Dynamically Refined Regularization for Improving Cross-corpora Hate Speech Detection
Tulika Bose, Nikolaos Aletras, Irina Illina, Dominique Fohr

To cite this version:
Tulika Bose, Nikolaos Aletras, Irina Illina, Dominique Fohr. Dynamically Refined Regularization for Improving Cross-corpora Hate Speech Detection. ACL 2022 - 60th meeting Association for Computational Linguistics Findings, May 2022, Dublin, Ireland. 10.18653/v1/2022.findings-acl.32 . hal-03690174

HAL Id: hal-03690174
https://inria.hal.science/hal-03690174
Submitted on 7 Jun 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Dynamically Refined Regularization for Improving Cross-corpora Hate Speech Detection

Tulika Bose † Nikolaos Aletras ‡ Irina Illina † Dominique Fohr †
† Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France
‡ University of Sheffield, United Kingdom
{tulika.bose, illina, dominique.fohr}@loria.fr
n.aletras@sheffield.ac.uk

Abstract

Warning: this paper contains content that may be offensive and distressing.

Hate speech classifiers exhibit substantial performance degradation when evaluated on datasets different from the source. This is due to learning spurious correlations between words that are not necessarily relevant to hateful language, and hate speech labels from the training corpus. Previous work has attempted to mitigate this problem by regularizing specific terms from pre-defined static dictionaries. While this has been demonstrated to improve the generalizability of classifiers, the coverage of such methods is limited and the dictionaries require regular manual updates from human experts. In this paper, we propose to automatically identify and reduce spurious correlations using attribution methods with dynamic refinement of the list of terms that need to be regularized during training. Our approach is flexible and improves the cross-corpora performance over previous work independently and in combination with pre-defined dictionaries.

1 Introduction

The relative sparsity of hateful content in the real world requires crawling of many of the standard hate speech corpora through keyword-based sampling (Poletto et al., 2021), rather than random sampling. Thus, hate speech classifiers (D’Sa et al., 2020; Mozafari et al., 2019; Badjatiya et al., 2017) often learn spurious correlations from the training corpus (Wiegand et al., 2019) leading to a substantial performance degradation when evaluated on a corpus with a different distribution (Yin and Zubiaga, 2021; Bose et al., 2021; Florio et al., 2020; Arango et al., 2019; Swamy et al., 2019; Karan and Šnajder, 2018).

Recent work has proposed regularization mechanisms to penalize spurious correlations by attempting to explain model predictions using feature attribution methods (Ross et al., 2017; Rieger et al., 2020; Adebayo et al., 2020). These methods assign importance scores to input tokens that contribute more towards a particular prediction (Lundberg and Lee, 2017). For instance, Liu and Avci (2019) penalize the attributions assigned to tokens contained in a manually curated dictionary consisting of group identifiers (e.g. women, jews) that are often known to be targets of hate. Kennedy et al. (2020) extract group identifiers manually from the top tokens indicated by a bag-of-words logistic regression model trained on the source corpus. However, regularizing only group identifiers limits the coverage of such approaches, and may not capture other forms of corpus-specific correlations learned by the classifier limiting its performance on a new corpus. Moreover, such manually curated lists may not always remain up-to-date because new terms emerge frequently (Grieve et al., 2018). While Yao et al. (2021) do not use such lists for refining models in different target-domains, their method still requires input from human annotators.

In this paper, we hypothesize that the classification errors in a small annotated subset from the target can reveal spurious correlations between tokens and hate speech labels learned from the source (see Table 1). To this end, we propose Dynamic Model Refinement (D-Ref), a new method to identify and penalize spurious tokens using feature attribution methods. We demonstrate that D-Ref improves the overall cross-corpora performance independently and in combination with pre-defined dictionaries.

<table>
<thead>
<tr>
<th>Target corpus utterances</th>
<th>Actual</th>
<th>Predicted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genocide is never ok</td>
<td>non-hate</td>
<td>hate</td>
</tr>
<tr>
<td>Women are goddesses</td>
<td>non-hate</td>
<td>hate</td>
</tr>
</tbody>
</table>

Table 1: Spurious correlations learned by the source classifier between the shaded tokens and the hate label.

1Code is available here: https://github.com/tbose20/D-Ref
2 Dynamic Model Refinement (D-Ref)

In this section, we describe the general theoretical framework of the proposed approach. We assume that during training our hate speech classification model has access to the source training corpus $D^{train}_S$ and a small validation set $D^{val}_T$ from a target corpus with different distribution, following a similar setting to Maharana and Bansal (2020). Our Dynamic Model Refinement (D-Ref) approach consists of 2 recurring steps across epochs: (i) we first extract a set of spurious tokens using $D^{val}_T$ at the end of every epoch; and (ii) then we penalize the extracted tokens during the next epoch.

2.1 Extraction of Spurious Tokens

Global token-ranking in source corpus: We first begin with identifying the tokens from $D^{train}_S$ that are highly correlated with hate/non-hate labels. These tokens are suitable candidates for causing source-specific spurious correlations, restricting generalizability to a new corpus.

For that purpose, at the end of every training epoch $e_{pi}$, we first obtain the global class-specific ranked list of tokens from $D^{train}_S$. This is achieved by computing global attributions per token $tok$ and class $c$ ($gl\text{-}atr^c_{tok}$) from its attribution per instance $j$ ($loc\text{-}atr^c_{tok}$) averaged across all training instances classified as $c$ by the source model trained until $e_{pi}$:

$$gl\text{-}atr^c_{tok} = \frac{\sum_{j \in [\text{hate, non-hate}], \hat{y}_j = c} \text{loc}\text{-}atr^c_{tok} \text{occurrence of tok in } j}{\sum_{j \in [\text{hate, non-hate}], \hat{y}_j = c} \#(\text{occurrence of tok in } j)}$$

Here $c \in \{\text{hate, non-hate}\}$, $\hat{y}$ is the predicted class and 1 is the indicator function. Prior to this, $loc\text{-}atr^c_{tok}$ are individually normalized using sigmoid to obtain values in a closed range. Rarely occurring tokens and stop-words are not considered for the global ranking. The $gl\text{-}atr^c_{tok}$ values are sorted from the highest globally attributed token to the lowest, which yields two ranked token-lists $[gl\text{-}hate, gl\text{-}nhate]_{e_{pi}}$.

