COLING

International Conference on Computational Linguistics

Proceedings of the Conference and Workshops
Copyright of each paper stays with the respective authors (or their employers).

ISSN 2951-2093
Introduction

As the number of users and their web-based interaction has increased, incidents of a verbal threats, aggression and related behaviour like trolling, cyberbullying, and hate speech have also increased manifold globally. The reach and extent of the Internet have given such incidents unprecedented power and influence to affect the lives of billions of people. Such incidents of online abuse have not only resulted in mental health and psychological issues for users, but they have manifested in other ways, spanning from deactivating social media accounts to instances of self-harm and suicide.

To mitigate these issues, researchers have begun to explore the use of computational methods for identifying such toxic interactions online. In particular, Natural Language Processing (NLP) and ML-based methods have shown great promise in dealing with such abusive behaviour through early detection of inflammatory content.

In fact, we have observed an explosion of NLP-based research on offensive content in the last few years. This growth has been accompanied by the creation of new venues such as the WOAH and the TRAC workshop series. Community-based competitions, like tasks 5/6 at SemEval-2019, task 12 at SemEval-2020, and task 5/7 at SemEval-2021 have also proven to be extremely popular. In fact, because of the huge community interest, multiple workshops are being held on the topic in a single year. For example, in 2018 ACL hosted both the Abusive Language Online workshop (EMNLP) as well as TRAC-1 (COLING). Both venues achieved healthy participation with 21 and 24 papers, respectively. Interest in the topic has continued to grow since then and given its immense popularity, we are proposing a new edition of the workshop to support the community and further research in this area.

As in the earlier editions, TRAC focuses on the applications of NLP, ML and pragmatic studies on aggression and impoliteness to tackle these issues. As such the workshop also includes shared tasks on ‘Aggression Identification. The task consisted of two sub-tasks - (1) Bias, Threat and Aggression Identification in Context and (2) Generalising across domains - COVID-19. For task 1, the participants were provided with a "thread" of comments with information about the presence of different kinds of biases and threats (viz. gender bias, gendered threat and none, etc) and its discursive relationship to the previous comment as well as the original post (viz. attack, abet, defend, counter-speech and gaslighting). In a series/thread of comments, participants were required to predict the presence of aggression and bias in each comment, possibly making use of the context. In this task, a total dataset of approximately 60k comments (approximately 180k annotation samples) in Meitei, Bangla and Hindi, compiled in the ComMA Project, were provided for training and testing.

Both the workshop and the shared task received a very encouraging response from the community. The proceedings include 4 oral, 3 posters, and 2 system description papers. In addition to this, the workshop also includes 1 Demo to be presented in the workshop.

We would like to thank all the authors for their submissions and members of the Program Committee for their invaluable efforts in reviewing and providing feedback to all the papers. We would also like to thank all the members of the Organising Committee who have helped immensely in various aspects of the organisation of the workshop and the shared task.

Workshop Chairs
Workshop Chairs

Ritesh Kumar, Dr. Bhimrao Ambedkar University, India  
Atul Kr. Ojha, University of Galway, Ireland & Panlingua Language Processing LLP, India  
Marcos Zampieri, George Mason University, USA  
Shervin Malmasi, Amazon Inc., USA  
Daniel Kadar, Research Institute for Linguistics, Hungarian Academy of Sciences, Hungary

Assistant Organisers

Siddharth Singh, Dr. Bhimrao Ambedkar University, India  
Shyam Ratan, Dr. Bhimrao Ambedkar University, India

Shared Task Organising Committee

Shervin Malmasi, Amazon Inc., USA  
Siddharth Singh, Dr. Bhimrao Ambedkar University, India  
Shyam Ratan, Dr. Bhimrao Ambedkar University, India  
Ritesh Kumar, Dr. Bhimrao Ambedkar University, India  
Atul Kr. Ojha, University of Galway, Ireland & Panlingua Language Processing LLP, India  
Bharathi Raja Chakravarthi, University of Galway

Programme Committee

Atul Kr. Ojha, University of Galway, Ireland & Panlingua Language Processing LLP, India  
Bharathi Raja Chakravarthi, University of Galway  
Bornini Lahiri, Indian Institute of Technology-Kharagpur, India  
Bruno Emanuel Martins, IST and INESC-ID  
Cheng-Te Li, National Cheng Kung University, Taiwan  
Chuan-Jie Lin, National Taiwan Ocean University, Taiwan  
David Jurgens, University of Michigan  
Denis Gordeev, The Russian Presidential Academy of National Economy and Public Administration under the President of the Russian Federation  
Dennis Tenen, Columbia University, USA  
Dhairya Dalal, University of Galway  
Els Lefever, LT3, Ghent University, Belgium  
Faneva Ramiandrisoa, IRIT  
Han Liu, Cardiff University  
Hugo Jair Escalante, INAOE, Mexico  
Koustava Goswami, University of Galway  
Liang-Chih Yu, Yuan Ze University, Taiwan  
Lun-Wei Ku, Academia Sinica, Taiwan  
Lütfiye Seda Mut Altın, Pompeu Fabra University Mainack Mondal, University of Chicago, USA  
Manuel Montes-y-Gómez, INAOE, Mexico  
Marco Guerini, Fondazione Bruno Kessler, Trento  
Ming-Feng Tsai, National Chengchi University, Taiwan  
Monojit Choudhury, Microsoft Turing  
Nemanja Djuric, Aurora Innovation  
Parth Patwa, Indian Institute of Information Technology, Sri City  
Preslav Nakov, Qatar Computing Research Institute, Qatar  
Priya Rani, University of Galway
Invited Speaker

Valerio Basile, University of Turin, Italy

Valerio Basile is an Assistant Professor at the Computer Science Department of the University of Turin, Italy, member of the Content-centered Computing group and the Hate Speech Monitoring lab. His work spans across several areas such as: formal representations of meaning, linguistic annotation, natural language generation, commonsense knowledge, semantic parsing, sentiment analysis, and hate speech detection, perspectives and bias in supervised machine learning, from data creation to system evaluation. He is currently PI of the project BREAKhateDOWN "Toxic Language Understanding in Online Communication", and among the main proponents of the Perspectivist Data Manifesto: https://pdai.info

Title: The Evaluation of Language Models for Undesirable Language Analysis

Abstract:

In the past five years, the field of Natural Language Processing has seen several important changes and paradigm shifts. Methodologically, large neural language models have taken the spotlight as the new state of the art for most classification (and other kinds of) tasks. At the same time, the focus of research has opened up more and more to the study of pragmatics phenomena in natural language. Among these, toxic, abusive, offensive language, hate speech, and other undesirable phenomena have been subject of the development of specialized models, language resources, and evaluation campaigns.

In this talk, he will give a partial overview of the design and the results of large-scale evaluation efforts, in a multilingual perspective. Quantitative results on such subjective and hard-to-define phenomena should not be taken at a face value. Rather, the quality of benchmarks, and the annotated data behind them, should be carefully analysed. Finally, he will briefly introduce the perspectivist framework and its potential impact on the evaluation of models for undesirable language analysis.

Panelists: Amitava Das (Wipro AI), Stavros Assimakopoulos (University of Malta), Pilar G. Blitvich (University of North Carolina) and Bertie Vidgen (The Alan Turing Institute)
# Table of Contents

**L3Cube-MahaHate: A Tweet-based Marathi Hate Speech Detection Dataset and BERT Models**  
Hrushikesh Patil, Abhishek Velankar and Raviraj Joshi .................................................. 1

**Which One Is More Toxic? Findings from Jigsaw Rate Severity of Toxic Comments**  
Millon Das, Punyajoy Saha and Mithun Das ................................................................. 10

**Can Attention-based Transformers Explain or Interpret Cyberbullying Detection?**  
Kanishk Verma, Tijana Milosevic and Brian Davis .......................................................... 16

**Bias, Threat and Aggression Identification Using Machine Learning Techniques on Multilingual Comments**  
Kirti Kumari, Shaurya Srivastav and Rajiv Ranjan Suman ............................................. 30

**The Role of Context in Detecting the Target of Hate Speech**  
Ilia Markov and Walter Daelemans .................................................................................. 37

**Annotating Targets of Toxic Language at the Span Level**  
Baran Barbarestani, Isa Maks and Piek Vossen ............................................................... 43

**Is More Data Better? Re-thinking the Importance of Efficiency in Abusive Language Detection with Transformers-Based Active Learning**  
Hannah Kirk, Bertie Vidgen and Scott Hale ......................................................................... 52

**A Lightweight Yet Robust Approach to Textual Anomaly Detection**  
Leslie Barrett, Robert Kingan, Alexandra Ortan and Madhavan Seshadri ......................... 62

**Detection of Negative Campaign in Israeli Municipal Elections**  
Marina Litvak, Natalia Vanetik, Sagiv Talker and Or Machlouf ........................................ 68

**Hypothesis Engineering for Zero-Shot Hate Speech Detection**  
Janis Goldzycher and Gerold Schneider ............................................................................ 75
Conference Program

Monday, October 17, 2022 (GMT+9)

09:00–09:15  Inaugural Session
Chair: Workshop Chairs

09:00–09:15  Welcome
Workshop Chairs

09:15–10:30  Q&A Session 1

09:15–09:30  L3Cube-MahaHate: A Tweet-based Marathi Hate Speech Detection Dataset and BERT Models
Hrushikesh Patil, Abhishek Velankar and Raviraj Joshi

09:30–09:45  Which One Is More Toxic? Findings from Jigsaw Rate Severity of Toxic Comments
Millon Das, Punyajoy Saha and Mithun Das

09:45–10:00  Can Attention-based Transformers Explain or Interpret Cyberbullying Detection?
Kanishk Verma, Tijana Milosevic and Brian Davis

10:00–10:15  Bias, Threat and Aggression Identification Using Machine Learning Techniques on Multilingual Comments
Kirti Kumari, Shaury Srivastav and Rajiv Ranjan Suman

10:15–10:30  The Role of Context in Detecting the Target of Hate Speech
Ilia Markov and Walter Daelemans

10:30–11:00  COFEE BREAK
Monday, October 17, 2022 (GMT+9) (continued)

11:00–12:30 Q&A Session 2

11:00–11:25  Annotating Targets of Toxic Language at the Span Level
Baran Barbarestani, Isa Maks and Piek Vossen

11:25–11:50  Is More Data Better? Re-thinking the Importance of Efficiency in Abusive Language Detection with Transformers-Based Active Learning
Hannah Kirk, Bertie Vidgen and Scott Hale

11:50–12:15  A Lightweight Yet Robust Approach to Textual Anomaly Detection
Leslie Barrett, Robert Kingan, Alexandra Ortan and Madhavan Seshadri

14:00–15:00 Keynote Talk

14:00–15:00  The Evaluation of Language Models for Undesirable Language Analysis
Valerio Basile, University of Turin

15:00–16:00  COFEE BREAK

16:00–17:00 Panel Discussion

16:00–17:00  The Role of Pragmatics in Offensive and Aggressive Language Identification Research
Amitava Das (Wipro AI), Stavros Assimakopoulos (University of Malta), Pilar G. Blitvich (University of North Carolina) and Bertie Vidgen (The Alan Turing Institute)
Monday, October 17, 2022 (GMT+9) (continued)

17:00–17:50  Q&A Session 3

17:00–17:25  Detection of Negative Campaign in Israeli Municipal Elections
Marina Litvak, Natalia Vanetik, Sagiv Talker and Or Machlouf

17:25–17:50  Hypothesis Engineering for Zero-Shot Hate Speech Detection
Janis Goldzycher and Gerold Schneider

17:50–18:00  Closing

17:50–18:00  Vote of Thanks
Workshop Chairs
L3Cube-MahaHate: A Tweet-based Marathi Hate Speech Detection Dataset and BERT models

Abhishek Velankar\textsuperscript{1,3}, Hrushikesh Patil\textsuperscript{1,3}, and Raviraj Joshi\textsuperscript{2,3}
\textsuperscript{1}Pune Institute of Computer Technology, Pune
\textsuperscript{2}Indian Institute of Technology Madras, Chennai
\textsuperscript{3}L3Cube, Pune
\{velankarabhishek,hrushi2900\}@gmail.com
ravirajoshi@gmail.com

Abstract

Social media platforms are used by a large number of people prominently to express their thoughts and opinions. However, these platforms have contributed to a substantial amount of hateful and abusive content as well. Therefore, it is important to curb the spread of hate speech on these platforms. In India, Marathi is one of the most popular languages used by a wide audience. In this work, we present L3Cube-MahaHate, the first major Hate Speech Dataset in Marathi. The dataset is curated from Twitter and annotated manually. Our dataset consists of over 25000 distinct tweets labeled into four major classes i.e hate, offensive, profane, and not. We present the approaches used for collecting and annotating the data and the challenges faced during the process. Finally, we present baseline classification results using deep learning models based on CNN, LSTM, and Transformers. We explore mono-lingual and multi-lingual variants of BERT like MahaBERT, IndicBERT, mBERT, and xlm-RoBERTa and show that mono-lingual models perform better than their multi-lingual counterparts. The MahaBERT model provides the best results on L3Cube-MahaHate Corpus. The data and models are available at https://github.com/l3cube-pune/MarathiNLP.

Keywords: Natural Language Processing, Convolutional Neural Networks, Long Short Term Memory, FastText, BERT, Hate Speech Detection.

1 Introduction

In the past decade, there has been an expeditious rise in the popularity of online social media platforms all over the globe. People have become more open to sharing their opinions without thinking excessively. This often leads to the spread of hate or offensive speech thereby causing violence and cyberbullying. Hate speech is a kind of abusive language directed towards a community that is underprivileged in terms of race, gender, ethnic origin, disability, etc., or can be an insult or threat to an individual (MacAvaney et al., 2019; Matamoros-Fernández and Farkas, 2021). The users often defy the boundaries of freedom of speech without even realizing it by posting harmful messages and comments (Waseem and Hovy, 2016). Therefore it is today’s need to neutralize these activities from proliferating further.

In this work, we consider hate speech detection in the Marathi language, a regional language in India, spoken by over 83 million people across the country (Joshi, 2022). Despite being one of the popular languages in India, work in the area of hate speech detection in Marathi is extremely limited (Mandl et al., 2021; Velankar et al., 2021; Glazkova et al., 2021; Bhatia et al., 2021) as compared to other languages (Del Vigna et al., 2017; Romim et al., 2021; Corazza et al., 2020; Schmidt and Wiegand, 2019). Even general text classification in Marathi has received limited attention (Kulkarni et al., 2022, 2021). In this paper, we present, L3Cube-MahaHate Corpus, the largest publicly available hate speech dataset in Marathi. The dataset is collected from Twitter, tagged with four fine-grained labels which are defined as follows-

Hate (HATE): A Twitter post abusing a specific group of people or community based on their religion, race, ethnic origin, gender, geographical location, etc. stimulating violent behaviors.
Offensive (OFFN): A tweet containing harmful language leading to insulting or dehumanizing, at times threatening a particular individual.

Profane (PRFN): A tweet including the use of typical swear words or profane, cursing language which is ordinarily insupportable.

Not (NOT): A post that does not contain any insulting or abusive content or profane words in the language used.

The dataset consists of over 25000 samples tagged manually with the classes explained above. We further provide an extensive study of the data collection approaches, different policies used, and challenges faced during the annotation process as well. We also provide the statistical analysis of our dataset along with the distribution of train, test, and validation data. Lastly, we perform multiple experiments to evaluate state-of-the-art deep learning models on the dataset and provide the baseline results to the community. All the resources will be publicly shared on Github.

The MahaBERT model fined-tuned on L3Cube-MahaHate is termed as MahaHateBERT and is shared publicly on model hub. All the resources are publicly shared on github.

2 Related Work

Hate speech detection is considered to be a highly critical problem and a lot of attempts have been made to control it. A significant amount of work can be seen in English text analysis. But recently, efforts have been made towards widening the research in regional languages like Marathi as well.

Gaikwad et al. (2021) presented the Marathi Offensive Language Dataset (MOLD), with nearly 2,500 annotated tweets labeled as offensive and not offensive. It is considered the first dataset for offensive language identification in Marathi. Also, they evaluated the performance of several traditional machine learning models and deep learning models (e.g. LSTM) trained on MOLD.

Bhardwaj et al. (2020) collected over 8200 hostile and non-hostile Hindi text samples from multiple social media platforms like Twitter, Facebook, WhatsApp. Hostile posts were further extended into fake, defamation, hate, and offensive. A total of 8192 posts were collected and tested on various machine learning models using mBERT encoding.

A Hindi-English code-mixed corpus was constructed in Bohra et al. (2018) using the tweets posted online for the duration of five years. Tweets were scrapped using Twitter python API by selecting certain hashtags and keywords from political events, public protests, riots, etc. After removing noisy samples a dataset of 4575 code-mixed tweets was created. The experiments were performed with SVM and Random Forest algorithms along with character and word N-gram features.

In Kulkarni et al. (2021) authors presented a dataset containing over 16000 Marathi tweets, manually tagged in three classes namely positive, negative and neutral. They also provided a policy for tagging sentences by their sentiment. Analysis was performed on CNN, BiLSTM, and BERT models.

Davidson et al. (2017) collected hate phrases identified by Hatebase.org and then used those phrases to collect English tweets from Twitter using Twitter API. The final set of 25k tweets was annotated by CrowdFlower workers with labels hate, offensive and neither. This dataset was then tested on Logistic Regression, Naive Bayes, Decision Trees, random forests, and linear SVMs.

In Geet D’Sa et al. (2021), the authors evaluated the effect of filtering the generated data used for Data Augmentation (DA). This demonstrates up to 7.3% and up to 25% of relative improvements on macro-averaged F1
on two widely used hate speech corpora.

Ajao et al. (2019) proposed a hypothesis that there exists a relation between fake messages or rumors and sentiments of the texts posted online. The experiments were performed on the standard Twitter fake news dataset and showed good improvement on the same.

Gao and Huang (2018) provided an annotated corpus of hate speech with the context information. This evaluates by using logistic regression and neural network models for hate speech detection around 3% and 4%, and it improves to 7% by combining these two models together.

Mathur et al. (2018) presented MIMCT to detect offensive (Hate or Abusive) Hinglish tweets from the proposed Hinglish Offensive Tweet dataset. Demonstrated the use of the multi-channel CNN-LSTM model for sentiment analysis.

3 Dataset Creation

3.1 Collection

We created the Hate Speech dataset using the tweets posted online by different users across the Maharashtra region considering the period of over the last 5 years. There are plenty of different python libraries available such as Twint⁴, GetOldTweets⁵, Snscrape⁶, etc. which can be used to collect Twitter posts. Twitter provides its own API as well. We used the Twint python library for scraping the tweets.

To obtain the hateful tweets, firstly, we created a list of over 150 bad words in Marathi which are predominantly used by online users to spread hostility. Some of these are typical swear words in Marathi and other offensive words. These words were in Marathi Devanagari script as we are not concerned about Roman or code-mixed text in this work. We will be publishing the final list on GitHub.

These words were used as a search query to obtain hate, offensive, and profane tweets. The majority of the tweets that we obtained are related to political and social issues. We also made a note of controversial events with their time frame happening in India in the last couple of years which particularly triggered violence on social media. To avoid bias towards certain words or phrases, we have limited the tweets for a particular search query to a number less than 150. Also, while collecting the tweets, we have not included any reference to the author of the tweet thereby eliminating the bias towards that author.

In our publicly available version of the dataset, we have kept all the hashtags, symbols, emojis, and URLs for anyone to experiment on. However, we have removed all of these while performing the baseline experiments. Furthermore, we will be removing the user mentions from the public dataset to maintain complete user anonymity.

3.2 Annotation

The entire dataset has been labelled manually by the 4 annotators considering four major classes viz. hate, offensive, profane, and not. All the annotators were native Marathi speakers and were fluent in reading and writing in Marathi. The annotation guidelines were set before the tagging exercise. The first 200 sentences were tagged together to further improve the consistency post which sentences were tagged in parallel except for ambiguous sentences. The tweets which were targeted at a single individual thereby criticizing or dehumanizing the individual are tagged as offensive. These tweets were mainly attributed to an individual politician, celebrity, or any random person with the use of singular phrases. These tweets which were targeted at a group of people describing the deficiencies towards race, political opinion, sexual orientation, gender, etc. are tagged as hate. These tweets were majorly concentrated towards political parties or the ruling government. Also, a few samples belong to negative comments on minority groups and gender bias. The tweets which contain swear or profane words are strictly tagged as profane,

⁴https://pypi.org/project/twint/
⁵https://pypi.org/project/GetOldTweets3/
⁶https://github.com/JustAnotherArchivist/snscrape
even if they describe the offensive or hateful category. The tweets that do not satisfy any of the above criteria are simply tagged as NOT. Congratulatory and thanking tweets are tagged as NOT as well. Some sample tweets for the above classes are given in Table 3.

In some cases, the intention of the user behind a tweet cannot be suitably identified. In such cases, the tweets were reviewed again and voting among 4 annotators was used to decide on the labels. Also, we encountered a few tweets where hateful comments were quoted by a news handle. As these posts may indirectly promote violence, we tagged them in the hateful category. To collect the NOT tweets, we selected many Marathi Twitter handles and scraped their tweets, which gave us unbiased data.

![Figure 1: Average characters and words per label](image1)

![Figure 2: Distribution of the length of a tweet](image2)

### 3.3 Dataset Details

Initially, we collected over 40k tweets in Marathi. Among these, we annotated ∼28000 samples. After removing over 3k noisy tweets which particularly included poorly written text i.e. the text with the use of regional words which are not commonly spoken in Marathi or a large number of grammatical mistakes, we randomly selected 6250 samples from each of the 4 classes giving the total count of 25000 tweets. Although this uniform distribution of tweets does not represent the true distribution it makes the model building easier and does not require imbalance handling. We analyzed a few statistics on the dataset. The average number of words per tweet in an entire dataset is 21 and the average number of characters is 113. The label-wise distribution is given in Figure 1. The length of samples varies in the range of 2 to 93. The distribution of the length of tweets and the number of characters per tweet is given in Figures 2 and 3 respectively. The dataset can be used for binary classification as well. To match the number of hateful samples viz. Hate, Offensive, Profane all included, we collected over 12500 extra NOT samples apart from that of 4-class corpus giving an equal distribution of 18750 samples in hateful and non-hateful categories. This binary corpus of 37.5k will also be provided along with the original dataset. The binary dataset is distributed into train, test and validation sets in the ratio of 80:10:10 percent of the total dataset. Table 1 shows the 4-class dataset distribution in training, testing and validation samples.

![Figure 3: Distribution of the number of characters in a tweet](image3)
<table>
<thead>
<tr>
<th>Split</th>
<th>HATE</th>
<th>OFFN</th>
<th>PRFN</th>
<th>NOT</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Train</td>
<td>5375</td>
<td>5375</td>
<td>5375</td>
<td>5375</td>
<td>21500</td>
</tr>
<tr>
<td>Test</td>
<td>500</td>
<td>500</td>
<td>500</td>
<td>500</td>
<td>2000</td>
</tr>
<tr>
<td>Validation</td>
<td>375</td>
<td>375</td>
<td>375</td>
<td>375</td>
<td>1500</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model</th>
<th>Variant</th>
<th>2-Class Accuracy</th>
<th>4-Class Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNN</td>
<td>Random</td>
<td>0.880</td>
<td>0.703</td>
</tr>
<tr>
<td></td>
<td>Trainable</td>
<td>0.866</td>
<td>0.710</td>
</tr>
<tr>
<td></td>
<td>Non-Trainable</td>
<td>0.870</td>
<td><strong>0.751</strong></td>
</tr>
<tr>
<td>LSTM</td>
<td>Random</td>
<td>0.857</td>
<td>0.681</td>
</tr>
<tr>
<td></td>
<td>Trainable</td>
<td>0.860</td>
<td>0.691</td>
</tr>
<tr>
<td></td>
<td>Non-Trainable</td>
<td><strong>0.869</strong></td>
<td><strong>0.751</strong></td>
</tr>
<tr>
<td>BiLSTM</td>
<td>Random</td>
<td>0.858</td>
<td>0.699</td>
</tr>
<tr>
<td></td>
<td>Trainable</td>
<td>0.860</td>
<td>0.664</td>
</tr>
<tr>
<td></td>
<td>Non-Trainable</td>
<td><strong>0.870</strong></td>
<td><strong>0.761</strong></td>
</tr>
<tr>
<td>BERT</td>
<td>IndicBERT</td>
<td>0.865</td>
<td>0.711</td>
</tr>
<tr>
<td></td>
<td>mBERT</td>
<td>0.903</td>
<td>0.783</td>
</tr>
<tr>
<td></td>
<td>xlm-RoBERTa</td>
<td>0.894</td>
<td>0.787</td>
</tr>
<tr>
<td></td>
<td>MahaALBERT</td>
<td>0.883</td>
<td>0.764</td>
</tr>
<tr>
<td></td>
<td>MahaBERT</td>
<td><strong>0.909</strong></td>
<td><strong>0.803</strong></td>
</tr>
<tr>
<td></td>
<td>MahaRoBERTa</td>
<td>0.902</td>
<td>0.803</td>
</tr>
</tbody>
</table>

Table 1: Dataset label distribution

Table 2: Classification results on different architectures

![Confusion Matrices](image)

4 Experiments

4.1 Model architectures

We have used multiple state-of-the-art deep learning architectures (Velankar et al., 2021), (Joshi et al., 2021), (Joshi et al., 2019) to obtain the baseline results on 2-class as well as 4-class classification. Before training the models, we have cleaned the data by removing unwanted symbols, user mentions, hashtags. Following algorithms are used for the evaluation of results:

- **CNN**: The CNN model has a 1D convolution layer with a filter of size 300 and a kernel of size 3. It used ReLU activation, followed by max-pooling with pool size 2. The same layers were added again which is
followed by a dense layer of size 50 and ReLU activation. Lastly, the layer with softmax activation and 2 nodes was used. A dropout of 0.3 was used after the 1D max-pooling layer.

**LSTM**: The LSTM layer with 32 nodes was used. It was followed by a 1D global max-pooling. The dense layer with 16 nodes along with ReLU activation was used, followed by 0.2 dropout. A dense layer with 2 nodes and softmax activation was used as a final layer of the model.

**BiLSTM**: Bi-LSTM layer with 300 nodes followed by a 1D global max-pooling layer was used. The dense layer was used with 100 nodes and ReLU activation was used with it. This was followed by a dropout of 0.2. At last, the final layer with 2 nodes with activation softmax was used.

**BERT**: BERT is a bi-directional transformer-based model (Devlin et al., 2019) pre-trained over large textual data to learn language representations. It can be fine-tuned for specific machine learning tasks. We used the following variations of BERT to obtain baseline results:

- Multilingual-BERT (mBERT) - trained on and usable with 104 languages with Wikipedia using a masked language modeling (MLM) objective (Devlin et al., 2018).
- IndicBERT - a multilingual ALBERT model released by Ai4Bharat, trained on large-scale corpora (Kakwani et al., 2020), covering 12 major Indian languages: Assamese, Bengali, English, Gujarati, Hindi, Kannada, Malayalam, Marathi, Oriya, Punjabi, Tamil, Telugu.
- XLM-RoBERTa - a multilingual version of RoBERTa (Conneau et al., 2019). It is pre-trained on 2.5TB of filtered CommonCrawl data containing 100 languages with the Masked language modeling (MLM) objective and can be used for downstream tasks.
- MahaBERT - a multilingual BERT model (Joshi, 2022) fine-tuned on L3Cube-MahaCorpus and other publicly available Marathi monolingual datasets containing a total of 752M tokens.

### 4.2 Results

We performed our experiments on CNN, LSTM, and Transformer based models. For CNN and LSTM models, we have used random and fast text initialization for the word embeddings. The pre-trained embeddings were used in both trainable and non-trainable modes. The former means it was used by letting the embedding layer adapt to the training data and the latter by preventing it from being updated during training. Additionally, we used pre-trained language models, particularly the variations of BERT such as IndicBERT, Multilingual BERT, XLM-RoBERTa, and a few custom BERT models to obtain the results. All the 2-class and 4-class accuracies are displayed in Table 2.

In CNN and LSTM based models, non-trainable fast text mode is outperforming other configurations in both the binary and 4-class results. All the monolingual Marathi BERT models are surpassing the multilingual versions of BERT models such as IndicBERT, mBERT, and xlm-RoBERTa. It was observed that the non-trainable fast text setting for CNN and LSTM based models is performing competitively with the BERT models even surpassing the indicBERT for both classes. The MahaBERT model gives the best binary classification results whereas MahaRoBERTa gives the best 4-class accuracy. The confusion matrices for respective best results are shown in figures 4a and 4b.

### 5 Conclusion

In this paper, we have presented L3Cube-MahaHate - a hate speech dataset containing 25000 distinct samples equally distributed in 4 classes. This is the first major dataset in the domain of hate speech. We also provide the binary version of the dataset of over 37500 samples. We further perform experiments to obtain baseline results on various deep learning models like CNN, LSTM, BiLSTM, and transformer-based BERT models such as IndicBERT,
<table>
<thead>
<tr>
<th>S.No.</th>
<th>Tweet</th>
<th>English Translation</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>अशा प्रकारे खोडसाळ बातम्या देणायचे म्हणजेच वृत्तसंस्थाना जोडले जाही.</td>
<td>In this way, the news agencies which spread vicious news should be beaten up by the pair of shoes.</td>
<td>HATE</td>
</tr>
<tr>
<td>2</td>
<td>स्वाभाविक भूमिका काशी भरत आहे. यांना सामान्य जनता मेलीत तरीही काही फरक पडत नाही. स्वाधीन राजकरणे नीच वृत्ती द्वारा लोकांची.</td>
<td>They are filling their own pockets. Even if the general public dies, it makes no difference to them. Selfish politics, and the mischievous attitude of these people.</td>
<td>HATE</td>
</tr>
<tr>
<td>3</td>
<td>काहीही माहिती नसल्याने दुसऱ्यांनी नालायक म्हणजेच तुझी खुप खुप शिक्षण झालेले आहे असं वाटते. मुझ्यांनी सर्वांनी ताज घालत जाऊके.</td>
<td>Calling others incompetent when you don’t know anything means you seem to have a lot of education. Idiot, don’t put your mouth everywhere, stupid.</td>
<td>OFFN</td>
</tr>
<tr>
<td>4</td>
<td>तुझी लायक वाढणाऱ्या तो बोलतो कोणा बदल काय लाज लजा आहे की नाही.</td>
<td>What are your qualifications? Who are you talking about? Do you have any shame or not?</td>
<td>OFFN</td>
</tr>
<tr>
<td>5</td>
<td>या मळला वेळी आपण नायकत पहाण भोगपलला तयार राहा.</td>
<td>Restrain this m***ker on time, otherwise be prepared to suffer the consequences.</td>
<td>PRFN</td>
</tr>
<tr>
<td>6</td>
<td>लोकांचे सर्वसत बुऱ्यांची काही हंसी घासून ठाकी आणि सर्वांनी जिल्हे परिषद शासनात शिकवा.</td>
<td>You make people moron like that.. Remove all reservations and teach everyone in Zilla Parishad schools..</td>
<td>PRFN</td>
</tr>
<tr>
<td>7</td>
<td>सरकारला आता उत्तर देते लागेल, सामान्य जनतेचा विचार करता लागेल आता.</td>
<td>The government has to answer now, need to think now of the general public.</td>
<td>NOT</td>
</tr>
<tr>
<td>8</td>
<td>तुमचां प्रेम आणि आशीर्वाद मायूसांच्या वाटचाल व्यवस्थित सुवाच आहे. अशीच साध कार्य मुळं घुंणून आहे. त्याल्याच मला मार्शल साहेबांच्या प्र्यात्म प्रेमते, त्यांच्या प्रेमान्धारी मोबल सांगाच्या बल मिळून.</td>
<td>Thanks to your love and blessings, my journey is going smoothly. Always keep up this support. It gives me strength to tell the questions of the people of the soil, their inspiring stories.</td>
<td>NOT</td>
</tr>
</tbody>
</table>
mBERT and RoBERTa. The dataset is also evaluated on monolingual Marathi BERT models like MahaBERT, MahaALBERT, and MahaRoBERTa. For CNN and LSTM based models, the non-trainable fast text mode outperforms its trainable counterpart in both binary and 4-class classification. In transformer-based models, MahaBERT and MahaRoBERTa give the best results in binary and 4-class classification respectively.

Acknowledgements

This work was done under the L3Cube Pune mentorship program. We would like to express our gratitude towards our mentors at L3Cube for their continuous support and encouragement.

References


Fabio Del Vigna, Andrea Cimmino, Felice Dell’Orletta, Marinella Petrocchi, and Maurizio Tesconi. 2017. Hate me, hate me not: Hate speech detection on facebook. In *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17)*, pages 86–95.


Lei Gao and Ruihong Huang. 2018. Detecting online hate speech using context aware models.


Which one is more toxic? Findings from Jigsaw Rate Severity of Toxic Comments

Millon Madhur Das, Punyajoy Saha, Mithun Das
Indian Institute of Technology, Kharagpur, India
millonmadhurdas@kgpian.iitkgp.ac.in, {punyajoys, mithundas}@iitkgp.ac.in

Abstract
The proliferation of online hate speech has necessitated the creation of algorithms which can detect toxicity. Most of the past research focuses on this detection as a classification task, but assigning an absolute toxicity label is often tricky. Hence, few of the past works transform the same task into a regression. This paper shows the comparative evaluation of different transformers and traditional machine learning models on a recently released toxicity severity measurement dataset by Jigsaw. We further demonstrate the issues with the model predictions using explainability analysis.

Note: This paper contains examples of toxic posts. But owing to the nature of work, we cannot avoid them.

1 Introduction
In social media, toxic language denotes a text containing inappropriate language in a post or a comment. The presence of toxic language on social media hampers the fabric of communication in the social media posts; e.g., toxic posts targeting some community might silence members of the community (Das et al., 2020). Subsequently, social media platforms like Facebook (Facebook, 2022) and Twitter (Twitter, 2022) have laid down moderation guidelines. They also employ various automatic and manual detection techniques to detect such forms of language and apply appropriate moderation (Schroepfer, 2021). Henceforth, researchers have started looking into this direction (Das et al., 2021b; Banerjee et al., 2021; Das et al., 2021a). Most of the past research focused on developing a classification task which again varies based on the classification labels the researchers choose, i.e., abusive/non-abusive, hate speech/offensive/normal, troll/non-troll etc. (Nobata et al., 2016; Mathew et al., 2021; Saha et al., 2021; Das et al., 2022a,b) This variation in the classification labels makes transferring models across different datasets tricky.

