HABERTOR: An Efficient and Effective Deep Hatespeech Detector

Thanh Tran*, Yifan Hu♦, Changwei Hu♦, Kevin Yen♦, Fei Tan♦, Kyumin Lee*, Serim Park♥

*Worcester Polytechnic Institute, ♦Yahoo! Research, ♥Twitter
{tdtran,kmlee}@wpi.edu
{yifanhu,changweih,kevinyen,fei.tan}@verizonmedia.com
serimp@twitter.com

Abstract

We present our HABERTOR model for detecting hatespeech in large scale user-generated content. Inspired by the recent success of the BERT model, we propose several modifications to BERT to enhance the performance on the downstream hatespeech classification task. HABERTOR inherits BERT’s architecture, but is different in four aspects: (i) it generates its own vocabularies and is pre-trained from the scratch using the largest scale hatespeech dataset; (ii) it consists of Quaternion-based factorized components, resulting in a much smaller number of parameters, faster training and inferencing, as well as less memory usage; (iii) it uses our proposed multi-source ensemble heads with a pooling layer for separate input sources, to further enhance its effectiveness; and (iv) it uses a regularized adversarial training with our proposed fine-grained and adaptive noise magnitude to enhance its robustness. Through experiments on the large-scale real-world hatespeech dataset with 1.4M annotated comments, we show that HABERTOR works better than 15 state-of-the-art hatespeech detection methods, including fine-tuning Language Models. In particular, comparing with BERT, our HABERTOR is 4~5 times faster in the training/inferencing phase, uses less than 1/3 of the memory, and has better performance, even though we pre-train it by using less than 1% of the number of words. Our generalizability analysis shows that HABERTOR transfers well to other unseen hatespeech datasets and is a more efficient and effective alternative to BERT for the hatespeech classification.

1 Introduction

The occurrence of hatespeech has been increasing (Barna, 2019). It has become easier than before to reach a large audience quickly via social media, causing an increase of the temptation for inappropriate behaviors such as hatespeech, and potential damage to social systems. In particular, hatespeech interferes with civil discourse and turns good people away. Furthermore, hatespeech in the virtual world can lead to physical violence against certain groups in the real world1,2, so it should not be ignored on the ground of freedom of speech.

To detect hatespeech, researchers developed human-crafted feature-based classifiers (Chatzakou et al., 2017; Davidson et al., 2017; Waseem and Hovy, 2016; MacAvaney et al., 2019), and proposed deep neural network architectures (Zampieri et al., 2019; Gambèck and Sidkar, 2017; Park and Fung, 2017; Badjatiya et al., 2017; Agrawal and Awekar, 2018). However, they might not explore all possible important features for hatespeech detection, ignored pre-trained language model understanding, or proposed uni-directional language models by reading from left to right or right to left.

Recently, the BERT (Bidirectional Encoder Representations from Transformers) model (Devlin et al., 2019) has achieved tremendous success in Natural Language Processing. The key innovation of BERT is in applying the transformer (Vaswani et al., 2017) to language modeling tasks. A BERT model pre-trained on these language modeling tasks forms a good basis for further fine-tuning on supervised tasks such as machine translation and question answering, etc.

Recent work on hatespeech detection (Nikolov and Radivchev, 2019) has applied the BERT model and has shown its prominent results over previous hatespeech classifiers. However, we point out its two limitations in hatespeech detection domain. First, the previous studies (ElSherief et al., 2018b,a) have shown that a hateful corpus owns distinguished linguistic/semantic characteristics compared to a non-hateful corpus. For instance, hatespeech sequences are often informal or even in-
tentionally mis-spelled (ElSherief et al., 2018a; Arango et al., 2019), so words in hateful sequences can sit in a long tail when ranking their uniqueness, and a comment can be hateful or non-hateful using the same words (Zhang and Luo, 2019). For example, “dick” in the sentence “Nobody knew dick about what that meant” is non-hateful, but “d1ck” in “You are a weak small-d1cked keyboard warrior” is hateful. Thus, to better understand hateful vocabularies and contexts, it is better to pre-train on a mixture of both hateful and non-hateful corpora. Doing so helps to overcome the limitation of using BERT models pre-trained on non-hateful corpora like English Wikipedia and BookCorpus. Second, even the smallest pre-trained BERT “base” model contains 110M parameters. It takes a lot of computational resources to pre-train, fine-tune, and serve. Some recent efforts aim to reduce the complexity of BERT model with the knowledge distillation technique such as DistillBert (Sanh et al., 2019) and TinyBert (Jiao et al., 2019). In these methods, a pre-trained BERT-alike model is used as a teacher model, and a student (smaller) model (i.e. TinyBERT, DistilBERT, etc) is trained to produce similar output to that of the teacher model. Unfortunately, while their complexity is reduced, the performance is also degraded in NLP tasks compared to BERT. Another direction is to use cross-layer parameter sharing, such as ALBERT (Lan et al., 2020). However, ALBERT’s computational time is similar to BERT, since the number of layers remains the same as BERT; likewise, its inference is equally expensive.