Instance-level local ranking in target corpus: We hypothesize that tokens highly correlated with hate/non-hate classes in the source, but also causing mis-classifications in the target, should most likely contribute to spurious source-specific correlations, and may not be important for hate speech labels. Thus, we identify the tokens that cause mis-classifications in $D^{val}_T$, and then obtain a list of spurious tokens dynamically after every epoch $e_{pi}$.

We rank the tokens in the target instances from $D^{val}_T$ based on their loc-attr$^t_{tok}$, starting from the highest attributed token per instance $j$ to the lowest. The top $k$ tokens in $j$ is given by $tok^j_{topk} = topk[\text{argsort}(loc\text{-}atr^t_{tok})]$, where $k$ is a hyper-parameter in $D^{val}_T$. We treat the two error cases of False Positives (FP) and False Negatives (FN) separately. Here the hate class is considered as the positive class.

Since the tokens responsible for FP may also be important for the True Positives (TP), we only extract those that have high attributions for FP, but not for TP. Further, another filtering step is applied, where only the tokens common to the top $N$ from the ranked $gl\text{-}hate$ are extracted. This results in discarding the tokens that may not be globally correlated with a class with respect to the source model. So $tok_{FP} = \{tok \in tok^k_{topk} \& tok \notin tok^{FP}_{topk} \cap topN(gl\text{-}hate) \} \forall \text{instances } j \in D^{val}_T$. Similarly, top $k$ tokens corresponding to FN instances are extracted, wherein those common to TN are discarded, and subsequent filtering based on the $gl\text{-}nhate$ is performed, i.e. $tok_{FN} = \{tok \in tok^k_{topk} \& tok \notin tok^{FN}_{topk} \cap topN(gl\text{-}nhate) \} \forall \text{instances } j \in D^{val}_T$. This step thus yields a list of possible spurious tokens at the end of $e_{pi}$, $S_{e_{pi}} = \{tok_{FP}, tok_{FN}\}_{e_{pi}}$.

2.2 Penalizing the Extracted Spurious Tokens

In this step, we attempt to reduce the importance assigned, by the source model, to the extracted spurious tokens by penalizing the terms in $S_{e_{pi}}$ during the next epoch $e_{pi+1}$. We propose three different ways for token penalization:

Tok-mask: In this case, we simply mask the tokens from $S_{e_{pi}}$ present in $D^{train}_S$ after every $e_{pi}$ and then train the source model during $e_{pi+1}$.

Reg: Since token masking might eliminate substantial information, we regularize the model using $S_{e_{pi}}$. The attributions assigned to these terms are pushed towards zero by the following learning objective on $D^{train}_S$:

$$L = L' + \lambda \mathcal{L}_{atr}(t) ; t \in S_{e_{pi}}; \mathcal{L}_{atr} = \sum_{t \in S_{e_{pi}}} \phi(t)^2$$

where $L'$ is the classification loss and $\mathcal{L}_{atr}$ is the attribution loss. Here $\phi(t)$ is the attribution score for the token $t$. Intuitively, this should reduce the importance of tokens contributing to source-specific patterns and encourage learning more general information. Both losses are computed over $D^{train}_S$. 

Comb: We finally combine $S_{ep}$, with the pre-defined group identifiers from Liu and Avci (2019) and Kennedy et al. (2020) to perform regularization using Equation 2.

We surmise that repeating these steps at the end of every epoch should reduce the source-specific correlations while the source model gets trained. We use three different attribution methods:

(i) Scaled Attention ($\alpha \nabla \alpha$) (Serrano and Smith, 2019): Here attention weights $\alpha_i$ are scaled with their corresponding gradients $\nabla \alpha_i = \frac{\partial \gamma}{\partial \alpha_i}$, where $\gamma$ is the predicted label. Serrano and Smith (2019) show that combining an attention weight with its gradient can better indicate token importance for model predictions, compared to only using the attention weights.

(ii) Integrated Gradients (IG) (Sundararajan et al., 2017): This method is based on the notion that the gradient of a prediction function with respect to input can indicate the sensitivity of the prediction for each input dimension. As such, it aggregates the gradients along a path from an un-informative reference input (e.g. zero embedding vector) towards the actual input such that the predictions change from uncertainty to certainty.

(iii) Deep Learning Important FeatUres (DeepLIFT/DL) (Shrikumar et al., 2017): This aims to explain the difference in the output from a reference output in terms of the difference of the input and a reference input. Given a target output neuron $t$, a reference activation $t^0$, and $\Delta t = t - t^0$, it computes the contribution scores $C_{\Delta x_i, \Delta t}$ of each input neuron $x_i$ that are necessary and sufficient to compute $t$, such that $\sum_{i=1}^{n} C_{\Delta x_i, \Delta t} = \Delta t$. The reference input could be the zero embedding vector.

3 Experiments and Results

3.1 Experimental Setup

Data We use three standard hate speech corpora: HatEval (Basile et al., 2019), Waseem (Waseem and Hovy, 2016) and Dynamic (Vidgen et al., 2021). Following previous work by Wiegand et al. (2019); Swamy et al. (2019), we consider the detection of hate vs non-hate, where the hate class covers all forms of hate. We split Waseem (26.8% hate) into train (80%; 8720), val (10%; 1090) and test (10%; 1090) sets as no standard splits are provided. We use the original splits for HatEval (42.1% hate; train: 8993\(^2\), val: 1000; test: 3000) and Dynamic (54.4% hate; train: 32497, val: 1016, test: 4062). We reduce the size of available $D_{val}^T$ in Dynamic by randomly sampling 25% of the validation set (4064). We remove URLs, split hashtags into words using the CrazyTokenizer\(^3\), remove infrequent Twitter handles, punctuation marks and numbers, and convert text into lower-case. See Appendix A for a detailed discussion on the corpora.

