Multi-Modal Personalized Hate Speech Analysis using Differential Dataset Cartography

Jan Kocoń, Joanna Baran and Kamil Kanclerz

Department of Artificial Intelligence, Wrocław University of Science and Technology, Poland

Abstract

In recognizing hate speech in text, a frequently overlooked aspect is the specific recipient of the content. Information about the user can be considered as another potential modality in addition to the textual representation. In this work, we present the multi-modal hate speech detection problem as a task of personalized prediction based on text and human representation learned from historical user decisions against offensive content, also as the subjective perception of humiliation, insult, sentiment, and violence. In addition, we present our Differential Data Maps method for visually comparing models for hate speech detection. Our results show that personalized models significantly better predict hate speech against a given individual, and the proposed explainable artificial intelligence method allows us to formulate new hypotheses about the impact of personalization on model performance.

Keywords

hate speech, natural language processing, personalization models, differential dataset cartography

1. Introduction

In the classical approach to text classification in natural language processing (NLP), the goal of a task is to assign one or more labels to a text based on its content [1, 2, 3, 4]. For example, it might be identifying fake news [5, 6], emotions [7, 3, 8, 9, 10, 11, 12], or hate speech [13, 14, 15]. However, it is difficult to define these tasks unambiguously, and one can find various definitions in the literature that are not consistent [16, 17]. Similarly, it is natural to react differently to the same content. These differences may be due to where we were born, how old we are, what kind of education we have, and what cultural background we belong to. A growing body of research shows that even with this information, we are not necessarily in a position to significantly better predict how a particular person would react to the content of a text [18, 17].

In recent years, personalized models have become increasingly popular in prediction tasks [18, 19, 20, 21]. These models get information about a person and the content as input. It turns out that the most important from the perspective of a subjective task (e.g., recognizing the offensiveness of a text) is at least minimal knowledge about a person in the form of his or her decisions concerning a few examples of content [22]. Moreover, this type of information
significantly improves the prediction quality, and the value of this improvement is much higher than if only demographic information is provided [23]. However, this approach tends to be more costly, requiring manual annotations from hundreds and sometimes even thousands of users for model development. Additionally, it is desirable (though not necessary) that multiple users evaluate the same text in such a collection [24]. Additionally, inference on a production model requires a minimum of information about the user for whom the model predicts potential responses [18, 19, 23].

There are many different ways to represent a human in such personalized architecture. In state-of-the-art approaches, this is usually trainable user embedding. It can be part of the transformer model, such as the UserId model [25]. Still, it can also be a separate component supporting the transformer model and conceptually similar to neural collaborative filtering, such as HuBi-Medium [19]. Analysis of results of such models from the literature for related tasks, e.g., emotion recognition in text [26, 23], shows that state-of-the-art models produce very similar results when using traditional measures such as F1-Score or R-Squared. However, detailed case analysis often shows that different personalized models improve different cases. It is essential to develop more sophisticated explainable artificial intelligence (XAI) methods that show differences that are not visible using standard classification or regression quality measures.

In this work, we present an adaptation of personalized models to analyze multi-modal hate speech in text. We consider modalities such as the content of the text and the identifier of the user who rated the text. In addition, we present our new XAI method called Differential Data Maps (DDM), which allows us to analyze differences in models that have similar classification results. We studied the Measuring Hate Speech dataset [27] for selected offensive categories. The results show that personalized models significantly improve hate speech prediction quality for known users. In addition, we present examples of hypotheses that can be drawn from analyses of differences between baseline and personalized models using DDM.

2. Related Work

The lack of a precise definition of hate speech makes it a rather complex phenomenon that requires additional expertise to conduct a proper analysis. One can take advantage of the user context to tackle the complex nature of detecting it. The use of user perspective appears to significantly improve the performance of many hate speech-related domains, including sarcasm detection [28, 29], sentiment analysis [30], self-deprecating humor recognition [31], offensive content detection [32], and general hate speech analysis [33, 16]. The assumption regarding the influence of user preferences on the final label is contrary to the concept of the gold standard, which is commonly used in many natural language processing tasks. Some authors [34] believe that the truth has a purely relative nature and is strongly related to agreement and consensus. However, there are many approaches focused on addressing the users’ various points of view. The most common is the generalized approach, which assumes that the majority’s perspective is the gold standard [35]. Another approach is to generate user clusters according to their beliefs and then represent each group’s point of view as a separate true label [36]. Experiments indicate that providing knowledge on diverse user perspectives outperforms a model trained on fully
aggregated data [37, 19].