Based on the above observation and analysis, we aim to investigate whether it is possible to achieve a better hatespeech prediction performance than state-of-the-art machine learning classifiers, including classifiers based on publicly available BERT model, while significantly reducing the number of parameters compared with the BERT model. By doing so, we believe that performing pre-training tasks from the ground up and on a hatespeech-related corpus would allow the model to understand hatespeech patterns better and enhance the predictive results. However, while language model pretraining tasks require a large scale corpus size, available hatespeech datasets are normally small: only 16K~115K annotated comments (Waseem and Hovy, 2016; Wulczyn et al., 2017). Thus, we introduce a large annotated hatespeech dataset with 1.4M comments extracted from Yahoo News and Yahoo Finance. To reduce the complexity, we reduce the number of layers and hidden size, and propose Quaternion-based Factorization mechanisms in BERT architecture. To further improve the model effectiveness and robustness, we introduce a multi-source ensemble-head fine-tuning architecture, as well as a target-based adversarial training. The major contributions of our work are:

- We reduce the number of parameters in BERT considerably, and consequently the training/inferencing time and memory, while achieving better performance compared to the much larger BERT models, and other state-of-the-art hatespeech detection methods.
- We pre-train from the ground up a hateful language model with our proposed Quaternion Factorization methods on a large-scale hatespeech dataset, which gives better performance than fine tuning a pretrained BERT model.
- We propose a flexible classification net with multi-sources and multi-heads, building on top of the learned sequence representations to further enhance our model’s predictive capability.
- We utilize adversarial training with a proposed fine-grained and adaptive noise magnitude to improve our model’s performance.

2 Related Work

Some of the earlier works in hatespeech detection have applied a variety of classical machine learning algorithms (Chatzakou et al., 2017; Davidson et al., 2017; Waseem and Hovy, 2016; MacAvaney et al., 2019). Their intuition is to do feature engineering (i.e. manually generate features), then apply classification methods such as SVM, Random Forest, and Logistic Regression. The features are mostly Term-Frequency Inverse-Document-Frequency scores or Bag-of-Words vectors, and can be combined with additional features extracted from the user account’s meta information and network structure (i.e., followers, followees, etc). Those methods are suboptimal as they mainly rely on the quality and quantity of the human-crafted features.

Recent works have used deep neural network architectures for hatespeech detection (Zampieri...
et al., 2019; Mou et al., 2020) such as CNN (Gambück and Sikdar, 2017; Park and Fung, 2017), RNN (i.e. LSTM and GRU) (Badjatiya et al., 2017; Agrawal and Awekar, 2018), combining CNN with RNN (Zhang et al., 2018), or fine tuning a pre-trained language models (Indurthi et al., 2019).

Another direction focuses on the testing generalization of the current hatespeech classifiers (Agrawal and Awekar, 2018; Dadvar and Eckert, 2018; Gröndahl et al., 2018), where those methods are tested in other datasets and domains such as Twitter data (Waseem and Hovy, 2016), Wikipedia data (Wulczyn et al., 2017), Formspring data (Reynolds et al., 2011), and YouTube comment data (Dadvar et al., 2014).

Unlike previous works, we pre-train a hateful language model, then build a multi-source multi-head hatespeech classifier with regularized adversarial training to enhance the model’s performance.

3 Problem Definition

Given an input text sequence $s = [w_1, w_2, ..., w_n]$ where $\{w_1, w_2, ..., w_n\}$ are words and $n = |s|$ is the maximum length of the input sequence $s$. The hate-speech classification task aims to build a mapping function $f : s = [w_1, w_2, ..., w_n] \rightarrow \mathcal{R} \in [0, 1]$, where $f$ inputs $s$ and returns a probability score $P(y = 1|s) \in [0, 1]$, indicating how likely $s$ is classified as hatespeech. In this paper, we approximate $f$ by a deep neural classifier, where we first pretrain $f$ with unsupervised language modeling tasks to enhance its language understanding. Then, we train $f$ with the hatespeech classification task to produce $P(y = 1|s)$.