Baselines We compare D-Ref with the following baselines: (i) BERT Van-FT (Devlin et al., 2019): vanilla fine-tuning on $D_{train}^S$ without regularization; (ii) Convolutional Neural Network with regularization of pre-defined group identifier terms using IG for feature attribution (Liu and Avci, 2019); (iii) BERT using two variations for regularization: (a) all the mentioned group identifiers, (b) group identifiers extracted from the top features of a bag-of-words logistic regression trained on each individual corpus (Kennedy et al., 2020)\(^4\); (iv) $\chi^2$-test with one degree of freedom and Yate’s correction (Kilgarriff, 2001) to extract tokens tok from $D_{train}^S$ that reject the null hypothesis with 95% confidence. The null hypothesis states that in terms of tok, both $D_{train}^S$ and $D_{val}^T$ are random samples of the same larger population. We, then, regularize the attribution scores\(^5\) assigned to these terms, with BERT. (v) Pre-def: BERT with regularizing the combined pre-defined group identifiers from (ii) and (iii).

Model training We use pre-trained BERT (Devlin et al., 2019) for our approach. We train all the models over $D_{train}^S$ from the source and evaluate over $D_{test}^T$ from the target. The best model for all the baselines and D-Ref are selected by tuning over $D_{val}^T$. See Appendix B on hyper-parameter tuning.

3.2 Cross-corpora Predictive Performance

Table 2 presents macro-F1 scores across five random initializations of each experiment using six cross-corpora pairs. We observe that overall, all feature-attribution methods with D-Ref yield improved performance compared to Van-FT and other baselines. While $\chi^2$ yields improvements over Van-FT, D-Ref still displays better performance in most of the cases. This could be attributed to the fact

\(^2\)We remove the instances that contain only URLs, reducing the train instances from 9000 to 8993.
\(^3\)https://redditscore.readthedocs.io
\(^4\)We use Sampling and Occlusion (Jin et al., 2020).
\(^5\)We use DL as it yields comparable or higher overall improvements taking Table 2 and Table 3 together.
We further compare D-Ref-Reg with various Do-
towards these tokens. Finally, it can incorporate the
mains, they may not necessarily be important for
that although the terms obtained through the \( \chi^2 \)
test from the source indicate differences across do-
not be important for the prediction of hate/ non-hate labels by the source
model, and may not contribute to source-specific spurious correlations.
We find that D-Ref-Reg with IG and DL achieves better average macro-F1 of 58.9 and 58.4 respec-
versus, compared to the corresponding Pre-def (IG) and Pre-Def (DL) that obtain an average of 57.6.
D-Ref-Reg (\( \alpha_{\nabla a} \)) provides an average macro-F1 of 58.7, comparable to Pre-def (\( \alpha_{\nabla a} \)) with 58.8. However, D-Ref-Reg achieves significantly improved scores in more cases, as compared to Pre-
def using all the attribution methods, i.e. 4/6 cases (\( \alpha_{\nabla a} \), 3/6 cases (IG) and 3/6 cases (DL) with
and none (DL) with Pre-def. D-Ref-Tok-mask exhibits improvements on average (\( \alpha_{\nabla a} \): 57.8, IG: 58.2,
58.7, 58.8) over Van-FT (57.3), demonstrating the effectiveness of the token extraction mechanism of D-
Finally, D-Ref-Comb displays the best overall performance, with the highest average score of 59.
We attribute this improvement from D-Ref to its increased coverage with dynamic token extraction,
and reduction of spurious source-specific correlations, while the baselines only penalize the group
identifiers. A dynamic approach also corrects the model during training before it can get fully biased
towards these tokens. Finally, it can incorporate the pre-defined lists along with the extracted tokens,
and further improve the performance.

### 3.3 Domain-Adaptation Approaches

We further compare D-Ref-Reg with various Do-
methods. However, such methods typically leverage the unlabeled train set
from the target domain (\( D_{T}^{\text{train}} \)). We first continue
pre-training BERT model on \( D_{T}^{\text{train}} \) following Ri-
etzler et al. (2020). Then, we perform supervised fine-tuning and regularization on \( D_{T}^{\text{train}} \) using D-
Ref-Reg (Masked Language Model + D-Ref-Reg). We compare against the following methods:

(i) **BERT Van-MLM-FT**: MLM training of BERT on \( D_{T}^{\text{train}} \) and supervised fine-tuning on \( D_{T}^{\text{train}} \).

(ii) **BERT PERL** (Pivot-based Encoder Representation of Language) (Ben-David et al., 2020): This performs pivot based fine-tuning using the MLM objective of BERT by masking and predicting the pivot terms present in the combination of \( D_{T}^{\text{train}} \) and the unlabeled \( D_{T}^{\text{train}} \). Here pivots are terms that are frequently present in the unlabeled data of both the source and target corpora, and are predictive of the source labels.

(iii) **BERT-AAD** (Adversarial Adaptation with Distillation) (Ryu and Lee, 2020), This is a domain adversarial approach with BERT where a target encoder is adapted with an adversarial objective that leverages \( D_{T}^{\text{train}} \) and \( D_{T}^{\text{train}} \).

(iv) **HATN** (Hierarchical Attention Transfer Network) (Li et al., 2018, 2017) This approach uses attention and a domain adversarial pivot extraction mechanism.