Secondly, assigning a label to a post in terms of toxicity labels is complicated as many of the posts can be subjective (Aroyo et al., 2019). Finally, a further challenge is that after encountering several highly toxic comments, an annotator might find subsequent moderately toxic comments as not toxic (Kurrek et al., 2020).

Research is currently trying to situate the toxicity detection tasks as regression tasks. In its simplest form, an annotator is provided two samples, and they have to decide which one is more toxic. Eventually, these annotated comparisons are converted to a scalar value which denotes the level of the toxicity of the post. Hada et al. (2021) uses best-worst scaling (Kiritchenko and Mohammad, 2017) to assign toxicity scores to a post based on the comparison annotated by annotators. Besides, another study (Kennedy et al., 2020) used Rasch measurement theory for converting the comparisons to scalar values.

In this shared task, Jigsaw released a new dataset for understanding the severity of toxic language. The organizers select a set of 14,000 datapoints. They used these datapoints to create multiple pairs, which were then annotated by some annotator. The annotators marked one of the comments as toxic based on their notion of toxicity. These comparisons were compared with the ones received from models, and average agreement was used as the final score.

Jigsaw is a unit within Google that explores threats to open societies, and builds technology that inspires scalable solutions. They forecast emerging threats like Disinformation, Censorship, Toxicity and Violent Extremism and explore how technology can protect individuals and societies.

In this paper, we focus on developing models for this task. Since the shared task did not provide any training dataset, we utilized different classification-based toxic language datasets and converted their labels to a scalar value based on various strategies.
Finally, we use simple models like TF-IDF to complex models like Transformers. We conclude the paper with a detailed error analysis to understand the behavior of the models.

2 Datasets

In this section, we illustrate the datasets used for this task. The first section 2.1 describes the task dataset, and the second section 2.2 exhibits the dataset used for training the models since we don’t have any training dataset associated with this task.

2.1 Task dataset

In the task dataset 1, pairs of comments were presented to expert raters, who marked one of two comments more harmful – each according to their notion of toxicity. The final label for each pair is decided with a majority vote. The validation dataset contains ∼30k data points where each datapoint was a pair of toxic posts with the annotation mentioning which one is more toxic. However, this data cannot be used to train the models as they do not contain a toxicity score value for each comment. Apart from this we were provided with 5% of the test dataset for validating our models. The rest, 95%, is private and was used as hidden test data. Our results are discussed for the validation dataset and entire test dataset (150k posts).

2.2 External datasets

2.2.1 Reddit

This dataset (Hada et al., 2021) contains English language Reddit comments that have fine-grained, real-valued scores between -1 (maximally supportive) and 1 (maximally offensive). The annotators were given a set of 4 comments and asked to arrange them in order of their toxicity/abusiveness. These were converted to scalar scores using best-worst scaling (Kiritchenko and Mohammad, 2017). We transformed these scores to a value between 0 and 1 to keep the distribution of values uniform to other datasets. This dataset contains ∼16k data points.

2.2.2 Jigsaw Toxic Comment Dataset (JTC)

This dataset contains a large number of Wikipedia comments labeled by human raters for toxic behavior. The types of toxicity are toxic, severe toxic, obscene, threat, insult, and identity hate. Each comment can have any one or more of these labels. It contains ∼230k data points. This dataset is a part of the Toxic Comment Classification Challenge hosted on Kaggle 2. We converted the labels into a single score. The different toxicity categories were given different weights, and the final toxicity score was the sum of weights for each example. Our final weighing scheme was, severe toxic:12, identity hate:9, threat:8, insult:6, obscene:5, toxic:4

2.2.3 Jigsaw Unintended Bias Dataset

This dataset is part of a Kaggle Competition, Jigsaw Unintended Bias in Toxicity Classification 3. Each comment has a toxicity label that lies between 0 and 1. It has ∼2 million samples. This attribute (and all others) are fractional values representing the fraction of human raters who believed the attribute applied to the given comment. For evaluation, test set examples with a target >= 0.5 will be considered to be in a positive class (toxic).

The data also has several toxicity sub-type attributes like severe toxicity, obscene, threat, insult, identity attack, and sexually explicit. We have used mapping similar to that used for the Jigsaw Toxic Comment dataset for assigning the toxicity score.

2.2.4 Davidson

The dataset is sourced from (Davidson et al., 2017). The data is compiled using a hate speech lexicon, and all the instances are from Twitter. A minimum of 3 coders labeled tweets into classes Hate speech, Offensive, and Neither. The final sample consisted of ∼24,000 examples, and only about 5% fell into the Hate Speech class. We map the toxicity score using the formula - (3∗(# hate speech annotations)+2∗(# offensive annotations)+(# neither annotations))/No.of labelers. We then normalise this value between 0 and 1.

2.2.5 Founta

Similar to the previous dataset, (Founta et al., 2018) analyzed comments from Twitter and published a dataset with ∼80k examples. It has three labels (0, 1, 2) with an increasing level of toxicity. We scaled it between 0 and 1 by normalizing it.

3 Methodology

We preprocessed the datasets using standard techniques like stemming, lemmatization, removing contractions, and hyperlinks. For the toxic severity rating, we first tried traditional techniques

1https://www.kaggle.com/c/jigsaw-toxic-severity-rating
2https://tinyurl.com/2p85bsnj
3https://tinyurl.com/9cbyp3ry
like TF-IDF (Rajaraman and Ullman, 2011) and doc2vec (Le and Mikolov, 2014) based regressors to set the baseline. We further add other deep learning setups based on Transformers (Vaswani et al., 2017) to check if the scores improve further.

3.1 Baselines
Initially, we used TF-IDF and Doc2Vec as feature extractors. TFIDF is a method to find the importance of a word to a document in a text corpus (Rajaraman and Ullman, 2011). Doc2Vec is an unsupervised method to represent a document as a vector. To train using these features, we use ridge regression, which enhances linear regression by adding L2 regularization.

We used a hyperparameter optimization framework, Optuna, to automate the hyperparameter search for TFIDF. We found the Tfidf vectorizer to work best with the ‘charwb’ analyzer, n-gram range (3,5) & vocabulary of ∼30k most frequent words. The ridge regressor had a regularization strength of ∼1.

Doc2Vec was trained with a feature vector of size 300, learning rate $\alpha$ of 0.025. Both distributed memory and distributed bag of words methods were tested. As the performance was unsatisfactory, we did not conduct hyperparameter tuning for doc2vec.

3.2 Transformers
We take a pre-trained transformers model (Vaswani et al., 2017) that outputs a 768-dimensional vector representation of an input sentence. As this output cannot be directly used as a score for toxicity, we added a single linear layer on top of the encoder to get a single value for toxicity. As we feed input data, the entire pre-trained transformers model and the additional untrained regression layer is trained on our specific task. We focused on tuning hyperparameters manually instead of using any hyperparameter search library due to resource constraints. All the transformers were trained for three epochs with a batch size of 16.

In the following section, we discuss the specifics of the pre-trained models used in detail.

3.2.1 bert-base-multilingual-cased (M-BERT)
This language representation model is a modification of BERT, introduced by (Devlin et al., 2018). It was pretrained on a large corpus of multilingual data from Wikipedia with the objective of Masked language modeling (MLM) in a self-supervised setting. In the masked language model pre-training, the model learns using predicting some of the mask tokens in the text, and it should also be noted that this model is case sensitive.

3.2.2 bert-base-uncased (BERT)
Similar to the above model, this was also pre-trained using MLM objective, except this model was trained only on English text corpus, specifically on the BookCorpus, and is not case sensitive.

3.2.3 Hate-speech-CNERG/dehatebert-mono-English(dehateBERT) (Aluru et al., 2020) benchmarked hate speech classification models for 9 different languages and 16 datasets. All their models are based on the multilingual BERT model. We used their model that was finetuned on an English text corpus.

3.2.4 cardiffnlp/twitter-roberta-base-hate(HRoBERTa)
This model is derived from the RoBERTa-base model (Liu et al., 2019) trained on ∼58M tweets and finetuned on for hate speech detection with the TweetEval benchmark (Barbieri et al., 2020). Unlike the previous two models, this is an end-to-end regression model, meaning given a sentence, it directly outputs a number between 0 and 1.

3.2.5 GroNLP/hateBERT
This is a re-trained BERT model for abusive language detection in English by (Caselli et al., 2020). It was trained using MLM objective on RAL-E, a large-scale dataset of Reddit comments in English.

3.2.6 sentence-transformer/mpnet-base-v2(mpnet)
This is a sentence embedding model introduced by (Reimers and Gurevych, 2019) trained using a self-supervised contrastive learning objective. It is trained on 1 billion sentence pairs and is based on the pretrained Masked and Permutated Network introduced by (Song et al., 2020). It solves the problems of MLM in BERT and PLM (permuted language modeling) in XLNet and achieves better accuracy.

3.3 Ensembles
Finally, we experimented with ensembles of the models described in the previous sections. To do the ensembling, we predict the scores for a typical post using various models and then combine the
scores using a weighted average. The weights are decided based on the performance of the validation dataset. We used the weights as a variable using the Limited-memory BFGS (LM-BFGS) method, which is an optimization function in the family of quasi-Newton methods that approximates the Broyden–Fletcher–Goldfarb–Shanno algorithm (BFGS) using a limited amount of computer memory. It is a popular algorithm for parameter estimation in machine learning. The algorithm’s target problem is to minimize \( f(x) \) over unconstrained values of the real-vector \( x \) where \( f \) is a differentiable scalar function.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Models</th>
<th>Val. Acc.</th>
<th>Test Acc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reddit</td>
<td>TF-IDF</td>
<td>57.54</td>
<td>69.38</td>
</tr>
<tr>
<td></td>
<td>M-BERT</td>
<td>59.83</td>
<td>74.71</td>
</tr>
<tr>
<td></td>
<td>BERT</td>
<td>60.71</td>
<td>78.41</td>
</tr>
<tr>
<td></td>
<td>HateBERT</td>
<td>61.06</td>
<td>79.47</td>
</tr>
<tr>
<td></td>
<td>DehateBERT</td>
<td>60.69</td>
<td>78.46</td>
</tr>
<tr>
<td></td>
<td>Doc2vec</td>
<td>58.52</td>
<td>71.28</td>
</tr>
<tr>
<td>JTC</td>
<td>TF-IDF</td>
<td>61.01</td>
<td>78.57</td>
</tr>
<tr>
<td></td>
<td>Doc2vec</td>
<td>59.87</td>
<td>78.80</td>
</tr>
<tr>
<td></td>
<td>M-BERT</td>
<td>61.31</td>
<td>79.17</td>
</tr>
<tr>
<td></td>
<td>BERT</td>
<td>61.32</td>
<td>78.79</td>
</tr>
<tr>
<td></td>
<td>HateBERT</td>
<td>61.53</td>
<td>80.16</td>
</tr>
<tr>
<td></td>
<td>DehateBERT</td>
<td>61.25</td>
<td>79.90</td>
</tr>
<tr>
<td>Founta</td>
<td>TF-IDF</td>
<td>64.58</td>
<td>72.66</td>
</tr>
<tr>
<td></td>
<td>BERT</td>
<td>51.50</td>
<td>75.67</td>
</tr>
<tr>
<td>Toxic</td>
<td>TF-IDF</td>
<td>62.64</td>
<td>72.87</td>
</tr>
<tr>
<td></td>
<td>BERT</td>
<td>59.92</td>
<td>77.70</td>
</tr>
<tr>
<td>Davidson</td>
<td>TF-IDF</td>
<td>62.64</td>
<td>72.47</td>
</tr>
<tr>
<td></td>
<td>BERT</td>
<td>52.38</td>
<td>76.64</td>
</tr>
<tr>
<td>A+B+C+D+E</td>
<td>76</td>
<td>80.74</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Performance on Jigsaw Rate Severity of Toxic Comment Dataset for the validation and entire test dataset.

4 Results and Inference

In this section, we present a detailed analysis of the performance of our models.

4.1 Comparative study of performance

Table 2 shows the performance of our model on the validation dataset and total test dataset. As expected, the transformer-based approaches outperform the traditional approaches like TF-IDF/doc2vec. We found that HRoBERTa model performed the best among the transformers models. It is interesting to note that BERT & M-BERT give comparable results to language models already pre-trained for detecting toxicity (HateBERT & DehateBERT). Experiments on the transformed Founta, Davidson, and Toxic unintended did not give good scores; hence we did not perform further experiments on them.

Our team secured a rank of 145 out of 2301 in the Kaggle Jigsaw Rate Severity of Toxic Comments Competition with an accuracy of 79.84% in the private leaderboard. However, one of our ensembles which was not part of our final submission, performed even better. We achieved an accuracy of 80.74% in the final standings (Table 2).

4.2 LIME

We also conducted local interpretable model-agnostic explanations extensively on our best model (HRoBERTa) to identify potential issues with model predictions on the validation dataset. The validation set contains pairs of sentences labeled as less toxic and more toxic.

We ranked the model predictions and checked the top 100 wrong predictions manually. The top 100 wrong predictions were found by ranking the difference between the score assigned to less toxic to more toxic sentence. For most of the cases, it was not the model but the human annotator who was at fault. There were several cases where we found
difficult to select the more toxic comment. We found 68 samples where the annotator was wrong, 3 samples where our model was wrong and found 29 samples to be equally toxic. We add some of the samples from each category in Table 1.

The top 100 worst predictions were selected on the following basis. At first, for each sample we compared the scores generated by our model. The samples where the more toxic sentence had a lower score than less toxic sentence(similarly, less toxic with higher score than more toxic sentence) were marked as incorrectly classified samples. For all the incorrect classifications, the difference between the scores generated for less toxic and more toxic comment was computed. This list was sorted in descending order according to the difference. The top 100 samples were selected for LIME analysis. Hence, the samples where the model is more confident about the prediction yet wrong are selected. We believe that this method captures the worst errors of the model.

5 Conclusion

We present a detailed analysis of both the traditional and modern machine learning algorithms for toxicity detection. Instead of a binary classification, a relatively new notion of toxic speech rating is explored. The existing toxicity classification datasets are modified to train the models to output a toxicity score in a continuous range. We test our models on a new dataset proposed by Jigsaw. Additionally we present the LIME analysis to understand the model predictions.

References


Mithun Das, Somnath Banerjee, and Animesh Mukherjee. 2022a. Data bootstrapping approaches to improve low resource abusive language detection for indic languages. pages 32–42.


Quoc Le and Tomas Mikolov. 2014. Distributed representations of sentences and documents. In International conference on machine learning, pages 1188–1196. PMLR.


Can attention-based transformers explain or interpret cyberbullying detection?

Kanishk Verma¹², Tijana Milosevic¹², Brian Davis¹
ADAPT Centre¹, DCU Anti Bullying Centre²,
Dublin City University, Ireland
kanishk.verma@adaptcentre.ie

Abstract

Automated textual cyberbullying detection is known to be a challenging task. It is sometimes expected that messages associated with bullying will either be a) abusive, b) targeted at a specific individual or group, or c) have a negative sentiment. Transfer learning by fine-tuning pre-trained attention-based transformer language models (LMs) has achieved near state-of-the-art (SOA) precision in identifying textual fragments as being bullying-related or not. This study looks closely at two SOA LMs, BERT and HateBERT, fine-tuned on real-life cyberbullying datasets from multiple social networking platforms. We intend to determine whether these finely calibrated pre-trained LMs learn textual cyberbullying attributes or syntactical features in the text. The results of our comprehensive experiments show that despite the fact that attention weights are drawn more strongly to syntactical features of the text at every layer, attention weights cannot completely account for the decision-making of such attention-based transformers.

1 Introduction

Repeated hostile and aggressive online behaviour to intentionally hurt or embarrass someone through digital communication technologies are generally understood as Cyberbullying. (Patchin and Hinduja, 2006). Recent research findings by (B et al., 2021) and (Milosevic, 2021), indicate that 44% children in 11 European countries and nearly 50% children in Ireland have reported an increase in cyberbullying during the COVID-19 lockdown restrictions across multiple social networking sites (SNS) and multiplayer online gaming (MOG) platforms. This growing amount of cyberbullying content emerging across multiple SNS and MOG platforms is alarming and necessitates more effective content moderation, as earlier studied by (Gillespie et al., 2020; Milosevic, 2018; Gillespie, 2018). Therefore, one crucial step toward efficient and effective content moderation is the ability to recognize and define the basis for automated cyberbullying detection systems to classify a textual expression or phrase as cyberbullying.

Recent computational cyberbullying research claim to have outstanding accuracy and precision in automating the identification of cyberbullying using state-of-the-art (SOA) deep learning algorithms like attention-based Transformers, Gated Recurrent Units (GRUs), Long-Short Term Memory (LSTMs). However, upon close examination of such research, including those by (Paul and Saha, 2020; Yadav et al., 2020; Behzadi et al., 2021; Tripathy et al., 2020; Pradhan et al., 2020; Fang et al., 2021) among others, reveal that they rely on datasets for hate-speech or personal-attacks by (Founta et al., 2018; Waseem and Hovy, 2016; Wulczyn et al., 2017) for cyberbullying identification. In reality, despite their inventive attempts, these studies can only determine whether a text is abusive or hateful. We consider it a poor decision to detect cyberbullying using such out-of-domain datasets.

Additionally, work by (Ruder et al., 2019; Howard and Ruder, 2018; Dodge et al., 2020) has demonstrated the efficacy of transfer learning by fine-tuning pre-trained deep layered language models (LMs) for a variety of natural language processing (NLP) tasks, such as text classification, thereby yielding impressive results. (Verma et al., 2022), have demonstrated that fine-tuning LMs like $BERT_{base-uncased}$ by (Devlin et al., 2018), and $Hate-BERT_{base-uncased}$ by (Caselli et al., 2020) outperform traditional machine learning algorithms and aid in more accurate detection of textual cyberbullying across multiple SNS platforms. Research by (Vaswani et al., 2017; Devlin et al., 2018) demonstrates that the attention-based mechanisms within the deeply layered architecture of such pre-trained LMs can display dependencies between input and output. High attention weights for
inputs (such as words) are frequently referred to be accountable for the output, which provides the model’s interpretability (Mullenbach et al., 2018; Xie et al., 2017; Martins and Astudillo, 2016; Lei et al., 2017; Choi et al., 2016; Xu et al., 2015). To our knowledge, these assertions and presumptions have not undergone a formal evaluation for user-generated content (UGC) datasets collected from various SNS and MOG platforms categorically labelled for cyberbullying. (Kitchin, 2017; Ananny and Crawford, 2018; Katzenbach and Ulbricht, 2019) question the existing opaqueness of automated algorithmic content moderation and decision-making practices by SNS and MOG platforms. It has thus become necessary to design and develop transparent and equitable algorithms for moderation and regulation. To that effect, we attempt to extend the work by (Verma et al., 2022) on multiple platform cyberbullying detection, by addressing the following research question,

• RQ.1 Can attention-weights of attention-based LMs fine-tuned on real-life cyberbullying datasets be relied upon to detect and explain cyberbullying in an interpretable and understandable way?

Hence, we hypothesize that if attention-based LMs fine-tuned on real-life cyberbullying datasets learn textual cyberbullying traits for detecting cyberbullying; they would have higher attention weights for a) Parts-of-speech (POS) tags like adjectives, nouns, proper nouns, pronouns, and b) words with more negative sentiment. We also hypothesize that this assumption will be valid for text samples categorically annotated as cyberbullying across different datasets sourced from varied SNS and MOG platforms.

Content Warning: This article contains examples of abusive language in Section 5.4. All examples are taken from existing datasets (Section 3) to illustrate its composition.

2 Related Work

2.1 Cyberbullying Detection on Multiple platforms

There has been research on cross-platform cyberbullying detection, but they have had a narrow focus. (Edwards et al., 2020) devise a dataset from direct messages (SMS) shared between participants across multiple SNS platforms, social media posts collected from now-defunct Formspring.me and tweets from Twitter focusing only on one topic (2016 USA elections). However, despite their novel attempts at developing a cross-platform cyberbullying dataset and devising supervised machine learning classifiers to identify cyberbullying, their focus on a specific type of text-based communication like SMS and only on two types of SNS platforms, of which one is now defunct. On the other hand, (Nikhila et al., 2020; Yi and Zubiaga, 2022) also devise novel techniques to identify textual cyberbullying using adversarial neural network algorithms. Nevertheless, for training the classifiers, they rely on datasets by (Waseem and Hovy, 2016; Wulczyn et al., 2017) marked for either personal attacks or hate speech. On the contrary, work by (Van Bruwaene et al., 2020) is both novel and apt for cyberbullying research. They devise a high-quality dataset and experiment with Support Vector Machines (SVM), Convolutional neural networks (CNNs), and XGBOOST algorithms to develop a cross-platform cyberbullying detection system. To our knowledge, the work by (Van Bruwaene et al., 2020) is the only one that leverages real-life cyberbullying datasets. However, due to proprietary reasons, it is not yet made publicly available. (Verma et al., 2022) leverage real-life cyberbullying datasets collected by computational researchers from multiple SNS and MOG platforms such as Instagram, Twitter, ASK.fm, now-defunct SNS platforms Formspring.me, and Vine. On training multiple binary cyberbullying classifiers on single platforms and benchmarking their efficacy on different platforms, they found that attention-based LMs could achieve better precision and recall than traditional machine learning algorithms at classifying cyberbullying samples as cyberbullying. However (Verma et al., 2022) were unable to determine why these phenomena occur, and were also unable to establish whether the attention-based LMs were dependent on any textual cyberbullying traits (e.g. profanities or negative sentiment words).
2.2 Analysing Attention in attention-based language models

Attention-based transformer LMs developed by (Devlin et al., 2018; Yang et al., 2019; Caselli et al., 2020) consists of a deep architecture with many hidden layers stacked on top of one another. Within these layers are many attention-heads or sub-layers that assign attention-weights to a token (word) for learning the importance of the token. Substantial research conducted by (Zhang et al., 2019; Adadi and Berrada, 2018; Sundararajan et al., 2017) and others have demonstrated frameworks for explaining and interpreting these deep-layered LMs by analyzing these attention-weights at every layer. Moreover, (Vig, 2019a; Vig and Belinkov, 2019) have developed tools and resources that aid in visualizing the attention weights. This allows human users to comprehend and trust the results of such deep-layered LMs. However, studies by (Jain and Wallace, 2019; Serrano and Smith, 2019; Sun and Lu, 2020; Vashishth et al., 2019) have demonstrated that these attention-based mechanisms solely cannot be relied upon for interpreting and explaining the intricate workings of LMs. The work by (Elsafoury et al., 2021) for interpreting the attention mechanism of BERT for cyberbullying is closest to our research. We thank the authors (Elsafoury et al., 2021) for their contributions and for making the code repository reproducible. However, they a) rely on out-of-domain datasets like hate speech and personal attack datasets and b) lack in-depth analysis of LMs decision-making for both textual cyberbullying and non-cyber bullying samples. Moreover, they do not report the attention-based LMs interpretation for real-world binary instances of cyberbullying in text.

3 Datasets

To overcome current dataset-related gaps in cyberbullying research, we select datasets that are a) annotated by either cyberbullying domain experts or b) clear and precise annotation guidelines aided the annotation for cyberbullying. To our knowledge, there are only seven real-life datasets in English language that have been devised for cyberbullying markers with such annotations. We categorise the seven datasets into four groups based on a) type of SNS or MOG platform and b) average length of tokens observed from each of the seven platforms (See Figure 1). These groups include,

- Question-answering SNS: Question-answering SNS are both anonymous and non-anonymous platforms like ASK.fm, Reddit, and Quora that allow platform users to respond to questions posted by other users. Dataset devised by (Van Hee et al., 2018) from the ASK.fm platform is available in both English and Dutch. Annotations in this dataset are both binary and fine-grained, i.e., it is annotated for different cyberbullying forms and varied cyberbullying participant roles. (Reynolds et al., 2011) collected English language dataset from now-defunct Formspring.me. Annotations in this dataset are binary, i.e., textual samples are labelled as cyberbullying and non-cyber bullying.

- Twitter SNS: (Xu et al., 2012) formulated a dataset by collecting tweets from Twitter in the English language. Their dataset annotations are annotated as binary textual cyberbullying samples and for varied author roles such as victim, bully, reporter, and others. (Salawu et al., 2020) formulated a dataset from tweets in the English language. They have various labels such as profanity, insult, spam, sarcasm, threat, exclusion, and bullying.

- User-comment SNS: User-comment SNS are platforms that allow users to comment on images or videos posted by other platform users. Such platforms include but are not limited to Instagram, Facebook, TikTok, Vine, etc. (Hosseinmardi et al., 2015) collected multi-modal data (inclusive of images and textual comments) from Instagram. The annotations in this dataset are for both cyberbullying and cyber aggression. (Rafiq et al., 2015) also collected multi-modal data (inclusive of videos and textual comments) from now-defunct Vine platform. The annotation in this dataset includes both cyberbullying and cyber-aggression.

- MOG platforms: On MOG platforms, players communicate on forums, in-game chats, or via voice (either in-built or by plug-in voice-call platforms like Discord). (Breitneider and Peters, 2016) collected text from fo-
rums of highly popular MOG platforms like World-of-Warcraft (WoW) and League-of-Legends (LoL). The annotations in this dataset are of two types: a) role-based binary annotations, i.e., bully and victim, and b) binary labels for cyberbullying for each text sample.

As seen in Table 1, number of sentences for cyberbullying content is very low across all seven datasets. Each of the four grouped datasets were split into training, validation, and test sets. The training set makes up 80% for each of the grouped dataset, while the validation set and test set each make up for 10% of the datasets. The test set was further broken into two parts: a) 90% was used to evaluate performance of fine-tuned LMs performed, and b) 10% was used to analyze attention weights and gradient-based feature importance scores for each layer and head in the architecture of the LMs.

4 Experiment Setup

Tasks depicted in the first block of Figure 7 (See Appendix A.3) are described in detail in sections 4.1 and 4.3. As depicted in other two blocks of the Figure 7, we discuss the strategies for fine-tuning, hyper-parameter optimization strategies, and the attention-weight and gradient-based feature importance score at each layer for both bullying and non-bullying sentences in Sections 4.2 and 4.4. The code repository for reproducing this study can be found online.

4.1 Data anonymization, pre-processing and handling data imbalance

4.1.1 Data Anonymization

Adhering to General Data Protection Regulation (GDPR) directive (Council of European Union, 2016), we fully anonymised and normalised the datasets for any Personally Identifiable Information (PII) data. Such data included but was not limited to email-address, user names, geographical locations, and user-profile details, among others. Using GATE Cloud (Tablan et al., 2013) and the TwitIE API (K. Bontcheva, 2013), PII data was de-identified by masking and replacing the original words with masked value. For example, the sentence "mary@gmail.com is based in London", was masked as "email-address is based in location".

4.1.2 Pre-processing

Due to the abundance of non-standard language in the datasets, including lexical variants like supa → super, and acronyms, e.g., tbh → to be honest, and spelling errors, we applied several normalization heuristics for spelling and slang corrections. We removed a) URLs, user mentions, and non-ASCII characters for all datasets, b) retweet (RT) markers in text for twitter datasets, and c) lower-cased all text, and d) converted contractions to formal format. We also gathered a list of slang words and acronyms with their standardized forms from an online website. Finally, we developed an algorithm (See Appendix A.1 for details) to fix spelling errors with the most accurate semantic corrections.

4.1.3 Data Imbalance

The percentage of cyberbullying content in Table 1 shows a high imbalance skewed towards the non-bullying class. Handling the imbalance was paramount to avoid learning the bias towards the majority class in imbalanced datasets. Due to the limited nature of the dataset and to avoid the risk of losing context and sequence of words in a sentence, we leveraged the simple random oversampling technique (Moreo et al., 2016) over Synthetic Minority Oversampling Technique (SMOTE) (Bunkhumpornpat et al., 2009). It is worth noting

---

11https://gitlab.computing.dcu.ie/vermak3/xai-cyberbullying-attention
12https://www.webopedia.com/reference/text-abbreviations/
that the random oversampling was done in only one training set, and data imbalance was not handled in the validation and test set to match real-life scenarios. Also, to verify if over-sampling techniques affect the classification models’ accuracy, we run experiments with imbalanced and over-sampled datasets.

### 4.2 Language Models and Hyper-parameters

To ascertain which SOA LMs is able to a) better capture dependencies and b) learn better representation of cyberbullying text from noisy UGC data, we leverage pre-trained BERT$_{base-uncased}$ by (Devlin et al., 2018), and Hate-BERT$_{base-uncased}$ by (Caselli et al., 2020). BERT$_{base-uncased}$ is a bi-directional auto-encoding attention-based transformer with twelve layered transformer blocks, with each block containing twelve self-attention layers and a total of 768 hidden layers, resulting in approximately 110 M parameters. Hate-BERT$_{base-uncased}$ is a BERT LM re-trained on hateful comments from RAL-E Reddit’s banned communities (Chandrasekharan et al., 2017). We utilized the implementation provided by Hugging-Face’s Transformer Library (Wolf et al., 2019) and by (Caselli et al., 2020), and follow (Verma et al., 2022) experiments to fine-tune the pre-trained LMs.

To find optimal hyper-parameters, we used the Weights & Biases (Biewald, 2020) plug-ins to conduct multiple grid-based experiments with a varied range of hyper-parameters and optimized it to achieve maximum validation accuracy. The range of hyper-parameters includes,

- Maximum Token Length(s): [128, 256]
- Batch-size(s): [8, 16, 32]
- Epochs: [2, 3, 4]
- Loss Function: Binary Cross Entropy
- Optimizer Function: Adam Weighted
- Learning Rate(s): $1e^{-5}, 2e^{-5}, 3e^{-5}, 4e^{-5}, 5e^{-5}$

### 4.3 Collecting Parts-of-speech (POS) Tags & Sentiment Scores

To formally evaluate our hypothesis and assumptions addressed in Section 1. As the datasets leveraged in this study are a) sourced from SNS and MOG platforms, b) are not in formal language, and c) do not include POS tags or sentiment scores, we leveraged Spacy’s POS tagger 13 (Honnibal and Montani, 2017) to collect POS tags and VADER by (Hutto and Gilbert, 2014) to collect sentiment scores. Please note that both POS tags and sentiment scores were collected only for 10% of the test-set, (See Table 4 in Appendix A.2).

### 4.4 Attention-weights and gradient-based importance scores

To address our RQ.1 and compare with other experiments (Jain and Wallace, 2019; Serrano and Smith, 2019; Sun and Lu, 2020; Vashishth et al., 2019), we extract attention-weights of the fine-tuned LM(s) on 10% of test-set reserved for attention analysis. Many experiments on transformer-based attention-analysis refer to gradient-based feature importance scores as a measure for providing importance of individual features with known semantics (Clark et al., 2019; Serrano and Smith, 2019; Sun and Lu, 2020). We leveraged the Integrated Gradients algorithm by (Sundararajan et al., 2017) for pytorch14 to model interpretability by (Kokhlikyan et al., 2020) to compute the gradient-based feature importance scores on 10% of the test-set reserved for attention analysis. As the pre-trained LMs used

---

13https://spacy.io/usage/linguistic-features#pos-tagging
14A python language framework for deep learning https://pytorch.org/
in this study have 12 transformer block layers and 12 attention heads, we computed the mean attention weights for each head of every layer. Extending (Jain and Wallace, 2019)’s work, we use Pearson’s correlation coefficient (PCC) to measure the linear correlation between mean importance scores and mean attention weights. Moreover, we also a) compute mean-attention weights and gradient-based feature importance scores for every token for every POS tag of the reserved test-set and b) observe both mean-attention weights and gradient-based feature importance scores for tokens in the reserved test-set that have a greater negative sentiment.

5 Results

5.1 Impact of Data Imbalance

To assess if our simple oversampling strategy on training data referred to in Section 4.1.3 yields any significant improvement over the no-sampling strategy on training data, we check the model’s validation accuracy on the non-sampled validation dataset. As depicted in Table 5 (See Appendix A.4), we find no significant differences in the performance of either oversampling or no-sampling when both BERT and HateBERT LMs are fine-tuned on user-comment, twitter, and question-answering datasets, except for the gaming dataset. Both LMs fine-tuned on over-sampled gaming dataset perform better than fine-tuning on non-sampled datasets. We believe this is because, as seen in Table 1, there are only 2.3% bullying samples in the gaming dataset, and it is highly skewed towards non-bullying samples.

5.2 Hyper-parameters Finetuning

As discussed in Section 4.2, we experiment with different combinations of hyper-parameters with the help of the Weights & Biases plug-in for grid-based experiments. Table 2 represents the results of optimal hyper-parameters on validation-set for both fine-tuned LMs on each of the four datasets. We find that hyper-parameters vary for each model on every dataset. Overall, optimal hyper-parameters include, token-length of 128, batch-sizes ranging from 8 to 32, learning-rates between 1e-5, 2e-5, 3e-5, and 5e-5, and with 2 Epochs. With the help of these hyper-parameters, maximum accuracy can be achieved on validation sets.

5.3 Cyberbullying Detection

After training and validating both $\text{BERT}_{\text{base-uncased}}$ and $\text{HateBERT}_{\text{base-uncased}}$ with the optimal hyper-parameters (See Table 2) for every dataset, we assessed both LMs performance for their F1-scores for a) bullying, and b) non-bullying samples. In cyberbullying detection, false negatives and false positives are crucial, especially in cases of imbalanced data. We believe that F1 scores for each class are an apt metric for evaluating classifiers. As depicted in the Table 3 fine-tuning the HateBERT LM for each of the four platform datasets, does perform better than just fine-tuning the BERT LM. Moreover, these generalized LMs perform better with the grouped Twitter datasets.

5.4 Attention-weights & Gradient-based feature analysis

5.4.1 Correlation between attention-weights & gradient-based feature importance scores

As observed in the Figure 2, the Pearson’s correlation coefficient (PCC) between attention-weights and gradient-based feature importance scores for fine-tuned HateBERT ranges from 0.0129 for bullying-samples in user-comment dataset to 0.1202 for bullying-samples in gaming datasets. Whereas, for fine-tuned BERT the PCC between attention-weights and gradient-based feature importance scores ranges from 0.0042 for bullying-samples in question-answering datasets to 0.19 in twitter dataset. Overall, as depicted in the Figure 2, this PCC is close to zero for both BERT and HateBERT LMs fine-tuned on user-comment dataset. For BERT LM fine-tuned on twitter and gaming datasets, the PCC between attention-weights and gradient-based feature importance scores is in the range of 0.08 to 0.19. However, for HateBERT LM fine-tuned on twitter datasets, this is not the case; the PCC between attention-weights and gradient-based feature importance for this data is nearly zero (0.070-0.078).