4 Our approach – HABERTOR

4.1 Tokenization

BERT model relies on WordPiece (WP) (Wu et al., 2016), a Google’s internal code that breaks down each word into common sub-word units (“word-pieces”). These sub-words are like character n-grams, except that they are automatically chosen to ensure that each of these sub-words is frequently observed in the input corpus. WP improves handling of rare words, such as intentionally misspelled abusive words, without the need for a huge vocabulary. A comparable implementation that is open sourced is SentencePiece (SP) (Kudo and Richardson, 2018). Like WP, the vocab size is predetermined. Both WP and SP are unsupervised learning models. Since WP is not released in public, we train a SP model using our training data, then use it to tokenize input texts.

4.2 Parameter Reduction with Quaternion Factorization

Denote $V$ the vocab size, $E$ the embedding size, $H$ the hidden size, $L$ the number of layers, and $F$ the feed-forward/filter size. In BERT, $F = 4H$, $E = H$, and the number of attention heads is $H/64$. Encoding the vocabs takes $VH$ parameters. Each BERT layer contains three parts: (i) attention, (ii) filtering/feedback, and (iii) output. Each of the three parts has $4H^2$ parameters. Thus, a BERT layer has $12H^2$ parameters and a BERT-base setting with 12 layers has $VH + 144H^2$ parameters. Please refer to Section A.3 in the Appendix for details.

Recently, Quaternion representations have shown its benefits over Euclidean representations in many neural designs (Parcollet et al., 2019; Tay et al., 2019): (i) a Quaternion number consists of a real component and three imaginary components, encouraging a richer extent of expressiveness; and (ii) a Quaternion transformation reduces 75% parameters compared to the traditional Euclidean transformation because of the weight sharing using the Hamilton product. Hence, we propose Quaternion factorization strategies to significantly reduce the model’s parameters as follows:

Vocab Factorization (VF): Inspired by Lan et al. (2020), we encode $V$ vocabs using Quaternion representations with an embedding size $E \ll H$. Then, we apply a Quaternion transformation to transform $E$ back to $H$, and concatenate all four parts of a Quaternion to form a regular Euclidean embedding. This leads to a total of $VE + EH/4$ parameters, compared to $VE + EH$ in ALBERT.

Attention Factorization (AF): If the input sequences have length $N$, the output of the multi-head attention is $N \times N$, which does not depend on the hidden size $H$. Hence, it is unnecessary to produce the attention Query, Key, and Value with the same input hidden size $H$ and cost $3H^2$ parameters per a layer. Instead, we produce the attention Query, Key, and Value in size $C \ll H$ using linear Quaternion transformations, leading to $3CH/4$ parameters.

Feedforward Factorization (FF): Instead of linearly transforming from $H$ to $4H$ (i.e. $4H^2$ parameters), we apply Quaternion transformations from $H$ to $I$, and from $I$ to $4H$, with $1 \ll H$ is an intermediate size. This leads to a total of $(HI/4 + IH)$ parameters.

Output Factorization (OF): We also apply
Quaternions transformations from 4H to I, then from I to H. This results in (HI + IH/4) parameters, compared to 4H² in BERT.

When we apply all the above compression techniques together, the total parameters are reduced to VE + EH/4 + L(3CH/4 + H² + 5HI/2). Particularly, with BERT-base settings of V=32k, H=768, L=12, if we set E=128, C=192, and I=128, the total of parameters is reduced from 110M to only 8.4M.

4.3 Pretraining tasks

Similar to BERT, we pre-train our HABERTOR with two unsupervised learning/language modeling tasks: (i) masked token prediction, and (ii) next sentence prediction. We describe some modifications that we made to the original BERT’s implementation as follows:

4.3.1 Masked token prediction task

BERT generates only one masked training instance for each input sequence. Instead, inspired by Liu et al. (2019), we generate τ training instances by randomly sampling with replacement masked positions τ times. We refer to τ as a masking factor. Intuitively, this helps the model to learn differently combined patterns of tokens in the same input sequence, and boosts the model’s language understanding. This small modification works especially well when we have a smaller pre-training data size, which is often true for a domain-specific task (e.g., hatespeech detection).