(v) **Sarwar and Murdock (2021)**: This adopts a data-augmentation strategy leveraging a negative emotion dataset (Go et al., 2009), for cross-domain hate-speech detection. They construct a weakly la-

tabeled augmented dataset by training a sequence

---

### Table 2: Macro-F1 (±std-dev) on source →target pairs (H : HatEval, D : Dynamic, W : Waseem). **Bold** denotes the best performing approach in each column for every feature attribution method. * denotes statistical significance compared to Van-FT with paired bootstrap (Dror et al., 2018; Efron and Tibshirani, 1993), 95% confidence interval.

<table>
<thead>
<tr>
<th>Approaches</th>
<th>H →D</th>
<th>D →H</th>
<th>H →W</th>
<th>W →H</th>
<th>D →W</th>
<th>W →D</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT Van-FT</td>
<td>52.1±1.0</td>
<td>63.2±1.8</td>
<td>67.6±1.1</td>
<td>52.6±2.4</td>
<td>60.3±1.0</td>
<td>46.7±1.0</td>
<td>57.3</td>
</tr>
<tr>
<td>Liu and Avci (2019)</td>
<td>45.1±4.5</td>
<td>59.5±0.7</td>
<td>57.2±1.8</td>
<td>52.6±0.8</td>
<td>57.1±2.7</td>
<td>39.6±2.0</td>
<td>51.9</td>
</tr>
<tr>
<td>Kennedy et al. (2020) (a)</td>
<td>52.2±1.2</td>
<td>62.0±1.6</td>
<td>62.7±2.9</td>
<td>50.1±0.8</td>
<td>53.5±2.0</td>
<td>45.1±2.3</td>
<td>54.3</td>
</tr>
<tr>
<td>Kennedy et al. (2020) (b)</td>
<td>52.0±1.8</td>
<td>61.9±1.7</td>
<td>63.6±3.7</td>
<td>54.8±1.6</td>
<td>57.0±1.7</td>
<td>46.8±1.9</td>
<td>56.0</td>
</tr>
<tr>
<td>BERT ( \chi^2 )-test</td>
<td>55.4±1.1</td>
<td>65.0±1.0</td>
<td>68.1±1.3</td>
<td>57.3±2.1</td>
<td>60.4±2.8</td>
<td>45.2±2.8</td>
<td>58.0</td>
</tr>
</tbody>
</table>

| Pre-def (\( \alpha_{\nabla a} \)) | 54.0±1.3 | 65.1±1.1 | 69.6±3.4 | 54.4±1.2 | 61.9±1.6 | 47.2±3.1 | 58.8     |
| D-Ref-Tok-mask (\( \alpha_{\nabla a} \)) | 58.0±0.6 | 64.9±0.7 | 68.9±3.3 | 53.6±3.0 | 59.6±2.2 | 45.8±3.7 | 57.8     |
| D-Ref-Reg (\( \alpha_{\nabla a} \)) | 54.9±1.2 | 65.1±1.0 | 68.6±4.0 | 54.1±1.0 | 59.0±1.5 | 46.7±3.3 | 59.0     |
| D-Ref-Comb (\( \alpha_{\nabla a} \)) | 55.0±1.6 | 64.7±1.2 | 69.9±1.6 | 55.3±1.3 | 61.0±2.8 | 48.1±1.0 | 59.0     |

| Pre-def (IG)               | 55.7±1.4 | 65.3±2.8 | 69.7±2.2 | 51.7±2.7 | 60.3±2.2 | 44.6±3.0 | 57.6     |
| D-Ref-Tok-mask (IG)        | 56.3±2.3 | 65.4±1.8 | 68.3±2.0 | 52.3±2.3 | 59.3±1.3 | 48.2±2.1 | 58.2     |
| D-Ref-Reg (IG)             | 56.4±1.4 | 65.5±0.8 | 69.2±2.5 | 53.8±0.7 | 60.6±1.7 | 47.3±3.6 | 58.9     |
| D-Ref-Comb (IG)            | 55.7±0.8 | 63.7±2.4 | 69.1±2.3 | 52.6±2.3 | 61.4±2.5 | 51.4±3.6 | 59.0     |

| Pre-def (DL)               | 54.2±1.6 | 60.4±1.9 | 68.1±1.5 | 52.9±1.2 | 62.0±1.8 | 44.5±1.3 | 57.6     |
| D-Ref-Tok-mask (DL)        | 54.1±1.4 | 64.9±1.7 | 67.2±3.6 | 52.1±1.9 | 60.5±2.5 | 47.2±3.1 | 57.8     |
| D-Ref-Reg (DL)             | 54.2±1.6 | 64.8±0.8 | 70.5±2.7 | 51.4±0.7 | 62.3±2.5 | 47.1±5.5 | 58.4     |
| D-Ref-Comb (DL)            | 55.2±1.8 | 64.0±0.9 | 69.5±3.3 | 54.0±0.8 | 61.5±2.3 | 48.1±2.7 | 58.8     |
tagger on $D_{train}^I$ and a TF-IDF based template matching with $D_{train}^T$.

(vi) $\chi^2$-test using $D_{S}^{train}$ and $D_{I}^{train}$.

For a fair comparison, we initialize (v) and (vi) with the MLM trained BERT on $D_{I}^{train}$, while the other methods already make use of $D_{train}^T$ for adaptation. We use $D_{I}^{val}$ from target for model selection for all the above methods.

Table 3 shows the results on comparing against other DA approaches. We note that the average performance of all the other DA approaches in this task is lower than Van-MLM-FT, as discussed in our previous work (Bose et al., 2021). $\chi^2$-test, on an average, fails to surpass the Vanilla baseline. Besides, the DA approach proposed for cross-domain hate-speech detection by Sarwar and Murdock (2021) also yields an overall drop in performance. They perform data-augmentation by replacing relevant words from an external negative emotion dataset with tagged hateful terms from the target domain. We find that a major portion of the augmented instances lack meaning, and this negatively impacts the adaptation. However, across all feature attribution methods, D-Ref-Reg improves the cross-corpora performance compared to Van-MLM-FT and the DA approaches, with average macro-F1 of 59.6 ($\alpha\nabla\alpha$), 59.8 (IG), and 60.8 (DL), compared to 58.1 from Van-MLM-FT. Since D-Ref-Reg and Van-MLM-FT use identical MLM pre-training on $D_{train}^I$, the improvements can be attributed to the dynamic token extraction of our method.