From Table 3, we can deduce that HateBERT LM fine-tuned on twitter datasets has better F-scores than BERT LM fine-tuning on the same dataset. The near zero-correlation observed between mean attention-weights and gradient-based importance scores for both generalized LMs, especially for better performing HateBERT LM fine-tuned on twitter datasets, helps us substantiate
<table>
<thead>
<tr>
<th>Model</th>
<th>Dataset</th>
<th>Token length</th>
<th>Batch-size</th>
<th>Learning Rate</th>
<th>Epochs</th>
<th>Val-Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT+</td>
<td>Gaming</td>
<td>128</td>
<td>8</td>
<td>5e⁻⁵</td>
<td>4</td>
<td>0.7746</td>
</tr>
<tr>
<td></td>
<td>UC</td>
<td>128</td>
<td>32</td>
<td>3e⁻⁵</td>
<td>2</td>
<td>0.7476</td>
</tr>
<tr>
<td></td>
<td>QA</td>
<td>128</td>
<td>8</td>
<td>5e⁻⁵</td>
<td>2</td>
<td>0.9496</td>
</tr>
<tr>
<td></td>
<td>Twitter</td>
<td>128</td>
<td>32</td>
<td>2e⁻⁵</td>
<td>2</td>
<td>0.7478</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model</th>
<th>Dataset</th>
<th>Token length</th>
<th>Batch-size</th>
<th>Learning Rate</th>
<th>Epochs</th>
<th>Val-Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>HateBERT+</td>
<td>Gaming</td>
<td>128</td>
<td>8</td>
<td>1e⁻⁵</td>
<td>2</td>
<td>0.7497</td>
</tr>
<tr>
<td></td>
<td>UC</td>
<td>128</td>
<td>16</td>
<td>3e⁻⁵</td>
<td>2</td>
<td>0.7497</td>
</tr>
<tr>
<td></td>
<td>QA</td>
<td>128</td>
<td>16</td>
<td>1e⁻⁵</td>
<td>2</td>
<td>0.9498</td>
</tr>
<tr>
<td></td>
<td>Twitter</td>
<td>128</td>
<td>32</td>
<td>5e⁻⁵</td>
<td>2</td>
<td>0.939</td>
</tr>
</tbody>
</table>

Table 2: Optimal Hyper-parameters for every model with every dataset
Note: UC → user-comment; QA → question-answering

<table>
<thead>
<tr>
<th>Model</th>
<th>Dataset</th>
<th>Bullying F1</th>
<th>Non-Bullying F1</th>
<th>Average F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT+</td>
<td>QA</td>
<td>0.62</td>
<td>0.68</td>
<td>0.65</td>
</tr>
<tr>
<td></td>
<td>UC</td>
<td>0.65</td>
<td>0.77</td>
<td>0.71</td>
</tr>
<tr>
<td></td>
<td>Twitter</td>
<td>0.75</td>
<td>0.79</td>
<td>0.77</td>
</tr>
<tr>
<td></td>
<td>Gaming</td>
<td>0.68</td>
<td>0.79</td>
<td>0.72</td>
</tr>
<tr>
<td>HateBERT+</td>
<td>QA</td>
<td>0.73</td>
<td>0.73</td>
<td>0.73</td>
</tr>
<tr>
<td></td>
<td>UC</td>
<td>0.68</td>
<td>0.84</td>
<td>0.76</td>
</tr>
<tr>
<td></td>
<td>Twitter</td>
<td>0.78</td>
<td>0.84</td>
<td>0.81</td>
</tr>
<tr>
<td></td>
<td>Gaming</td>
<td>0.74</td>
<td>0.78</td>
<td>0.76</td>
</tr>
</tbody>
</table>

Table 3: Cyberbullying Classification Results
Note: UC → user-comment; QA → question-answering

the claims by (Jain and Wallace, 2019; Serrano and Smith, 2019; Sun and Lu, 2020; Vashishth et al., 2019). They claim that while attention-mechanisms improve classification performance, relying on attention-weights for interpretation is questionable at best, holds true even for real-life SNS and MOG cyberbullying datasets.

5.4.2 Layer-wise attention Analysis

In this section, we examine the mean-attention weights at each layer for each POS tag as well as sentences with both stronger negative & positive sentiment that were taken from fine-tuned LMs that had a) a higher positive correlation between the mean attention weights and the mean gradient-based feature importance scores and b) a higher classification F-1 score. These models are BERT+/twitter and HateBERT+/gaming as depicted in the Table 3 and the Figure 2. So, using data from both Twitter and gaming datasets, we provide layer-wise analysis as follows,

- **Layer-wise Attention for Parts-of-speech Tags &**

In Figures 3 and 4, we represent mean-attention attention weights at each layer for every POS tag in the twitter and gaming datasets. For adjectives in both bullying and non-bullying samples in these datasets, fine-tuned BERT and HateBERT models have mean attention weights ranging from 0.051 to 0.062. For verbs in bullying samples, fine-tuned BERT has 0.1 mean attention weight at layer 6, and at the end of layer 12, it drops to 0.09, whereas in the fine-tuned HateBERT model for bullying samples, the mean attention weight is as low as it is for adjectives. For nouns in bullying samples, fine-tuned BERT has a mean attention weight of 0.051, and fine-tuned HateBERT has a lower mean attention weight of 0.051 throughout all layers. This, in a way, disproves our hypothesis that words that are adjectives, verbs, nouns, and proper nouns will have higher mean attention weights. As depicted in Figures 3 and 4, mean
attention weights for auxiliaries, determiners, ad-positions, conjunctions, and interjections in comparison to adjectives, verbs and nouns are consistently higher at almost all layers for fine-tuned BERT and HateBERT models in both bullying and non-bullying samples.

- **Negative Words & Attention**
  As discussed in an earlier section, we assume that negative sentiment words will have greater mean attention weights, so we compare these weights with the mean attention weights of positive sentiment words. Also, as mentioned in Section 4.3, we leveraged Vader to generate sentiment scores for all tokens in the reserved test set. We selected four words with greater negative sentiment (f*ck, a*s, b*tch, stu*id) and four words with greater positive sentiment (like, cute, pretty, truth). The Figures 5 and 6 represent mean-attention weights per layer for each of the words. We find that the positive sentiment word pretty has a similar mean attention weight as the negative sentiment words b*tch and a*s at all layers for both fine-tuned BERT and HateBERT models. This disproves our second assumption that negative sentiment words will have greater mean attention weights. For brevity, our analysis on two sample sentences at every layer and head are briefly discussed in Appendix A.5.

6 Conclusion & Future Work

Our comprehensive experiments using two LMs and four grouped real-life cyberbullying datasets from various SNS and MOG platforms revealed that: a) a fine-tuned HateBERT is better at classifying cyberbullying samples as cyberbullying; b) there is almost no correlation between the attention-weights and gradient-based feature importance scores; and c) an attention-based transformer model tuned for cyberbullying classification relies more on syntactical features in text, and d) attention-based transformer model fine-tuned for cyberbullying classification have similar “attention” for both negative and positive sentiment words. While our experiments show that to some level, attention-based transformers fine-tuned on real-life cyberbullying datasets do aid in interpreting and explaining its decision-making based on cyberbullying features, there is still a lot more work to be done in devising transparent and fair LM(s) for cyberbullying.
detection. While we demonstrate comprehensive methods to interpret and explain fine-tuned LMs on real-life SNS and MOG text cyberbullying classification, we acknowledge that due to the diverse forms and roles of cyberbullying, our work is limited by binary cyberbullying categories. Due to the current paucity of fine-grained cyberbullying datasets, in the future, we will attempt to use the learned representation of these fine-tuned LM(s) on fine-grained pre-adolescent datasets by (Sprugnoli et al., 2018).

7 Acknowledgements

We thank the authors (Van Hee et al., 2018; Reynolds et al., 2011; Xu et al., 2012; Salawu et al., 2020; Hosseini-Marandi et al., 2015; Rafaq et al., 2015; Bretschneider and Peters, 2016) for sharing the dataset. The research conducted in this publication was funded by the Irish Research Council and Google, Ireland, under grant number EP-SPG/2021/161.

References


A.1 Data Normalisation Algorithm

As SNS and MOG text is short, an incorrect replacement of misspelt words can make the sentence lose its context. For example, if in the sentence "i got a tkn to play" "tkn" is replaced as "taken" instead of "token", the sentence will lose its meaning. So, to avoid such an incorrect spell correction, it is important to understand the context of the sentence. To that effect we developed an algorithm 1 to fix spelling spelling errors with the most accurate semantic corrections by leveraging the existing python library py-spell-checker\(^\text{15}\) and (Goldberg and Levy, 2014)'s word2vec word embedding technique. The python spell-check library py-spell-checker\(^\text{16}\) checks every word for a misspelling and suggests two or more possible correct words. The original sentence is then parsed through the word2vec (Goldberg and Levy, 2014) model to get obtain its word embedding. The candidate words suggested by the spell check library are then replaced in the original sentence, and the new sentence is parsed through the word2vec model again. We then calculate the cosine distances between the original and possible replacement sentences, and the sentence with the highest cosine score or cosine score above 0.9 i.e., most similar to the original sentence, replaces the original sentence in the dataset.

\(^{15}\)https://pypi.org/project/pyspellchecker/
\(^{16}\)https://pypi.org/project/pyspellchecker/

A.2 Dataset Split

The table 4 represents each grouped dataset’s training, validation, and test-set size.

A.3 Experiment Schema

A.4 Imbalance Handling Results

Table 5 presents the results of no-sampling and over-sampling techniques leveraged in this study.
<table>
<thead>
<tr>
<th>Dataset-Type</th>
<th>Total Size</th>
<th>Training-set</th>
<th>Validation-set</th>
<th>Test-set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question-Answering</td>
<td>139,500</td>
<td>111,600</td>
<td>13,950</td>
<td>12,555</td>
</tr>
<tr>
<td>User-Comment</td>
<td>110,323</td>
<td>88,259</td>
<td>11,032</td>
<td>9,929</td>
</tr>
<tr>
<td>Twitter</td>
<td>13,974</td>
<td>11,179</td>
<td>1,397</td>
<td>1,258</td>
</tr>
<tr>
<td>Gaming</td>
<td>34,229</td>
<td>27,383</td>
<td>3,423</td>
<td>3,081</td>
</tr>
</tbody>
</table>

Table 4: Dataset split-size

Figure 8: Attention analysis for Positive Sentiment Word

Figure 9: Attention analysis for Negative Sentiment Word

for fine-tuning pre-trained LMs.

### A.5 Sentiment Attention Analysis

To analyse if negative and positive sentiment words have more attention in a text sequence. We selected the following two sentences, "f*ck the st*pid b*tch" (negative sentiment), and "i love this person" (positive sentiment), and visualized the sequence to sequence attention by leveraging BertViz (Vig, 2019b). Our findings for both positive and negative words in sample sentences for almost all layers and attention-heads on both fine-tuned BERT and HateBERT are depicted in Figure 8 and 9. As seen in Figure 8, the word "love" in positive sentence "i love the person", has higher attention distribution with neutral words like "the" and "person". As seen in Figure 9, the word "b*tch" in negative sentence has higher attention distribution with neutral words like "i, the" and "person". This too disproves our hypothesis, and shows attention is not fully at negative sentiment words, instead its similar for positive sentiment words and at times higher for neutral sentiment words.
<table>
<thead>
<tr>
<th>Model</th>
<th>Dataset</th>
<th>No-sampling</th>
<th>Oversampling</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT+</td>
<td>Gaming</td>
<td>0.7478</td>
<td>0.7746</td>
</tr>
<tr>
<td></td>
<td>UC</td>
<td>0.8476</td>
<td>0.8224</td>
</tr>
<tr>
<td></td>
<td>QA</td>
<td>0.9496</td>
<td>0.939</td>
</tr>
<tr>
<td></td>
<td>Twitter</td>
<td>0.94</td>
<td>0.365</td>
</tr>
<tr>
<td>HateBERT+</td>
<td>Gaming</td>
<td>0.6857</td>
<td>0.7468</td>
</tr>
<tr>
<td></td>
<td>UC</td>
<td>0.8497</td>
<td>0.8261</td>
</tr>
<tr>
<td></td>
<td>QA</td>
<td>0.9498</td>
<td>0.9076</td>
</tr>
<tr>
<td></td>
<td>Twitter</td>
<td>0.939</td>
<td>0.938</td>
</tr>
</tbody>
</table>

Table 5: Model’s performance on balanced and imbalanced training datasets
Note: UC → user-comment; QA → question-answering
Bias, Threat and Aggression Identification using Machine Learning Techniques on Multilingual Comments

Kirti Kumari, Shaurya Srivastav, Rajiv Ranjan Suman

Abstract

In this paper, we presented our team “IIIT Ranchi” for the Trolling, Aggression and Cyberbullying (TRAC-3) 2022 shared tasks. Aggression and its different forms on social media and other platforms had tremendous growth on the Internet. In this work we have tried upon different aspects of aggression, aggression intensity, bias of different forms and their usage online and its identification using different Machine Learning techniques. We have classified each sample at seven different tasks namely aggression level, aggression intensity, discursive role, gender bias, religious bias, caste/class bias and ethnicity/racial bias as specified in the shared tasks. Both of our teams tried machine learning classifiers and achieved the good results. Overall, our team “IIIT Ranchi” ranked first position in this shared tasks competition.

Keywords— Aggression, Multilingual comments, Tokenization, TF-IDF, BoG, Logistic Regression.

1 Introduction

Social media is an open platform where users can interact, share, learn and behave openly with other online users. Due to the high demand and popularity of these media, aggression and its manifestations in different forms have taken unprecedented proportions. Users of these media are generally writing their posts in multilingual forms (Kumar et al., 2022; Kumari and Singh, 2020b,a). So, identification of such kinds of aggression, threats and biases are not an easy task due to various reasons like these comments are unstructured, multilingual, short forms and highly contextual in nature. Due to these challenges, the research communities are very much interested in such kinds of automated identification. We have tried to develop systems that could automatically identify and separate these posts from the normal posts on the aggression shared dataset (Kumar et al., 2022).

For the given tasks, we have attempted all seven different categories of the text and classified them into their classes using different machine learning classifiers. The main motive of the work is to develop an efficient Machine Learning system to detect the aggression, biased and threatening contents on the social media platform which can be removed and altered afterwards. This will prevent the negative impact on many users and hate that may spread in society. The proposed models have different machine learning algorithms and we have fine tuned the models with different hyper-parameters which we have found for testing and cross validation phases. We found better results for all the shared tasks and ranked first. Our team (IIIT Ranchi) ranked first on all the Task1, Task1 surprise tests, and also in Task2.

In the preceding section, we have discussed a detailed description of the some related works, dataset, the preprocessing steps involved, the initial challenges and the models which we used for our use case.

2 Related Work

The variety of aggression related works have been proposed by researchers in the last few years. Aggression related shared tasks were proposed by the organising team of Shared Tasks on Aggression Identification in every second year 2018 (Kumar et al., 2018), 2020 (Bhattacharya et al., 2020) and 2022 (Kumar et al., 2022). Some of the recent works are discussed as:

At first, we are discussing some of the important works on 2018 aggression dataset (Kumar et al., 2018). The work (Risch and Krestel, 2018) used ensemble learning and data augmentation techniques. They augmented English training dataset with the help of machine translation using three languages (French, German and Spanish) by preserving the meaning of comments with different wording. Their system was not stable for Hindi dataset across the platforms (Facebook and Twitter). Their system is not stable, especially for Hindi dataset for the same domain it was performed well, but for other domain, it fails to classify the tweets with good accuracy. Aroyehun and Gelbukh (Aroyehun and Gelbukh, 2018) used various deep learning models such as Long Short Term Memory (LSTM), CNN, and FastText as word representation and data augmentation techniques by machine-translating the original post into different languages and then translated back to the original language. Their system was not clearly classified covertly aggressive comments from overly aggressive comments with significant accuracy. Julian and Krestel
(Risch and Krestel, 2018) and Aroyehun and Gelbukh (Aroyehun and Gelbukh, 2018) found that augmentation of training data gives a better result. Raiyani et al. (Raiyani et al., 2018) used dense system architecture and compared several models such as dense neural network, FastText and voting-based ensemble model. They found that simple three-layer dense neural network was performing better than the other two (FastText and voting-based ensemble classification) models. Their system has continued to suffer from false-positive cases and has also overlooked words that are not available in their vocabulary.

Some important works on 2020 aggression dataset (Bhattacharya et al., 2020; Kumar et al., 2020). Julian and Krestel (Risch and Krestel, 2020) uses transformer based multiple fine-tuned BERT models based on bagging technique and found very good results. The work (Mishra et al., 2020) also used the transformer based BERT models and achieved good performance.

3 Dataset

In this section, we discuss brief descriptions about datasets (Kumar et al., 2022) and given shared tasks.

3.1 Tasks

The following tasks defined by the organizing teams as: (a) Aggression, Gender Bias, Racial Bias, Religious Intolerance and Bias and Casteist Bias on social media and (b) the “discursive role” of a given comment in the context of the previous comment(s). Further these task are subdivided into some subclasses as: Gender Bias: It has three subclasses problem: Gender (GEN), Gender Threat (GENT) and Non-Gender (NGEN). Ethnicity/Racial Bias: It has three subclasses Ethnic/Racial comments (ETH), Ethnic/Racial Threat(ETHT), Non Ethnic/Racial comments(NCOM). Communal bias: It has three subclasses Communal (COM), Communal Threat (COMT), Non-Communal (NCOM). Caste/class bias: It has three subclasses Caste/classist comments (CAS), Caste/classist Threat (CAST), Non-Casteist/Classist comments (NCAS). Aggression Level: It has three subclasses ‘Overtly Aggressive’(OAG), ‘Covertly Aggressive’(CAG) and ‘Non-aggressive’(NAG) text data. Aggression Intensity: This level gives a 4-way classification in between ‘Physical Threat’(PTH), ‘Sexual Threat’(STH), ‘Non-threatening Aggression’(NtAG) and ‘Curse/Abuse’(CuAG). Religious Bias: At the level E, the task is to develop a 3-way classifier for classifying the text as ‘communal’ (COM), ‘Communal Threat’(COMT) and ‘non-communal’(NCOM).

The dataset (Kumar et al., 2022) is multilingual with a total of over 140,000 samples (over 60,000 unique samples) for training and development and over 15,000 unique samples for testing in four Indian languages Meitei, Bangla (Indian variety), Hindi and English. The dataset consists of comments from a total of 158 videos i.e., it has a comment thread in total. All the data is collected from YouTube. This dataset is manually annotated by multiple annotators. The phenomena of aggression/bias is a function of certain parameters. These parameters have been discussed properly in the article (Agha, 2006). The three contextual factors included in the tasks are aggression, gender bias and communal bias. The training data contains a mixed corpus of multilingual code-mixed comments in four Indian languages:

- Meitei
- Bangla
- Hindi
- English

Language-wise distribution is approximately 26.3% Meitei, 27.8% Bangla, 45.9% Hinglish(Hindi and English). The detailed description of the dataset can be found in the article (Kumar et al., 2022).

![Figure 1: Pie chart for language-wise distribution of the given training dataset.](image)

3.2 Initial challenges

The major challenges in the dataset were the unwanted words and the code-mixed nature of the dataset. We started out by cleaning the dataset with the help of certain techniques. We went for transliteration first but due to the change in meaning of many words we didn’t go forward with that method. We then used some of the text data preprocessing techniques and discussed in the following section.

4 Preprocessing

In this section we are going to describe the preprocessing steps we did for cleaning the dataset.

4.1 Removing noise:

The dataset has data from youtube hence mention of users, other hyperlinks are noise for us. Simple regex(regular expression) based rules were used to remove discrepancy : The general method was

- Anything which was followed by @ such as @user was removed as it didn’t add much of a context to our tasks.
- Anything starting with https:// was removed.
• Unidentified characters such as emojis with no general meanings were also removed.

4.2 Removing Punctuation and special symbols:
Since, we were going for Bag of Words (BoG) model and Term-Frequency Inverse Document Frequency (TF-IDF) vectorizer concept usage of punctuation didn’t have any impact on the dataset, hence we removed the punctuations and other special characters as well.

4.3 Lowering of dataset:
We have lowered the case of the sentences of the dataset to form uniformity in the dataset and we don’t have to care about the case of the dataset then for code-mixed data. Words such as ‘ACHA’ were converted to ‘acha’ for uniformity and space complexity constraints.

4.4 One Hot Encoding:
Categorical values corresponding to each class were label encoded as 0,1,2,3 to respective tasks having different classes.

4.5 Vectorization:
For vectorization, we used TF-IDF vectorizer as we used classical Machine Learning (ML) models for classification. Since the tasks were binary in nature (mostly as we had to predict whether a certain comment was aggressive or not and then its extent) so just the presence of certain words made it offensive and non-offensive and aggressive and non-aggressive. Therefore a simpler approach such as TF-IDF was used instead of the word2vec technique. Example: @user Agiye cholo aamra aachhi #goodfeels After cleaning we get - Agiye cholo aamra aachhi. goodfeels The final sparse matrix after vectorization was then feeded to the models for predictions.

5 Models
We have considered Naïve Bayes, Decision Tree based Random Forest, Logistic Regression and Support Vector Machines (SVM) for text classifications. We have used training data on each model by performing GridSearchCV for all the combinations of feature parameters. We have analyzed performance on the basis of a weighted average micro f1-score of the cross validation.

5.1 Support Vector Machine
The first model with which we started out was SVM as its state of the art for classification tasks. The parameters we used were C = 1 and the kernel was linear but it didn’t perform well mostly due to the non linearly separable nature of the dataset. Then we moved on to the polynomial kernel. With degrees as high as 8-9 also the model didn’t perform well as it failed to generalize. The next change we made was: kernel = ‘rbf’ C = 1, this performed well on train data. This model generalized well and gave better classification results as compared to above methods.

5.2 Multinomial Bayes (MNB)
The next model we used was Multinomial Bayes which is commonly used for text classification. The initial model didn’t perform well with value of = 0 as the minimum count of many words was zero in many of the cases so the joint probability was returning zero and hence the classes were being misclassified. We used grid search cross validation for finding the best and found best results on train data with = 1e-03 But due to a sparse dataset from TfidfVectorizer it had some limitations and even with hyper parameter tuning the performance didn’t improve much.

5.3 Decision Trees and Random Forest
We started the tree methods with a decision trees classifier but even with higher values of max depth and other parameters it didn’t perform well. Then we moved to ensemble techniques such as random forest. Random Forest overfitted on the training dataset, and hence it was not able to capture a general trend in the dataset and failed to provide good results on validation set. We choose the criterion for split to be entropy and the max depth of each tree to be 4 in Random Forest.

5.4 Logistic Regression (LR)
The last model, we used was Logistic Regression. A simple classifier model with different C values. Due to its (almost) binary nature and multi-class solver newton-cg logistic regression performed really well on the training dataset. We got a very generalized model for all tasks. We modified the value of penalty parameter C to higher values also and got the best result at C = 5. With the generalized models ready, we used these models to assess the results on the unseen testing data which contained three types - dataset with surprise text, COVID comments dataset and data with no surprise text.

5.5 Ensemble techniques
We then moved on with ensemble based boosting methods. We used XGB Classifier and Adaboost techniques in view of better variance and better results.

5.5.1 XGB classifier
Due to the sparse nature of the data, single decision trees couldn’t perform well. We chose many hyperparameters for this model but it failed to provide better results. Hence we didn’t move forward with this model in the training phase. We choose the criterion for split to be entropy and the max depth of each tree to be 4 in XGB classifier and the final criteria to be Softmax.

5.5.2 AdaBoost
The last model we used was Ada Boost. Being a boosting method we expected the variance to be better in this case. For base learners we chose a decision tree with max-depth =3 and the criterion of split to be entropy. Since the model was unable to make proper decisions on the basis of sparse data the performance was not par with the models we used before.
With the generalized models ready, we used these models to assess the results on the unseen testing data which contained three types - dataset with surprise text, covid comments dataset and data with no surprise text.

6 Results and Discussion

In this section, we present our findings and observations of this work.

6.1 Training data

The results, we present here are based on a weighted average micro F1-Score and some abbreviation used as: *LR - logistic regression *MNB - Multinomial bayes *SVM - support vector machines *RF- random forest *ADB - Adaboost * XGB - XG boost

The SVM model tends to fit perfectly to training data with a weighted average micro f1-score over 0.90 for many of the tasks due to its soft margin nature and flexibility in C value. The kernel used is Gaussian hence the model tends to mimic the training data really well.

6.2 Testing data

The testing data consisted of three tasks which had different datasets for evaluation in the competition.

- Task-1 Data without surprise language
- Task-2 Covid comments data
- Task-3 Data with surprise language

6.2.1 Task-1 Data without surprise data

In the above task we have seen, Logistic Regression performs better in all tasks even though SVM performed better on train dataset.

6.3 Task-2 Data with Covid-19 comments

This data contains comments in codemixed languages where the context is based on Covid-19. So many of the texts are offensive and many have negative aspects to it as well. Logistic regression again outperforms all other models.

6.3.1 Task-3 Data with surprise data

In this case Logistic Regression and MNB both perform equally but MNB performs well on each of the subtasks individually.

6.4 Reasons for not moving towards deep learning techniques

When we talk about Natural Language Processing task, we directly take into account the popular models such as various forms of BERT models. But since in our case the simpler model (Logistic Regression) was performing well, hence we didn’t move on to the deep learning model. While analysing our dataset, we found that the BERT based existing models had tokenizers which use sentence piece methods and hence while our dataset was code-mixed it would break the useful words into irrelevant tokens can be seen in the following example. For example: BERT’s tokenizer doesn’t have the word ‘ANNA’ (brother). So, it breaks down the word into ‘AN’, ‘NA’, which isn’t even close to brother. One of the other major reasons was the size of the dataset, since it was small, we couldn’t make our own embeddings for better performance as many of the things were required such as sentence piece tokenization and that requires a lot of data. The other reason was, these were simple classification tasks: i.e: whether a sentence is aggressive...
or not. So the presence of certain words were the only parameters we had to take care of. Hence, in our case Logistic Regression performed really well. We used Sklearn package (Pedregosa et al., 2011) to develop the models.

7 Error Analysis

In this section, we presented error analysis of our models. The size of training data was sufficient for ML models as we came across a large number of vocabulary. Since the metric used was micro F1-Score and most of the tasks had only 2-3 classes we got good results as the micro F1-Score came out to be above 0.70 on an average therefore class wise classification scores were also better. Model performs well on most of the tasks. By good performance, we mean good class wise F1-Score on all the respective classes. Few of the tasks where there was a surplus of one class had a lesser macro average due to absence of context aware classification but mostly the model has outperformed all other techniques. The confusion matrix and classification reports of Logistic Regression model’s performance on training data are given below: All the respective classes are encoded to one categorical numeral below is the dictionary for that.

‘Aggression’: ‘CAG’: 0, ‘OAG’: 1, ‘NAG’: 2,

Figure 2: Classification report for Aggression task on training data.

‘Aggression Intensity’: ‘NtAG’: 0, ‘NA’: 1, ‘CuAG’: 2, ‘STH’: 3, ‘PTH’: 4,

Figure 3: Confusion matrix for Aggression Intensity task on training data.

‘Discursive Role’: ‘NA’: 0, ‘CNS’: 1, ‘ATK’: 2, ‘AIN’: 3, ‘DFN’: 4, ‘GSL’: 5,

Figure 4: Classification Report for Discursive Role task on training data.

‘Caste/Class Bias’: ‘NCAS’: 0, ‘CAS’: 1, ‘CAST’: 2,

Figure 5: Confusion Matrix for Discursive Role task on training data.

‘Ethnicity/Racial Bias’: ‘NETH’: 0, ‘ETH’: 1, ‘ETHT’: 2

8 Conclusion

Our team secured the first position in the competition of the given shared tasks on bias, threat and aggression detection for given datasets. We found that the Logistic
Regression classifier outperforms all the models on test data due to more generalization and better prediction nature in sparse data. The possible reason was that the dataset in sparse form was linearly separable, but the SVM model being soft margin was not a generalized model for our case. SVM model was overfitting on train data but Logistic Regression generalized the metrics and hence performed really well in our case. At the end, we would like to conclude with the possibility that there exists many of the techniques other than what we have presented in this paper. In order to improve the model’s performance, we can go for ensemble techniques of the models which have performed well in order to increase the variance and make the model more generalized.

9 Acknowledgement

We would like to thank Mrinmoy Mahato, Amitesh Patel, Aman Kapoor and Ankit Kumar of Department...
of Computer Science and Engineering, Indian Institute of Information Technology RANCHI - 834004 for their help in preprocessing steps.

References


The Role of Context in Detecting the Target of Hate Speech
Ilia Markov
CLTL, Vrije Universiteit Amsterdam
Amsterdam, The Netherlands
i.markov@vu.nl
Walter Daelemans
CLiPS, University of Antwerp
Antwerp, Belgium
walter.daelemans@uantwerpen.be

Abstract
Online hate speech detection is an inherently challenging task that has recently received much attention from the natural language processing community. Despite a substantial increase in performance, considerable challenges remain and include encoding contextual information into automated hate speech detection systems. In this paper, we focus on detecting the target of hate speech in Dutch social media: whether a hateful Facebook comment is directed against migrants or not (i.e., against someone else). We manually annotate the relevant conversational context and investigate the effect of different aspects of context on performance when adding it to a Dutch transformer-based pre-trained language model, BERTje.

We show that performance of the model can be significantly improved by integrating relevant contextual information.

1 Introduction
Hate speech detection models play an important role in online content moderation and promotion of healthy online debates (Halevy et al., 2020). This has motivated a considerable interest in the task within a variety of disciplines, including social sciences and the natural language processing (NLP) community.

Recent advances in the field of NLP, which include the use of deep learning and ensemble architectures, have led to the development of automated hate speech detection approaches with an increased performance (Kumar et al., 2020; Zampieri et al., 2020; Markov and Daelemans, 2021). However, the task remains challenging from multiple perspectives, e.g., the use of figurative language and cross-domain scalability, amongst others (van Aken et al., 2018; Vidgen and Derczynski, 2020; Pamungkas et al., 2021; Lemmens et al., 2021). These challenges constrain the performance and generalizability of hate speech detection models, and include the problem of integrating contextual information, that is, improving hate speech detection models by making them context aware (Pavlopoulos et al., 2020; Menini et al., 2021; Vidgen et al., 2021).

Modeling contextual information is indisputably important for developing robust hate speech detection systems (de Gibert et al., 2018; Pavlopoulos et al., 2020; Vidgen et al., 2021). For instance, the comment ‘go back home’ is clearly hate speech if it is posted under a news article about refugees and asylum seekers. However, previous work on detecting both the type and target of online hate speech has mostly focused on message content alone, without accounting for the context of the target comments (Risch and Krestel, 2020; Zampieri et al., 2020). This is partially related to the lack of contextual information in the vast majority of datasets annotated for hate speech, which implies that hate speech detection models cannot exploit the conversational context when they are trained on existing datasets (Vidgen and Derczynski, 2020).

More recent studies have specifically looked into the effect of context on hate speech detection. For instance, Pavlopoulos et al. (2020) experimented with various strategies for integrating contextual information into BiLSTM and BERT models, where context is limited to the preceding (‘parent’) comment in the Wikipedia conversations dataset. The authors report that though context significantly affects annotation process by both amplifying or mitigating the perceived toxicity of posts, they found no evidence that adding context leads to a large or consistent improvement in performance of the examined models. Menini et al. (2021) highlighted similar challenges: while showing that context affects annotation process (fewer tweets were annotated as abusive when context was provided to annotators), they report that when experimenting with different models (BERT, BiLSTM, SVM) and a context window ranging from one to all preceding tweets, contextual information did not lead to a better classifier performance. Vidgen et al. (2021) introduced
the Contextual Abuse Dataset composed of Reddit messages, where previous or several previous messages were considered as the context and “every annotation has a label for whether contextual information was needed to make the annotation”. The authors report that 25-32% of content was labelled as context-dependent, and these messages are more challenging for detection, leaving integrating context for future work.

In this paper, we address hate speech target detection in hateful Dutch Facebook comments: whether the target of hateful content is the social group of interest, that is, migrants or someone else (see Section 2). While in previous work the preceding comment(s) in the discussion thread or the text of the post was used as context (Gao and Huang, 2017; Karan and Śnajder, 2019; Pavlopoulos et al., 2020; Menini et al., 2021; Lemmens et al., 2022), we manually annotate the relevant context, that is, we look specifically at the part of the prior conversation that provides the context, and use that annotation to demonstrate its utility in hate speech target prediction by adding relevant contextual information to a Dutch transformer-based pre-trained language model, BERTje (de Vries et al., 2019).

Hate speech is deeply contextual, and while most previous work ignores the conversational context, and more recent work, which looked into it based on previous comments or post, comes away concluding that such surface-level information is not helpful in prediction, this study shows and quantifies the impact that can be brought by relevant context on classifier performance when detecting the target of online hate speech.

2 Data

We used the LiLaH dataset, as in (Markov et al., 2021). The dataset is composed of Facebook posts by mainstream media outlets in Dutch (i.e., news articles that were published by the media outlets and are (re-)published or shared as Facebook posts) and readers’ comments on these posts in a comment section, which were manually annotated by three trained annotators for fine-grained types and targets of hate speech (see below in this section) with a ‘moderate’ agreement. The annotations were performed in-context, that is, annotators first read entire comment threads and then labeled each comment.

We randomly selected a subset of the dataset composed of 35 posts and around 6,000 comments discussing the migrants topic and annotated this data for context dependency: if context influences the annotators’ decision to assign a label to a comment, that is, if assigning hatefulness to a comment depends on understanding its context, or if the target of hate speech is not sufficiently clear without the context, the annotator marked the target comment as context-sensitive and indicated the ID of the post or the ID of the previous comment (not necessarily directly preceding) in the discussion thread that serves as the corresponding context. For example, the comment ‘Ik zou varkenslapjes geserveerd hebben’ (I would have served pork steaks) is hate speech directed against migrants if we take into account that the article is about a Muslim woman who was served alcohol at a show and was upset since this was against her religion. In this case, the annotator would mark the comment as context-dependent and indicate the ID of the post under which the comment was made.