4.3.2 Next sentence prediction task

In BERT, the two input sentences are already paired and prepared in advanced. In our case, we have to preprocess input text sequences to prepare paired sentences for the next sentence prediction task. We conduct the following preprocessing steps:

**Step 1:** We train an unsupervised sentence tokenizer from nltk library. Then we use the trained sentence tokenizer to tokenize each input text sequence into (splitted) sentences.

**Step 2:** In BERT, 50% of the chance two consecutive sentences are paired as next, and 50% of the chance two non-consecutive sentences are paired as not next. In our case, our input text sequences can be broken into one, two, three, or more sentences. For input text sequences that consist of only one tokenized sentence, the only choice is to pair with another random sentence to generate a not next example. By following our 50-50 rule described in the Appendix, we ensure generating an equal number of next and not next examples.

4.4 Training the hatespeech prediction task

For hatespeech prediction task, we propose a multi-source multi-head HABERTOR classifier. The architecture comparison of the traditional fine-tuning BERT and our proposal is shown in Figure 1. We note two main differences in our design as follows.

First, as shown in Figure 1b, our HABERTOR has separated classification heads nets for different input sequences of different sources but with a shared language understanding knowledge. Intuitively, instead of measuring the same probabilities $P(y|s)$ for all input sequences, it injects additional prior source knowledge of the input sequences to measure $P(y|s, “news”) or P(y|s, “finance”).

Second, in addition to multi-source, HABERTOR with an ensemble of h heads provides even more capabilities to model data variance. For each input source, we employ ensemble of several classification heads (i.e. two classification heads for each source in the Figure 1b) and use a pooling layer on top to aggregate results from those classification heads. We use three pooling functions: min, max, mean. min pooling indicates that HABERTOR classifies an input comment as a hateful one if all of the heads classify it as hatespeech, which put a more
Thus, HABERTOR is more flexible than the conventional fine-tuning BERT. Also, HABERTOR is optimal, as different adversarial directions of different adversarial dimensions. Moreover, the running time of our proposal compared to FGM is similar.

The basic idea of the adversarial training is to add a small perturbation noise $\delta$ on each of the token embeddings that makes the model misclassify hateful comments as normal comments, and vice versa. Given the input sequence $s_i = [w_1^{(i)}, w_2^{(i)}, ..., w_u^{(i)}]$ with ground truth label $y_i$, let $\hat{y}_i$ be the adversarial target class of $s_i$ such that $\hat{y}_i \neq y_i$. In the hatespeech detection domain, our model is a binary classifier. Hence, when $y_i = 1$ ($s_i$ is a hateful comment), $\hat{y}_i = 0$ and vice versa. Then, the perturbation noise $\delta$ is learned by minimizing the following cost function:

$$
\mathcal{L}_{adv} = \arg\min_{\delta, \delta \in [a, b]} - \sum_{i=1}^{S} \log P(\hat{y}_i | s_i + \delta; \hat{\theta}) \tag{1}
$$

Note that in Eq. (1), $\delta$ is constrained to be less than a predefined noise magnitude scalar in the traditional FGM method. In our proposal, $\delta$ is constrained within a range $[a, b]$ (i.e. $\min(\delta) \geq a \land \max(\delta) \leq b$). Solving Eq. (1) is expensive and not easy, especially with complicated deep neural networks. Thus, we approximate each perturbation noise $\delta_i$ for each input sequence $s_i$ by linearizing partial loss $-\log P(\hat{y}_i | s_i + \delta; \hat{\theta})$ around $s_i$. Particularly, $\delta_i$ is measured by:

$$
\delta_i = -\epsilon \times \frac{\nabla s_i (\log P(\hat{y}_i | s_i; \hat{\theta}))}{\| \nabla s_i (\log P(\hat{y}_i | s_i; \hat{\theta})) \|_2} \tag{2}
$$

In Eq. (2), $\epsilon$ is a learnable vector, with the same dimensional size as $\delta_i$. Solving the constraint $\delta_i \in [a, b]$ in Eq. (1) becomes restricting $\epsilon \in [a, b]$, which is trivial by projecting $\epsilon$ in $[a, b]$.