More generally, when the larger set of target domain unannotated instances $D_{S}^{train}$ are unavailable, D-Ref can identify and correct spurious correlations on source using a small amount of annotated instances from the target $D_{I}^{val}$, as demonstrated in Section 3.2. When sufficient number of unannotated instances from the target corpus are available, D-Ref can yield further cross-corpora improvements by leveraging the unannotated target instances with the MLM pre-training.

3.4 Qualitative Analysis

Table 4 shows the change in attributions for some instances in $D_{S}^{test}$ from Dynamic that were misclassified by Van-FT but correctly classified by our D-Ref-Reg (IG). Van-FT wrongly attributes higher importance to ‘f*cking’ and ‘s*cks’ for the hate class in the first example, and ‘blacks’ and ‘queers’ for non-hate in the second due to source-specific correlations. However, D-Ref-Reg (IG), extracts and penalizes abusive tokens like {s*ck, a**hole, d*ck} for the former causing FP and {africans, dark, queer} for the latter causing FN. Our approach not only penalizes the exact tokens, but also those with similar meaning (e.g. ‘blacks’ is contextually close to ‘dark’, ‘africans’), giving more importance to the context around the spurious tokens. See Appendix C for the token-lists.

4 Conclusion

We proposed a dynamic approach for automatic token extraction with regularization of the source model such that the spurious source specific correlations are reduced. Our approach shows consistent cross-corpora performance improvements both independently and in combination with pre-defined tokens. Future work includes applying our method on other cross-domain text classification tasks and exploring how explanation faithfulness can be improved in out-of-domain settings (Chrysostomou and Aletras, 2022).

<table>
<thead>
<tr>
<th>Approaches</th>
<th>H $\rightarrow$ D</th>
<th>D $\rightarrow$ H</th>
<th>H $\rightarrow$ W</th>
<th>W $\rightarrow$ H</th>
<th>D $\rightarrow$ W</th>
<th>W $\rightarrow$ D</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT Van-MLM-FT</td>
<td>56.6±0.1</td>
<td>62.2±0.4</td>
<td>70.0±2.5</td>
<td>50.2±0.1</td>
<td>64.1±2.4</td>
<td>43.5±1.9</td>
<td>58.1</td>
</tr>
<tr>
<td>BERT PERL</td>
<td>54.1±0.7</td>
<td>60.0±0.6</td>
<td>60.1±2.0</td>
<td>55.2±0.7</td>
<td>55.5±1.0</td>
<td>37.8±1.2</td>
<td>53.8</td>
</tr>
<tr>
<td>BERT-AAD</td>
<td>56.6±1.3</td>
<td>53.9±3.5</td>
<td>68.8±2.5</td>
<td>50.7±1.4</td>
<td>48.3±4.7</td>
<td>53.0±1.7</td>
<td>55.2</td>
</tr>
<tr>
<td>HATN</td>
<td>48.4±1.6</td>
<td>59.1±0.4</td>
<td>59.7±2.9</td>
<td>51.4±1.8</td>
<td>60.0±2.6</td>
<td>45.4±2.7</td>
<td>54.0</td>
</tr>
<tr>
<td>MLM + Sarwar and Murdock (2021)</td>
<td>55.0±0.1</td>
<td>66.2±2.0</td>
<td>68.8±1.1</td>
<td>48.2±3.1</td>
<td>57.9±1.3</td>
<td>36.2±1.1</td>
<td>55.4</td>
</tr>
<tr>
<td>MLM + $\chi^2$-test</td>
<td>57.9±1.6</td>
<td>67.1±1.7</td>
<td>69.8±0.8</td>
<td>48.2±3.1</td>
<td>60.4±2.8</td>
<td>44.1±3.4</td>
<td>57.9</td>
</tr>
<tr>
<td>MLM + D-Ref-Reg (α = 0.5)</td>
<td>57.9±1.9</td>
<td>66.2±1.2</td>
<td>70.7±1.2</td>
<td>52.9±3.0</td>
<td>62.8±1.4</td>
<td>48.8±4.4</td>
<td>59.8</td>
</tr>
<tr>
<td>MLM + D-Ref-Reg (IG)</td>
<td>58.6±1.2</td>
<td>66.8±0.5</td>
<td>70.1±1.5</td>
<td>52.1±3.0</td>
<td>62.5±3.0</td>
<td>48.9±4.4</td>
<td>59.8</td>
</tr>
<tr>
<td>MLM + D-Ref-Reg (DL)</td>
<td>58.8±1.2</td>
<td>66.7±0.6</td>
<td>70.5±1.3</td>
<td>52.4±3.5</td>
<td>64.7±2.1</td>
<td>51.5±4.9</td>
<td>60.8</td>
</tr>
</tbody>
</table>

Table 3: Comparison of DA approaches with D-Ref + MLM. Macro-F1 (±std-dev) on different source $\rightarrow$ target pairs. H : HatEval, D : Dynamic, W : Waseem. * denotes the significantly improved scores w.r.t. Van-MLM-FT.

