown in Figure 4. As shown in the first row, to infer the type of variable is Fatal, the original model trained with standard IID split focuses merely on spurious shortcuts e.g. Error, isFatal, etc., while ignoring the ground-truth evidence false in the declaration body, thus it erroneously predicts the boolean variable as type error. As shown in the second row, after mitigation with adversarial training, though model starts paying attention to false, it unexpectedly biases on a new shortcut stackTrace and still fails to make the right prediction. Finally, with the incorporation of BPR, it is obvious that model robustly infers based only on the ground truth evidence while completely removing the bias reliance. The results indicate that BPR can effectively mitigate bias learning behavior by regularizing model's learning using logic relations among samples (Refer to Appendix C for more cases).

3.4 Hyperparameter Analysis

We evaluate the model performance with the change of batch size on both tasks. The results are illustrated in Figure 5. It is observed that as the batch size increases, the robustness accuracy of the model trained with mere adversarial training converge and stabilize when batch size reaches 16. Whereas when combined with BPR, there is a considerable surge in performance as the batch size continues to increase. The results indicate that BPR benefits from larger batch size as more logically related samples can be clustered together to form *environments* that are representative of different syntactic or semantic evidence.

4 Conclusion and Future Work

In this work, we analyze the project-specific bias learning behavior of CodeBert, which renders it ungeneralizable to inter-project OOD or adversarial settings. We observe that this phenomenon can be interpreted via the Cond-Idf distribution. Furthermore, we propose a general mitigation mechanism BPR that forces model to infer based on robust representation via regularization of its behavior using logic relations among samples. Experimental results on two representative big code benchmarks validate BPR improves OOD generalization and adversarial robustness while not sacrificing IID performance. In the future, we plan to study bias learning behavior on more benchmarks and investigate more complicated types of bias beyond lexical bias.

Ethics Statement

We state that the vulnerability detection dataset we used in this work are collected from Github via keyword mapping in commit message and have been through rigorous human review, in which all vulnerabilities are fully disclosed and repaired by developers, and shall contain no sensitive information nor exposure of privacy. Thus it would not produce any potential negative societal consequences.

References

- [Arjovsky *et al.*, 2019] Martin Arjovsky, Léon Bottou, Ishaan Gulrajani, and David Lopez-Paz. Invariant risk minimization. *arXiv preprint arXiv:1907.02893*, 2019.
- [Bielik and Vechev, 2020] Pavol Bielik and Martin Vechev. Adversarial robustness for code. In *International Conference on Machine Learning*, pages 896–907. PMLR, 2020.
- [Clark *et al.*, 2019] Christopher Clark, Mark Yatskar, and Luke Zettlemoyer. Don't take the easy way out: Ensemble based methods for avoiding known dataset biases. *arXiv* preprint arXiv:1909.03683, 2019.
- [Du et al., 2021] Mengnan Du, Varun Manjunatha, Rajiv Jain, Ruchi Deshpande, Franck Dernoncourt, Jiuxiang Gu, Tong Sun, and Xia Hu. Towards interpreting and mitigating shortcut learning behavior of nlu models. arXiv preprint arXiv:2103.06922, 2021.
- [Feng et al., 2020] Zhangyin Feng, Daya Guo, Duyu Tang, Nan Duan, Xiaocheng Feng, Ming Gong, Linjun Shou, Bing Qin, Ting Liu, Daxin Jiang, et al. Codebert: A pre-trained model for programming and natural languages. arXiv preprint arXiv:2002.08155, 2020.
- [Floyd, 1962] Robert W Floyd. Algorithm 97: shortest path. *Communications of the ACM*, 5(6):345, 1962.
- [Ganin et al., 2016] Yaroslav Ganin, Evgeniya Ustinova, Hana Ajakan, Pascal Germain, Hugo Larochelle, François Laviolette, Mario Marchand, and Victor Lempitsky. Domain-adversarial training of neural networks. *The journal of machine learning research*, 17(1):2096–2030, 2016.
- [Geirhos *et al.*, 2020] Robert Geirhos, Jörn-Henrik Jacobsen, Claudio Michaelis, Richard Zemel, Wieland Brendel, Matthias Bethge, and Felix A Wichmann. Shortcut learning in deep neural networks. *Nature Machine Intelligence*, 2(11):665–673, 2020.
- [Goodfellow *et al.*, 2014] Ian J Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*, 2014.
- [Guo et al., 2020] Daya Guo, Shuo Ren, Shuai Lu, Zhangyin Feng, Duyu Tang, Shujie Liu, Long Zhou, Nan Duan,

- Alexey Svyatkovskiy, Shengyu Fu, et al. Graphcodebert: Pre-training code representations with data flow. *arXiv* preprint arXiv:2009.08366, 2020.
- [He *et al.*, 2019] He He, Sheng Zha, and Haohan Wang. Unlearn dataset bias in natural language inference by fitting the residual. *arXiv preprint arXiv:1908.10763*, 2019.
- [Hellendoorn et al., 2018] Vincent J Hellendoorn, Christian Bird, Earl T Barr, and Miltiadis Allamanis. Deep learning type inference. In *Proceedings of the 2018 26th acm joint meeting on european software engineering conference and symposium on the foundations of software engineering*, pages 152–162, 2018.
- [Jesse et al., 2021] Kevin Jesse, Premkumar T Devanbu, and Toufique Ahmed. Learning type annotation: is big data enough? In Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, pages 1483–1486, 2021.
- [Kim et al., 2019] Byungju Kim, Hyunwoo Kim, Kyungsu Kim, Sungjin Kim, and Junmo Kim. Learning not to learn: Training deep neural networks with biased data. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pages 9012–9020, 2019.
- [Madry et al., 2017] Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. Towards deep learning models resistant to adversarial attacks. arXiv preprint arXiv:1706.06083, 2017.
- [Minervini and Riedel, 2018] Pasquale Minervini and Sebastian Riedel. Adversarially regularising neural nli models to integrate logical background knowledge. *arXiv* preprint arXiv:1808.08609, 2018.
- [Montavon *et al.*, 2018] Grégoire Montavon, Wojciech Samek, and Klaus-Robert Müller. Methods for interpreting and understanding deep neural networks. *Digital Signal Processing*, 73:1–15, 2018.
- [Schuster *et al.*, 2019] Tal Schuster, Darsh J Shah, Yun Jie Serene Yeo, Daniel Filizzola, Enrico Santus, and Regina Barzilay. Towards debiasing fact verification models. *arXiv preprint arXiv:1908.05267*, 2019.
- [Stacey *et al.*, 2020] Joe Stacey, Pasquale Minervini, Haim Dubossarsky, Sebastian Riedel, and Tim Rocktäschel. Avoiding the hypothesis-only bias in natural language inference via ensemble adversarial training. *arXiv* preprint *arXiv*:2004.07790, 2020.
- [Sundararajan *et al.*, 2017] Mukund Sundararajan, Ankur Taly, and Qiqi Yan. Axiomatic attribution for deep networks. In *International Conference on Machine Learning*, pages 3319–3328. PMLR, 2017.
- [Yefet et al., 2020] Noam Yefet, Uri Alon, and Eran Yahav. Adversarial examples for models of code. Proceedings of the ACM on Programming Languages, 4(OOPSLA):1–30, 2020.

[Zhou *et al.*, 2019] Yaqin Zhou, Shangqing Liu, Jingkai Siow, Xiaoning Du, and Yang Liu. Devign: Effective vulnerability identification by learning comprehensive program semantics via graph neural networks. *arXiv preprint arXiv:1909.03496*, 2019.