Finally, HABERTOR aims to minimize the following cost function:

$$
\mathcal{L} = \mathcal{L}_{hs} + \lambda_{adv}\mathcal{L}_{adv} - \lambda_c \| \epsilon \|_2, \tag{3}
$$

where $\| \epsilon \|_2$ is an additional term to force the model to learn robustly as much as possible, and $\lambda_c$ is a hyper-parameter to balance its effect. Note that, we first learn the optimal values of all token embeddings and HABERTOR’s parameters before learning adversarial noise $\delta$. Also, regularizing adversarial training only increases the training time, but not the inferencing time since it does not introduce extra parameters for the model during the inference.

4.5 Parameter Estimation

Estimating parameters in the pretraining tasks in our model is similar to BERT, and we leave the details in the Appendix due to space limitation.

For hatespeech prediction task, we use the transformed embedding vector of the [CLS] token as a summarized embedding vector for the whole input sequence. Let $S$ be a collection of sequences $s_i$. Note that $s_i$ is a normal sequence, not corrupted or concatenated with another input sequence. Given that $y_i$ is the supervised ground truth label for the input sequence, and $\hat{y}_i = P(y_i | s_i, “news”)$(Figure 1b, 1b) where $s_i$ is a news input sequence, or $\hat{y}_i = P(y_i | s_i, “finance”)$, or $\hat{y}_i$ is a finance input sequence. The hateful prediction task aims to minimize the following binary cross entropy loss:

$$
\mathcal{L}_{hs} = \arg\min_{\hat{\theta}} - \sum_{i=1}^{S} y_i \log (\hat{y}_i) + (1 - y_i) \log (1 - \hat{y}_i)
$$

Regulate with adversarial training: To make our model more robust to perturbations of the input embeddings, we further regularize our model with adversarial training. There exist several state-of-the-art target-based adversarial attacks such as Fast Gradient Method (FGM) (Miyato et al., 2017), Basic Iterative Method (Kurakin et al., 2016), and Carlini L2 attack (Carlini and Wagner, 2017). We use the FGM method as it is effective and efficient according to our experiments.

In FGM, the noise magnitude is a scalar value and is a manual input hyper-parameter. This is sub-optimal, as different adversarial directions of different dimensions are scaled similarly, plus, manually tuning the noise magnitude is expensive and not optimal. Hence, we propose to extend FGM with a learnable and fine-grained noise magnitude, where the noise magnitude is parameterized by a learnable vector, providing different scales for different adversarial dimensions. Moreover, the running time of our proposal compared to FGM is similar.
Table 1: Statistics of the three datasets.

<table>
<thead>
<tr>
<th>Statistics/Datasets</th>
<th>Yahoo</th>
<th>Twitter</th>
<th>Wiki</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>1.4M</td>
<td>16K</td>
<td>115K</td>
</tr>
<tr>
<td># Hateful</td>
<td>100K</td>
<td>5K</td>
<td>13K</td>
</tr>
<tr>
<td>% of hate speech</td>
<td>7%</td>
<td>31%</td>
<td>12%</td>
</tr>
</tbody>
</table>

5 Empirical Study

5.1 Experiment Setting

Dataset: Our primary dataset was extracted from user comments on Yahoo News and Finance for five years, and consisted of 1,429,138 labeled comments. Among them, 944,391 comments are from Yahoo News and 484,747 comments are from Yahoo Finance. There are 100,652 hateful comments. The 1.4M labeled data was collected as follows (Nobata et al., 2016): comments that are reported as “abusive” for any reason by users of Yahoo News and Finance are sent to in-house trained raters for review and labeling.

To further validate the generalizability of HABERTOR, we perform transfer-learning experiments on other two publicly available hatespeech datasets: Twitter (Waseem and Hovy, 2016), and Wikipedia (i.e., Wiki) (Wulczyn et al., 2017). The Twitter dataset consists of 16K annotated tweets, including 5,054 hateful tweets (i.e., 31%). The Wiki dataset has 115K labeled discussion comments from English Wikipedia talk’s page, including 13,590 hateful comments (i.e., 12%). The statistics of 3 datasets are shown in Table 1.

Train/Dev/Test split: We split the dataset into train/dev/test sets with a ratio 70%/10%/20%. We tune hyper-parameters on the dev set, and report final results on the test set. Considering critical mistakes reported at Arango et al. (2019) when building machine learning models (i.e., extracting features using the entire dataset, including testing data, etc.), we generate vocabs, pre-train the two language modeling tasks, and train the hatespeech prediction task using only the training set.