<table>
<thead>
<tr>
<th>Approaches</th>
<th>TP with Van-FT</th>
<th>TN with D-Ref-Reg (IG)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wildlife</td>
<td>belongs in</td>
<td>the Wildlife</td>
</tr>
<tr>
<td>F*cking wild</td>
<td>wild</td>
<td>NHS</td>
</tr>
<tr>
<td>S*cks</td>
<td>NHS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approaches</th>
<th>TP with Van-FT</th>
<th>TN with D-Ref-Reg (IG)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black</td>
<td>are savages</td>
<td>Black</td>
</tr>
<tr>
<td>Queers</td>
<td>can’t be true</td>
<td>Queers</td>
</tr>
<tr>
<td>Happy</td>
<td>Happy</td>
<td></td>
</tr>
</tbody>
</table>

Table 4: Change in attributions with D-Ref-Reg (IG).
Ethical Considerations

The approach proposed in the paper is aimed at supporting robust and accurate detection of online hate speech. The datasets used in the work are publicly available and referenced appropriately. The dataset creators have presented, in detail, the data collection process and annotation guidelines in peer-reviewed articles. The offensive terms presented, as examples, are only intended for better analysis of the models for research purposes.

Acknowledgements

This work was supported partly by the french PIA project “Lorraine Université d’Excellence”, reference ANR-15-IDEX-04-LUE. Experiments presented in this article were carried out using the Grid’5000 testbed, supported by a scientific interest group hosted by Inria and including CNRS, NATER and several Universities as well as other organizations (see https://www.grid5000.fr). We thank the anonymous reviewers for their valuable feedback and suggestions. We would also like to thank George Chrysostomou for his help and suggestions regarding the work during informal discussions.

References


While which are also determined to a large extent by the\cite{Wiegand2019} used in Dynamic Twitter, for instance, in Waseem induced with such focused sampling procedures of dataset bias with spurious correlations are been collected across different time frames, and model-in-the-loop process. These corpora have


\section*{A Data Description}

While HatEval and Waseem are sampled from Twitter, Dynamic is generated using a human-and-model-in-the-loop process. These corpora have been collected across different time frames, and hence they involve different topics of discussion, which are also determined to a large extent by the keywords used for sampling. As such, the problem of dataset bias with spurious correlations are induced with such focused sampling procedures \cite{Wiegand2019} used in Waseem and HatEval. For instance, in Waseem, a large amount of tweets, available at the time of our experiments, consist of hate tweets directed against women, which results in False Positives for instances from other corpora that contain women related terms. We observed that most of the racist tweets were already removed and were unavailable for experiments. HatEval, on the other hand, has a mix of tweets directed against women and immigrants, and hence it demonstrates decent performance when evaluated over Waseem that consists of sexist tweets. On the contrary, Dynamic contains annotator-generated tweets that includes challenging perturbations. For instance, it includes non-hate instances like ‘It’s wonderful having gay people around here’, ‘I hate the concept of hate’, ‘Tea is f*cking disgusting’, which can easily fool a classifier learned on biased datasets, and result in classifying these instances as hateful. Moreover, this corpus covers different targets of hate. As such, when Dynamic is used as the target corpus, the spurious correlations learned by the source classifier become relatively well-visible, which are captured and penalized by D-Ref while the source model gets trained.

The data used in the work are publicly available, and download links are provided in the respective original articles, which are referenced in this paper. However, in the case of Waseem, where only tweet IDs are provided, some tweets might be unavailable.

\section*{B Implementation Details}

We leverage the pretrained BERT-base model\footnote{https://github.com/huggingface/transformers} for our experiments. We use a batch size of 8, learning rate of $1 \times 10^{-5}$ and Adam optimizer with decoupled weight decay regularization \cite{VanHout} for Van-FT, Van-MLM-FT, D-Ref and Pre-def. For Integrated Gradients, following Liu and Avci (2019), the interpolated embeddings are treated as constants while back-propagating the loss from the regularization term. An all zero embedding vector is used as the baseline input for both Integrated Gradients and DeepLIFT. We use the original code, as provided by the respective authors, for all the prior-arts. For Pre-Def, we combined the pre-defined lists from Kennedy et al. (2020) and Liu and Avci (2019) and regularized their attribution scores over BERT with $\alpha$V, IG, and DL as feature attribution methods.

We implement the data-augmentation approach
proposed by Sarwar and Murdock (2021) ourselves due to the absence of an available implementation. Following the description present in the paper, we prepare the training data for the sequence tagger by labeling all the terms in the hateful instances from the source corpus that are also present in the lexicon from hatebase.org. However, we do not tokenize the lexicon obtained from hatebase.org while searching for the corresponding matching terms in the source corpus. We convert the lexicon into lower-case and look for the exact match in the source corpus.

For D-Ref, we set the value of top $N$ tokens used from ranked \{glist-hate, glist-nhate\} as 500. The values of $k \in \{10\%, \, 20\%, \, 30\%, \, 40\%\}$ of the instance-length in D-Ref, and $\alpha$ in both D-Ref and Pre-def are selected through hyper-parameter tuning over $D_{val}^{\alpha}$ using a random seed. For $\alpha \nabla \alpha$ and DeepLIFT, $\lambda \in \{0.1, \, 0.5, \, 1, \, 10, \, 20, \, 30, \, 40, \, 50, \, 60\}$ and for IG, $\lambda \in \{1, \, 10, \, 20, \, 30, \, 40, \, 50, \, 60\}$. We run supervised fine-tuning on $D_{train}$ for 6 epochs with all the BERT models (prior-arts and D-Ref). We select the models (prior-arts and D-Ref) by tuning over $D_{val}$ from the target corpus, with respect to macro-F1 scores. Table 5 presents the macro-F1 scores obtained on the validation set for D-Ref and the prior arts.

C Tokens extracted in different epochs

The list of error-causing tokens for False Positives (FP) and False Negatives (FN) in $D_{T}^{val}$, extracted for the cases presented in Section 3.4, is given below. We underline the tokens present in the visualization examples (both Table 4 in Section 3.4 and below) and ones similar in meaning to them.