We merged the fine-grained types of hate speech present in the data (e.g., violence, offensiveness, threat) into a single hate speech category, removing comments that belong to the non-hate speech class, which is the commonly used set-up for the hate speech target detection task (Zampieri et al., 2019a,b; Caselli et al., 2021), and used the binary target classes within the hateful messages. That is, we distinguish between migrants as the target of hate speech and merge all other fine-grained target classes into the ‘other’ category in order to have a sufficient amount of training and test examples per class. In more detail, the ‘other’ category consists of hate speech directed against (1) the article’s author or the media spreading the article; (2) the author of another preceding comment under the same post; (3) other entities related to the migrants group, as they represent a positive attitude towards this group; and (4) people or institutions that do not belong to any of the above categories. For the binary target classes used in this study, the inter-annotator agreement was ‘moderate’ (Cohen’s Kappa = 0.46).

We used training and test partitions splitting the dataset by post boundaries in order to avoid within-post bias, that is, all comments belonging to the same thread are in the same split. The splitting was done so that the distribution of ‘migrants’ and ‘other’ classes is as balanced as possible (roughly 40%-60%, respectively), while the proportion of 80% training and 20% test messages is preserved.
The statistics of the dataset used in terms of the number of posts, number of comments per class and the percentage of messages annotated as context-dependent within each class is provided in Table 1. We note that context-sensitive comments are frequent within both categories. Context-dependent messages within the ‘migrants’ category (59.8%; 750 messages) are more frequent than within the ‘other’ category (30.8%; 644 messages), which could be explained by the characteristics of the dataset used: it consists of discussion threads on the migrants topic, while in order to direct hate speech against someone else (e.g., previous commenter, article’s author) hateful content creators would have to deviate from the original discussion topic by explicitly specifying the target of their hate speech. Out of 1,394 messages labeled as context-dependent, the vast majority (88%) refer to original post as the source of relevant context, 7% to previous comment and 5% to a comment located higher up in the discussion thread.

3 Experiments and Results

We use the monolingual Dutch transformer-based pre-trained language model, BERTje (de Vries et al., 2019), from the Hugging Face transformers library¹, which showed near state-of-the-art results in previous work on Dutch hate speech detection, e.g., (Caselli et al., 2021; Markov et al., 2022). The model was pre-trained using the same architecture and parameters as the original 768-dimensional BERT model (Devlin et al., 2019) on a dataset of 2.4 billion tokens.

We set the maximum sequence length parameter to 512 in order to account for the context, the other parameters have default values, and fine-tune the model for a single epoch. Following the approach proposed in (Pavlopoulos et al., 2020), we concatenate the context and the text of the target comment separated by BERTje’s [SEP] token, as in the next sentence prediction task in BERTje’s pre-training stage, and fine-tune the model on this data.

We use only the content of the target comment as the baseline and examine the following ways for adding contextual information: (1) adding the text of the post on which the comment was made (comment & post); (2) adding the preceding comment (if any) in the discussion thread (comment & preceding comment); (3) adding the preceding comment and the post (comment & preceding comment & post); and (4) adding the relevant annotated context (comment & context). Since BERTje is sensitive to random seeds, we report the results in terms of precision, recall and F1-score (macro) averaged over five runs, and standard deviations in Table 2.

The obtained results are in line with previous findings in the sense that adding the content of a preceding comment does not facilitate classifier performance (Karan and Šnajder, 2019; Pavlopoulos et al., 2020; Menini et al., 2021). However, we observe a moderate improvement by adding the content of the post (2 F1 points) and a significant improvement (according to McNemar’s significance test (McNemar, 1947) with $\alpha < 0.05$) caused by pointing at the actual context in the discussion thread (6 F1 points). The results partially reflect the annotation process, described in Section 2, where most of the hateful messages contain the relevant context in the post text.

To further examine the importance of contextual information, we conducted an additional experiment using only the relevant context (while discarding the content of the target message), obtaining the following results: precision = 0.60 (±0.009), recall = 0.60 (±0.007), F1 = 0.60 (±0.009) (average over 5 runs). Considering that the majority baseline precision = 0.32, recall = 0.50, and F1 = 0.39, this experiment confirms that context contains useful information and can be used in isolation to predict the label of the target message.

The detailed results per class for one of the experiments reported in Table 2 for the baseline (comment only) and ‘comment & context’ strategies are presented in Table 3. We note that with the

<table>
<thead>
<tr>
<th></th>
<th><strong>Train</strong> (28 posts)</th>
<th><strong>Test</strong> (7 posts)</th>
<th><strong>Total</strong> (35 posts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrants</td>
<td># messages</td>
<td>% context</td>
<td># messages</td>
</tr>
<tr>
<td></td>
<td>1,017</td>
<td>60.2</td>
<td>238</td>
</tr>
<tr>
<td>Other</td>
<td>1,660</td>
<td>28.9</td>
<td>431</td>
</tr>
<tr>
<td>Total</td>
<td>2,677</td>
<td>40.8</td>
<td>669</td>
</tr>
</tbody>
</table>

Table 1: Statistics of the dataset used in terms of the number of posts, number of comments per class and the percentage of messages annotated as context-dependent within each class.

¹https://huggingface.co/GroNLP/bert-base-dutch-cased
additional contextual information, there is an improvement in performance for both ‘migrants’ and ‘other’ categories in terms of both precision and recall. In line with de Gibert et al. (2018) and Vidgen et al. (2021), we observed that context-sensitive messages are more challenging for classification: out of 302 context-dependent messages within the both categories 57% were identified correctly by the baseline approach, while out of 367 messages not dependent on the context, 71% were assigned the correct label. Integrating the relevant context lead to an improvement for both context-dependent and independent messages, resulting in 60% and 87% correctly-identified messages, respectively.

While for the ‘migrants’ class integrating the context lead to an improvement for the context-dependent messages (81% instead of 67% were identified correctly after adding the context), and no improvement was observed for the context-independent messages (65% vs. 71% without the context), for the ‘other’ class, the main source of improvement is the context-independent messages (84% instead of 72% were identified correctly), while the number of correctly-identified context-dependent messages within this category dropped from 48% to 42%. Zooming in on the fine-grained classes within the ‘other’ category, we note that the results are improved for all the classes, except for the hate speech directed towards article’s author or media spreading the news, where only two more messages were misclassified after adding the contextual information.

The confusion matrices for this experiment, presented in Figure 1, demonstrate that integrating the context improves the results both in terms of false positives and false negatives, providing additional evidence that context plays an important role in detecting the target of online hateful comments.

4 Conclusions

Despite recent advances, there are multiple challenges that remain and limit the development of ro-
bust real-world hate speech detection systems. One of such challenges, addressed in this work, is to explicitly account for relevant conversational context when developing context-aware hate speech detection approaches.

While prior work has shown that the easy-to-obtain contextual information such as previous comment or post does not provide a large or consistent improvement, we demonstrated that if the model can zoom in on the relevant context, the performance increases significantly.

A limitation of this work is that we use hand-labeled contextual information, and thus report an upper bound of improvement in performance. Nonetheless, we believe that this study is an important step towards developing more robust and context-aware automated hate speech detection approaches.

Given the great potential for encoding contextual information and its significant effect on detecting the target of hate speech presented in this work, the directions for future work include detecting relevant context for a target comment automatically and exploring its effect on performance, as well as investigating the impact of context on detecting fine-grained types and targets of online hate speech.

Acknowledgements

This research has been supported by the Flemish Research Foundation through the bilateral research project FWO G070619N “The linguistic landscape of hate speech on social media”. The research also received funding from the Flemish Government (AI Research Program). This research has also been supported by Huawei Finland through the DreamsLab project. All content represented the opinions of the authors, which were not necessarily shared or endorsed by their respective employers and/or sponsors.

References


Annotating Targets of Toxic Language at the Span Level

Baran Barbarestani and Isa Maks and Piek Vossen
CLTL Lab, Vrije Universiteit Amsterdam
De Boelelaan 1105, 1081 HV Amsterdam, The Netherlands
{b.barbarestani, isa.maks, piek.vossen}@vu.nl

Abstract

In this paper, we discuss an interpretable framework to integrate toxic language annotations. Most data sets address only one aspect of the complex relationship in toxic communication and are inconsistent with each other. Enriching annotations with more details and information is, however, of great importance in order to develop high-performing and comprehensive explainable language models. Such systems should recognize and interpret both expressions that are toxic as well as expressions that make reference to specific targets to combat toxic language. We, therefore, create a crowd-annotation task to mark the spans of words that refer to target communities as an extension of the HateXplain data set. We present a quantitative and qualitative analysis of the annotations. We also fine-tune RoBERTa-base on our data and experiment with different data thresholds to measure their effect on the classification. The F1-score of our best model on the test set is 79%. The annotations are freely available and can be combined with the existing HateXplain annotations to build richer and more complete models.

1 Introduction

Communication through social media has exploded in the last decades. The ease of posting opinions and the relative anonymity of posters has also unleashed problematic communication that can take many different forms: offensive language, hate speech, discriminatory language, abusive language, cyberbullying, etc., which can be all captured under the umbrella term toxic. Such communication is often very complex and involves different values and perspectives. A comprehensive interpretation of such communication requires different aspects to be detected and combined, among which expressions that make a judgement or suggest negative implications and expressions that refer to targets such as a specific group of people or an individual belonging to such a group. An explainable system that can act as an automated moderator should be capable of "understanding" such phrases, reason over their content and bring specific aspects to posters’ attention to explain what is wrong with a post and why it has to be, for example, removed by moderators (Kiritchenko and Nejadgholi, 2020). An explainable model not only produces the desired outputs, but also explains why such output are produced.

The Natural Language Processing community has started many initiatives to automatically detect and classify toxic language and created a plethora of datasets (Vidgen and Derczynski, 2020; Poletto et al., 2021). However, these data sets often address only one of the above-mentioned aspects. Furthermore, they use slightly different terminologies and definitions for annotation and their annotation guidelines lack compatibility, which makes it difficult to combine their annotations. Another problem is that annotation is often done at a global level, such as the whole sentence instead of specific phrases and tokens. Some recent initiatives have started to annotate specific spans within the text itself (Mathew et al., 2020; Pavlopoulos et al., 2021) but this is limited to toxic spans only.

Although previous studies did annotate the target community (e.g., women, Muslims, immigrants, etc.) at the post level, none of these studies marked the words that describe or refer to such a group. Being able to detect these phrases is, however, crucial to reason over who is targeted and how they are referenced. Furthermore, annotating references to targets separately from toxic spans makes it possible to also process larger contexts of communication, among which conversations where references to targets and toxic expressions may be dispersed over multiple posts. By building a framework where target spans are annotated, it is possible to train explainable models that not only tell which community groups are targeted in a piece of text, but
also indicate which words and phrases this decision is based on. This will make the model and its decision more understandable for end users.

In this study, we describe a crowd-annotation task to annotate such target spans. We used this framework to add target spans to the HateXplain data set (Mathew et al., 2020) and tested classification models by fine-tuning with different quality selections of data.

Our contributions are as follows:

- An explainable framework to combine different toxic data annotations has been discussed.
- A crowd-annotation task, which aims at the identification of target spans, i.e., sequences of targeting tokens that together refer to a target community, has been created.
- An existing data set has been extended (Mathew et al., 2020) with annotations of target spans.
- A preliminary quantitative and qualitative analysis of the annotations has been provided.
- Three RoBERTa-base models have been fine-tuned on our data and the results have been reported.

The paper is organized as follows. In Section 2, we summarize the related work on target annotations and position our work. In Section 3, we describe the resources that we use to sample data in order to obtain sufficiently diverse annotations from each source. Section 4 explains our annotation framework and the crowd-annotation task that we designed, while in Section 5 we describe the results of the annotation. In section 6, we report on the language models we fine-tuned with our data and explain the results. We conclude and discuss future work in Section 7.

Please beware that this paper may contain some examples of hateful content. This is strictly for the purpose of enabling this research and we seek to minimize the number of examples wherever possible. Please be aware that this content may be offensive and cause you distress, which is certainly not the intention of the authors of this article.

2 Related work

The number of studies on the automatic identification of hate speech and other forms of toxic language has rapidly increased in recent years. Several definitions for toxic language have been proposed and many different annotation schemes have been designed and applied.

Part of these annotation studies focuses on the target community that has been victimized by such language and acknowledges that the description of these targets is relevant in different ways for the automatic detection of toxic language. Early studies (De Gibert et al., 2018), (Davidson et al., 2017) presented this task as a binary task labeling data as hateful or not. In these studies, only toxic expressions targeting people were considered hateful. For example, according to the annotation guidelines of (De Gibert et al., 2018), an expression should be labeled as hate speech only if all of the three following conditions are met: (1) There is a deliberate attack. (2) The attack is on a specific group of people. (3) The motive for this attack regards aspects of the group’s identity. Although the identity of the target group is decisive in determining whether an expression is considered hate speech or not, no details on this were annotated.

Another widely used annotation scheme (see e.g. (Basile et al., 2019), (Zampieri et al., 2020)) was developed by (Zampieri et al., 2019) who addressed the need for identifying more specific information about the target communities and therefore introduced several annotation layers as follows: (1) Determine whether the message is offensive. (2) If the message is offensive, determine whether it is targeting people or not. (3) If the message is targeting people, determine (a) whether the message is targeting an individual, or (b) whether the message is targeting a group or member of a group considered a unity due to the same ethnicity, gender or sexual orientation or any other common characteristic, or (c) whether the message is targeting other entities like an organization, a situation or an event.

Finally and most recently, several studies ((Mollas et al., 2022),(Kennedy et al., 2020), (Vidgen et al., 2021), (Ousidhoum et al., 2019)) have taken the target annotations one step further by providing the group aspect on which basis it was targeted (e.g. gender, race, national origin, disability, religion, sexual orientation, etc.) and by mentioning the specific target communities (e.g. Africans, immigrants, Muslims, homosexuals, politicians, etc.) This information would allow further research into differences in the framing of specific target communities and the building of classifiers that avoid bias in hate speech detection (Shah et al., 2021))
or permit researchers to delve into issues related to such bias. Although all of these studies considered target detection in hate speech as challenging and important, none of them annotated target spans at the token level.

Our work builds on the already existing annotations of the HateXplain data set (Mathew et al., 2020) by adding such span annotations that refer to a target/target community. In combination with the annotations already present in HateXplain, this allows us to train systems to detect both the phrases making reference to the targets as well as inferring the group aspect of these targets together with pointing at the phrases that represent the insulting content or judgement expressed about them.

3 Source data overview and sampling

HateXplain is the first hate speech data set that covers many aspects of toxic language (Mathew et al., 2020). Each post in this data set has been annotated from three different perspectives: 1) the three main classes: hate speech, offensive or normal 2) the target community (i.e., the community that has been the victim of hate speech/offensive language in the post) 3) rationales that are the parts of a post based on which annotators have decided to label it as such. The annotations were carried out at the word and phrase levels except for the target information which was done at the utterance level. According to (Mathew et al., 2020), the data was collected from Twitter and Gab with a total of 9,055 and 11,093 samples, respectively.1

For this study, we added target spans to the already existing annotations in this data set. This means that, for each sample targeting a target community, we wanted to determine which tokens in that sentence referred to that target community. For this reason, we selected only those samples that a) were instances of offensive language or hate speech b) targeted only one target community c) at least 2 out of 3 annotators agreed on its target label and d) had more than two and fewer than 61 tokens. We had extracted the distribution graphs of sentences per number of words and noticed that there are very few sentences that had more than 60 words in our data set. Also, the more words a sentence has, the more complex it becomes. In addition sentences with fewer than 3 words seem to have not enough and useful information for analysis. That is why we selected only sentences whose number of words was within the range described. The reason why we chose sentences with only one target group was mainly to make the task as easy and simple as possible for the crowd. Nonetheless, we later found that there were still a number of sentences that targeted more than one target group even though they were annotated in HateXplain as having only one target group. This is also referred to and explained in 5.4. As a result, a total of 6,445 samples were selected. From these, we selected 3,480 samples that were representative of different target communities and data sources, which constituted about 54% of the full sample set. The number of selected samples per target community are shown in Table 1. Only those target communities that appeared at least 10 times are shown in the table. The rest of them together with the "Other" target community are referred to as "Other target communities".

<table>
<thead>
<tr>
<th>Target community</th>
<th>Gab</th>
<th>Twitter</th>
<th>Other</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hispanic</td>
<td>160</td>
<td>2</td>
<td>0</td>
<td>162</td>
</tr>
<tr>
<td>Men</td>
<td>5</td>
<td>7</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>Homosexual</td>
<td>457</td>
<td>331</td>
<td>2</td>
<td>790</td>
</tr>
<tr>
<td>Islam</td>
<td>145</td>
<td>111</td>
<td>0</td>
<td>256</td>
</tr>
<tr>
<td>Arab</td>
<td>64</td>
<td>39</td>
<td>0</td>
<td>103</td>
</tr>
<tr>
<td>Refugee</td>
<td>103</td>
<td>83</td>
<td>1</td>
<td>189</td>
</tr>
<tr>
<td>Asian</td>
<td>82</td>
<td>68</td>
<td>0</td>
<td>150</td>
</tr>
<tr>
<td>Disability</td>
<td>5</td>
<td>29</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>African</td>
<td>355</td>
<td>278</td>
<td>0</td>
<td>633</td>
</tr>
<tr>
<td>Jewish</td>
<td>75</td>
<td>47</td>
<td>0</td>
<td>122</td>
</tr>
<tr>
<td>Caucasian</td>
<td>47</td>
<td>94</td>
<td>0</td>
<td>141</td>
</tr>
<tr>
<td>Women</td>
<td>225</td>
<td>385</td>
<td>0</td>
<td>610</td>
</tr>
<tr>
<td>Other target communities</td>
<td>150</td>
<td>130</td>
<td>0</td>
<td>280</td>
</tr>
<tr>
<td>Total</td>
<td>1873</td>
<td>1604</td>
<td>3</td>
<td>3480</td>
</tr>
</tbody>
</table>

Table 1: Data selected for annotation across target communities and sources (Gab, Twitter, Other)

To prepare the data set for the crowd-annotation task described in the next section, we sorted the data per target community and created separate batches of 30 samples. Each batch contained 29 samples from HateXplain and 1 attention check sentence randomly selected from a list of 60 sentences. These attention check sentences were manually generated and annotated, and were both targeting and toxic. Attention check sentences were included to inspect the crowd-annotators’ annotation and make sure that they did not simply annotate the data samples haphazardly or even skip them. The total number of batches amounted to 120. The first 25 batches only contained "Hispanic" and Homosexual" target communities. From batch 26 onward, however, each batch contained a mix-

---

1However, we observed that only 9,027 samples were labelled with the source Twitter, resulting in 28 samples that were not identified.
ture from different target communities and sources (Gab and Twitter) to reduce imbalanced data bias.

4 Crowd annotation task

For the crowd-annotation task, annotators were provided with batches of 30 toxic sentences presented one-by-one, where each sentence was followed by a list of tokens with tick-boxes. They were asked to read each sentence carefully before determining who the target was and select the tokens that referred to that target. At the start, they received an instruction page with examples. They were instructed to choose all the words - including the pronouns - that referred to the target no matter how many times they appeared in the sentence. Also, complete noun phrases including any adjectives had to be selected. Below are a few examples that demonstrate how sentences should be annotated:

1. You Bangladeshi guys are f**king gangsta.
   Target spans: You, Bangladeshi, guys

2. Just because we don’t let groups of creepy Moroccan rapists into the club doesn’t make us racist.
   Target spans: creepy, Moroccan, rapists

3. They do no shit other than going to the mosque.
   Target spans: They

4. Fuck the ignorant assholes from America, UK, and all other countries who try and soil the wonderful ties between all democratic nations.
   Target spans: the, ignorant, assholes, from, America, UK, and, all, other, countries

5. SHUT UP WHITE BOY!
   Target spans: WHITE, BOY

6. What’s up nigger?
   Target spans: nigger

7. You spics are worthless.
   Target spans: You, spics

8. He is a stupid Muslim.
   Target spans: He, a, stupid, Muslim

9. I need a new gay hashtag.
   Target spans: gay

It is worth noting that there are certain words and phrases that are toxic and specifically used for referring to a target community, such as "spic" in 7, which generally refers to Hispanics, or "nigger" in 6, which refers to Black people. These words should be also annotated as target words although they are toxic as well, because they are ultimately used to address specific target communities.

We used LINGOTurk (Pusse et al., 2016) as the platform to design our task, which is a free and available crowdsourcing client/server experiment management system. Furthermore, we used Prolific (Palan and Schitter, 2018), as the online platform for recruiting crowdworkers. The advantage of Prolific over other crowdsourcing platforms, such as Amazon Mechanical Turk, is that it provides more prescreening options, such as nationality, first language, ethnicity, political affiliation, socio-economic status, etc. Also, Prolific is not only limited to US participants. When recruiting annotators, we clearly described the aim of the study to them and explained what they had to do in detail. No specific sensitive information about annotators was stored. We also informed them beforehand that they should be aware of the inappropriate content of the sentences and they were not supposed to participate in this study if they were not comfortable with being exposed to such a language.

Since the study was closely related to one’s cultural understanding of the context and there were a lot of slang words and phrases used, we recruited only participants that met the following criteria:

- Both their nationality and country of birth had to be at least one of the following: United Kingdom (England, Wales, Scotland, Northern Ireland), United States, Ireland, Australia, Canada, Guyana, Jamaica, Liberia, New Zealand
- Their first, fluent, and primary language had to be English.

In order to determine the optimal number of annotators to recruit for each batch, we ran a test batch with 15 annotators and then extracted 10 random subsets, once with 5 and once with 10 annotators. Following the CrowdTruth framework (Dumitracche et al., 2018), we used the Media Unit Quality Score (UQS) to analyze the collected results from different sets of annotators. UQS expresses the overall worker agreement over a so-called media unit. In our case, each token was considered to be a media unit with the binary classification as
either targeting (1) or non-targeting (0). In order to calculate the UQS, one needs to first calculate the average cosine similarity between all worker vectors, weighted by the worker quality (WQS) and annotation quality (AQS). For more details on how each of these scores is calculated, please refer to (Dumitrache et al., 2018). The advantage of using UQS in comparison to other metrics for calculating the inter-annotator agreement is that CrowdTruth interprets both the disagreement among the annotators and the ambiguity of the token. The quality of an annotation is considered as the interaction between the quality of the annotator in terms of how often she/he agrees with others as well as the complexity of the input data and set of annotation categories.

We calculated the UQS for the complete set with 15 annotators and each of its subsets including 10 and 5 annotators, respectively. Next, we took the average of the obtained results over all subsets. By doing so, we could test in which cases and with what number of annotators the results were more consistent. In Table 2, the average overall UQS, average UQS for targeting tokens, and average UQS for non-targeting tokens across the test batch with different numbers of annotators are given. Targeting tokens refer to the tokens the majority of annotators labeled as targeting while non-targeting tokens refer to the tokens labeled as non-targeting by the majority. Also, the standard deviations of the 3 metrics per subset are given. In the case where there were 15 annotators, the average was taken over the media units and not different subsets, since no subset was created in this case. The closer the UQS and standard deviation are to 1 and 0, respectively, the higher the quality is.

<table>
<thead>
<tr>
<th>Number of annotators</th>
<th>15</th>
<th>10</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg UQS</td>
<td>0.81</td>
<td>0.80</td>
<td>0.80</td>
</tr>
<tr>
<td>Avg UQS for targeting tokens</td>
<td>0.78</td>
<td>0.80</td>
<td>0.80</td>
</tr>
<tr>
<td>Avg UQS for non-targeting tokens</td>
<td>0.86</td>
<td>0.86</td>
<td>0.87</td>
</tr>
<tr>
<td>SD of Avg UQSs</td>
<td>0.17</td>
<td>0.18</td>
<td>0.23</td>
</tr>
<tr>
<td>SD of Avg UQSs for targeting tokens</td>
<td>0.16</td>
<td>0.14</td>
<td>0.16</td>
</tr>
<tr>
<td>SD of Avg UQSs for non-targeting tokens</td>
<td>0.12</td>
<td>0.12</td>
<td>0.14</td>
</tr>
</tbody>
</table>

Table 2: Comparison of the annotation quality with different numbers of annotators. Avg=average; SD = standard deviation;

As can be seen in Table 2, the differences between the values are quite marginal and, especially for 10 and 15 annotators, most values are the same. Therefore, we decided to recruit 10 annotators per batch to do the annotations.

To select 10 annotators within the Prolific platform, the above pre-screening criteria were applied to the total pool of annotators. After running each batch, we analyzed the data to make sure the annotation quality was good enough and annotators acted according to our instructions. In order to do so, we compared the performance of each annotator to that of other participants, validated the attention check sentences, and considered the time taken on the whole for each annotator to finish the task. We also validated the annotations of some other randomly selected sentences. Finally, we checked whether the data provided by each participant corresponded with their Prolific ID and if they had entered a completion code showing that they had completed the whole task. If annotators failed any of the above-mentioned criteria, their submissions were rejected and another annotator was recruited in their place. We added the IDs of rejected annotators to our blocklist after each batch, which would exclude them from the next batches. In the next section, the results will be described in more detail.

5 Annotated Data

5.1 Statistical analysis of the crowd labels

We ran the batches for several weeks on the Prolific platform to obtain 10 annotations per sentence, eliminating problematic annotators as explained above. Table 3 gives a numerical overview of the result of the crowd annotation. In total, 5,799 target spans were identified, of which 4,747 (82%) were single-token. Interestingly, Gab samples had more references to target communities (the average number of target spans per sample was 1.82) than tweets did (with 1.48 spans on average). Additionally, the target spans found in Gab were a bit longer (with 1.52 tokens per span on average) than those found in tweets (1.44 tokens on average). These numbers can be explained by the fact that the Gab samples were generally longer than tweets, having 24.8 tokens on average, whereas this number was 14.6 for Tweets. However, it also shows that the two data sources had different characteristics with respect to how they referred to target communities.

5.2 Gold data annotated by experts

To get an independent evaluation of the quality of the crowd annotation, we did an expert annotation on two batches (2 and 23) through the same
platform. The annotators were the authors of this paper (A1, A2, A3). We calculated the Cohen’s kappa coefficient per pair of annotators. The results can be seen in Table 4.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Kappa score</td>
<td>0.67</td>
<td>0.65</td>
<td>0.67</td>
<td></td>
</tr>
<tr>
<td>Batch 23</td>
<td>Percent agreement</td>
<td>0.67</td>
<td>0.65</td>
<td>0.67</td>
</tr>
<tr>
<td>Kappa score</td>
<td>0.62</td>
<td>0.66</td>
<td>0.69</td>
<td></td>
</tr>
</tbody>
</table>

Table 4: Inter-annotator agreements among expert annotators (A1, A2, and A3) on the batches 2 and 23

The results show a reasonable agreement with kappa scores ranging from 0.62 to 0.69 across different annotators, different batches, and different classes (targeting vs. non-targeting). The percent agreement scores are above 87%. We discussed each case of disagreement and resolved these using predefined guidelines in order to have a fully adjudicated gold data set with expert annotations. The adjudicated annotations were used to determine the optimal settings for selecting the final label assigned to each token (see section 5.3).

5.3 Aggregating the crowd annotations

The expert annotation was used to determine the best threshold for selecting the labels of the tokens annotated by 10 annotators. We used the already explained UQS score per token as a basic measure to assign the final label and compared the results with the expert annotations for batches 2 and 23. We repeated this 3 times with different UQS thresholds: 50, 60, and 70. Tokens below these thresholds were considered as non-targeting since the crowd could not reach sufficient consensus. For the tokens with a UQS above these thresholds, we selected the label with the highest majority score, which could be either targeting or non-targeting.

Table 5 shows the Kappa scores by comparing the crowd data with different UQS thresholds to the expert annotations.

<table>
<thead>
<tr>
<th>Batch</th>
<th>UQS 50</th>
<th>UQS 60</th>
<th>UQS 70</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.55</td>
<td>0.48</td>
<td>0.37</td>
</tr>
<tr>
<td>23</td>
<td>0.58</td>
<td>0.56</td>
<td>0.45</td>
</tr>
</tbody>
</table>

Table 5: Kappa scores comparing the crowd data to the expert data with different UQS thresholds

The highest agreement using the lowest UQS threshold, which was 50. Therefore, we selected this threshold for creating a test set from the crowd annotations done on all batches.

5.4 Patterns of agreement and disagreement in the crowd annotations

We performed an error analysis in order to find which disagreement issues occurred most frequently and whether we could find any patterns. We illustrate the issues by making references to the examples below. The tokens marked with [T] are those that were annotated by a vast majority of annotators as targeting, tokens marked with [T*] were annotated by only a small number of annotators as targeting, which caused disagreement. The underlined tokens are those that were considered to be targeting by the authors of this paper.

2. One must wonder how long she[T*] will do in jail[T*] on the taxpayers dime before they decide to toss her[T*] spic[T] ass[T] out; as for the guy[T*] castrate[T*] him[T*] and jail[T*] him[T*] for life
3. I[T*] am black[T*] with all white[T*] friends[T*], taco[T] man[T*]
4. the wall is not the final solution these[T*] beaners[T] will keep having babies[T*] keep balkanizing[T*] our society(T*)
5. i saw a[T*] couple[T*] of[T*] baums[T*] and[T*] steins[T*]
6. as if it only okay when you are a cute gay[T] boy

The main sources of disagreement can be summarised as follow:

Length of target span
Not all annotators annotated the complete target span. Typically the beginning (cf. these in ex. 4 and her in ex. 2) or the end (cf. man in ex. 3) are missing.
Additional information about the target community  It seems that some annotators annotated properties, descriptions and behaviours of the target communities, whereas these tokens are not references to the community, but describing them (cf. France in ex. 1; jail in ex. 3; babies, balkanizing, society in ex. 4)

Inconsistent identification of referring pronouns Pronouns that refer to the target community were often missed (cf. you in ex. 1; she, her, him, him in ex. 2). This pattern is further confirmed by the words listed in Table 6: the references with the highest agreement were ethnic slurs (right column), whereas the references with the lowest agreement were pronouns (left column).

Multiple candidate target communities  Apparently, there was confusion among annotators when multiple communities were referred to. In ex.3, black and white friends were both incorrectly annotated as targeting, whereas no target community was targeted in this particular sample.

Different interpretations  In many cases, annotators did not agree about whether a reference to a target community was toxic or not. For example, those who considered the expression 'Baums and Steins’ (cf. ex. 5) to be ironic rather than offensive, did not label it as a targeting expression. xxxxxcbIn these cases it is not much possible to give the correct answers as these considerably depend both on the context and the annotator’s individual perspective (cf. (Basile et al., 2021)).

No explicit target word  There were cases where no target community was explicitly targeted, but because of the assumption that all sentences must be targeting (as explained in the instructions), annotators selected the existing community referred to in the sentence despite the absence of any obvious toxic reference to it (cf. ex. 6).

The analysis showed that toxic references to the target communities (such as beaners, her spic ass) were more easily identified than neutral ones such as man and the pronominal references. Moreover, it showed that annotations with a relatively low agreement required further analysis.

6 Automatic classification

After having obtained the labels for each token and having determined the best UQS threshold, we tested how well a language model could learn to detect the target spans and which UQS threshold for the training data would work best. Setting a high UQS threshold would give fewer data with a higher consensus, whereas a UQS threshold of 50, which had resulted in the highest Kappa score when the crowd annotations were compared with the expert annotations, would give us more targeting samples in the training data.

To test this, we fine-tuned a pretrained language model for a token classification task to predict whether each token was targeting or non-targeting. In (Sharma et al., 2021), the performances of a number of language models for detecting toxic spans in a sentence were compared. The best-performing model (RoBERTa-base) had the highest F1-score on the test set with a value of 68.41%. Therefore, we chose RoBERTa-base as our pretrained model. For fine-tuning, we converted the data to the IOB (Inside-Outside-Beginning) format, which is widely used in token classification tasks (Evang et al., 2013).

We created a separate test set consisting of 20% of the whole data, but ensured that it was representative of all target communities and data sources. The test set was generated by setting the UQS threshold to 50, as this threshold had previously resulted in the highest agreement when the crowd annotations were compared with the expert annotations. For the training, on the other hand, we generated three different training sets with UQS thresholds of 50, 60, and 70, to test the effects on the predictions. All other hyperparameters and arguments remained the same in all three cases. Furthermore, we selected 10% of the training data as the validation set. The training set, test set, and validation set included each 2227, 696, and 557 samples (sentences), respectively. Arguments and hyperparameters used for the training are as follows: batch size=16; epochs=3; learning rate=2e-5; weight decay=0.01. To prepare the data for fine-tuning our models, they were tokenized using AutoTokenizer from Hugging Face2.

### Table 6: Most frequent words targeting tokens: high vs. low agreement

<table>
<thead>
<tr>
<th>Low UQS</th>
<th>High UQS</th>
</tr>
</thead>
<tbody>
<tr>
<td>You (206)</td>
<td>Nigger (357)</td>
</tr>
<tr>
<td>They (90)</td>
<td>Faggot (263)</td>
</tr>
<tr>
<td>The (77)</td>
<td>Bitch (211)</td>
</tr>
</tbody>
</table>

2https://huggingface.co
During fine-tuning, evaluation was done at the end of each epoch. We batched our data with a data collator while using padding to make them all the same size. Each pad was padded to the length of its longest sample. We padded not only the inputs, but also the labels. We evaluated our model and its predictions on the test set with accuracy, precision, recall, and f1-score. After the predictions had been made, we needed to do some postprocessing. We picked the predicted index (with the maximum logit) for each token, converted it to its string label and ignored wherever we put a -100 label.

We repeated the training procedure with the three training sets, each generated with a different UQS threshold as described earlier. Table 7 shows the results on the test data, both overall and per class.

Overall, our model showed a good performance predicting the target spans. The scores for the dominant class “non-targeting” (0) were higher than the scores for the “targeting” class. The Weighted F1 scores ranged from 74 to 79%, which is significantly higher than the results for the toxic span detection task in (Sharma et al., 2021) although the tasks, data and annotations are different across these tasks. The best results were again obtained when the UQS threshold was set to 50.