Baselines, our Models and hyper-parameter Settings: We compare our models with 15 state-of-the-art baselines: Bag of Words (BOW) (Dinakar et al., 2011; Van Hee et al., 2015), NGRAM, CNN (Kim, 2014), VDCNN (Conneau et al., 2017), FastText (Joulin et al., 2016), LSTM (Cho et al., 2014), att-LSTM, RCNN (Lai et al., 2015), att-BiLSTM (Lin et al., 2017), Fermi (best hate-speech detection method as reported in Basile et al. (2019)) (Indurthi et al., 2019), Q-Transformer (Tay et al., 2019), Tiny-BERT (Jiao et al., 2019), DistilBERT-base (Sanh et al., 2019), ALBERT-base (Lan et al., 2020), and BERT-base (Devlin et al., 2019; Nikolov and Radivchev, 2019). We are aware of other recent language models such as Transformer-XL (Dai et al., 2019), RoBERTa (Liu et al., 2019), DialoGPT (Zhang et al., 2020), to name a few. However, as these models are even heavier than BERT-base, we do not compare with them. The detailed description of the baselines and hyper-parameter settings is described in the Appendix.

Our models: We denote HABERTOR as our model without using any factorization, HABERTOR-VQF as HABERTOR + Vocab Quaternion Factorization, HABERTOR-VAQF as HABERTOR + Vocab + Attention Quaternion Factorization, HABERTOR-VAFOQF as HABERTOR + Vocab + Attention + Feedforward Quaternion Factorization, and HABERTOR-VAFOQF as HABERTOR + Vocab + Attention + Feedforward + Output Quaternion Factorization.

Measurement: We evaluate models on seven metrics: Area Under the Curve (AUC), Average Precision (AP), False Positive Rate (FPR), False Negative Rate (FNR), F1 score\(^4\). In real world, for imbalanced datasets, we care more about FPR and FNR. Thus, we report FPR at 5% of FNR (FPR@5%FNR), meaning we allow 5% of hateful texts to be misclassified as normal ones, then report FPR at that point. Similarly, we report FNR at 5% of FPR (FNR@5%FPR). Except for AUC and AP, the other metrics are reported using an optimal threshold selected by using the development set.

Model size comparison: HABERTOR has 26M of parameters. HABERTOR-VQF and HABERTOR-VAQF have 16.2M and 13.4M of parameters, respectively. HABERTOR-VAFOQF has 10.3M and 7.1M of parameters, respectively. The size of all five models is much

---

\(^4\)Both AP and F1 account for Precision and Recall so we do not further report Precision and Recall for saving space.
smaller than BERT-base (i.e., 110M of parameters). The configuration comparison of HABERTOR-VAFOQF and other pretrained language models is given in Table 2. HABERTOR-VAQFQ has less than 2 times compared to TinyBERT’s parameters, less than 9 times compared to Distil-BERT’s size, and is equal to 0.59 ALBERT’s size.

5.2 Experimental results

5.2.1 Performance comparison

Table 3 shows the performance of all models on Yahoo dataset. Note that we train on the Yahoo training set that contains both Yahoo News and Finance data, and report results on Yahoo News and Finance separately, and report only AUC and AP on both of them (denoted as column “Yahoo” in Table 3). We see that Fermi worked worst among all models. It is mainly because Fermi transfers the pre-trained embeddings from the USE model to a SVM classifier without further fine-tuning. This limits Fermi’s ability to understand domain-specific contexts. Q-Transformer works the best among non-LM baselines, but worse than LM baselines as it is not pretrained. BERT-base performed the best among all baselines. Also, distilled models worked worse than BERT-base due to their compression nature on BERT-base as the teacher model.

Next, we compare the performance of our proposed models against each other. Table 3 shows that our models’ performance is decreasing when we compress more components (p-value < 0.05 un-
Table 4: Generalizability of HABERTOR and top baselines. Report AUC, AP, and F1 on each test set.