HatEval → Dynamic

- **Epoch 1**: FP: \{idiots, conservative, countries, p*ssy, bloody, americans, move, a**hole, hating, beings, feminist, africans, resources, d*ck, resist, females, attacks, dude, anger\}
  FN: \{hitler, plague, ##urs, crisis, rescue, funding, gorgeous, treason, journalist, lawyers, agenda, roles, principles, bloody, intern\}

- **Epoch 2**: FP: \{race, hating, flights, sheep, females, ignorant, feminist, resist, attacks, d*ck, kill, boat, countries, p*ssy, refugee, bloody\}
  FN: \{president, foreigners, illegal, betrayal, lgbt, riots, gorgeous, treason, joking, chris, intelligent, arguments, humans\}

- **Epoch 3**: FP: \{countries, race, hating, females, fascist, africans, ridiculous, d*ck, express, comments, organized, s*ck, allow, bloody\}
  FN: \{illegal, hitler, generally, david, intelligent, secret, chris, equality, dating, yellow, treason, abuses, ##gb, humans, plague, dear, nonsense\}

- **Epoch 4**: FP: \{isis, genocide, indians, society, supported, females, feminist, attacks, s*ck, destroy, migrants\}
  FN: \{hitler, opportunities, sister, betrayal, ##ame, gorgeous, ##heads, dating, riots, bank, murders, arguments, humans, fights, plague, influence, targeting, supporters, coordination, lies, ##boys\}

- **Epoch 5**: FP: \{clean, ignorant, slave, feminist, punish, africans, ##ache, d*ck, ##fs, ars, destroy, status, race, p*ssy, western, send\}
  FN: \{statement, gross, hitler, sending, yellow, waste, hopefully, trapped, riots, bait, sister, coordination, humans\}

- **Epoch 6**: FP: \{soft, suicide, countries, p*ssy, bloody, genocide, punish, destroy, migrants, vile, beings, savage, feminist, tory, awful, ignorant, ##ists, spend, send\}
  FN: \{gross, secret, influence, yellow, crime, abuses, participate, approach\}

A non-hate comment in Dynamic test set for the above case, wrongly classified as hate by Van-FT and correctly classified as non-hate with D-Ref-Reg (IG), is given below. Darker the shade, higher is the attribution:

**Van-FT**: There is so much cancer patients in the world but it is mostly the young females who are worstly affected by this disease.

**D-Ref-Reg**: There is so much cancer patients in the world but it is mostly the young females who are worstly affected by this disease.

Waseem → Dynamic

- **Epoch 1**: FP: \{female, ##ists, fe, sex, feminist, rap\}
  FN: \{cast, coward, queer, equality, ##bi , cost, ##sy, born, asian, nazis, kids, cancer, gender, hiring, funded\}

- **Epoch 2**: FP: \{##ists, her, sex, worse, feminist, ##nt, outraged\}
  FN: \{welcome, caused, cancer. drag, ##bi, pressure, parent, nazis, troll, cast, trash, ruins, lesbian, attacking, chinese\}

---

7https://hatebase.org/
Table 5: Validation set \( (\hat{D}_T) \) macro F1 \( (\pm \text{std-dev}) \) on source \( \rightarrow \) target pairs (H : HatEval, D : Dynamic, W : Waseem).

<table>
<thead>
<tr>
<th>Approaches</th>
<th>H ( \rightarrow ) D</th>
<th>D ( \rightarrow ) H</th>
<th>H ( \rightarrow ) W</th>
<th>W ( \rightarrow ) H</th>
<th>D ( \rightarrow ) W</th>
<th>W ( \rightarrow ) D</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT Van-FT</td>
<td>54.7 \pm 1.0</td>
<td>64.7 \pm 1.1</td>
<td>65.6 \pm 4.5</td>
<td>59.4 \pm 1.2</td>
<td>61.9 \pm 1.1</td>
<td>46.9 \pm 4.7</td>
<td>58.9</td>
</tr>
<tr>
<td>Liu and Avci (2019)</td>
<td>45.3 \pm 2.1</td>
<td>50.3 \pm 1.1</td>
<td>57.1 \pm 2.4</td>
<td>49.7 \pm 0.5</td>
<td>56.8 \pm 3.2</td>
<td>39.3 \pm 2.0</td>
<td>49.8</td>
</tr>
<tr>
<td>Kennedy et al. (2020) (a)</td>
<td>53.5 \pm 1.1</td>
<td>62.8 \pm 1.5</td>
<td>60.3 \pm 2.5</td>
<td>53.9 \pm 8.8</td>
<td>51.3 \pm 2.3</td>
<td>43.6 \pm 2.3</td>
<td>54.2</td>
</tr>
<tr>
<td>Kennedy et al. (2020) (b)</td>
<td>54.8 \pm 4.2</td>
<td>55.5 \pm 3.9</td>
<td>62.1 \pm 1.8</td>
<td>61.3 \pm 0.9</td>
<td>58.6 \pm 4.4</td>
<td>46.3 \pm 2.7</td>
<td>56.4</td>
</tr>
</tbody>
</table>

Table 6: In-corpus macro F1 \( (\pm \text{std-dev}) \), i.e. the source corpus performance, obtained after refining the source model for the target corpus (present at the right hand side of the arrows) using D-Ref-Reg. H : HatEval, D : Dynamic, W : Waseem. For D-Ref-Reg, model-selection and early-stopping is done over the validation set from the target corpus.