Modern artificial intelligence (AI) methods are characterized by complex nature. A large number of parameters allows them to learn intricate data patterns. However, there is a risk that the model has memorized specific examples from the training set but does not have general knowledge of the phenomenon it should learn about. To prevent this, explainable artificial intelligence methods should be used to understand the model behavior [38, 39]. Moreover, identifying a missing part can significantly improve the effectiveness of a model [40].

On the other hand, apart from scientists, there is a growing need for everyday users to understand AI solutions thoroughly. AI’s ethics, trust, and bias are difficult to pinpoint when the algorithm is treated as a black box [41]. Explanations must make the AI algorithm expressive, improving human understanding and confidence that the model makes just and impartial decisions [42]. Furthermore, to guarantee the personalized model’s trust, transparency, and fairness, it is necessary to provide an advanced evaluation procedure focused on explaining the impact of user context on model behavior.

3. Dataset

To evaluate various personalized architectures, we leveraged the Measuring Hate Speech (MHS) dataset [27]. It contains 39,565 samples representing comments obtained from social media services, including YouTube, Twitter, and Reddit. The texts are annotated by 7,912 people from the Amazon Mechanical Turk platform. The users focused on intensity levels for five types of offensiveness: (1) hate speech, (2) humiliation, (3) insult, (4) sentiment, and (5) violence. We treated each type as another NLP task – a distinct output of the model. The distribution of labels for each task is presented in Figure 1. Most MHS dimensions are heavily unbalanced, like

![Figure 1: MHS dataset label distribution across different modalities. The diversity of values between similar dimensions demonstrates the subjective nature of the offensiveness detection.](image-url)
hate speech, sentiment, and violence. An inverse correlation has been observed between the last two.

4. Personalized Models

To explore the impact of providing knowledge about the user, we selected four different neural-based architectures: one non-personalized (Baseline) and three personalized (HuBi-Medium, UserId, and UserIdentifier). We used the backpropagation algorithm during the training procedure for all described models.

1. **HuBi-Medium** [19] – leveraging the idea of collaborative filtering [43], this architecture learns a personal vector representation that encapsulates personal preferences about the selected task. Similar to the original collaborative filtering, the user vector is multiplied using Hadamard product operation with the textual vector. The final vector is then fed to linear layers.

2. **UserId** [17] – this model represents the information about the user by appending their unique ID token to the beginning of the text. The vector representation is obtained via the transformer model by encoding the concatenation of the text and user ID. We manually added the user ID tokens to the model’s special token set to avoid splitting them during the tokenization procedure.

3. **UserIdentifier** [18] takes into account the identity of the text’s author. A data augmentation method involves adding tokens that identify the user. The string is generated from the username or sampled uniformly from the tokenizer vocabulary and then appended to the beginning of a text. UserIdentifier uses the same set of parameters to embed both sample content and user identifiers, which is more straightforward than relying on user-specific embeddings and has been shown to achieve high performance.

5. Differential Data Maps

The idea was inspired by work [44]. The authors present a Data Maps method using a machine learning model to visualize a dataset. It allows seeing how specific elements of the training set are characterized during the learning process. The intuition behind training dynamics is that the model learns to recognize some elements immediately. For other elements, the model needs more learning epochs, during which it can interchangeably make good or bad decisions relative to the ground truth. Finally, the model cannot learn the ground truth for the last group of elements. Three major training dynamics measures for the $i$th sample in the dataset were introduced:

1. **Confidence**, \( \hat{\mu}_i \) – captures how confidently the model assigned a true label to the sample, calculated as a mean probability across epochs;

2. **Variability**, \( \hat{\sigma}_i \) – measures how the model was indecisive about sample label during training using standard deviation (low value means the stable prediction of one label, and high value - often change of assigned label);
3. **Correctness**, $\hat{c}_i$ – a fraction of correctly predicted labels for the sample across training epochs.