<table>
<thead>
<tr>
<th>Model</th>
<th>Twitter AUC</th>
<th>Twitter AP</th>
<th>Twitter F1</th>
<th>Wiki AUC</th>
<th>Wiki AP</th>
<th>Wiki F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fermi</td>
<td>89.03</td>
<td>79.23</td>
<td>74.52</td>
<td>96.59</td>
<td>84.26</td>
<td>75.51</td>
</tr>
<tr>
<td>TinyBERT</td>
<td>92.23</td>
<td>83.88</td>
<td>78.33</td>
<td>97.10</td>
<td>87.64</td>
<td>79.70</td>
</tr>
<tr>
<td>DistBERT</td>
<td>92.13</td>
<td>80.21</td>
<td>77.89</td>
<td>97.23</td>
<td>88.16</td>
<td>80.21</td>
</tr>
<tr>
<td>ALBERT</td>
<td>92.55</td>
<td>86.51</td>
<td>78.76</td>
<td>97.66</td>
<td>89.91</td>
<td>80.66</td>
</tr>
<tr>
<td>BERT</td>
<td>93.21</td>
<td>86.76</td>
<td>79.68</td>
<td>97.75</td>
<td>89.23</td>
<td>80.73</td>
</tr>
<tr>
<td>HABERTOR</td>
<td>93.52</td>
<td>88.57</td>
<td>81.22</td>
<td>97.46</td>
<td>88.65</td>
<td>80.81</td>
</tr>
<tr>
<td>HABERTOR-VQF</td>
<td>93.94</td>
<td>88.45</td>
<td>81.21</td>
<td>97.40</td>
<td>88.64</td>
<td>80.66</td>
</tr>
<tr>
<td>HABERTOR-VAFQF</td>
<td>93.57</td>
<td>87.66</td>
<td>80.23</td>
<td>97.45</td>
<td>88.61</td>
<td>80.63</td>
</tr>
<tr>
<td>HABERTOR-VAFQFQF</td>
<td>93.51</td>
<td>87.38</td>
<td>80.16</td>
<td>97.37</td>
<td>88.21</td>
<td>80.23</td>
</tr>
<tr>
<td>HABERTOR-VAFQF</td>
<td>93.49</td>
<td>87.14</td>
<td>80.06</td>
<td>97.23</td>
<td>87.94</td>
<td>79.61</td>
</tr>
</tbody>
</table>

number of layers as BERT-base, leading to a similar computational expense as BERT-base.

Our HABERTOR-VQF and HABERTOR-VAFQF have a very similar parameter size with TinyBERT and their train/inference time are similar. Interestingly, even though HABERTOR has 26M of parameters, its runtime is also competitive with TinyBERT. This is because among 26M of parameters in HABERTOR, 15.4M of its total parameters are for encoding 40k vocabs, which are not computational parameters and are only updated sparsely during training. HABERTOR-VAFQF and HABERTOR-VAFQFQF significantly reduce the number of parameters compared to TinyBERT, leading to a speedup during training and inference phases. Especially, our experiments on 4 K80 GPUs with a batch size of 128 shows that HABERTOR-VAFQFQF is 2.1 times faster than TinyBERT.

Memory consumption: Our experiments with a batch size of 128 on 4 K80 GPUs show that among LM baselines, TinyBERT and ALBERT are the most lightweight models, consuming 13GB of GPU memory. Compared to TinyBERT and ALBERT, HABERTOR takes an additional 4GB of GPU memory, while HABERTOR-VQF, HABERTOR-VAFQF hold a similar memory consumption, HABERTOR-VAFQF and HABERTOR-VAFQFQF reduces 1~3 GB of GPU memory.

Compared to BERT-base: In general, HABERTOR is 4~5 times faster, and 3.1 times GPU memory usage smaller than BERT-base. Our most lightweight model HABERTOR-VAFQFQF even reduces 3.6 times GPU memory usage, while remains as effective as BERT-base. The memory saving in our models also indicates that we could increase the batch size to perform inference even faster.

5.2.3 Generalizability analysis

We perform hatespeech Language Model transfer learning on other hateful Twitter and Wiki datasets to understand our models’ generalizability. We use our models’ pre-trained language model checkpoint learned from Yahoo hateful datasets, and fine tune them on Twitter/Wiki datasets. Note that the fine-tuned training also includes regularized adversarial training for best performance. Next, we compare the performance of our models with Fermi and four LM baselines – best baselines reported in Table 3.