<table>
<thead>
<tr>
<th>UQS</th>
<th>Class</th>
<th>Recall</th>
<th>Precision</th>
<th>F1-score</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>All</td>
<td>81%</td>
<td>78%</td>
<td>79%</td>
<td>14404</td>
</tr>
<tr>
<td>0</td>
<td>96%</td>
<td>97%</td>
<td>96%</td>
<td>14404</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>73%</td>
<td>73%</td>
<td>73%</td>
<td>2051</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>73%</td>
<td>64%</td>
<td>69%</td>
<td>906</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>All</td>
<td>75%</td>
<td>81%</td>
<td>77%</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>97%</td>
<td>95%</td>
<td>96%</td>
<td>14404</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>68%</td>
<td>76%</td>
<td>72%</td>
<td>2051</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>58%</td>
<td>72%</td>
<td>64%</td>
<td>906</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>All</td>
<td>67%</td>
<td>82%</td>
<td>74%</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>99%</td>
<td>93%</td>
<td>96%</td>
<td>14404</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>61%</td>
<td>76%</td>
<td>68%</td>
<td>2051</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>42%</td>
<td>76%</td>
<td>54%</td>
<td>906</td>
<td></td>
</tr>
</tbody>
</table>

Table 7: Test results overall and per class when the UQS threshold on the training set is 50, 60 or 70; class 0 = non-targeting; class 1= targeting-beginning; class 2= targeting-inside

7 Conclusion

We presented an extension to the HateXplain data set with annotations for target spans using crowd-annotation. The extended data set will enable the community to train and test models that recognize not only toxic language, but also the referents that are targeted. This is essential for future systems that need to comment on “wrong” behaviour in possibly interactive settings, discussing who has been targeted by what aspect and what toxic comments are used against the targeted person or community.

We provided the guidelines and instructions with clear examples of what we meant by target in a toxic sentence. We collected expert-annotated data for two of the batches with reasonable agreement among annotators. We obtained crowd annotations for target tokens in 3,480 sentences that targeted one target community. We also analyzed frequent patterns observed in the annotations and provided a statistical overview of the collected annotations.

We fine-tuned three RoBERTa-base language models with our data and investigated how changing the UQS threshold would affect the results. Our best model resulted in an F1-score of 79% on the test set, which was higher than other works in the field of toxic span classification. All the required information regarding the data and models is available on our Github repository.

In future work, we will extend the data to multiple languages as well as to richer and longer contexts, such as in conversational settings, where toxic expressions and targets can be mentioned sparsely. We want to explore other language models and compare their results by changing the hyperparameters and training arguments. Also, we are keen to compare the predictions of these models to the crowd-annotations and perform some error analysis.

Acknowledgements

This research was supported by Huawei Finland through the DreamsLab project. All content represented the opinions of the authors, which were not necessarily shared or endorsed by their respective employers and/or sponsors.

References


Valerio Basile, Michael Fell, Tommaso Fornaciari, Dirk Hovy, Silvius Paun, Barbara Plank, Massimo Poesio, and Alexandra Uma. 2021. We need to consider...


Is More Data Better? Re-thinking the Importance of Efficiency in Abusive Language Detection with Transformers-Based Active Learning

Hannah Rose Kirk\textsuperscript{1,2,3†}, Bertie Vidgen\textsuperscript{1,3}, Scott A. Hale\textsuperscript{1,2,4}

\textsuperscript{1}University of Oxford, \textsuperscript{2}The Alan Turing Institute, \textsuperscript{3}Rewire, \textsuperscript{4}Meedan

\textsuperscript{†}hannah.kirk@oii.ox.ac.uk

Abstract

Annotating abusive language is expensive, logistically complex and creates a risk of psychological harm. However, most machine learning research has prioritized maximizing effectiveness (i.e., F1 or accuracy score) rather than data efficiency (i.e., minimizing the amount of data that is annotated). In this paper, we use simulated experiments over two datasets at varying percentages of abuse to demonstrate that transformers-based active learning is a promising approach to substantially raise efficiency whilst still maintaining high effectiveness, especially when abusive content is a smaller percentage of the dataset. This approach requires a fraction of labeled data to reach performance equivalent to training over the full dataset.

1 Introduction

Online abuse, such as hate and harassment, can inflict psychological harm on victims (Gelber and McNamara, 2016), disrupt communities (Mohan et al., 2017) and even lead to physical attacks (Williams et al., 2019). Machine learning solutions can be used to automatically detect abusive content at scale, helping to tackle this growing problem (Gillespie, 2020). An effective model is one which makes few misclassifications, minimizing the risk of harm from false positives and negatives: false negatives mean that users are not fully protected from abuse while false positives constrain free expression. Most models to automatically detect abuse are trained to maximize effectiveness via “passive” supervised learning over large labeled datasets. However, although collecting large amounts of social media data is relatively cheap and easy, annotating data is expensive, logistically complicated and creates a risk of inflicting psychological harm on annotators through vicarious trauma (Roberts, 2019; Steiger et al., 2021). Thus, an efficient model, which achieves a given level of performance with few labeled examples, is highly desirable for abusive content detection.

Our central objective is to demonstrate how to maximize efficiency and effectiveness when training abuse detection systems, and in this paper, we focus on active learning (AL). AL is an iterative human-in-the-loop approach that selects entries for annotation only if they are ‘informative’ (Lewis and Gale, 1994; Settles, 2009). While AL has shown promise for abusive language dataset creation (Charitidis et al., 2020; Mollas et al., 2020; Rahman et al., 2021; Bashar and Nayak, 2021; Abidin et al., 2021), there are several open questions about the most appropriate configuration and use. In particular, only one paper uses transformers-based AL for abusive language detection (Ein-Dor et al., 2020) to our knowledge, although the benefits of AL for other classification tasks is clear (Schröder et al., 2022; Ein-Dor et al., 2020; Yuan et al., 2020). Pre-trained transformer models have been widely adopted for abuse detection, but while they can be fine-tuned on relatively few examples for specific tasks (Devlin et al., 2018; Qiu et al., 2020), they are still commonly used with large datasets (e.g. Mozafari et al., 2019; Mutanga et al., 2020; Isaksen and Gambäck, 2020; Koufakou et al., 2020). Our first subquestion asks, RQ1.1: What effect do model pre-training and architecture have on efficiency and effectiveness? To answer RQ1.1, we evaluate transformers- and traditional-based AL.
in a simulated setup using two already-labeled abusive language datasets.

One challenge in abusive language detection is class imbalance as, although extremely harmful, abuse comprises a small portion of online content (Vidgen et al., 2019). Prior AL work primarily uses datasets at their given class imbalances and thus has not disentangled how class imbalance versus linguistic features affect the design choices needed for efficient AL. This is a problem given that most abusive language datasets do not reflect the imbalance actually observed in the wild. Our second subquestion addresses this issue, **RQ1.2: What effect does class imbalance have on efficiency and effectiveness?** To answer RQ1.2, we artificially-rebalance the datasets at different percentages of abuse.

In addressing these questions, we find that more data is not always better and can actually be worse, showing that effectiveness and efficiency are not always in tension with one another. With extensive pre-training and greater model complexity, a transformers-based AL approach achieves high performance with only a few hundred examples. Crucially, we show that the value of transformers-based AL (relative to random sampling) is larger for more imbalanced data (i.e., data that more closely reflects the real-world). For 5% abuse, the performance of a transformers-based AL strategy over 3% of a 20k dataset can even surpass the F1 of a model passively trained over the full dataset by 5 percentage points (Fig. 1). In §4 we describe caveats of our findings and implications for future research in abusive language detection.1

## 2 Methods

### 2.1 Active Learning Set-Up

AL typically consists of four components: 1) a classification model, 2) pools of unlabeled data \( \mathcal{U} \) and labeled data \( \mathcal{L} \), 3) a query strategy for identifying data to be labeled, and 4) an ‘oracle’ (e.g., human annotators) to label the data. First, seed examples are taken from \( \mathcal{U} \) and sent to the oracle(s) for labeling. These examples initialize the classification model. Second, batches of examples are iteratively sampled from the remaining unlabeled pool, using a query strategy to estimate their ‘ informativeness’ to the initialized classification model.2

### 2.2 Dataset Selection and Processing

AL is path-dependent—i.e., later decisions are dependent upon earlier ones; so, experimenting in real-world settings is prohibitively costly and risky to annotator well-being. To reproduce the process without labeling new data, we use existing labeled datasets but withhold the labels until the model requests their annotation. We examined a list of publicly available, annotated datasets for abusive language detection4 and found two that were sufficiently large and contained enough abusive instances to facilitate our experimental approach. The *wiki* dataset (Wulczyn et al., 2017) contains comments from Wikipedia editors, labeled for whether they contain personal attacks. A test set is pre-defined; we take our test instances from this set. The *tweets* dataset (Founta et al., 2018) contains tweets which have been assigned to one of four classes. We binarize by combining the abusive and hate speech classes (=1) and the normal and spam classes (=0) to allow for cross-dataset comparison (Wiegand et al., 2019; Ein-Dor et al., 2020). A test set is not pre-defined; so, we set aside 10% of the data for testing that is never used for training.

To disentangle the merits of AL across class imbalances, we construct three new datasets for both *wiki* and *tweets* that have different class distributions: 50% abuse, 10% abuse and 5% abuse. This creates 6 datasets in total (see Tab. 1). To control for annotator well-being. To reproduce the process without labeling new data, we use existing labeled datasets but withhold the labels until the model requests their annotation. We examined a list of publicly available, annotated datasets for abusive language detection4 and found two that were sufficiently large and contained enough abusive instances to facilitate our experimental approach. The *wiki* dataset (Wulczyn et al., 2017) contains comments from Wikipedia editors, labeled for whether they contain personal attacks. A test set is pre-defined; we take our test instances from this set. The *tweets* dataset (Founta et al., 2018) contains tweets which have been assigned to one of four classes. We binarize by combining the abusive and hate speech classes (=1) and the normal and spam classes (=0) to allow for cross-dataset comparison (Wiegand et al., 2019; Ein-Dor et al., 2020). A test set is not pre-defined; so, we set aside 10% of the data for testing that is never used for training.

To disentangle the merits of AL across class imbalances, we construct three new datasets for both *wiki* and *tweets* that have different class distributions: 50% abuse, 10% abuse and 5% abuse. This creates 6 datasets in total (see Tab. 1). To control for annotator well-being. To reproduce the process without labeling new data, we use existing labeled datasets but withhold the labels until the model requests their annotation. We examined a list of publicly available, annotated datasets for abusive language detection4 and found two that were sufficiently large and contained enough abusive instances to facilitate our experimental approach. The *wiki* dataset (Wulczyn et al., 2017) contains comments from Wikipedia editors, labeled for whether they contain personal attacks. A test set is pre-defined; we take our test instances from this set. The *tweets* dataset (Founta et al., 2018) contains tweets which have been assigned to one of four classes. We binarize by combining the abusive and hate speech classes (=1) and the normal and spam classes (=0) to allow for cross-dataset comparison (Wiegand et al., 2019; Ein-Dor et al., 2020). A test set is not pre-defined; so, we set aside 10% of the data for testing that is never used for training.

To disentangle the merits of AL across class imbalances, we construct three new datasets for both *wiki* and *tweets* that have different class distributions: 50% abuse, 10% abuse and 5% abuse. This creates 6 datasets in total (see Tab. 1). To control for annotator well-being. To reproduce the process without labeling new data, we use existing labeled datasets but withhold the labels until the model requests their annotation. We examined a list of publicly available, annotated datasets for abusive language detection4 and found two that were sufficiently large and contained enough abusive instances to facilitate our experimental approach. The *wiki* dataset (Wulczyn et al., 2017) contains comments from Wikipedia editors, labeled for whether they contain personal attacks. A test set is pre-defined; we take our test instances from this set. The *tweets* dataset (Founta et al., 2018) contains tweets which have been assigned to one of four classes. We binarize by combining the abusive and hate speech classes (=1) and the normal and spam classes (=0) to allow for cross-dataset comparison (Wiegand et al., 2019; Ein-Dor et al., 2020). A test set is not pre-defined; so, we set aside 10% of the data for testing that is never used for training.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Imbalance abuse</th>
<th>non-abuse</th>
<th>Test abuse</th>
<th>non-abuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>wiki</td>
<td>12%</td>
<td>10.834</td>
<td>81.852</td>
<td>2.756</td>
</tr>
<tr>
<td>wiki50</td>
<td>50%</td>
<td>10.000</td>
<td>10.000</td>
<td>2.500</td>
</tr>
<tr>
<td>wiki10</td>
<td>10%</td>
<td>2.000</td>
<td>18.000</td>
<td>500</td>
</tr>
<tr>
<td>wiki5</td>
<td>5%</td>
<td>1.000</td>
<td>19.000</td>
<td>250</td>
</tr>
<tr>
<td>tweets</td>
<td>32%</td>
<td>28.955</td>
<td>61.041</td>
<td>3.160</td>
</tr>
<tr>
<td>tweets50</td>
<td>50%</td>
<td>10.000</td>
<td>10.000</td>
<td>2.500</td>
</tr>
<tr>
<td>tweets10</td>
<td>10%</td>
<td>2.000</td>
<td>18.000</td>
<td>500</td>
</tr>
<tr>
<td>tweets5</td>
<td>5%</td>
<td>1.000</td>
<td>19.000</td>
<td>250</td>
</tr>
</tbody>
</table>

Notes: 1 Train is used as the unlabeled pool (\( n = 20,000 \))  
2 Test is used for held-out evaluation (\( n = 5,000 \))
dataset size and ensure we have sufficient positive instances for all imbalances, we assume that each unlabeled pool has 20,000 examples. We experiment with multiple AL strategies to select 2,000 examples for annotation as early experiments showed further iterations did not affect performance.

2.3 Experimental Setup

We use 2 model architectures, 2 query strategies and 6 artificially-rebalanced datasets, giving 24 experiments each of which we repeat with 3 random seeds. Each experiment uses the same sized unlabeled pool, training budget and test set (see Tab. 1). In figures, we present the mean run (line) and standard deviation (shaded). For transformers-based AL, we use distil-roBERTa (dBERT), which performs competitively to larger transformer models (Sanh et al., 2019), also in an AL setting (Schröder et al., 2022). For traditional AL without pre-training, we use a linear support vector machine (SVM) as a simple, fast and lightweight baseline. For active data acquisition, we try three AL strategies; LeastConfidence, which selects items close to the decision boundary (Lewis and Gale, 1994), is presented in the paper while the other strategies are in the Appendix. For comparison, we randomly sample items from the unlabeled pool at each iteration. Alongside model and query strategy, AL requires an initial seed size, seed acquisition strategy and batch size. We experimentally determined the best values for these parameters: an initial seed of 20 examples selected via a keyword-heuristic (Ein-Dor et al., 2020) and batches of 50 examples.

2.4 Evaluation

As a baseline, we use the passive macro-F1 score over the full dataset of 20,000 entries (F120k). For each AL strategy, we measure efficiency on the held-out test set as the number of examples needed to surpass 90% of F120k, which we call N90. For effectiveness, we use the maximum F1 score achieved by each AL strategy, which we call F1_AL.

### Table 2: Efficiency and effectiveness of each classifier (transformers vs SVM) with LeastConfidence sampling.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Classifier</th>
<th>F1_AL</th>
<th>F1_20k</th>
<th>N90</th>
</tr>
</thead>
<tbody>
<tr>
<td>wiki50</td>
<td>dBERT</td>
<td>0.920</td>
<td>0.920</td>
<td>170</td>
</tr>
<tr>
<td></td>
<td>SVM</td>
<td>0.875</td>
<td>0.836</td>
<td>1570</td>
</tr>
<tr>
<td>wiki10</td>
<td>dBERT</td>
<td>0.885</td>
<td>0.866</td>
<td>170</td>
</tr>
<tr>
<td></td>
<td>SVM</td>
<td>0.809</td>
<td>0.810</td>
<td>320</td>
</tr>
<tr>
<td>wiki5</td>
<td>dBERT</td>
<td>0.807</td>
<td>0.855</td>
<td>220</td>
</tr>
<tr>
<td></td>
<td>SVM</td>
<td>0.785</td>
<td>0.780</td>
<td>170</td>
</tr>
<tr>
<td>tweets50</td>
<td>dBERT</td>
<td>0.939</td>
<td>0.938</td>
<td>170</td>
</tr>
<tr>
<td></td>
<td>SVM</td>
<td>0.931</td>
<td>0.926</td>
<td>220</td>
</tr>
<tr>
<td>tweets10</td>
<td>dBERT</td>
<td>0.904</td>
<td>0.902</td>
<td>220</td>
</tr>
<tr>
<td></td>
<td>SVM</td>
<td>0.893</td>
<td>0.901</td>
<td>170</td>
</tr>
<tr>
<td>tweets5</td>
<td>dBERT</td>
<td>0.844</td>
<td>0.856</td>
<td>300</td>
</tr>
<tr>
<td></td>
<td>SVM</td>
<td>0.825</td>
<td>0.830</td>
<td>170</td>
</tr>
</tbody>
</table>

Notes: \* global metric from passive training over full, re-balanced dataset

3 Results

**Efficiency & Effectiveness** For each dataset, we find active strategies that need just 170 examples (0.8% of the full dataset) to reach 90% of passive supervised learning performance (see Tab. 2). When training over the full dataset, dBERT always outperforms SVM, models have worse performance on more imbalanced datasets, and wiki is harder to predict than tweets (Tab. 2). In all cases, LeastConfidence outperforms the random baseline, and the gain is larger for lower percentages of abuse: for wiki10 and wiki5, N90 is lower by 150 and 100 examples, respectively. AL can even outperform passive supervised learning over the full dataset, showing there is no efficiency–effectiveness trade-off. For the majority of datasets, dBERT with LeastConfidence over 2,000 examples matches or surpasses the F1 score of a model trained passively over the whole dataset (F1_AL ≥ F1_20k in Tab. 2). For wiki5, it is 5 percentage points (pp) higher (Fig. 1).

**The Effect of Pre-Training** We find AL has a bigger impact for SVM than dBERT, shown by the larger gap to the random baselines (Fig. 2). With its extensive pre-training, dBERT achieves high performance with few examples, even if randomly selected. Nonetheless, an AL component still enhances dBERT performance above the random baseline especially with imbalanced data (as found by Schröder et al., 2022; Ein-Dor et al., 2020), requiring 150 and 100 fewer examples for N90, and raising F1 score by 2pp and 4pp, for wiki5 and wiki10 respectively.

**Train Distribution** To assess why AL is more impactful with imbalanced data, we evaluate the
distribution of the labeled pool at each iteration (Fig. 3). The random baseline tends to the original distribution as expected but the LeastConfidence strategy actively selects abusive examples from the pool and tends toward a balanced distribution.

**Out-of-domain Testing** The high performance of models trained on few examples raises a risk that they are overfitting and may not generalize. We take the models trained on each of the three class imbalances for wiki and test them on their equivalent tweets dataset, and vice versa. As with in-domain results, models trained on wiki and applied to tweets reach F1_{20k} within few iterations. The gap between LeastConfidence and the random baseline is larger for out-of-domain evaluation versus in-domain (Fig. 4). A similar pattern occurs for other imbalances (see Appendix D). This suggests that our results for these two datasets are not overfitting.

4 Discussion

In response to our central research objective, we find strategies which are both effective and efficient, requiring far fewer examples to reach performance equivalent to passive training over the full dataset. These results suggest that passive approaches may be needlessly expensive and place annotators at unnecessary risk of harm. For RQ1.1, we find that coupling pre-trained transformers with AL is a successful approach which leverages the benefits of careful training data selection with the previously demonstrated strong capabilities of pre-trained language models for few-shot learning (Brown et al., 2020; Gao et al., 2021; Schick and Schütze, 2021).

However, the compute required to fine-tune a new transformer model in each iteration means AL may have a large environmental footprint (Bender et al., 2021). In some instances, SVMs with AL produce competitive results and have smaller environmental costs. For RQ1.2, we find transformers-based AL is particularly valuable under more extreme class imbalance because it iteratively balances the distribution. Our findings are subject to some limitations, which present avenues for future work.

**How does data sampling, class labels and linguistic diversity affect performance?** We evaluate against two datasets with pre-existing labels, which we simplify into a binary task. This binarization was required to allow comparison across datasets. The wiki dataset samples banned comments and tweets samples with keywords and sentiment analysis. While these datasets were the only
publicly-available datasets large enough for this work, Wiegand et al. (2019) shows that they lack diversity, contain numerous biases, and cover abuse which is mostly explicit. This may make it easier for models to learn the task and generalize in fewer examples. Future work should evaluate the success and generalizability of AL for fine-grained labels and implicit abuse.

**How does the number of model parameters affect performance?** For computational feasibility and environmental concerns, we use distil-BERT but future work could assess if larger transformers models set higher baselines from passive training over the full dataset.

**Are certain AL strategies well-suited to abusive language detection?** We evaluate three commonly-used AL strategies, finding that Least-Confidence performs best, but none are tailored explicitly to abusive language. Constrastive Active Learning (Margatina et al., 2021) may be particularly useful: by finding linguistically similar entries on either side of the decision boundary, it may prevent overfitting to certain slurs, profanities or identities.

**Do the experimental findings generalize to real-world settings?** Our motivation for maximizing efficiency is to reduce financial costs and risk of harm to annotators, which we operationalize in terms of the number of labeled examples they view. In practice, costs are variable because entries which are more ‘uncertain’ to the model may also be more time-consuming, challenging or harmful for humans to label (Haertel et al., 2015). In a real-world setting, the work of the human annotators must be scaled up and down in response to labeling demands, which may incur additional costs. Crowd-sourced annotators can provide labels on demand when a new batch of entries is launched. With an expert annotation team, there may be a cost of paying annotators during re-training. Furthermore, it is important to note that the scope and scale of realized harm depends on both the total number of annotators as well as their identity, positionality and working conditions. While our approach simulates the labeling process with one groundtruth label, we make no assumptions on how this groundtruth is obtained—either via a single annotator or with some aggregation function over multiple annotator votes—so, our method is applicable to any number or constitution of annotators. We only make the light assumption that less exposure to harm is a good thing—whether that is many people being exposed a little less or few people being exposed a lot less. Future work is needed beyond our simulated set-up to calculate a more realistic cost-benefit ratio of AL, both in terms of financial and psychological costs.

We are exploring these questions in future work but simultaneously encourage the community to consider the need for efficiency in abusive language detection because of the costs, complexities and risk of harm to annotator well-being from inefficient data labeling.

**Acknowledgments**

This work was supported in part by JADE: Joint Academic Data science Endeavour - 2 under the EPSRC Grant EP/T022205/1, and by the The Alan Turing Institute under EPSRC grant EP/N510129/1. Hannah Rose Kirk was supported by the Economic and Social Research Council grant ES/P000649/1. We thank Paul Röttger and our anonymous reviewers for their comments.

**References**


 Ioannis Mollas, Zoe Chrysopoulou, Stamatis Karlos, and Grigorios Tsoumakas. 2020. ETHOS: an Online Hate Speech Detection Dataset.


A Details of Dataset Processing and Model Training

We use two English-language datasets which were curated for the task of automated abuse detection (Wulczyn et al., 2017; Founta et al., 2018). The wiki dataset can be downloaded from https://github.com/ewulczyn/wiki-detox and is licensed under Apache License, Version 2.0. The tweets dataset can be downloaded with tweet ids from https://github.com/ENCASEH2020/hatespeech-twitter.

These datasets cover two different domains: Wikipedia and Twitter. Each dataset is cleaned by removing extra white space, dropping duplicates and converting usernames, URLs and emoji to special tokens.

We fine-tune distil-roBERTa using the transformers integration with the small-text python package (Wolf et al., 2019; Schröder et al., 2021). distil-roBERTa has six layers, 768 hidden units, and 82M parameters. We encode input texts using the distil-roBERTa tokenizer, with added special tokens for usernames, URLs and emoji. All models were trained for 3 epochs with early stopping based on the cross-validation loss, a learning rate of $2e^{-5}$ and a weighted Adam optimizer. All other hyperparameters are set to their small-text defaults. In each active learning iteration, we use 10% of each labeled batch for validation. As a baseline to transformers-based AL, we use a support vector machine with no pre-training which we implement with sklearn. To encode a vector representation of input texts, we use a TF-IDF transformation fitted to the training dataset.

All experiments were run on the JADE-2 cluster using one NVIDIA Tesla V100 GPU per experiment. For transformer-models, it took on average 1.5 hours to run each experiment. For SVM, it took less than a minute to run each experiment and these can be easily be run on a CPU. We repeat each experiment three times using three seeds to initialize a pseudo-random number generator.

B Sampling with Keywords

We use a heuristic to weakly label examples from the unlabeled pool to be selected for the initial seed. Keywords are a commonly-used approach (e.g. see Ein-Dor et al., 2020) and searching for text matches is computationally efficient over a large pool of unlabeled examples. However, the keyword heuristic only approximates the true label and can introduce biases due to non-abusive use of offense and profanities. In our data, we rely on a keyword density measure ($K$) which equals the number of keyword matches over the total tokens in a text instance. We then experiment with varied thresholds of $K \in [1\%, 5\%, 10\%, 25\%]$ for a weak label of abusive text. A higher threshold reduces false positives but also decreases true positives. We find a threshold of 5% best balances these directional effects. Making predictions using a keyword heuristic with a 5% cut-off achieves an F1-score relative to the true labels of 69% for wiki and 80% for tweets. Using this threshold, examples are expected to be abusive if the percentage of keywords in total tokens exceeds 5%. We then sample equal numbers of expected abusive and non-abusive examples from the pool, reveal their true labels and initialize the classifier by training over this seed.

C Additional Experimental Analysis

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Classifier</th>
<th>Best AL Combinations</th>
<th>$F_{1_{\text{global}}}$</th>
<th>$F_{1_{\text{AL}}}$</th>
<th>$N_{90}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>wiki1</td>
<td>SVM</td>
<td>20 Random 50 LC</td>
<td>0.765</td>
<td>0.780</td>
<td>170</td>
</tr>
<tr>
<td>wiki10</td>
<td>SVM</td>
<td>20 Random 50 LC</td>
<td>0.839</td>
<td>0.866</td>
<td>170</td>
</tr>
<tr>
<td>wiki5</td>
<td>SVM</td>
<td>20 Random 50 LC</td>
<td>0.907</td>
<td>0.938</td>
<td>170</td>
</tr>
<tr>
<td>tweets50</td>
<td>SVM</td>
<td>20 Random 50 LC</td>
<td>0.839</td>
<td>0.855</td>
<td>220</td>
</tr>
<tr>
<td>tweets10</td>
<td>SVM</td>
<td>20 Random 50 LC</td>
<td>0.765</td>
<td>0.780</td>
<td>170</td>
</tr>
<tr>
<td>tweets5</td>
<td>SVM</td>
<td>20 Random 50 LC</td>
<td>0.904</td>
<td>0.902</td>
<td>220</td>
</tr>
<tr>
<td></td>
<td>dBERT</td>
<td>20 Heuristic 50 LC</td>
<td>0.893</td>
<td>0.901</td>
<td>170</td>
</tr>
<tr>
<td></td>
<td>SVM</td>
<td>20 Random 50 LC</td>
<td>0.939</td>
<td>0.938</td>
<td>170</td>
</tr>
<tr>
<td></td>
<td>dBERT</td>
<td>20 Random 50 LC</td>
<td>0.931</td>
<td>0.926</td>
<td>220</td>
</tr>
</tbody>
</table>

Notes: † global metric from passive training over the full dataset ‡ calculated by averaging the rank performance on $F_{1_{\text{AL}}}$, $N_{90}$
variable for both datasets and classifiers. In each panel of Fig. 6, we vary one parameter whilst holding all others fixed. This allows us to evaluate the impact of one variable, ceteris paribus. Namely, the reference values are those reported in the main paper: seed size of 20 selected by heuristics-based sampling and a batch size of 50 queried by LeastConfidence strategy.

**Seed and Batch Size** We test two choices for seed size (20, 200), and three choices for batch size (50, 100, 500). We find AL is more efficient with smaller seeds and batch sizes. The F1 score achieved with a seed of 20 and four AL iterations of 50 (|L| = 220) exceeds that reached with a seed of 200 and 0 iterations (|L| = 200) by 55pp for wiki50, 4pp for wiki10, and 10pp for wiki5. Batch sizes of 100 and 500 are less efficient than 50, with 700–1,100 and 150–200 more examples needed for N90, respectively.

**Seed Acquisition Strategy (Cold)** We evaluate two choices to select the examples for the seed. (1) **Random**: Seed examples are randomly selected. Depending on the class distribution of the unlabeled pool (which, in real world settings, is unknown) only non-abusive content might be identified. For datasets expected to be approximately balanced, a randomly-selected seed has a high probability of including both class labels. (2) **Heuristics**: Seed examples are selected using keywords (n = 652), taken from the abusive language literature (Davidson et al., 2017; ElSherief et al., 2018a,b; Gabriel, 2018). For wiki50, random and heuristics-based initialization achieve equivalent N90. However, with a seed of 20, a third of randomly-initialized experiments fail on wiki10 and all experiments fail for wiki5. This shows that when the data is imbalanced, a random seed is suboptimal because both class labels are not observed.

**Query Strategy** In addition to LeastConfidence (LC), we evaluate two further strategies coupled with dBERT: 1) **GreedyCoreSet** is a data-based diversity strategy which selects items representative of the full set (Sener and Savarese, 2017) and 2) **EmbeddingKMeans** is a data-based diversity strategy which uses a dense embedding representation (such as BERT embeddings) to cluster and sample from the nearest neighbors of the k centroids (Yuan et al., 2020). On our datasets, these two strategies are high performing in terms of the maximum F1 score they achieve over 2,000 examples, but take longer to learn and are less efficient than LeastConfidence.

**D Generalizability of Performance**

In the main paper, we present the results of cross-dataset generalization with 5% abuse. In Fig. 5, we demonstrate the equivalent results for all class imbalances and both datasets. In general, tweets is harder to predict than wiki, so we see a larger change in performance when training on tweets and evaluating on wiki. For 50% and 10% abuse, performance is similar across test sets. For 5% abuse, there is a larger difference especially for the random baseline. However, in all cases, the performance of the LeastConfidence strategy generalizes well to out-of-domain testing, at least for these two datasets which are similar in their proportion of explicit abuse (Wiegand et al., 2019).
Figure 6: Learning curves per dataset-class imbalance pair showing the effect of isolated experimental variables on traditional (SVM) and transformers-based (dBERT) active learning.
A Lightweight yet Robust Approach to Textual Anomaly Detection

Leslie Barrett, Robert Kingan, Alexandra Ortan and Madhavan Seshadri
Bloomberg LP
{lbarrett4, rkingan, aortan, mseshadri}@bloomberg.net

Abstract
Highly imbalanced textual datasets continue to pose a challenge for supervised learning models. However, viewing such imbalanced text data as an anomaly detection (AD) problem has advantages for certain tasks such as detecting hate speech, or inappropriate and/or offensive language in large social media feeds. There the unwanted content tends to be both rare and non-uniform with respect to its thematic character, and better fits the definition of an anomaly than a class. Several recent approaches to textual AD use transformer models, achieving good results but with trade-offs in pre-training and in-flexibility with respect to new domains. In this paper we compare two linear models within the NMF family, which also have a recent history in textual AD. We introduce a new approach based on an alternative regularization of the NMF objective. Our results surpass other linear AD models and are on par with deep models, performing comparably well even in very small outlier concentrations.

1 Introduction
Anomaly detection (AD), also known as Outlier Detection, is a well-researched area of machine learning. Traditional machine learning approaches to AD include proximity-based models where points that are separated from the rest of the data by a certain distance are considered outliers. These fall into several subclasses. There are cluster-based methods, such as k-means (MacQueen, 1967), where the point is an outlier if there is a large distance between the point and the nearest cluster, density-based methods, such as LOF (Breunig et al., 2000) and DBSCAN (Ester et al., 1996), where an object is an outlier if its density is lower than that of its neighbors and distance-based methods, such as k-NN (Cover and Hart, 1967), where the outlier neighborhood has few other points.

Most recently, Transformer models (Manolache et al., 2021) and word embeddings with multi-head self-attention (Ruff et al., 2019) have been applied in textual AD models, surpassing previously top-performing reconstruction-based approaches using Non-negative Matrix Factorization (NMF) as in (Kannan et al., 2017).

But detecting hate speech and offensive language is a challenging task because these may take various forms, change dynamically and be found in only a small minority of relatively short texts. Recent studies (Yin and Zubiaga, 2021) have pointed to concerns about generalizing results where even the best performing models show large variances in quality from one dataset to another in this domain.

We propose a new NMF-based approach as an alternative to recent transformer models. We improve upon previous NMF outlier detection approaches by replacing the usual squared norm of the error term in the objective function by a correntropy-based metric, which we argue is better tailored for textual outliers. This approach, we argue, is not only well-suited to the task of textual AD in general due to its lightweight architecture and flexibility but is also the better choice versus recent supervised models for hate-speech detection.

This paper is organized as follows: Previous approaches are discussed in Section 2, Data and Methods are discussed in Section 3, our results are in Section 4 and the Conclusion and plans for future work in section 5. Code to reproduce our results can be found here: (github repo provided upon acceptance)

2 Previous Work
While Anomaly Detection in text does not have a particularly deep history in the literature, there is some notable research. For example, Guthrie (2008) and Guthrie et al. (2007) consider texts that are unusual because of author, genre, style or emotional tone.

Peng et al. (2014), analyzed idiom recognition as a type of outlier detection. Idioms have certain key properties that make detection more likely using methods for finding outliers. Examples in English include “kick the bucket” or “have a cow” where the non-compositionality yields highly unusual lexical properties that can be recognized as anomalies.

Other studies (Manevitz and Yousef (2002), Kannan et al. (2017), Barrett et al. (2019), Ruff et al. (2019), Manolache et al. (2021)), treat textual anomalies as top-i ca intrusions, where the texts from one topic constitute the “inliers” and a smaller set of intrusion texts constitute the “outliers”. We use this data definition for our anomaly detection task.

Among topic-intrusion type models, the cur-
rently best-performing is the transformer approach in Manolache et al. (2021), a discriminator-generator model that outperformed the previously top performing OCSVM approach in Ruff et al. (2019). A non-negative matrix factorization model was used in Kannan et al. (2017). All three approaches have outperformed traditional AD models like Isolation Forests (Désir et al., 2013) on text.