<table>
<thead>
<tr>
<th>Approaches</th>
<th>HatEval</th>
<th>Dynamic</th>
<th>Waseem</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT Van-FT</td>
<td>43.3 \pm 1.8</td>
<td>85.1 \pm 0.5</td>
<td>85.4 \pm 0.7</td>
<td>71.3</td>
</tr>
</tbody>
</table>

Table: In-corpus performance on source \( (\leftarrow \text{of arrows}) \) while refining the source model for the target \( (\rightarrow \text{of arrows}) \) arrows)

<table>
<thead>
<tr>
<th>Approaches</th>
<th>H ( \rightarrow ) D</th>
<th>H ( \rightarrow ) W</th>
<th>D ( \rightarrow ) H</th>
<th>D ( \rightarrow ) W</th>
<th>W ( \rightarrow ) H</th>
<th>W ( \rightarrow ) D</th>
<th>( \pm \text{std-dev} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>D-Ref-Reg ( (\hat{\alpha} \nabla \alpha) )</td>
<td>39.7 \pm 3.2</td>
<td>38.4 \pm 1.7</td>
<td>84.1 \pm 1.0</td>
<td>84.2 \pm 0.8</td>
<td>84.4 \pm 0.7</td>
<td>78.8 \pm 8.0</td>
<td>68.3</td>
</tr>
<tr>
<td>D-Ref-Reg (IG)</td>
<td>40.5 \pm 2.0</td>
<td>37.7 \pm 2.1</td>
<td>84.0 \pm 0.4</td>
<td>84.5 \pm 0.4</td>
<td>84.6 \pm 1.0</td>
<td>85.3 \pm 1.4</td>
<td>69.4</td>
</tr>
<tr>
<td>D-Ref-Reg (DL)</td>
<td>37.1 \pm 1.8</td>
<td>38.1 \pm 2.9</td>
<td>84.7 \pm 0.6</td>
<td>84.3 \pm 1.2</td>
<td>84.4 \pm 0.5</td>
<td>80.7 \pm 6.4</td>
<td>68.2</td>
</tr>
</tbody>
</table>

D In-corpus performance

We present the in-corpus performance, i.e. the performance on the source corpus in terms of macro-F1 scores, obtained when the source model is refined for the corresponding target corpus using D-Ref-Reg, in Table 6. For D-Ref-Reg, the model is tuned over the target corpus validation set. Here

- **Epoch 3:** FP: {female, ##ja, might, men, feminist} FN: {quoting, govt, referring, nazis, troll, lesbian, rogue, date, chinese, typically}
- **Epoch 4:** FP: {communism, her, openly, intelligent, many, Barbie, chicks, females, arguing} FN: {date, suggest, ##lat, referring, police, chinese, cancer, voice, native, lesbian}
- **Epoch 5:** FP: {term, f^ck, ##ng, woman, ##ist, feminist, females, prison} FN: {removed, educate, freaking, queer, wow, ending, referring, dye, ##wat, issues, africans, vast, chinese, dark}
- **Epoch 6:** FP: {whore, her, ##ots, role, sweden, pay, d^ck, trump, feminist, females, american, arguing} FN: {bat, everyday, freak, argument, movement, chinese, tho, feature, lesbian}

A hate comment in Dynamic test set for the above case, wrongly classified as non-hate by Van-FT and correctly classified as hate with D-Ref-Reg (IG), is given below. Darker the shade, higher is the attribution:

Don't get me wrong I don't hate Van-FT: asians, but I definitely don't like them

Don't get me wrong I don't hate D-Ref-Reg: asians, but I definitely don't like them

Since, the Waseem dataset is made available as tweet IDs, we observed that it mostly contains sexist comments, while most of the racist content must have been removed before we could crawl it. Hence, the tokens related to race mostly occur in non-hate contexts causing FN.

Even though some error-causing tokens remain in the list until the end, their overall effect should be reduced as the regularization is performed throughout the training procedure, which causes improvement in macro F1.
BERT Van-FT gives the original performance of the source model, when no refinement is performed, as a reference. In this case, the model is tuned over the in-corpus validation set. The HatEval corpus is part of a shared task and involves a challenging test set with low in-corpus performance. The drop across in-corpus performance with D-Ref-Reg is expected, as the main goal of the proposed approach is to make the source model best suited for the target corpus.

### E Pre-defined group identifiers

The combined list of pre-defined group identifiers from Liu and Avci (2019) and Kennedy et al. (2020) are given below:

\{lesbian, gay, bisexual, trans, cis, queer, lgbt, lgbtq, straight, heterosexual, male, female, non-binary, african, african american, european, hispanic, latino, latina, latinx, canadian, american, asian, indian, middle eastern, chinese, japanese, christian, buddhist, catholic, protestant, sikh, taoist, old, older, young, younger, teenage, millenial, middle aged, elderly, blind, deaf, paralyzed, muslim, jew, jews, white, islam, blacks, muslims, women, whites, gay, black, democrat, islam, allah, jewish, lesbian, transgender, race, brown, woman, mexican, religion, homosexual, homosexuality, africans\}

### F Computational Efficiency

We present the per epoch training time for D-Ref-Reg with different source corpora in Table 7. The training times of D-Ref-Reg \((α∇α)\) are less than 2 times of that with Van-FT. With D-Ref-Reg (DL), the training time is approximately 4.5 times of that with Van-FT. This demonstrates the computational efficiency of our approach. In the case of D-Ref-Reg (IG), the computation time is indeed high. This occurs due to the aggregation of gradients using a path integral and computing gradients over gradients, as also discussed in Kennedy et al. (2020); Liu and Avci (2019). However, our approach is not dependent on any particular feature attribution method, as demonstrated with our experiments.

<table>
<thead>
<tr>
<th>Approaches</th>
<th>HatEval</th>
<th>Dynamic</th>
<th>Waseem</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT Van-FT</td>
<td>1 m 25 s</td>
<td>3 m 52 s</td>
<td>2 m</td>
</tr>
<tr>
<td>D-Ref-Reg ((α∇α))</td>
<td>1 m 39 s</td>
<td>7 m</td>
<td>3 m 33 s</td>
</tr>
<tr>
<td>D-Ref-Reg (IG)</td>
<td>9 m 37 s</td>
<td>59 m</td>
<td>19 m 7 s</td>
</tr>
<tr>
<td>D-Ref-Reg (DL)</td>
<td>4 m 4 s</td>
<td>18 m 36 s</td>
<td>8 m 44 s</td>
</tr>
</tbody>
</table>

Table 7: Per epoch training time on different source corpora.