Table 4 shows that BERT-base performed best compared to other fine-tuned LMs, which is consistent with our reported results on Yahoo datasets in Table 3. When comparing with BERT-base’s performance (i.e. best baseline) on the Twitter dataset, all our models outperformed BERT-base. On Wiki dataset, interestingly, our models work very competitively with BERT-base, and achieve similar F1-score results. Recall that BERT-base has a major advantage of pre-training on 2,500M Wiki words, thus potentially understands Wiki language styles and contexts better. In contrast, HABERTOR and its four factorized versions are pre-trained on 33M words from Yahoo hatespeech dataset. As shown in the ablation study (refer to AS2 in Section A.6 of the Appendix), a larger pre-training data size leads to better language understanding and a higher hatespeech prediction performance. Hence, if we acquire larger pre-training data with more hateful representatives, our model’s performance can be further boosted. All of those results show that our models generalize well on other hatespeech datasets compared with BERT-base, with significant model complexity reduction.

5.2.4 Ablation study

Effectiveness of the adversarial attacking method FGM with our proposed fine-grained and adaptive noise magnitude: To show the effectiveness of the FGM attacking method with our proposed fine-grained and adaptive noise magnitude, we
We conduct several ablation studies to understand HABERTOR’s sensitivity. Due to space limitation, we summarize the key findings as follows, and leave detailed information and additional study results in the Appendix:

(i) A large masking factor in HABERTOR is helpful to improve its performance; (ii) Pretraining with a larger hatespeech dataset or a more fine-grained pretraining can improve the hatespeech prediction performance; and (iii) Our fine-tuning architecture with multi-source and ensemble of classification heads helps improve the performance.

5.2.5 Further application discussion

Our proposals were designed for the hatespeech detection task, but in an extent, they can be applied for other text classification tasks. To illustrate the point, we experiment our models (i.e. all our pretraining and fine-tuning designs) on a sentiment classification task using Amazon Prime Pantry reviews. Particularly, we used 471k Amazon-Prime-Pantry reviews (McAuley et al., 2015), which is selected due to its reasonable size for fast pretraining, fine-tuning and result attainment. After some preprocessings (i.e. duplicated reviews removal, convert the reviews with rating scores $\geq 4$ as positive, rating $\leq 2$ as negative, and no neutral class for easy illustration), we obtained 301k reviews and split into 210k-training/30k-development/60k-testing with a ratio 70/10/20. Next, we pretrained our models on 210k training reviews which contain 5.06M of words. Then, we fine-tuned our models on the 210k training reviews, selected a classification threshold on the 30k development reviews, and report AUC, AP, and F1 on the 60k testing reviews. We compare the performance of our models with fine-tuned BERT-base and ALBERT-base – two best baselines. We observe that though pretraining on only 5.06M words of 210k training reviews, HABERTOR performs very similarly to BERT-base, while improving over ALBERT-base. Except HABERTOR-VAFQF with a little bit smaller F1-score compared to ALBERT-base, our other three compressed models worked better than ALBERT-base, showing the effectiveness of our proposals.

6 Conclusion

In this paper, we presented the HABERTOR model for detecting hatespeech. HABERTOR understands the language of the hatespeech datasets better, is 4-5 times faster, uses less than 1/3 of the memory, and has a better performance in hatespeech classification. Overall, HABERTOR outperforms 15 state-of-the-art hatespeech classifiers and generalizes well to unseen hatespeech datasets, verifying not only its efficiency but also its effectiveness.

ACKNOWLEDGMENTS

This work was supported in part by NSF grant CNS-1755536.
References


Aymé Arango, Jorge Pérez, and Barbara Poblete. 2019. Hate speech detection is not as easy as you may think: A closer look at model validation. In SIGIR, pages 45–54.


Thomas Davidson, Dana Warmsley, Michael Macy, and Ingrid Weber. 2017. Automated hate speech detection and the problem of offensive language. In ICWSM.


Karthik Dinakar, Roi Reichart, and Henry Lieberman. 2011. Modeling the detection of textual cyberbullying. In ICWSM.


Mai ElSherief, Shirin Nilizadeh, Dana Nguyen, Giovanni Vigna, and Elizabeth Belding. 2018b. Peer to peer hate: Hate speech instigators and their targets. In ICWSM.


Tommi Gröndahl, Luca Pajola, Mika Juuti, Mauro Conti, and N Asokan. 2018. All you need is: Evading hate speech detection. In AISEC, pages 2–12.


Chikashi Nobata, Joel Tetreault, Achint Thomas, Yashar Mehdad, and Yi Chang. 2016. Abusive language detection in online user content. In WWW.