3 Proposed Methods

We propose a lightweight alternative Non-negative Matrix Factorization (NMF) model that improves upon the results of Kannan and also provides comparable results to deep models without pre-training, or attention layers. We use simple frequency-based document representations and do not rely on trained embeddings. We show results on benchmark datasets and also on a dataset of hate speech in order to show the power and adaptability of our approach to an important NLP problem. Overall, our model is tested on four datasets in multiple combinations with different outlier-inlier concentrations.

Matrix factorization models like TONMF find outliers through a reconstruction process that isolates outlier documents as residual noise. In this approach, \( A \) is the term-document matrix where terms correspond to rows and documents correspond to columns, \( W \) is the term-topic matrix and \( H \) is the topic-document matrix. The residual matrix \( Z \) is intended to capture outliers depending on the configuration of its norm. The idea is that if a document is not representable as a linear combination of topics, the corresponding column in \( Z \) will have more entries. The quality of the result depends on manipulating norms on both the residual matrix and the low-rank approximation of the input matrix. Kannan et al. (2017) for example use the following optimization:

\[
\arg \min_{W \geq 0, H \geq 0, Z} \frac{1}{2} \|A - WH - Z\|_F^2 + \alpha \|Z\|_{1,2} + \beta \|H\|_1
\]

Here, the standard Frobenius norm is applied to the main error term. The \( \ell_{1,2} \) penalty norm is applied to the outlier matrix \( Z \) in order to minimize the sum of \( \ell_2 \) column norms, which can be seen as the outlier scores of each document. The last term is added for regularization, to produce a more interpretable low rank matrix \( WH \) with sparse coefficients. The \( \alpha \) and \( \beta \) parameters control the weight of the residual and regularization terms over the recovery of a low-rank approximation to \( A \).

3.1 Matrix Factorization with Additional Constraints

We used the basic model architecture in Kannan et al. (2017) to gauge the effect of changing the main objective function. This design includes a residual matrix representing the outlying points not producible by the main factorization process.

We set up two competing NMF-based models. Our baseline model is a hierarchical least-squares (HALS) approach (Cichocki et al., 2008), which is the base model architecture of Kannan et al. (2017). HALS solves the non-negative least squares sub-problem by updating each column of \( W \) separately, and generally can converge to a stationary point. Each column of \( W \) is successively updated, using gradient descent to solve each column-wise sub-problem. This has been shown to converge faster than a matrix-wise iterative updating procedure (Cichocki et al., 2008). We refer to this approach as H-NMF, henceforth in this paper.

3.2 Alternative Updating

Our experimental model uses a different updating approach entirely, replacing the squared error function with an alternative. We use an NMF approach leveraging the Correntropy-induced metric (Liu et al., 2006) in which the similarity between two variables (or sub-matrices in the NMF case) is determined through applying the Gaussian kernel to the error term:

\[
V_{\sigma}(x, y) = \frac{1}{n} \sum_{i=1}^{n} k_{\sigma}(x_i - y_i)
\]

where \( k_{\sigma} \) is the kernel function. CIM-based NMF substitutes the squared error on each entry with the kernel function. We take this a step farther following Du et al. (2012), wherein the CIM-based NMF optimizes on the row level, substituting the squared residuals on each row rather than each entry. We combine this optimization with the constrained residual matrix in the objective function as follows:

\[
\frac{1}{2} \sum_{i=1}^{n} [w_i \| (A - Z)_i - W_i H_i \|^2 + \phi(w_i)] + \alpha \|Z\|_{1,2}
\]

where the weight factor is defined as:

\[
w_i = \exp \left( - \frac{\| (A - Z)_i - W_i H_i \|^2}{2\sigma^2} \right)
\]

The half-quadratic optimization method used here and in Du et al. (2012) has been used in the past to detect and correct errors in facial recognition problems (He et al., 2014). This method sets up a robust strategy for identifying text segments that are topically anomalous not just because of bursty word distributions but because of the topicality of the entire segment. We refer to this approach as R-NMF, henceforth in this paper.

Both our baseline and experimental models leave the residual matrix constraints fixed and focus on the main objective function, in an effort to improve the quality of outliers that are passed as residuals.

4 Experimental Results

Below we describe the datasets and preparation. All models were run on four public datasets representing distinct genres (listserv, news, wiki and hate speech). We used three outlier-inlier concentrations for each.
4.1 Data and Experimental Design

The 20Newsgroups dataset is a publicly available collection of approximately 20,000 newsgroup documents organized into 20 topical subgroups. Some newsgroups are similar (e.g., IBM/Mac hardware), while others are highly unrelated (e.g., for sale/Christian religion).

Reuters-21578 is a publicly available dataset of stories appearing on Reuters’ newswire in 1987. It contains 21,578 documents indexed and assigned categories by members of the Reuters Ltd. staff.

WikiPeople is the subset of the English language Wikipedia dump consisting of the 945,662 articles in the category “living people”.

Our dataset of Hate Speech is from de Gibert et al. (2018) and contains 9,916 samples in total of forum posts from Stormfront, a white-supremacy based forum where the “hate” class represents 11 percent of the corpus.

For each dataset, we blend the inlier classes listed in Table 1 with a sample from the outlier class to achieve three concentrations: .01, .025 and .05. The size of these concentrations is based on rare event analysis where such events have a chance of occurrence of < 0.05. In this case it would correspond to selecting an anomalous sample from our dataset. When such a sample is too small, we omit the .01 concentration. Our strategy for selecting inlier and outlier samples was to select topics that had reasonably close topical content. That is, avoiding highly diverse samples which might make the classification task easier than it should be to create a robust test of the compared approaches.

When evaluating, we take the number of top results corresponding to our outlier concentration and record the number of actual outlier samples in that concentration.

For both NMF models, we parse the input text into word count vectors using sklearn’s CountVectorizer with all default parameters. We call the factorization routine on the sparse word-document matrix to obtain low-rank matrices W and H and outlier matrix Z. Following the methodology in Kannan et al. (2017), we then use the \( \ell_2 \) norm of each column in the Z matrix as the outlier score for every document. For both models, we use 3 CPU cores with 8 GB RAM.

We also train the DATE model (Manolache et al., 2021) on our data as a benchmark, as it represents the current SOTA on textual AD. We use the the code provided by the authors to run experiments. We use a learning rate of \( 1e^{-5} \) and sequences of maximum length 128. Training is stopped at convergence, which occurs after 5000 steps on average. We use the same evaluation framework as proposed by the authors to report results. For the DATE experiments, we use 2 Tesla V100 GPU nodes each with 32 GB RAM and 6 CPU cores.

4.2 Model Results

We show results from H-NMF, R-NMF and the DATE model of Manolache et al. (2021). Model results are shown in Table 1. We list the AUC results for each dataset for each sample and concentration, along with the inlier and outlier classes we used to create each sample. For background on reporting AD model quality as AUC see Aggarwal (2016). The size of the inlier class is listed in parenthesis below the inlier class name. The outliers are sampled at random from the outlier class so as to achieve the specified outlier/inlier concentration.

Winners are shown in bold.

The results are the best from a sweep of eight values of the hyper-parameter \( k \) within the range [1,128] and 5 values of alpha within the range [1,16], for both the H-NMF baseline and R-NMF. The beta parameter, commonly used for the degree of sparseness is only used for H-NMF, and there we use a sweep in the range [1,16].

4.3 Results Analysis

The results show that the rCIM model (R-NMF) outperforms baseline (H-NMF) overall and in particular on Reuters and WikiPeople but is outperformed by DATE on 20Newsgroups and Reuters in the larger concentrations using the “trade” class as outliers. For the Hate Speech corpus, rCIM does better in the lowest concentration, whereas HALS has a slight edge in larger concentrations. Both NMF-based models outperform DATE on this dataset in all concentrations. DATE generally seems to favor the larger concentrations slightly but the NMF-based approaches do not show that same trend.

All models achieved the best AUC on the Reuters data, with the more challenging datasets being WikiPeople and 20Newsgroups. The greatest difference between the two NMF-based approaches is found on the Reuters data where rCIM has the stronger results. Note that the results are better for all three models when the outlier class is “trade” than when it is “interest”, possibly because the “interest” topic is more closely related to and thus harder to distinguish from the inlier topics “earn” and “acq”.

In the Hate Speech data, both NMF-based models outperform the transformer-based model. In addition our model required considerably fewer compute resources, running on 3 CPU cores, compared to 2 GPUs and 6 cores for the transformer. Other recent supervised models trained on Hate Speech alone (not developed for AD) (Wullach et al. (2021)), show good performance for corpora including the de Gibert et al. (2018), but...
Table 1: AUROC Results. Bolded values indicate the best performance for each dataset blend.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Inliers</th>
<th>Outliers</th>
<th>Concentration</th>
<th>H-NMF</th>
<th>R-NMF</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>20Newsgroups</td>
<td>pc/mac.hardware</td>
<td>ms-windows.misc</td>
<td>0.025</td>
<td>0.600</td>
<td>0.592</td>
<td>0.650</td>
</tr>
<tr>
<td></td>
<td>(2000)</td>
<td></td>
<td>0.05</td>
<td>0.543</td>
<td>0.559</td>
<td>0.767</td>
</tr>
<tr>
<td>20Newsgroups</td>
<td>pc/mac.hardware</td>
<td>comp.windows.x</td>
<td>0.025</td>
<td>0.567</td>
<td>0.595</td>
<td>0.691</td>
</tr>
<tr>
<td></td>
<td>(2000)</td>
<td></td>
<td>0.05</td>
<td>0.557</td>
<td>0.555</td>
<td>0.712</td>
</tr>
<tr>
<td>Reuters-21578</td>
<td>earn+acq</td>
<td>interest</td>
<td>0.01</td>
<td>0.741</td>
<td>0.769</td>
<td>0.691</td>
</tr>
<tr>
<td></td>
<td>(5795)</td>
<td></td>
<td>0.025</td>
<td>0.725</td>
<td>0.766</td>
<td>0.712</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.05</td>
<td>0.716</td>
<td>0.777</td>
<td>0.725</td>
</tr>
<tr>
<td>Reuters-21578</td>
<td>earn+acq</td>
<td>trade</td>
<td>0.01</td>
<td>0.871</td>
<td>0.889</td>
<td>0.886</td>
</tr>
<tr>
<td></td>
<td>(5795)</td>
<td></td>
<td>0.025</td>
<td>0.826</td>
<td>0.859</td>
<td>0.905</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.05</td>
<td>0.848</td>
<td>0.877</td>
<td>0.894</td>
</tr>
<tr>
<td>WikiPeople</td>
<td>life</td>
<td>career</td>
<td>0.025</td>
<td>0.675</td>
<td>0.694</td>
<td>0.548</td>
</tr>
<tr>
<td></td>
<td>(5000)</td>
<td></td>
<td>0.05</td>
<td>0.690</td>
<td>0.707</td>
<td>0.617</td>
</tr>
<tr>
<td>Hate Speech</td>
<td>noHate</td>
<td>hate</td>
<td>0.01</td>
<td>0.688</td>
<td>0.702</td>
<td>0.508</td>
</tr>
<tr>
<td></td>
<td>(9507)</td>
<td></td>
<td>0.025</td>
<td>0.697</td>
<td>0.693</td>
<td>0.499</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.05</td>
<td>0.679</td>
<td>0.675</td>
<td>0.505</td>
</tr>
</tbody>
</table>

5 Conclusion and Future Work

Although recent approaches to textual Anomaly Detection using deep models are very robust, our rCIM model on the other hand shows the best performance on very small concentrations. Since posts containing hate speech or offensive language tend to be in a small minority in the real world, our model is ideally suited for practical application and does not have to compensate for data imbalance issues.

6 Ethical Considerations

Anomaly detection is a type of classification model which may have imperfect Precision and Recall. As such it may classify hateful or toxic language incorrectly and should be subject to human review in contexts of high risk. Risks if deployed in the context of a real listserv or subscription media product could include users being banned due to false positive outputs as well as unwanted or offensive posts being allowed due to false negatives.
A Appendix: Examples

Examples of Hate Speech from the de Gibert et al. (2018) corpus are shown in Table 2.

<table>
<thead>
<tr>
<th>TEXT</th>
<th>CLASS</th>
</tr>
</thead>
<tbody>
<tr>
<td>As of March 13th, 2014 the booklet had been downloaded over 18,300 times and counting.</td>
<td>no_hate</td>
</tr>
<tr>
<td>In order to help increase it would be great if all Stormfronters who had YouTube accounts could display the following text in the description boxes of their uploaded YouTube videos.</td>
<td>no_hate</td>
</tr>
<tr>
<td>Simply copy and paste the following text into your YouTube videos description boxes.</td>
<td>no_hate</td>
</tr>
<tr>
<td>Click below for a FREE download of a colorfully illustrated 132 page e-book on the Zionist-engineered INTENTIONAL destruction of Western civilization.</td>
<td>hate</td>
</tr>
<tr>
<td>She may or may not be a Jew she seems to think the Blacks won’t kill her alongside every other White they can get their dirty hands on , what a muppet!</td>
<td>hate</td>
</tr>
<tr>
<td>Thank you for posting your story.</td>
<td>no_hate</td>
</tr>
<tr>
<td>I think you should write a book as well.</td>
<td>no_hate</td>
</tr>
<tr>
<td>And the sad thing is the white students at those schools will act like that too.</td>
<td>hate</td>
</tr>
</tbody>
</table>

Table 2: Examples of inliers (no_hate) and outliers (hate) from the hate speech dataset.

B Appendix: Hyper-parameters

The hyper-parameter values that yielded the best results for each dataset blend. These were obtained from a sweep of eight values of k within the range [1,128], 5 values of alpha within the range [1,16], and 5 values of beta within the range [1,16]. The beta parameter is only used for H-NMF.
<table>
<thead>
<tr>
<th>Dataset</th>
<th>Inliers/Outliers</th>
<th>Concentration</th>
<th>Best Model</th>
<th>k</th>
<th>alpha</th>
<th>beta</th>
</tr>
</thead>
<tbody>
<tr>
<td>20Newsgroups</td>
<td>pc/mac.hardware</td>
<td>0.025</td>
<td>H-NMF</td>
<td>100</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>ms-windows.misc</td>
<td>0.05</td>
<td>R-NMF</td>
<td>64</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>20Newsgroups</td>
<td>pc/mac.hardware</td>
<td>0.025</td>
<td>R-NMF</td>
<td>64</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>comp.windows.x</td>
<td>0.05</td>
<td>H-NMF</td>
<td>32</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Reuters-21578</td>
<td>earn+acq</td>
<td>0.01</td>
<td>R-NMF</td>
<td>16</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interest</td>
<td>0.025</td>
<td>R-NMF</td>
<td>16</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.05</td>
<td>R-NMF</td>
<td>16</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Reuters-21578</td>
<td>earn+acq</td>
<td>0.01</td>
<td>R-NMF</td>
<td>16</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td></td>
<td>trade</td>
<td>0.025</td>
<td>R-NMF</td>
<td>8</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.05</td>
<td>R-NMF</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>WikiPeople</td>
<td>life</td>
<td>0.025</td>
<td>R-NMF</td>
<td>8</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td></td>
<td>career</td>
<td>0.05</td>
<td>R-NMF</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Hate Speech</td>
<td>noHate</td>
<td>0.01</td>
<td>R-NMF</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hate</td>
<td>0.025</td>
<td>H-NMF</td>
<td>8</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.05</td>
<td>H-NMF</td>
<td>16</td>
<td>8</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 3: Best hyper-parameters for each dataset blend.
Detection of Negative Campaign in Israeli Municipal Elections
Natalia Vanetik Sagiv Talker Or Machlouf Marina Litvak

Department of Software Engineering
Shamoon College of Engineering
{natalyav,Orma5,Sagivta,marinal}@ac.sce.ac.il

Abstract

Political competitions are complex settings where candidates use campaigns to promote their chances to be elected. One choice focuses on conducting a positive campaign that highlights the candidate’s achievements, leadership skills, and future programs. The alternative is to focus on a negative campaign that emphasizes the negative aspects of the competing person and is aimed at offending opponents or the opponent’s supporters. In this proposal, we concentrate on negative campaigns in Israeli elections. This work introduces an empirical case study on automatic detection of negative campaigns, using machine learning and natural language processing approaches, applied to the Hebrew-language data from Israeli municipal elections. Our contribution is multi-fold: (1) We provide TONIC—daTaset fOr Negative poLitical Campaign in Hebrew—which consists of annotated posts from Facebook related to Israeli municipal elections; (2) We introduce results of a case study, that explored several research questions. RQ1: Which classifier and representation perform best for this task? We employed several traditional classifiers which are known for their excellent performance in IR tasks and two pre-trained models based on BERT architecture; several standard representations were employed with traditional ML models. RQ2: Does a negative campaign always contain offensive language? Can a model, trained to detect offensive language, also detect negative campaigns? We are trying to answer this question by reporting results for the transfer learning from a dataset annotated with offensive language to our dataset. RQ3: Does a negative campaign necessarily express negative sentiment? Can sentiment analysis help to detect negative campaigns? We experiment with sentiment labels to enrich data representation and report our findings.

Our dataset and pre-trained models will be freely available for researchers.

1 Introduction

Political competitions aim at promoting the candidates’ chances to be elected. The main decision in such competitions regards the nature of the campaign – that is, whether a candidate should apply a positive campaign that highlights the candidate’s achievements, leadership skills, and future programs, or focus on a negative campaign that emphasizes the negative sides of the competitors (Bernhardt and Ghosh, 2020; Invernizzi, 2019; Martin, 2004; Skaperdas and Grofman, 1995).

Our work introduces a new dataset of Facebook posts, published by candidates during municipal elections in Israel. We annotated this dataset with binary labels, where we distinguish between negative campaigns and other campaign-related content. In addition to the dataset, we report the results of extensive experiments, aimed at answering multiple research questions: Which supervised model and representation are more effective at automatically detecting negative campaigns? Can we effectively detect negative campaigns with a model trained to identify offensive language? Can sentiment analysis boost negative campaign detection?

Our contribution is multi-fold: (1) We introduce a new annotated dataset in Hebrew for negative political Campaign in Hebrew—which consists of annotated posts from Facebook related to Israeli municipal elections; (2) We introduce results of a case study, that explored several research questions. RQ1: Which classifier and representation perform best for this task? We employed several traditional classifiers which are known for their excellent performance in IR tasks and two pre-trained models based on BERT architecture; several standard representations were employed with traditional ML models. RQ2: Does a negative campaign always contain offensive language? Can a model, trained to detect offensive language, also detect negative campaigns? We are trying to answer this question by reporting results for the transfer learning from a dataset annotated with offensive language to our dataset. RQ3: Does a negative campaign necessarily express negative sentiment? Can sentiment analysis help to detect negative campaigns? We experiment with sentiment labels to enrich data representation and report our findings.

2 Related Work

The scholarly literature has investigated various aspects related to negative campaigns (Asunka et al., 2019; Chaturvedi, 2005; Martin, 2004; Skaperdas and Grofman, 1995). It points out that this phenomenon exists in many areas such as competition over jobs in the workplace, yet in the politi-
cal arena there are several special characteristics. A major characteristic is a fact that participants in electoral competition often hold positions of power as well as public and private resources to finance their efforts (Bernhardt and Ghosh, 2020; Invernizzi, 2019). In many cases, they also set the rules of the competition as opposed to other areas where the contest organizer sets the rules of the game. Indeed, in recent years, we witness more and more political candidates that do not play by the rules, both formally and informally. A specific feature of this trend is the intensive use of negative campaigns which target the weaknesses and failures of the opponents promising to do the opposite (Invernizzi, 2019; Martin, 2004; Skaperdas and Grofman, 1995).

The implementation of language technologies in the political sciences is recently in high demand. While computational political scientists are looking for NLP tools to assist automatic analysis of campaign-related content and predict outcomes, computational linguistics explores real-world use cases in political domains. The recent Workshop on Natural Language Processing for Political sciences (PoliticalNLP) (Afli et al., 2022) is an example of the rising popularity of this interdisciplinary research. However, despite some works dedicated to the analysis of elections-related materials (Baran et al., 2022; Abdine et al., 2022; Sanders and van den Bosch, 2022), in this workshop or anywhere else, we were unable to find any work on automated negative campaign analysis and detection.

As a majority of text classification tasks last years are efficiently performed by pre-trained language models and transformers, we follow this approach in our study. We apply BERT, its multilingual (mBERT) and Hebrew (AlephBERT) versions. mBERT serves us both as an encoder (feature extractor) and end-to-end classifier.

1 We did not apply AlephBERT as feature extractor because its implementation does not comply with the sentence transformers package and does not allow extraction of sentence vectors.

3 Case Study

3.1 TONIC dataset

The data was collected from Facebook accounts of local politicians from several big Israeli cities running for mayor’s offices. There were total of 12 cities and 27 mayor candidates whose number for elections that took place in 2018. Data statistics appear in Table 1. The data is freely available for download from GitHub at https://github.com/NataliaVanetik1/TOMIC.

Table 3 displays two instances of comments from the TONIC dataset that have been translated into English.

The collected posts were first manually filtered as related or unrelated to political campaigns, and only campaign-related messages were kept. Those texts were annotated as either negative or not by two independent annotators; in case of a disagreement between them, the third annotator decided on a final label. The annotators were instructed to label a post as “negative campaign” only if it contained a negative (but not necessarily offensive) content about the opponent of the post’s owner or her supporter. Kappa agreement between the annotators was 0.862, which is considered to be an excellent agreement. The statistics for campaign-related posts for all cities are given in Table 2.

3.2 Method

Our approach to text representation and classification consists of the following steps:

1. Representing texts with one of the following:
   - tf*idf vectors, where every post is treated as a separate document;
   - character n-grams with n = 1, 2, 3;
   - pre-trained BERT vectors obtained from a multilingual BERT model (Sanh et al., 2019).

2. Enhancing the above representations with sentiment weights produced by the pre-trained HeBERT model (Chriqui and Yahav, 2021). This model produces weights as a probability distribution for positive, negative, and neutral sentiments.

3. Training and application of supervised ML models (see Section 3.4) on all of the above data representations.

The approach is depicted in Figure 1.
3.3 Data representation

We employed three different representation models for input texts, as follows.

**Tf-idf**, short for term frequency-inverse document frequency, is a numerical statistic that is intended to reflect how important a word is to a document in a collection or corpus. The tf-idf value increases proportionally to the number of times a word appears in the document and is offset by the number of documents in the corpus that contain the word. In our case, we treated every post as a separate document and the whole dataset as a corpus.

**N-grams** are the sequences of \( n \) consecutive words seen in the text, where \( n \) is a parameter. In our evaluation, we used the values \( n = 1, 2, 3 \).
BERT sentence embeddings of length 512 were obtained using the pre-trained multilingual BERT model trained in 104 languages, including Hebrew.

3.4 Models

We applied three traditional ML algorithms—Random Forest (RF) (Pal, 2005), Logistic Regression (LR) (Wright, 1995), and Extreme Gradient Boosting (XGB) (Chen et al., 2015). All three were applied to texts represented by each of three representations, described in Section 3.3.

Also, we employed the BERT transformer (Devlin et al., 2018) trained for sentence classification. We applied two different pre-trained models for our task. The first one is a multilingual model called bert-base-multilingual-cased (denoted as mBERT) introduced in (Devlin et al., 2018). The second is the AlephBERT (Seker et al., 2021), a large pre-trained language model for Modern Hebrew, which is trained on a larger vocabulary and a larger dataset than any Hebrew pre-trained language model before. Both of these models were fine-tuned on the train portion of our data.

3.5 Experiments

Our experiments aim at evaluation of and comparison of various models and text representations for the purpose of detecting negative campaigns in political posts. Additionally, we explore two research questions.

In the first question, we want to understand whether general offensive language data in the same language (Hebrew) can be used for transfer learning with the proposed methodology. For answering that, we perform cross-domain experiments with a dataset with Hebrew messages annotated with offensive language.

In the second question, we explore whether the sentiment analysis can boost the negative campaign detection accuracy. For answering that, we compare between performance scores of our models with and without sentiment labels in the data representation.

3.6 Data Setup

For the experiments on TONIC, RF, LR, and XGB were trained on 80% of the data and evaluated on the remaining 20%. Fine-tuned BERT was trained a 75% of the data with the validation set containing 5% of the data, and it was tested on the remaining 20%. Fine-tuning was run for 10 epochs with batch size 16.

For the cross-domain experiments, we used the Hebrew offensive language dataset (Litvak et al., 2021) called OLaH. It is composed of Facebook comments written in Hebrew and annotated by humans. The dataset contains 2,025 annotated comments, out of which 821 are labeled positive (i.e., they do contain offensive content).

3.7 Software Setup

For the purpose of reproducibility, we present below the setup of our experiments. All non-neural models are implemented in sklearn (Pedregosa et al., 2011) python package. Our neural model is implemented with Keras (Chollet et al., 2015) with the TensorFlow backend (Abadi et al., 2015). Experiments were performed on google colab (Bisong, 2019) with standard settings and GPU runtime type. Runtime for every experiment setting (mono- or cross-domain) was less than 10 minutes.

3.8 Evaluation Results

Table 4: Mono-domain evaluation results on the TONIC dataset

<table>
<thead>
<tr>
<th>Model</th>
<th>P</th>
<th>R</th>
<th>F1</th>
<th>Acc</th>
<th>P</th>
<th>R</th>
<th>F1</th>
<th>Acc</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlephBERT</td>
<td>0.7318</td>
<td>0.6616</td>
<td>0.6949</td>
<td>0.7040</td>
<td>0.7288</td>
<td>0.6792</td>
<td>0.7031</td>
<td>0.7590</td>
</tr>
<tr>
<td>mBERT</td>
<td>0.8004</td>
<td>0.5490</td>
<td>0.6513</td>
<td>0.8008</td>
<td>0.8507</td>
<td>0.6550</td>
<td>0.7401</td>
<td>0.8425</td>
</tr>
<tr>
<td>RF_{f1df}</td>
<td>0.7774</td>
<td>0.5597</td>
<td>0.6508</td>
<td>0.8027</td>
<td>0.8517</td>
<td>0.6877</td>
<td>0.7610</td>
<td>0.8539</td>
</tr>
<tr>
<td>RF_{f1df+SA}</td>
<td>0.8157</td>
<td>0.5414</td>
<td>0.6508</td>
<td>0.7989</td>
<td>0.8372</td>
<td>0.6168</td>
<td>0.7103</td>
<td>0.8273</td>
</tr>
<tr>
<td>RF_{nq1}</td>
<td>0.7711</td>
<td>0.5329</td>
<td>0.6239</td>
<td>0.7913</td>
<td>0.8482</td>
<td>0.6506</td>
<td>0.7364</td>
<td>0.8406</td>
</tr>
<tr>
<td>RF_{nq2}</td>
<td>0.8485</td>
<td>0.5383</td>
<td>0.6587</td>
<td>0.7989</td>
<td>0.8508</td>
<td>0.7355</td>
<td>0.7890</td>
<td>0.8691</td>
</tr>
<tr>
<td>RF_{nq3}</td>
<td>0.7731</td>
<td>0.5338</td>
<td>0.6329</td>
<td>0.7931</td>
<td>0.8530</td>
<td>0.7399</td>
<td>0.7924</td>
<td>0.8710</td>
</tr>
<tr>
<td>LRF_{f1df}</td>
<td>0.7341</td>
<td>0.6571</td>
<td>0.6935</td>
<td>0.8159</td>
<td>0.8474</td>
<td>0.7928</td>
<td>0.8192</td>
<td>0.8843</td>
</tr>
<tr>
<td>LRF_{f1df+SA}</td>
<td>0.6551</td>
<td>0.6491</td>
<td>0.6521</td>
<td>0.7685</td>
<td>0.7455</td>
<td>0.7501</td>
<td>0.7478</td>
<td>0.8273</td>
</tr>
<tr>
<td>LRF_{nq1}</td>
<td>0.6551</td>
<td>0.6491</td>
<td>0.6521</td>
<td>0.7685</td>
<td>0.7455</td>
<td>0.7501</td>
<td>0.7478</td>
<td>0.8273</td>
</tr>
<tr>
<td>LRF_{nq2}</td>
<td>0.7864</td>
<td>0.6075</td>
<td>0.6855</td>
<td>0.8178</td>
<td>0.8096</td>
<td>0.7851</td>
<td>0.7972</td>
<td>0.8672</td>
</tr>
<tr>
<td>LRF_{nq3}</td>
<td>0.8195</td>
<td>0.5948</td>
<td>0.6893</td>
<td>0.8178</td>
<td>0.8072</td>
<td>0.7699</td>
<td>0.7881</td>
<td>0.8634</td>
</tr>
<tr>
<td>LRF_{nq+1+SA}</td>
<td>0.8151</td>
<td>0.7724</td>
<td>0.7932</td>
<td>0.8672</td>
<td>0.8007</td>
<td>0.5892</td>
<td>0.6789</td>
<td>0.8140</td>
</tr>
<tr>
<td>LRF_{nq1+SA}</td>
<td>0.8303</td>
<td>0.7879</td>
<td>0.8085</td>
<td>0.8767</td>
<td>0.7168</td>
<td>0.5978</td>
<td>0.6519</td>
<td>0.8027</td>
</tr>
<tr>
<td>LRF_{nq2+SA}</td>
<td>0.8121</td>
<td>0.7787</td>
<td>0.7950</td>
<td>0.8672</td>
<td>0.7241</td>
<td>0.5991</td>
<td>0.6557</td>
<td>0.8046</td>
</tr>
<tr>
<td>LRF_{nq3+SA}</td>
<td>0.8072</td>
<td>0.7699</td>
<td>0.7881</td>
<td>0.8634</td>
<td>0.6733</td>
<td>0.5798</td>
<td>0.6231</td>
<td>0.7894</td>
</tr>
<tr>
<td>LRF_{bert}</td>
<td>0.8208</td>
<td>0.7887</td>
<td>0.8044</td>
<td>0.8729</td>
<td>0.8208</td>
<td>0.7887</td>
<td>0.8044</td>
<td>0.8729</td>
</tr>
</tbody>
</table>

Evaluation results for the TONIC dataset as both train and test sets are presented in Table 4. We can
make the following conclusions from these results.

First, there is a shred of strong evidence that sentiment labels boost classification performance. Second, the best recall, f-measure, and accuracy were produced by LR with unigrams enriched with sentiment labels, and the best precision was obtained by the same LR but with tf-idf and sentiment labels.

3.9 Error Analysis
We used the top-performing model (LRng1 + SA) to analyze the misclassification errors in the monodomain classification instance (Logistic Regression with unigrams and sentiment labels as a text representation). This model’s confusion matrix is as follows: \( TP = 72, \quad TN = 394, \quad FP = 19, \quad FN = 42 \), with precision of 0.79 and recall of 0.63 respectively. These results show that the model does a good job of identifying and eliminating negative samples (non-negative campaigns), but it misses positive samples (negative campaign). As a result, \( TN \) is the most important accuracy compound, while \( FN \) represents the biggest amount of errors.

In a 30 misclassified case sample that we manually examined, 22 cases are from the \( FN \) group and only 8 cases are from the \( FP \) category. The majority of errors (23), including 19 samples incorrectly identified as negative campaigns when we actually found them to be neutral and 4 samples incorrectly labeled as neutral, were the result of incorrect labeling by our annotators. Due to a variety of factors, the model incorrectly classified four neutral posts as negative campaigns, including one sample that was actually negative but was correctly categorized as neutral because it wasn’t addressed to a specific person, and two samples that contained words that were likely to have influenced the classification. One sample was incorrectly categorized for an unidentified reason; the cause is likely due to the negative campaign writing style, which is characterized by frequent mentions of individuals. The model missed three unfavorable marketing materials, most likely as a result of the neutral vocabulary (no offensive content in these samples).

<table>
<thead>
<tr>
<th>Model</th>
<th>P</th>
<th>R</th>
<th>F1</th>
<th>Acc</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlephBERT</td>
<td>0.4988</td>
<td>0.3916</td>
<td>0.4387</td>
<td>0.7818</td>
</tr>
<tr>
<td>mBERT</td>
<td>0.5135</td>
<td><strong>0.6025</strong></td>
<td>0.5545</td>
<td>0.7799</td>
</tr>
<tr>
<td>RF jerkdf</td>
<td>0.4536</td>
<td>0.4959</td>
<td><strong>0.4738</strong></td>
<td>0.7723</td>
</tr>
<tr>
<td>RF jerkdf+SA</td>
<td>0.5356</td>
<td>0.5054</td>
<td>0.5201</td>
<td>0.7723</td>
</tr>
<tr>
<td>RF ng1</td>
<td>0.4530</td>
<td>0.4779</td>
<td>0.4651</td>
<td>0.7192</td>
</tr>
<tr>
<td>RF ng1+SA</td>
<td>0.5599</td>
<td>0.5079</td>
<td>0.5326</td>
<td>0.7761</td>
</tr>
<tr>
<td>RF ng2</td>
<td>0.4779</td>
<td>0.4886</td>
<td>0.4832</td>
<td>0.7211</td>
</tr>
<tr>
<td>RF ng2+SA</td>
<td>0.5222</td>
<td>0.5072</td>
<td>0.5146</td>
<td>0.7552</td>
</tr>
<tr>
<td>RF ng3</td>
<td>0.4727</td>
<td>0.4867</td>
<td>0.4796</td>
<td>0.7230</td>
</tr>
<tr>
<td>RF ng3+SA</td>
<td>0.5031</td>
<td>0.5009</td>
<td>0.5020</td>
<td>0.7552</td>
</tr>
<tr>
<td>RF nert</td>
<td>0.3910</td>
<td>0.4952</td>
<td>0.4370</td>
<td>0.7761</td>
</tr>
<tr>
<td>RF nert+SA</td>
<td>0.4628</td>
<td>0.4971</td>
<td>0.4793</td>
<td>0.7742</td>
</tr>
<tr>
<td>LR jerkdf</td>
<td>0.3918</td>
<td>0.5000</td>
<td>0.4393</td>
<td>0.7837</td>
</tr>
<tr>
<td>LR jerkdf+SA</td>
<td>0.3914</td>
<td>0.4976</td>
<td>0.4382</td>
<td>0.7799</td>
</tr>
<tr>
<td>LR ng1</td>
<td>0.4723</td>
<td>0.4850</td>
<td>0.4786</td>
<td>0.7154</td>
</tr>
<tr>
<td>LR ng1+SA</td>
<td>0.5222</td>
<td>0.5072</td>
<td>0.5146</td>
<td>0.7552</td>
</tr>
<tr>
<td>LR ng2</td>
<td>0.5417</td>
<td>0.5396</td>
<td>0.5406</td>
<td>0.6964</td>
</tr>
<tr>
<td>LR ng2+SA</td>
<td>0.5484</td>
<td>0.5382</td>
<td>0.5433</td>
<td>0.7192</td>
</tr>
<tr>
<td>LR ng3</td>
<td>0.5417</td>
<td>0.5396</td>
<td>0.5406</td>
<td>0.6964</td>
</tr>
<tr>
<td>LR ng3+SA</td>
<td>0.5484</td>
<td>0.5382</td>
<td>0.5433</td>
<td>0.7192</td>
</tr>
<tr>
<td>LR nert</td>
<td>0.4623</td>
<td>0.4942</td>
<td>0.4777</td>
<td>0.7647</td>
</tr>
<tr>
<td>LR nert+SA</td>
<td>0.5592</td>
<td>0.5039</td>
<td>0.5301</td>
<td>0.7799</td>
</tr>
<tr>
<td>XGB jerkdf</td>
<td>0.5352</td>
<td>0.5027</td>
<td>0.5184</td>
<td>0.7780</td>
</tr>
<tr>
<td>XGB jerkdf+SA</td>
<td>0.7265</td>
<td>0.5076</td>
<td>0.5976</td>
<td>0.7856</td>
</tr>
<tr>
<td>XGB ng1</td>
<td>0.4617</td>
<td>0.4914</td>
<td>0.4761</td>
<td>0.7552</td>
</tr>
<tr>
<td>XGB ng1+SA</td>
<td><strong>0.7946</strong></td>
<td>0.5163</td>
<td><strong>0.6259</strong></td>
<td><strong>0.7894</strong></td>
</tr>
<tr>
<td>XGB ng2</td>
<td>0.5315</td>
<td>0.5174</td>
<td>0.5244</td>
<td>0.7362</td>
</tr>
<tr>
<td>XGB ng2+SA</td>
<td>0.6214</td>
<td>0.5262</td>
<td>0.5699</td>
<td>0.7799</td>
</tr>
<tr>
<td>XGB ng3</td>
<td>0.5609</td>
<td>0.5388</td>
<td>0.5496</td>
<td>0.7400</td>
</tr>
<tr>
<td>XGB ng3+SA</td>
<td>0.5789</td>
<td>0.5162</td>
<td>0.5458</td>
<td>0.7742</td>
</tr>
<tr>
<td>XGB nert</td>
<td>0.4680</td>
<td>0.4892</td>
<td>0.4784</td>
<td>0.7419</td>
</tr>
<tr>
<td>XGB nert+SA</td>
<td>0.5460</td>
<td>0.5113</td>
<td>0.5281</td>
<td>0.7666</td>
</tr>
</tbody>
</table>

Cross-domain experiments in Table 5 show that using an offensive language dataset as a training set decreases classification accuracy for all the models, indicating that the task of detecting negative campaigns is different from the task of offensive language detection. Despite enhancing data with SA obviously improve results, only a few models trained on offensive language data achieved accuracy that is slightly higher than or equal to the majority rule. XGB with unigrams and sentiment labels achieved the best precision, f-measure, and accuracy, while the best recall was obtained by mBERT.

4 Future Work and Conclusions
In this paper, we introduce a new dataset that can help researchers to study negative campaigns. The dataset contains only Hebrew-written content posted by Israeli politicians on Facebook. We report the results of extensive experiments which include multiple classifiers and representations and answer two research questions: whether transfer learning from offensive language to negative campaign can be efficiently applied and whether sentiment analysis can boost negative campaign detection. We can conclude that traditional models with unigrams and sentiment labels as text representation performed best in both scenarios. This
is probably due to a small training set which is not sufficient for efficient fine-tuning of pre-trained transformers with a large number of parameters, but big enough to train a relatively simple classification function with fewer parameters. Also, unigrams seem to be most efficient in representing Hebrew texts — due to the rich morphology of Hebrew and ambiguous tokenization, simple BOW (and tf-idf) cannot provide enough semantic information. It also might be the case of political rhetoric which is similar across candidates and campaigns of different political parties. Based on our results, we can conclude that sentiment analysis obviously boosts negative campaign detection. However, there is no strong relation between offensive language and negative campaigns. Therefore, transfer learning with models trained to detect offensive content is inefficient for the detection of a negative campaign.

In the future, we plan to apply our analysis to elections to the Israeli government. We also would like to see whether cross-lingual and cross-country learning is efficient for negative campaign detection. We’d like to explore the common characteristics and differences between political campaigns in different countries. We hypothesize that an engagement of a candidate in a negative campaign can be dependent on the candidate’s gender, perceived strength, initial support, etc. We intend to study these possible relations in the future.

References


François Chollet et al. 2015. Keras. https://github.com/fchollet/keras.


Hypothesis Engineering for Zero-Shot Hate Speech Detection

Janis Goldzycher and Gerold Schneider
Department of Computational Linguistics
University of Zurich
{goldzycher,gschneid}@cl.uzh.ch

Abstract

Standard approaches to hate speech detection rely on sufficient available hate speech annotations. Extending previous work that repurposes natural language inference (NLI) models for zero-shot text classification, we propose a simple approach that combines multiple hypotheses to improve English NLI-based zero-shot hate speech detection. We first conduct an error analysis for vanilla NLI-based zero-shot hate speech detection and then develop four strategies based on this analysis. The strategies use multiple hypotheses to predict various aspects of an input text and combine these predictions into a final verdict. We find that the zero-shot baseline used for the initial error analysis already outperforms commercial systems and fine-tuned BERT-based hate speech detection models on HateCheck. The combination of the proposed strategies further increases the zero-shot accuracy of 79.4% on HateCheck by 7.9 percentage points (pp), and the accuracy of 69.6% on ETHOS by 10.0pp.1

1 Introduction

With the increasing popularity of social media and online forums, phenomena such as hate speech, offensive and abusive language, and personal attacks have gained a powerful medium through which they can propagate fast. Due to the sheer number of posts and comments on social media, manual content moderation has become unfeasible, thus the automatic detection of harmful content becomes essential. In natural language processing, there now exist established tasks with the goal of detecting offensive language (Pradhan et al., 2020), abusive language (Nakov et al., 2021), hate speech (Fortuna and Nunes, 2018) and other related types of harmful content (Poletto et al., 2021). In this work, we focus on the detection of hate speech, which is typically defined as attacking, abusive or discriminatory language that targets people on the basis of identity defining group characteristics such as gender, sexual orientation, disability, race, religion, national origin etc. (Fortuna and Nunes, 2018; Poletto et al., 2021; Yin and Zubiga, 2021). Most current hate speech detection approaches rely on either training models from scratch or fine-tuning pre-trained language models (Jahan and Oussalah, 2021). Both types of approaches need large amounts of labeled data which are only available for a few high-resource languages (Poletto et al., 2021) and costly to create. Therefore, exploring data-efficient methods for hate speech detection is an attractive alternative.

In this paper, we build on Yin et al. (2019) who proposed to re-frame text classification tasks as natural language inference, enabling high accuracy zero-shot classification. We exploit the fact that we can create arbitrary hypotheses to predict aspects of an input text that might be relevant for hate speech detection. To identify effective hypotheses, we first find a well-performing hypothesis formulation that claims that the input text contains hate speech. An error analysis based on HateCheck (Röttger et al., 2021) shows that given a well-performing formulation the model still struggles with multiple phenomena, including (1) abusive or profane language that does not target people based on identity-defining group characteristics, (2) counterspeech, (3) reclaimed slurs, and (4) implicit hate speech. To mitigate these misclassifications, we develop four strategies. Each strategy consists of multiple hypotheses and rules that combine these hypotheses in order to address one of the four identified error types.

We show that the combination of all proposed strategies improves the accuracy of vanilla NLI-based zero-shot prediction by 7.9pp on HateCheck (Röttger et al., 2021) and 10.0pp on ETHOS (Mollas et al., 2022). An error analysis shows that
the overall gains in accuracy largely stem from increased performance on previously identified weaknesses, demonstrating that the strategies work as intended.

Overall, our primary contributions are the following:

C1 An error analysis of vanilla NLI-based zero-shot hate speech detection.

C2 Developing strategies that combine multiple hypotheses to improve zero-shot hate speech detection.

C3 An evaluation and error analysis of the proposed strategies.

2 Background and Related Work

Early approaches to hate speech detection have focused on English social media posts, especially Twitter, and treated the task as binary or ternary text classification (Waseem and Hovy, 2016; Davidson et al., 2017; Founta et al., 2018). In more recent work, additional labels have been introduced that indicate whether the post is group-directed or not, who the targeted group is, if the post calls for violence, is aggressive, contains stereotypes, if the hate is expressed implicitly, or if sarcasm or irony is used (Mandl et al., 2019, 2020; Sap et al., 2020; ElSherief et al., 2021; Röttger et al., 2021; Mollas et al., 2022). Sometimes hate speech is not directly annotated but instead labels, such as racism, sexism, homophobia that already combine hostility with a specific target are annotated and predicted (Waseem and Hovy, 2016; Waseem, 2016; Saha et al., 2018; Lavergne et al., 2020).

While early approaches relied on manual feature engineering (Waseem and Hovy, 2016), most current approaches are based on pre-trained transformer-based language models that are then fine-tuned on hate speech datasets (Florio et al., 2020; Uzan and HaCohen-Kerner, 2021; Banerjee et al., 2021; Lavergne et al., 2020; Das et al., 2021; Nghiem and Morstatter, 2021).

Some work has focused on reducing the need for labeled data by multi-task learning on different sets of hate speech labels (Kapil and Ekbal, 2020; Safi Samghabadi et al., 2020) or adding sentiment analysis as an auxiliary task (Plaza-Del-Arco et al., 2021). Others have worked on reducing the need for non-English annotations by adapting hate speech detection models from high- to low-resource languages in a cross-lingual zero-shot setting (Stappen et al., 2020; Pamungkas et al., 2021). However, the approach has been criticized for being unreliable when encountering language-specific taboo interjections (Nozza, 2021).

2.1 Zero-Shot Text Classification

The advent of large language models has enabled zero-shot and few-shot text classification approaches such as prompting (Liu et al., 2021), and task descriptions (Raffel et al., 2020), which convert the target task to the pre-training objective and are usually only used in combination with large language models. Chiu and Alexander (2021) use the prompts “Is this text racist?” and “Is this text sexist?” to detect hate speech with GPT-3. Schick et al. (2021) show that toxicity in large generative language models can be avoided by using similar prompts to self-diagnose toxicity during the decoding.

In contrast, NLI-based prediction in which a target task is converted to an NLI-task and fed into an NLI model converts the target task to the fine-tuning task. Here, a model is given a premise and a hypothesis and tasked to predict if the premise entails the hypothesis, contradicts it, or is neutral towards it. Yin et al. (2019) proposed to use an NLI model for zero-shot topic classification, by inputting the text to classify as the premise and constructing for each topic a hypothesis of the form “This text is about <topic>”. They map the labels neutral and contradiction to not-entailment. We can then interpret a prediction of entailment as predicting that the input text belongs to the topic in the given hypothesis. Conversely, not-entailment implies that the text is not about the topic. Wang et al. (2021) show for a range of tasks, including offensive language identification, that this task reformulation also benefits few-shot learning scenarios. Recently, AlKhamsi et al. (2022) obtained large performance improvements in few-shot learning for hate speech detection by (1) decomposing the task into four subtasks and (2) additionally training the few-shot model on a knowledge base.

<table>
<thead>
<tr>
<th>name</th>
<th># examples</th>
<th>classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HateCheck</td>
<td>3,728</td>
<td>hateful (64.1%), non-hate (31.2%)</td>
</tr>
<tr>
<td>ETHOS (binary)</td>
<td>997</td>
<td>hate speech (64.1%), not-hate speech (25.9%)</td>
</tr>
</tbody>
</table>

Table 1: The number of examples and the class balance of the datasets.
3 Data

HateCheck  Röttger et al. (2021) introduce this English, synthetic, evaluation-only dataset, annotated for a binary decision between hate speech and not-hate speech. It covers 29 functionalities that are either a type of hate speech or challenging types of non-hate speech that could be mistaken for hate speech by a classifier. The examples for each of these functionalities have been constructed on the basis of conversations with NGO workers. Each of these templates contains one blank space to be filled with a protected group. The authors fill these templates with seven protected groups, namely: women, gay people, transgender people, black people, Muslims, immigrants, and disabled people. Overall the dataset contains 3,728 examples.

ETHOS  The ETHOS dataset (Mollas et al., 2022) is split into two parts: one part is annotated for the presence of hate speech. The other part contains fine-grained annotations that indicate which characteristics have been targeted (gender, sexual orientation, race, ethnicity, religion, national origin, disability), whether the utterance calls for violence, and whether it is directed at an individual or a general statement about a group. The dataset is based on English comments from Youtube and Reddit. For this work, we will only make use of the binary hate speech annotations. These annotations are continuous values between 0 (indicating no hate speech at all) and 1 indicating clear hate speech. We rounded all annotations to either 0 or 1 using a threshold of 0.5.

Table 1 displays the class balances of the two datasets.

4 Evaluating Standard Zero-Shot Prediction

The evaluation of standard zero-shot NLI-based hate speech detection has two goals: To (1) obtain an error analysis that serves as the starting point for developing zero-shot strategies in Section 5, and (2) establish a baseline for those strategies.

Experiment setup  To test if an input text contains hate speech, we need a hypothesis expressing that claim. However, there are many ways how the claim, that a given text contains hate speech, can be expressed. Choosing a sub-optimal way to express this claim will result in lower accuracy. Wang et al. (2021) already tested four different hypotheses for hate speech or offensive language. We conduct an extensive evaluation by constructing and testing all grammatically correct sentences built with the following building blocks: *(Is/That/This + example/text + contains/is hate speech/hateful/hateful content)*. We conduct all experiments with a BART-large model (Lewis et al., 2020) that was fine-tuned on the Multi-Genre Natural Language Inference dataset (MNLI) (Williams et al., 2018) and has been made available via the Huggingface transformers library (Wolf et al., 2020) as bart-large-mnli. This model predicts either contradiction, neutral, or entailment. We follow the recommendation of the model creators to ignore the logits for neutral and perform a softmax over the logits of contradiction and entailment. If the probability for entailment is equal or higher than 0.5 we consider this a prediction of entailment and thus hate speech.\(^3\) We evaluate on HateCheck since the functionalities in this dataset allow for an automatic in-depth error analysis and compare our results to the baselines provided by Röttger et al. (2021).

Results  Table 2 shows an abbreviated version of the results. The full results are given in Appendix A. The hypothesis “That contains hate speech.” obtains the highest accuracy and beats the Google-Jigsaw API by 2.8pp. This is remarkable, since we can assume that the commercial systems were all trained to detect hateful content or hate speech, while this model has not been trained on a single

---

\(^2\)Google Jigsaw has since released a new version of the model powering the Perspective API (Lees et al., 2022). We assume that the new model would score higher on HateCheck.

\(^3\)This procedure is equal to taking the argmax over contradiction and entailment.

---

Table 2: Evaluation of hypotheses for zero-shot hate speech detection on HateCheck. The top rows contain the two lowest scoring hypotheses, the highest scoring hypothesis and the average score for all tested hypotheses. The bottom rows contain the HateCheck baselines computed by Röttger et al. (2021). The full results for all tested hypotheses are listed in Appendix A.
Figure 1: FBT Standard zero-shot entailment predictions would wrongly predict the input text as containing hate speech. Using additional hypotheses it is possible to check if a protected group is targeted and if necessary to override the original prediction.

Figure 2: FCS If a text contains quotations the quoted text is replaced with a variable X using a regular expression. Then, the two hypotheses are tested: The first hypothesis serves as a test checking if the text inside the quotes is hate speech. If that is predicted to be the case, the second hypothesis is used to predict if the quoted text is supported or denounced by the post.

example of hate speech detection or a similar task. The two lowest scoring hypotheses lead to an accuracy of 66.6% meaning that an unlucky choice of hypothesis can cost more than 12pp accuracy.

Error Analysis Column “No Strat.” in Table 4 shows the accuracy per HateCheck functionality for the hypothesis “That contains hate speech.”. Most notably, the model wrongly predicted all denouncements of hate (F20 and F21) as hate speech. In four functionalities (F22, F11, F23, F20) the model predicted hate speech even though no one or no relevant group was targeted. Finally, we see that the model often fails at analyzing sentences with negations (F15) and that it fails at recognizing when slurs are reclaimed and used in a positive way (F9). In what follows, we will present and evaluate strategies to avoid these errors.

5 Methods

In this section, we present four methods, which we call strategies, that aim to improve zero-shot hate speech detection. A strategy has the following components and structure: The aim is to assign a label \( y = \{0, 1\} \) to input text \( t \), where 1 corresponds to the class hate speech and 0 corresponds to the class not-hate speech. The input text \( t \) can be used in one or multiple premises \( p_0 \) to \( p_m \), that are used in conjunction with the main hypothesis \( h_0 \) and one or multiple supporting hypotheses \( \{h_1, ..., h_n\} \) to obtain NLI model predictions \( m(p_i, h_j) \in \{0, 1\} \) where 0 corresponds to contradiction and 1 corresponds to entailment. The variables \( i \) and \( j \) are defined as: \( i \in \{0, ..., m\} \) and \( j \in \{0, ..., n\} \). The rules for how to combine model predictions to obtain the final label \( y \) are given by the individual strategies. As the main hypothesis we use “That contains hate speech.”, since it lead to the highest accuracy on HateCheck in Section 4. The supporting hypotheses used to implement the strategies are listed in Table 3.

5.1 Filtering By Target (FBT)

The error analysis showed that we can improve zero-shot classification accuracy significantly by avoiding predictions of hate speech where no relevant target group occurs. We thus propose to avoid false positives by constructing a set of supporting hypotheses \( \{h_1, ..., h_n\} \) to predict if text \( t \) actually targets or mentions a protected group or characteristic. If no protected group or characteristic is
5.3 Filtering Reclaimed Slurs (FRS)

As shown in Table 4, slurs that are reclaimed by members of a targeted group are often miss-classified as hate speech. Based on the observation that a reclaimed slur is often ascribed to oneself, we propose to use a supporting hypothesis that indicates if text is self-directed. If the model predicts self-directedness a potential prediction of hate speech is overridden to not-hate speech.

5.4 Catching Dehumanizing Comparisons (CDC)

One way of expressing hate towards a group and dehumanizing said group is to draw unflattering comparisons with animals. Such comparisons tend to be missed by hate speech detection systems, since the use of hateful or aggressive words is not needed to convey the hateful message. In HateCheck, this phenomenon is subsumed under “Implicit derogation”. Standard zero-shot prediction obtains a moderately good accuracy of 89.3%. We test if false negatives can be caught with a three-step combination of supporting hypotheses: (1) use the supporting hypotheses of FBT to predict if a protected group is mentioned in text, (2) predict if text is self-directed, and (3) predict if text has a negative sentiment. If all conditions are met, override a prediction of not-hate speech to hate speech.

6 Experiments

We use the same model and adopt the entailment threshold of 0.5 from Section 4 for the main and all supporting hypotheses. Further, we take the hypothesis leading to the highest accuracy in Section 4 as the main hypothesis.

Since the main hypothesis in our experiments is chosen for maximum accuracy on HateCheck (based on the experiment in Section 4) and the strategies developed are based on an error analysis on HateCheck, the overall system might be overfitting on this specific dataset. An evaluation on this dataset might thus lead to results that overestimate a potential positive effect of the proposed strategies. We therefore also evaluate on ETHOS as an “unseen” dataset.

---

Table 3: The supporting hypotheses used to implement the proposed strategies. For filtering by target we used the group-hypotheses for the HateCheck dataset and the characteristics-hypotheses for the ETHOS dataset, to account for differing hate speech definitions.

<table>
<thead>
<tr>
<th>FBT groups</th>
<th>This text is about women.</th>
<th>This text is about trans people.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This text is about gay people.</td>
<td>This text is about gay people.</td>
</tr>
<tr>
<td></td>
<td>This text is about black people.</td>
<td>This text is about disabled people.</td>
</tr>
<tr>
<td></td>
<td>This text is about Muslims.</td>
<td>This text is about immigrants.</td>
</tr>
<tr>
<td></td>
<td>This text is about gender.</td>
<td>This text is about sexual orientation.</td>
</tr>
<tr>
<td></td>
<td>This text is about race.</td>
<td>This text is about religion.</td>
</tr>
<tr>
<td></td>
<td>This text is about ethnicity.</td>
<td>This text is about national origin.</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>FBT characteristics</td>
<td>This text supports [X].</td>
<td>This text supports [X].</td>
</tr>
<tr>
<td></td>
<td>This text contains [X].</td>
<td>This text contains [X].</td>
</tr>
<tr>
<td></td>
<td>This text is about myself.</td>
<td>This text is about myself.</td>
</tr>
<tr>
<td></td>
<td>This text is about apes.</td>
<td>This text is about apes.</td>
</tr>
<tr>
<td></td>
<td>This text is about rats.</td>
<td>This text is about rats.</td>
</tr>
<tr>
<td></td>
<td>This text is about insects.</td>
<td>This text is about insects.</td>
</tr>
<tr>
<td></td>
<td>This text has a negative sentiment.</td>
<td>This text has a negative sentiment.</td>
</tr>
</tbody>
</table>

predicted to occur in $t$, a potential prediction of hate speech is overridden to not-hate speech. Figure 1 illustrates the method.

5.2 Filtering Counterspeech (FCS)

Our zero-shot model wrongly classifies all examples of counterspeech that quote or reference hate speech as actual hate speech. References to hate speech without quotation marks are hard to identify. Thus, for this work, we limit ourselves to counterspeech that quotes hate speech explicitly. We propose a three-stage strategy to this phenomenon: (1) quotation identification, (2) hate speech classification of the quoted content, (3) detecting the stance of the post towards the quoted content. Formally, the input text $t$ is divided into premise $p_0$ which contains the quoted text and premise $p_1$ which contains the text around the quotes. The quoted text is represented as “[X]” in $p_1$. Using the main hypothesis $h_0$ we predict if $p_0$ contains hate speech or not. We use the supporting hypothesis “This text supports [X].” ($h_1$) to predict the stance of $p_1$ towards $p_0$. If $p_0$ contains hate speech and $p_1$ has a supportive stance towards $p_0$, $t$ is classified as hate speech, otherwise it is classified as not-hate speech. The strategy is depicted in Figure 2.

---

2Of course there are counterexamples to this rule, where reclaimed slurs are directed to others and not oneself. However, as long this approximation, as crude as it may be, helps to reduce false positives, it is a useful approximation.
Table 4: Analysis of how individual functionalities are affected by the proposed strategies. The functionality descriptions are taken from Röttger et al. (2021). No Strat. refers to using only the hypothesis “That contains hate speech.”. Accuracies below 70% are marked in red. All refers to combining all four proposed strategies. The columns FBT, FCS, FRS, CDC and All contain the difference in percentage point (pp) accuracy compared to No Strat.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>No Strat.</th>
<th>FBT</th>
<th>FCS</th>
<th>FRS</th>
<th>CDC</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1: Expression of strong negative emotions (explicit)</td>
<td>100.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
</tr>
<tr>
<td>F2: Description using very negative attributes (explicit)</td>
<td>98.6</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
</tr>
<tr>
<td>F3: Dehumanisation (explicit)</td>
<td>100.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
</tr>
<tr>
<td>F4: Implicit derogation</td>
<td>89.3</td>
<td>+5.0</td>
<td>+0.0</td>
<td>-10.0</td>
<td>+0.0</td>
<td>-12.5</td>
</tr>
<tr>
<td>F5: Direct threat</td>
<td>100.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
</tr>
<tr>
<td>F6: Threat as normative statement</td>
<td>99.3</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
</tr>
<tr>
<td>F7: Hate expressed using slur</td>
<td>85.4</td>
<td>-14.6</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+2.8</td>
<td>-12.5</td>
</tr>
<tr>
<td>F8: Non-hateful homonyms of slurs</td>
<td>76.7</td>
<td>+6.7</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+6.7</td>
</tr>
<tr>
<td>F9: Reclaimed slurs</td>
<td>33.3</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+32.1</td>
<td>+0.0</td>
<td>+32.1</td>
</tr>
<tr>
<td>F10: Hate expressed using profanity</td>
<td>97.9</td>
<td>-0.7</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.7</td>
</tr>
<tr>
<td>F11: Non-hateful use of profanity</td>
<td>43.0</td>
<td>-64.0</td>
<td>+0.0</td>
<td>+23.0</td>
<td>+0.0</td>
<td>+53.0</td>
</tr>
<tr>
<td>F12: Hate expressed through reference in subsequent clauses</td>
<td>100.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>-2.9</td>
<td>+0.0</td>
<td>-2.9</td>
</tr>
<tr>
<td>F13: Hate expressed through reference in subsequent sentences</td>
<td>97.7</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
</tr>
<tr>
<td>F14: Hate expressed using negated positive statement</td>
<td>100.0</td>
<td>-2.9</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>-2.9</td>
</tr>
<tr>
<td>F15: Non-hate expressed using negated hateful statement</td>
<td>33.1</td>
<td>+5.3</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+5.3</td>
</tr>
<tr>
<td>F16: Hate phrased as a question</td>
<td>99.3</td>
<td>+0.0</td>
<td>+0.0</td>
<td>-5.0</td>
<td>+0.0</td>
<td>-5.0</td>
</tr>
<tr>
<td>F17: Hate phrased as an opinion</td>
<td>100.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>-2.3</td>
<td>+0.0</td>
<td>-2.3</td>
</tr>
<tr>
<td>F18: Neutral statements using protected group identifiers</td>
<td>96.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
</tr>
<tr>
<td>F19: Positive statements using protected group identifiers</td>
<td>97.4</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
</tr>
<tr>
<td>F20: Denouncements of hate that quote it</td>
<td>0.0</td>
<td>+8.7</td>
<td>+100.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+100.0</td>
</tr>
<tr>
<td>F21: Denouncements of hate that make direct reference to it</td>
<td>0.0</td>
<td>+7.8</td>
<td>+0.0</td>
<td>+1.4</td>
<td>+0.0</td>
<td>+8.5</td>
</tr>
<tr>
<td>F22: Abuse targeted at objects</td>
<td>63.1</td>
<td>+36.9</td>
<td>+0.0</td>
<td>+9.2</td>
<td>+0.0</td>
<td>+36.9</td>
</tr>
<tr>
<td>F23: Abuse targeted at individuals (not as member of a prot. group)</td>
<td>7.7</td>
<td>+70.8</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+70.8</td>
<td></td>
</tr>
<tr>
<td>F24: Abuse targeted at nonprotected groups (e.g. professions)</td>
<td>11.3</td>
<td>+88.9</td>
<td>+0.0</td>
<td>+3.2</td>
<td>+83.0</td>
<td></td>
</tr>
<tr>
<td>F25: Swaps of adjacent characters</td>
<td>97.7</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.0</td>
</tr>
<tr>
<td>F26: Missing characters</td>
<td>88.6</td>
<td>-1.4</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.7</td>
<td>-0.7</td>
</tr>
<tr>
<td>F27: Missing word boundaries</td>
<td>87.9</td>
<td>-4.3</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+1.4</td>
<td>-3.5</td>
</tr>
<tr>
<td>F28: Added spaces between chars</td>
<td>97.7</td>
<td>-11.0</td>
<td>+0.0</td>
<td>-0.6</td>
<td>+0.0</td>
<td>-11.6</td>
</tr>
<tr>
<td>F29: Leet speak spellings</td>
<td>93.1</td>
<td>-12.7</td>
<td>+0.0</td>
<td>+0.0</td>
<td>+0.6</td>
<td>-12.1</td>
</tr>
</tbody>
</table>

*Overall* 79.4 | +3.3 | +4.6 | +0.7 | +0.2 | +7.9 |

Table 5: Accuracy scores on ETHOS. The three top rows show baselines computed by Mollas et al. (2022). TG refers to using target characteristics to implement FBT and TC refers to using target characteristics for FBT.

ETHOS does not refer to protected groups in its definition and annotation of hate speech, but instead to protected characteristics. Thus, in the hypotheses for FBT we replace protected groups with the protected characteristics listed in Table 3.

6.1 Results

HateCheck The bottom row *Overall* in Table 4 shows the results for the proposed strategies and their combination on the HateCheck dataset. Each strategy leads to an improvement in accuracy. But while FBT and FCS lead to large increases, FRS and CDC only lead to minor increases. Combining all proposed strategies leads to an increase in accuracy of 7.9pp.

ETHOS The results of evaluating the same strategies on ETHOS (Mollas et al., 2022) are given in Table 5. As additional baselines compared to zero-shot prediction using just one hypothesis, we include the performance of three models trained on ETHOS by Mollas et al. (2022).

The combination of all strategies leads to an increase of 10.0pp, which is an even greater increase than on HateCheck. However, the gains are more unevenly distributed across the proposed strategies. Filtering by target characteristics alone leads to an increase of 9.1pp. Filtering reclaimed slurs still has a positive effects of 1.7pp. However, filtering counterspeech, the best performing strategy on HateCheck, does not have any effect at all. And
catching dehumanizing comparisons even reduces performance by 0.1pp. The comparison to the baselines provided by Mollas et al. (2022) shows that zero-shot prediction using the hypothesis “That contains hate speech.” already outperforms a trained SVM by more than 3pp but still underperforms the fine-tuned BERT by more than 10pp. However, applying the proposed strategies almost closes the gap to the fine-tuned models.

6.2 Analysis of Affected Functionalities

We analyse if the observed performance gains actually stem from improvements on the functionalities targeted by the proposed strategies. Table 4 shows for each functionality how it was affected by each strategy.

**Filtering by Target** The results for filtering by target show dramatic accuracy increases for HateCheck functionalities containing abuse and proficiency that is not targeted at a protected group. These are exactly the functionalities this strategy aimed at. The performance for spelling variations and implicit derogation decreases slightly. This can be explained by the model failing to correctly recognize spelling variations of target groups and by the fact that the target group might only be implied in implicit derogation leading to false negatives.

**Filtering Counterspeech** The counterspeech filter increases the accuracy of the respective functionality from 0% to 100%. Thus, detecting quoted hate speech as well as detecting the stance towards the quote worked exactly as intended on HateCheck.

**Filtering Reclaimed Slurs** The functionality with the largest gains when filtering reclaimed slurs is “reclaimed slurs”, showing that the strategy works as intended. However, the performance increase of this method is not as high as for example filtering by target. The functionality “non-hateful use of proficiency” also benefits from this strategy. We assume that such uses of proficiency often are also not directed at other people and thus sometimes predicted to be directed at oneself. This is a beneficial side-effect of the strategy.

**Catching Dehumanizing Comparisons** This strategy only leads to minor a minor overall improvement of 0.2pp. We observe no effect on the targeted functionality, but a small positive effect on F7, “Hate expressed using slur”, which could indicate that the model associates slurs with negatively coded animals. Additionally, the strategy has minor positive effects on functionalities that contain spelling variations.

7 Discussion

**Supporting Hypotheses** The performance of NLI-strategies largely depends on the accuracy of the supporting hypotheses. Testing the accuracy of each supporting hypothesis is not always possible, since annotated data for the predicted aspect of the input text might not be available. Indeed, one of the strengths of our approach is that it can use aspects for which no annotated data exists. Another uncertainty lies in the formulation of supporting hypotheses. A suboptimal formulation of supporting hypotheses negatively affects the overall results. By using annotated targets in HateCheck and inferring stance labels as well as self-directedness from HateCheck functionalities, we compute and compare the accuracy of multiple supporting hypothesis formulations. The results (in Appendix B) show that testing for the presence of a target group mostly leads to accuracies above 90%, independent of the specific formulation. Detecting the outer stance towards the inner text obtained a perfect accuracy of 100% and testing for self-directedness leads to low accuracies, which are probably partly due to faulty label inferences from functionalities. Overall, the results indicate that the supporting hypotheses provide reliable information.

**Generality** There are two ways in which the proposed strategies might not generalize. First, the strategies might be specific to the model used for the experiments. In order to answer this question, repeating the experiments with other NLI models will be necessary. Second, the strategies might be specific to HateCheck and not generalize to other datasets, since they specifically target HateCheck functionalities. The evaluation on ETHOS shows
Table 6: Evaluation of FCS variants. The two bottom rows display the variants adjusted for detecting Hate Speech in $p_1$. The functionality F20 contains Denouncements of hate that quote it. The scores are given in accuracy (%) and change in accuracy compared to No strategy.

| strategy          | F20 overall | | change in accuracy |
|-------------------|-------------|---------------------------|
| No strategy       | 0.0         | 79.4                      |
| FCS               | +100        | +4.6                      |
| FCS$_{p_1}$       | -3.0        | -+0.0                     |
| FCS$_{p_1,FBT}$   | +6.9        | +0.3                      |

that this is generally not case, since the results for the best strategy combination on ETHOS even exceed the results for the best combination on HateCheck.

While our experiments did not show problems in generalization, we can imagine the following weakness for the FCS strategy: Given an input text $t$ that contains a quote and hate speech, where the hate speech does not occur inside of the quotes, the current FCS strategy would fail, since it only detects hate speech in $p_0$, that is inside the quotes. Such an example is given in Figure 3.

The obvious solution to avoid this problem is to not only apply the main hypothesis $h_0$ on the premise $p_0$ but also on premise $p_1$, which contains the text outside the quotes. In a follow-up experiment we implement this modified strategy (FCS$_{p_1}$) and evaluated it on HateCheck. Note, that since such a case is not covered by HateCheck or ETHOS there is no increase in accuracy to be expected - we can only test if accounting for this case leads to a decrease in accuracy through unwanted side effects.

The results, displayed in Table 6 show that this modification removes all the gains obtained through FBT. We assume that this is due to the fact that the counterspeech often also conveys strong negative emotions that are mistaken by the model for hate speech.

We further test if this problem can be alleviated by applying the FBT strategy if hate speech is detected in $p_1$ (i.e. outside of the quotes) as depicted in Figure 3. The results in Table 6 (row FCS$_{p_1,FBT}$) show that additionally applying FBT only recovers a fraction of the positive effect of FCS. We assume that this is due to counterspeech including or being associated with target groups. Thus, further research that investigates how the problem can be alleviated is needed.

**Efficiency** In the proposed setup each new hypothesis necessitates an additional forward pass, which means that the computational cost linearly increases with adding new hypotheses. This leads to a difficult trade-off between accuracy and efficiency. A possible solution was recently proposed by Müller et al. (2022), who embed premises and hypotheses independently, thereby keeping the computational cost during inference time with respect to the number of hypotheses constant.

**Prerequisites of FBT** FBT presumes that the target groups or characteristics are known beforehand. This prerequisite is unproblematic when using FBT to detect hate speech against well known targets of hate speech or discrimination. However, it makes this method unsuitable for tasks such as vulnerable group identification (Mossie and Wang, 2020).

**Flexibility** Single hypotheses or entire strategies can be easily added to or removed from a system. This modularity makes the approach easily adjustable to different scenarios or use cases. For example, if precision is the main concern, the catching dehumanizing comparisons can be dropped and if recall is the main concern, filters can be removed. Instead of adding or removing strategies, it is also possible to manipulate the precision-recall trade-off by adjusting confidence thresholds for particular hypotheses.

8 Conclusion

In this work, we combine hypotheses to create more accurate NLI-based zero-shot hate speech detection systems. Specifically, we develop four simple strategies, filtering by target, filtering counter speech, filtering reclaimed-slurs, and catching dehumanizing comparisons, that target specific model weaknesses. We evaluate the strategies on HateCheck, which served as the basis for developing these strategies, and on ETHOS, which acts as an “unseen” dataset. The NLI-based zero-shot baseline already outperforms fine-tuned models on HateCheck and beats an SVM baseline on ETHOS. Using all four proposed strategies leads to a further performance increase of 7.9% on HateCheck and 10.0% on ETHOS. However, the contribution of the strategies to the performance increases varies, with catching dehumanizing comparisons even having a small negative effect on the accuracy on ETHOS.

The proposed approach is simple and modular making it easy to implement and adjust to different
scenarios.

In future work, we plan to evaluate such strategies in a multi-lingual setup and in a few-shot scenario. Further, this works leads to the question how effective supporting hypotheses could be searched and generated automatically.

Acknowledgements

We thank Chantal Amrhein, Jonathan Schaber, Aneta Zuber, and the anonymous reviewers for their helpful feedback. This work was funded by the University of Zurich Research Priority Program (project “URPP Digital Religion(s)”\(^5\)).

Ethical Considerations

The goal of this article is to contribute to the development of sophisticated hate speech detection methods, and thus to contribute to an online environment that is less hateful. However, we can imagine multiple ways how such methods, and our proposed approach in particular, can lead to harm: (1) Deploying the exact system that we propose would lead to not detecting hate speech against protected groups that are not explicitly included in the two datasets we worked with and thus not covered by the FBT-method. Thus, before deploying such a method, careful consideration of which protected groups or group characteristics are covered is needed. (2) Overconfident claims about the accuracy of hate speech detection methods could lead to the false impression that content moderation can be left to automatic methods with no human intervention. (3) Hate speech detection in general is prone to misuse and repurposing in order to prohibit other kinds of speech. Detecting if a text revolves around a protected group could be misused to detect and prohibit important discussion around topics connected to a protected group.

However, we believe that a decomposition of hate speech into more specific aspects is important for more accurate, interpretable and modular hate speech detection methods (Khurana et al., 2022). Thus, detecting such components of hate speech is also strongly beneficial for effective content moderation and a less hateful online environment.

\(^5\)https://www.digitalreligions.uzh.ch/en.html

References


Zeerak Waseem. 2016. Are You a Racist or Am I Seeing Things? Annotator Influence on Hate Speech Detection on Twitter. In NLP+CSS@EMNLP.


A Zero-Shot Results: Comparing Hypotheses

Table 7, the extended version of Table 2, contains all results for comparing hypotheses for zero-shot hate speech detection on HateCheck. “average:<expression>” refers to the average accuracy of all hypotheses containing expression. The highest accuracy is in bold.

<table>
<thead>
<tr>
<th>hypothesis</th>
<th>accuracy (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contains hate speech.</td>
<td>74.7</td>
</tr>
<tr>
<td>Contains hate speech.</td>
<td>78.6</td>
</tr>
<tr>
<td>Hate speech.</td>
<td>72.9</td>
</tr>
<tr>
<td>Hateful.</td>
<td>71.8</td>
</tr>
<tr>
<td>It contains hate speech.</td>
<td>78.7</td>
</tr>
<tr>
<td>It is hateful.</td>
<td>75.0</td>
</tr>
<tr>
<td>It contains hate speech.</td>
<td>78.7</td>
</tr>
<tr>
<td>It is hate speech.</td>
<td>70.8</td>
</tr>
<tr>
<td>It is hateful.</td>
<td>75.0</td>
</tr>
<tr>
<td>That contains hate speech.</td>
<td>79.4</td>
</tr>
<tr>
<td>That contains hateful content.</td>
<td>78.0</td>
</tr>
<tr>
<td>That example contains hateful content.</td>
<td>77.8</td>
</tr>
<tr>
<td>That example is hate speech.</td>
<td>66.6</td>
</tr>
<tr>
<td>That example is hateful.</td>
<td>76.8</td>
</tr>
<tr>
<td>That is hateful.</td>
<td>66.6</td>
</tr>
<tr>
<td>That text contains hate speech.</td>
<td>78.8</td>
</tr>
<tr>
<td>That text contains hateful content.</td>
<td>78.6</td>
</tr>
<tr>
<td>That text is hate speech.</td>
<td>69.2</td>
</tr>
<tr>
<td>That text is hateful.</td>
<td>77.2</td>
</tr>
<tr>
<td>This contains hate speech.</td>
<td>79.1</td>
</tr>
<tr>
<td>This contains hateful content.</td>
<td>78.2</td>
</tr>
<tr>
<td>This example contains hate speech.</td>
<td>77.3</td>
</tr>
<tr>
<td>This example contains hateful content.</td>
<td>77.8</td>
</tr>
<tr>
<td>This example is hate speech.</td>
<td>67.2</td>
</tr>
<tr>
<td>This example is hateful.</td>
<td>77.4</td>
</tr>
<tr>
<td>This is hateful.</td>
<td>70.6</td>
</tr>
<tr>
<td>This text contains hate speech.</td>
<td>78.8</td>
</tr>
<tr>
<td>This text contains hateful content.</td>
<td>78.3</td>
</tr>
<tr>
<td>This text is hate speech.</td>
<td>69.5</td>
</tr>
<tr>
<td>This text is hateful.</td>
<td>78.7</td>
</tr>
<tr>
<td>average: It</td>
<td>74.8</td>
</tr>
<tr>
<td>average: This</td>
<td>75.7</td>
</tr>
<tr>
<td>average: That</td>
<td>74.9</td>
</tr>
<tr>
<td>average: hateful</td>
<td>75.8</td>
</tr>
<tr>
<td>average: hateful content</td>
<td>78.1</td>
</tr>
<tr>
<td>average: hate speech</td>
<td>74.5</td>
</tr>
<tr>
<td>average: example</td>
<td>74.4</td>
</tr>
<tr>
<td>average: text</td>
<td>76.1</td>
</tr>
<tr>
<td>average: is</td>
<td>73.9</td>
</tr>
<tr>
<td>average: contain</td>
<td>78.2</td>
</tr>
<tr>
<td>SiftNinja</td>
<td>33.5</td>
</tr>
<tr>
<td>BERT fine-tuned on Davidson et al. (2017)</td>
<td>60.2</td>
</tr>
<tr>
<td>BERT fine-tuned on Founta et al. (2018)</td>
<td>63.2</td>
</tr>
<tr>
<td>Google-Jigsaw</td>
<td>76.6</td>
</tr>
</tbody>
</table>

Table 7: Full evaluation of hypotheses, that claim hate speech exists in the input text, on HateCheck.

B Evaluating Supporting Hypotheses

B.1 Target Groups and Target Characteristics

Each example in HateCheck which mentions a protected group or revolves around a protected group is annotated with said group. If no group is targeted the example is annotated with an empty string. By using these annotations as labels, we can create a binary classification task for each protected group: for detecting a mention of a specific protected group \(x\), we convert label \(x\) to 1 and all other labels (i.e. all other protected groups) to 0.

We use the same model and as in the previous zero-shot experiments for evaluation and test the performance for detecting mentions for all protected groups in HateCheck. We additionally test the detection of the supercategory queer people covering the two protected groups gay people and transgender people in HateCheck. When testing if a text revolves around gender, we treat both women and transgender people as positive classes and all other protected groups as negative classes. While this mapping obviously can result in incorrect labels (a text can be about gender even if another group is targeted), we assume that it holds true for examples in the HateCheck dataset.

Table 8 shows the results for detecting if black people are mentioned, Table 9 for mentions of Muslims, Table 10 for mentions of immigrants, Table 11 for mentions of disabled people, Table 12 for mentions of gay people, Table 13 for mentions of transgender people, Table 14 for mentions of queer people, and Table 16 for detecting if a text is about gender.

The results show that in many cases the detection of a mentioned group is surprisingly accurate. The difference in accuracy between the best performing hypothesis and the worst performing hypothesis does not exceed 12%. This is a similar range to the differences found between hypotheses when testing if a text contains hate speech (see Table 2 and Table 7). However, when looking at \(F_1\) scores the differences are much larger, with more general terms, such as faith or ethnicity preforming worse than the specific terms Muslims and black people.

Detecting if a text revolves around gender performs worst, compared to detecting other protected groups or characteristics. This is mostly due to low precision scores. We assume that this is a consequence of sexual orientation (gay people) being closely associated in the embedding space with gender and thus leading to false positives.

B.2 Self-Directedness

Evaluating the accuracy of detecting self-directedness is difficult, because there exist no
Table 8: Results for supporting hypotheses aimed at detecting mentions of black people. The hypotheses are sorted by macro $F_1$-score in descending order. Note, that some of the hypotheses listed use broader terms (“people of colour”, “race”, “ethnicity”) that should also detect the mentions of other target groups. However, in the context of HateCheck, we can only test the detection of mentioning black people.

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Accuracy (%)</th>
<th>$F_1$ (%)</th>
<th>Recall (%)</th>
<th>Precision (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>That example is about black people</td>
<td>97.9</td>
<td>92.0</td>
<td>93.8</td>
<td>90.2</td>
</tr>
<tr>
<td>This example is about black people</td>
<td>97.6</td>
<td>90.9</td>
<td>94.0</td>
<td>88.0</td>
</tr>
<tr>
<td>That text is about black people</td>
<td>96.4</td>
<td>87.1</td>
<td>93.2</td>
<td>81.8</td>
</tr>
<tr>
<td>That is about black people</td>
<td>95.8</td>
<td>85.0</td>
<td>92.5</td>
<td>78.7</td>
</tr>
<tr>
<td>This text is about black people</td>
<td>95.2</td>
<td>83.6</td>
<td>94.4</td>
<td>75.0</td>
</tr>
<tr>
<td>This is about black people</td>
<td>95.0</td>
<td>83.0</td>
<td>93.6</td>
<td>74.5</td>
</tr>
<tr>
<td>That example is about people of colour</td>
<td>94.3</td>
<td>80.7</td>
<td>92.7</td>
<td>71.4</td>
</tr>
<tr>
<td>That example is about race</td>
<td>94.0</td>
<td>79.8</td>
<td>91.3</td>
<td>70.9</td>
</tr>
<tr>
<td>This example is about people of colour</td>
<td>93.8</td>
<td>79.3</td>
<td>92.3</td>
<td>69.5</td>
</tr>
<tr>
<td>That is about race</td>
<td>94.6</td>
<td>77.5</td>
<td>72.6</td>
<td>83.1</td>
</tr>
<tr>
<td>This example is about race</td>
<td>90.9</td>
<td>72.3</td>
<td>91.7</td>
<td>59.6</td>
</tr>
<tr>
<td>That text is about people of colour</td>
<td>89.8</td>
<td>70.6</td>
<td>94.2</td>
<td>56.4</td>
</tr>
<tr>
<td>That example is about ethnicity</td>
<td>90.5</td>
<td>69.8</td>
<td>85.3</td>
<td>59.1</td>
</tr>
<tr>
<td>This is about race</td>
<td>88.9</td>
<td>67.6</td>
<td>89.4</td>
<td>54.4</td>
</tr>
<tr>
<td>That text is about race</td>
<td>87.8</td>
<td>66.3</td>
<td>92.3</td>
<td>51.7</td>
</tr>
<tr>
<td>That is about people of colour</td>
<td>87.4</td>
<td>65.9</td>
<td>93.8</td>
<td>50.8</td>
</tr>
<tr>
<td>This text is about race</td>
<td>86.5</td>
<td>64.5</td>
<td>94.6</td>
<td>48.9</td>
</tr>
<tr>
<td>This text is about people of colour</td>
<td>84.9</td>
<td>62.1</td>
<td>96.1</td>
<td>45.9</td>
</tr>
<tr>
<td>That example is about ethnicity</td>
<td>85.6</td>
<td>62.1</td>
<td>91.1</td>
<td>47.1</td>
</tr>
<tr>
<td>This is about ethnicity</td>
<td>85.4</td>
<td>58.1</td>
<td>78.4</td>
<td>46.2</td>
</tr>
<tr>
<td>That text is about ethnicity</td>
<td>81.5</td>
<td>56.1</td>
<td>91.3</td>
<td>40.5</td>
</tr>
<tr>
<td>This text is about ethnicity</td>
<td>80.2</td>
<td>55.0</td>
<td>93.6</td>
<td>38.9</td>
</tr>
<tr>
<td>That is about people of colour</td>
<td>74.8</td>
<td>49.4</td>
<td>95.2</td>
<td>33.3</td>
</tr>
<tr>
<td>This text is about race</td>
<td>87.0</td>
<td>28.4</td>
<td>19.9</td>
<td>49.7</td>
</tr>
</tbody>
</table>

One possibility, that follows the motivation for introducing the FRS-method, is to treat all examples of functionality F9 (“reclaimed_slur”) as self-directed and examples of all other functionalities as not self-directed. We conducted this experiment. The results are given in Table 17. However, one should keep in mind that this disregards that reclaimed slurs can be used in a not-self directed manner and that other functionalities, such as functionality F11 *non-hateful use of profanity*, might contain examples of self-directed speech.

### B.3 Counterspeech

We perform a simple evaluation of the supporting hypothesis that predicts the stance of an outer text towards its quoted inner text (see Section 5.2 for an explanation) using only functionality F20 (*Denouncement of hate that quote it*) as an evaluation set. We treat stance detection here as a binary task with the labels *is_for* or *is_against*.

How these labels are mapped onto NLI labels depends on the specific hypothesis. If the hypothesis claims that the outer text denounces the quoted text, then *is_for* is mapped to *contradiction* and *is_against* is mapped to *entailment*.

We test various formulations including the verbs “supports [X]” and “is for [X]”. The results are given in Table 18. Since all examples in this category are considered hate speech, that is denounced by the outer text, the true label is always *is_against*. We only report accuracy, since there can be no false positives and true negatives, which makes precision and recall lose its usefulness.
<table>
<thead>
<tr>
<th>hypothesis</th>
<th>accuracy (%)</th>
<th>$F_1$ (%)</th>
<th>recall (%)</th>
<th>precision (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>That example is about Muslims.</td>
<td>98.3</td>
<td>93.1</td>
<td>90.7</td>
<td>95.6</td>
</tr>
<tr>
<td>This example is about Muslims.</td>
<td>98.1</td>
<td>92.7</td>
<td>90.7</td>
<td>94.8</td>
</tr>
<tr>
<td>This text is about Muslims.</td>
<td>98.1</td>
<td>92.6</td>
<td>90.3</td>
<td>95.0</td>
</tr>
<tr>
<td>That text is about Muslims.</td>
<td>98.0</td>
<td>92.3</td>
<td>90.3</td>
<td>94.4</td>
</tr>
<tr>
<td>That example is about Muslim people.</td>
<td>98.0</td>
<td>92.0</td>
<td>90.7</td>
<td>93.4</td>
</tr>
<tr>
<td>This example is about Muslim people.</td>
<td>97.9</td>
<td>92.0</td>
<td>90.9</td>
<td>93.0</td>
</tr>
<tr>
<td>This is about Muslims.</td>
<td>97.8</td>
<td>91.6</td>
<td>90.7</td>
<td>92.4</td>
</tr>
<tr>
<td>This text is about Muslim people.</td>
<td>97.8</td>
<td>91.5</td>
<td>90.7</td>
<td>92.2</td>
</tr>
<tr>
<td>That text is about Muslim people.</td>
<td>97.7</td>
<td>91.1</td>
<td>90.1</td>
<td>92.2</td>
</tr>
<tr>
<td>This example is about religion.</td>
<td>97.7</td>
<td>90.3</td>
<td>83.3</td>
<td>98.5</td>
</tr>
<tr>
<td>This text is about religion.</td>
<td>97.5</td>
<td>89.7</td>
<td>83.9</td>
<td>96.4</td>
</tr>
<tr>
<td>This is about Muslim people.</td>
<td>97.3</td>
<td>89.6</td>
<td>89.9</td>
<td>89.3</td>
</tr>
<tr>
<td>That text is about religion.</td>
<td>97.5</td>
<td>89.5</td>
<td>82.9</td>
<td>97.3</td>
</tr>
<tr>
<td>That is about Muslims.</td>
<td>97.2</td>
<td>89.1</td>
<td>88.6</td>
<td>89.6</td>
</tr>
<tr>
<td>That example is about religion.</td>
<td>97.3</td>
<td>88.5</td>
<td>80.2</td>
<td>98.7</td>
</tr>
<tr>
<td>That is about Muslim people.</td>
<td>96.8</td>
<td>87.8</td>
<td>89.7</td>
<td>85.9</td>
</tr>
<tr>
<td>That is about religion.</td>
<td>96.4</td>
<td>84.5</td>
<td>74.8</td>
<td>97.1</td>
</tr>
<tr>
<td>That example is about faith.</td>
<td>95.0</td>
<td>78.2</td>
<td>69.2</td>
<td>89.8</td>
</tr>
<tr>
<td>This text is about faith.</td>
<td>95.0</td>
<td>78.1</td>
<td>69.0</td>
<td>90.0</td>
</tr>
<tr>
<td>This is about faith.</td>
<td>94.4</td>
<td>74.2</td>
<td>62.4</td>
<td>91.5</td>
</tr>
<tr>
<td>That example is about faith.</td>
<td>93.4</td>
<td>68.9</td>
<td>56.6</td>
<td>88.1</td>
</tr>
<tr>
<td>That is about faith.</td>
<td>92.0</td>
<td>63.3</td>
<td>52.9</td>
<td>78.8</td>
</tr>
<tr>
<td>That is about religion.</td>
<td>89.6</td>
<td>34.5</td>
<td>21.1</td>
<td>95.3</td>
</tr>
<tr>
<td>That is about faith.</td>
<td>88.3</td>
<td>21.9</td>
<td>12.6</td>
<td>82.4</td>
</tr>
</tbody>
</table>

Table 9: Results for supporting hypotheses aimed at detecting mentions of Muslim people. Note, that some of the hypotheses listed use broader terms ("faith", "religion") that should detect other target groups too. However, in the context of HateCheck their applicability is restricted to Muslim people, since no other religion occurs in HateCheck.

<table>
<thead>
<tr>
<th>hypothesis</th>
<th>accuracy (%)</th>
<th>$F_1$ (%)</th>
<th>recall (%)</th>
<th>precision (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>That example is about immigrants.</td>
<td>97.8</td>
<td>91.2</td>
<td>92.4</td>
<td>89.9</td>
</tr>
<tr>
<td>This example is about immigrants.</td>
<td>97.7</td>
<td>90.8</td>
<td>92.4</td>
<td>89.2</td>
</tr>
<tr>
<td>That is about immigrants.</td>
<td>97.2</td>
<td>88.8</td>
<td>89.2</td>
<td>88.4</td>
</tr>
<tr>
<td>That text is about immigrants.</td>
<td>97.0</td>
<td>88.6</td>
<td>92.2</td>
<td>85.2</td>
</tr>
<tr>
<td>This text is about immigrants.</td>
<td>96.3</td>
<td>86.4</td>
<td>93.7</td>
<td>80.1</td>
</tr>
<tr>
<td>That is about immigrants.</td>
<td>96.4</td>
<td>86.2</td>
<td>91.6</td>
<td>81.4</td>
</tr>
<tr>
<td>That text is about national origin.</td>
<td>77.7</td>
<td>42.2</td>
<td>65.4</td>
<td>31.1</td>
</tr>
<tr>
<td>That text is about national origin.</td>
<td>78.0</td>
<td>41.3</td>
<td>62.4</td>
<td>30.9</td>
</tr>
<tr>
<td>That is about national origin.</td>
<td>83.4</td>
<td>37.0</td>
<td>39.3</td>
<td>35.0</td>
</tr>
<tr>
<td>That example is about national origin.</td>
<td>81.4</td>
<td>30.0</td>
<td>32.2</td>
<td>28.1</td>
</tr>
<tr>
<td>This example is about national origin.</td>
<td>79.8</td>
<td>30.0</td>
<td>34.8</td>
<td>26.3</td>
</tr>
<tr>
<td>That is about national origin.</td>
<td>86.5</td>
<td>24.6</td>
<td>17.7</td>
<td>40.2</td>
</tr>
</tbody>
</table>

Table 10: Results for supporting hypotheses aimed at detecting mentions of immigrants.

<table>
<thead>
<tr>
<th>hypothesis</th>
<th>accuracy (%)</th>
<th>$F_1$ (%)</th>
<th>recall (%)</th>
<th>precision (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>That example is about disabled people.</td>
<td>98.4</td>
<td>93.7</td>
<td>90.3</td>
<td>97.3</td>
</tr>
<tr>
<td>This example is about disabled people.</td>
<td>98.4</td>
<td>93.5</td>
<td>90.1</td>
<td>97.1</td>
</tr>
<tr>
<td>This text is about disabled people.</td>
<td>98.0</td>
<td>92.3</td>
<td>91.3</td>
<td>93.2</td>
</tr>
<tr>
<td>That example is about disability.</td>
<td>97.9</td>
<td>91.9</td>
<td>92.4</td>
<td>91.4</td>
</tr>
<tr>
<td>That text is about disabled people.</td>
<td>97.9</td>
<td>91.3</td>
<td>87.0</td>
<td>96.1</td>
</tr>
<tr>
<td>That example is about disability.</td>
<td>97.7</td>
<td>91.3</td>
<td>93.0</td>
<td>89.6</td>
</tr>
<tr>
<td>That is about disabled people.</td>
<td>97.7</td>
<td>90.9</td>
<td>87.2</td>
<td>94.8</td>
</tr>
<tr>
<td>That is about disability.</td>
<td>97.4</td>
<td>89.9</td>
<td>90.3</td>
<td>89.5</td>
</tr>
<tr>
<td>That text is about disability.</td>
<td>96.6</td>
<td>87.6</td>
<td>91.5</td>
<td>84.1</td>
</tr>
<tr>
<td>That is about disability.</td>
<td>96.6</td>
<td>86.0</td>
<td>80.4</td>
<td>92.4</td>
</tr>
<tr>
<td>That example is about disability.</td>
<td>94.8</td>
<td>82.0</td>
<td>91.7</td>
<td>74.1</td>
</tr>
<tr>
<td>This example is about disability.</td>
<td>94.5</td>
<td>81.6</td>
<td>94.4</td>
<td>71.9</td>
</tr>
</tbody>
</table>

Table 11: Results for supporting hypotheses aimed at detecting mentions of disabled people.
<table>
<thead>
<tr>
<th>hypothesis</th>
<th>accuracy (%)</th>
<th>$F_1$ (%)</th>
<th>recall (%)</th>
<th>precision (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>That example is about gay people.</td>
<td>99.1</td>
<td>96.7</td>
<td>94.2</td>
<td>99.4</td>
</tr>
<tr>
<td>This example is about gay people.</td>
<td>99.0</td>
<td>96.6</td>
<td>94.0</td>
<td>99.2</td>
</tr>
<tr>
<td>This text is about gay people.</td>
<td>98.8</td>
<td>95.9</td>
<td>92.9</td>
<td>99.0</td>
</tr>
<tr>
<td>This is about gay people.</td>
<td>98.8</td>
<td>95.8</td>
<td>92.6</td>
<td>99.2</td>
</tr>
<tr>
<td>That text is about gay people.</td>
<td>98.5</td>
<td>94.6</td>
<td>90.0</td>
<td>99.6</td>
</tr>
<tr>
<td>That is about gay people.</td>
<td>98.4</td>
<td>94.4</td>
<td>90.4</td>
<td>98.8</td>
</tr>
</tbody>
</table>

Table 12: Results for supporting hypotheses aimed at detecting mentions of gay people.

<table>
<thead>
<tr>
<th>hypothesis</th>
<th>accuracy (%)</th>
<th>$F_1$ (%)</th>
<th>recall (%)</th>
<th>precision (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>That example is about transgender people.</td>
<td>99.0</td>
<td>95.8</td>
<td>92.7</td>
<td>99.1</td>
</tr>
<tr>
<td>That text is about transgender people.</td>
<td>99.0</td>
<td>95.6</td>
<td>92.2</td>
<td>99.3</td>
</tr>
<tr>
<td>This text is about transgender people.</td>
<td>98.9</td>
<td>95.6</td>
<td>92.9</td>
<td>98.4</td>
</tr>
<tr>
<td>This example is about transgender people.</td>
<td>98.9</td>
<td>95.4</td>
<td>92.2</td>
<td>98.8</td>
</tr>
<tr>
<td>That is about transgender people.</td>
<td>98.8</td>
<td>94.9</td>
<td>92.0</td>
<td>97.9</td>
</tr>
<tr>
<td>That text is about transgender people.</td>
<td>98.7</td>
<td>94.6</td>
<td>92.2</td>
<td>97.0</td>
</tr>
</tbody>
</table>

Table 13: Results for supporting hypotheses aimed at detecting mentions of transgender people.

<table>
<thead>
<tr>
<th>hypothesis</th>
<th>accuracy (%)</th>
<th>$F_1$ (%)</th>
<th>recall (%)</th>
<th>precision (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is about queer people.</td>
<td>94.3</td>
<td>88.6</td>
<td>81.3</td>
<td>97.5</td>
</tr>
<tr>
<td>That example is about queer people.</td>
<td>93.7</td>
<td>87.1</td>
<td>77.9</td>
<td>98.8</td>
</tr>
<tr>
<td>This example is about queer people.</td>
<td>93.2</td>
<td>85.9</td>
<td>76.2</td>
<td>98.5</td>
</tr>
<tr>
<td>This text is about queer people.</td>
<td>93.1</td>
<td>85.7</td>
<td>76.4</td>
<td>97.5</td>
</tr>
<tr>
<td>That is about queer people.</td>
<td>92.4</td>
<td>84.0</td>
<td>73.5</td>
<td>98.2</td>
</tr>
<tr>
<td>That text is about queer people.</td>
<td>91.7</td>
<td>82.3</td>
<td>70.8</td>
<td>98.4</td>
</tr>
</tbody>
</table>

Table 14: Results for supporting hypotheses aimed at detecting mentions of queer people, which in HateCheck corresponds to the categories gay people and transgender people.

<table>
<thead>
<tr>
<th>hypothesis</th>
<th>accuracy (%)</th>
<th>$F_1$ (%)</th>
<th>recall (%)</th>
<th>precision (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This example is about women.</td>
<td>97.2</td>
<td>90.2</td>
<td>94.1</td>
<td>86.6</td>
</tr>
<tr>
<td>That example is about women.</td>
<td>97.2</td>
<td>90.1</td>
<td>94.1</td>
<td>86.5</td>
</tr>
<tr>
<td>This example is about gender.</td>
<td>96.2</td>
<td>86.6</td>
<td>88.6</td>
<td>84.6</td>
</tr>
<tr>
<td>This text is about women.</td>
<td>95.9</td>
<td>86.1</td>
<td>93.9</td>
<td>79.5</td>
</tr>
<tr>
<td>That text is about women.</td>
<td>95.7</td>
<td>85.3</td>
<td>91.6</td>
<td>79.8</td>
</tr>
<tr>
<td>This is about women.</td>
<td>94.8</td>
<td>83.0</td>
<td>92.7</td>
<td>75.0</td>
</tr>
</tbody>
</table>

Table 15: Results for supporting hypotheses aimed at detecting mentions of women.

<table>
<thead>
<tr>
<th>hypothesis</th>
<th>accuracy (%)</th>
<th>$F_1$ (%)</th>
<th>recall (%)</th>
<th>precision (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>That example is about gender.</td>
<td>90.0</td>
<td>81.8</td>
<td>85.8</td>
<td>78.2</td>
</tr>
<tr>
<td>This example is about gender.</td>
<td>89.0</td>
<td>80.5</td>
<td>87.0</td>
<td>74.9</td>
</tr>
<tr>
<td>That text is about gender.</td>
<td>88.4</td>
<td>79.6</td>
<td>86.8</td>
<td>73.5</td>
</tr>
<tr>
<td>This text is about gender.</td>
<td>87.9</td>
<td>79.3</td>
<td>88.9</td>
<td>71.5</td>
</tr>
<tr>
<td>That is about gender.</td>
<td>87.1</td>
<td>75.1</td>
<td>74.7</td>
<td>75.5</td>
</tr>
<tr>
<td>That text is about gender.</td>
<td>81.6</td>
<td>52.9</td>
<td>39.5</td>
<td>79.8</td>
</tr>
</tbody>
</table>

Table 16: Results for supporting hypotheses aimed at detecting texts concerning gender, which in HateCheck corresponds to the categories transgender people and women.

<table>
<thead>
<tr>
<th>hypothesis</th>
<th>accuracy (%)</th>
<th>$F_1$ (%)</th>
<th>recall (%)</th>
<th>precision (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>That text is about myself.</td>
<td>97.4</td>
<td>38.5</td>
<td>37.0</td>
<td>40.0</td>
</tr>
<tr>
<td>This text is about myself.</td>
<td>96.4</td>
<td>33.7</td>
<td>42.0</td>
<td>28.1</td>
</tr>
<tr>
<td>That is about myself.</td>
<td>97.3</td>
<td>33.3</td>
<td>30.9</td>
<td>36.2</td>
</tr>
<tr>
<td>That is about myself.</td>
<td>97.0</td>
<td>31.3</td>
<td>30.9</td>
<td>31.6</td>
</tr>
<tr>
<td>That example is about myself.</td>
<td>96.2</td>
<td>31.2</td>
<td>39.5</td>
<td>25.8</td>
</tr>
<tr>
<td>That text is about myself.</td>
<td>95.9</td>
<td>31.1</td>
<td>42.0</td>
<td>24.6</td>
</tr>
<tr>
<td>This text is about us.</td>
<td>85.1</td>
<td>16.8</td>
<td>69.1</td>
<td>9.6</td>
</tr>
<tr>
<td>That text is about us.</td>
<td>89.4</td>
<td>16.2</td>
<td>46.9</td>
<td>9.8</td>
</tr>
<tr>
<td>That is about us.</td>
<td>88.3</td>
<td>14.8</td>
<td>46.9</td>
<td>8.8</td>
</tr>
<tr>
<td>That example is about us.</td>
<td>77.4</td>
<td>12.8</td>
<td>76.5</td>
<td>7.0</td>
</tr>
<tr>
<td>That example is about us.</td>
<td>75.8</td>
<td>12.1</td>
<td>76.5</td>
<td>6.6</td>
</tr>
<tr>
<td>That is about us.</td>
<td>73.9</td>
<td>10.3</td>
<td>69.1</td>
<td>5.6</td>
</tr>
</tbody>
</table>

Table 17: Results for supporting hypotheses aimed detecting if a text is self-directed.
### Table 18: Results for supporting hypotheses aimed at detecting the stance of an outer text $p_1$ towards its inner, quoted text $p_0$. Precision, recall and $F_1$-score are omitted, since with only positive test examples no false positives and true negatives are possible.

<table>
<thead>
<tr>
<th>hypothesis</th>
<th>accuracy (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This text supports [X].</td>
<td>100.0</td>
</tr>
<tr>
<td>This supports [X].</td>
<td>100.0</td>
</tr>
<tr>
<td>That supports [X].</td>
<td>100.0</td>
</tr>
<tr>
<td>This example supports [X].</td>
<td>91.9</td>
</tr>
<tr>
<td>That example supports [X].</td>
<td>91.9</td>
</tr>
<tr>
<td>That text supports [X].</td>
<td>85.5</td>
</tr>
<tr>
<td>This text is for [X].</td>
<td>69.4</td>
</tr>
<tr>
<td>This is for [X].</td>
<td>50.9</td>
</tr>
<tr>
<td>That is for [X].</td>
<td>46.8</td>
</tr>
<tr>
<td>That text is for [X].</td>
<td>38.7</td>
</tr>
<tr>
<td>This example is for [X].</td>
<td>18.5</td>
</tr>
<tr>
<td>That example is for [X].</td>
<td>0.0</td>
</tr>
</tbody>
</table>

This supports [X]. 100.0
That supports [X]. 100.0
That supports [X]. 100.0
This example supports [X]. 91.9
That example supports [X]. 91.9
That text supports [X]. 85.5
This text is for [X]. 69.4
This is for [X]. 50.9
That is for [X]. 46.8
That text is for [X]. 38.7
This example is for [X]. 18.5
That example is for [X]. 0.0
Author Index

Barbarestani, Baran, 43
Barrett, Leslie, 62
Daelemans, Walter, 37
Das, Millon, 10
Das, Mithun, 10
Davis, Brian, 16
Goldzycher, Janis, 75
Hale, Scott, 52
Joshi, Raviraj, 1
Kegan, Robert, 62
Kirk, Hannah, 52
Kumari, Kirty, 30
Litvak, Marina, 68
Machlouf, Or, 68
Maks, Isa, 43
Markov, Ilia, 37
Milosevic, Tijana, 16
Ortan, Alexandra, 62
Patil, Hrushikesh, 1
Saha, Punyajoy, 10
Schneider, Gerold, 75
Seshadri, Madhavan, 62
Srivastav, Shaury, 30
Suman, Rajiv Ranjan, 30
Talker, Sagiv, 68
Vanetik, Natalia, 68
Velankar, Abhishek, 1
Verma, Kanishk, 16
Vidgen, Bertie, 52
Vossen, Piek, 43