In this work, we extend the idea of Data Maps by proposing visualizing the differences between models in the listed training dynamics measures. Our new method, Differential Data Maps, allows us to interpret differences in the performance of different model architectures and analyze the effect of selected characteristics describing the data on the difference in training dynamics on the same dataset. We define three new metrics based on those presented for Data Maps. Let M1 and M2 be different models trained on the same dataset. Then for $i$th sample in this dataset, we define new measures:

1. **Confidence change**: $\hat{\mu}_C^i = \hat{\mu}_{M2}^i - \hat{\mu}_{M1}^i$
2. **Variability change**: $\hat{\sigma}_C^i = \hat{\sigma}_{M2}^i - \hat{\sigma}_{M1}^i$
3. **Correctness change**: $\hat{c}_C^i = \hat{c}_{M2}^i - \hat{c}_{M1}^i$

### 6. Experiments

The experimental part was performed on the previously described MHS dataset, which was divided into three sets to provide sufficient prior knowledge in training set about users’ profiles. For this purpose, the data were grouped by `annotator_id` and filtered out those who gave less than 20 reviews. The entries rated by the same annotator were then divided between the splits in a ratio of 6:2:2. The final statistics of the training and evaluation data are shown in Table 1.

<table>
<thead>
<tr>
<th>Split</th>
<th>#Samples</th>
<th>Avg text count per user</th>
</tr>
</thead>
<tbody>
<tr>
<td>Train</td>
<td>29,170</td>
<td>12.6 ± 0.8</td>
</tr>
<tr>
<td>Validation</td>
<td>9,817</td>
<td>4.2 ± 0.4</td>
</tr>
<tr>
<td>Test</td>
<td>10,888</td>
<td>4.7 ± 0.5</td>
</tr>
</tbody>
</table>

RoBERTa-base pretrained language model [45] was used as a baseline and in personalized approaches. Models were fine-tuned using AdamW optimizer with learning rate 1e-5 and batch size equal to 32. Additionally, we used a linear warm-up schedule for 1000 training steps. The maximum sequence length was set to 512. The best model was selected according to the validation F-score across 30 epochs. For UserIdentifier, we took ten tokens drawn from the tokenizer vocabulary as an identifier. This has enabled better differentiation between users than relying on usernames or strings of numbers. On the other hand, the UserId model leveraged the embedding of a special ID token, which is a concatenation of the word `user`, an underscore character (\_), and a unique index number for a specific user, i.e., `user_1`.

All experiments were repeated ten times with the same data order but different weights (the model seed was changing). To plot DDM, training dynamics were also logged after each epoch. Two classification metrics were reported to compare model performance. In the last step, we assessed the statistical significance of achieved results differences between each method. After checking the assumptions of the t-student test, its score was calculated accordingly. The Mann-Whitney U test was applied if t-test conditions were not met for independent samples.
7. Results

Table 2 shows the results of the Baseline model and the other three personalized models. The models were evaluated on an MHS dataset for five dimensions of offensiveness. We measured the performance quality using the macro F1-score and accuracy. Analysis of the results shows that for the F1-macro measure for all dimensions of offensiveness, a significant quality gain is observed relative to the baseline for personalized models. The best among them is the HuBi-Medium model, for which the gain is 7.03 pp for hate speech, 4.2 pp for insult, 9.54 pp for violence, 4.08 pp for humiliate and 3.2 pp for sentiment, respectively. For the Accuracy measure, statistically significant quality gains were observed for three of the five dimensions, i.e., hate speech, violence, and humiliate. Further analysis showed no significant differences between the personalized models for this measure.

It is much more interesting to analyze the differences between the baseline and personalized models using DDC. Figure 2 shows the original DC graph, generated using the method described in [44]. For virtually all dimensions, the graphs for the baseline model look very similar, and larger differences are observed between the graphs of the various personalized models. The original DC graph, however, is difficult to interpret, as all that can be said is how the distribution of confidence and variability values changes in a general way for all cases. There are some dimensions (e.g., sentiment) for which the DC charts are very similar, regardless of the model used. However, significant differences can be seen by analyzing the DDC graph for data samples; see Figure 3. For the sentiment, it can be seen that the UserIdentifier model improves the correctness of the model for the vast majority of samples. At the same time, for Userld, there appears to be a smaller but significantly large group of samples for which the correctness decreases. Paradoxically, for the best model, HuBi-Medium, we observe the largest groups of cases characterized by the greatest decrease in correctness. We hypothesize that the person component of the multimodal model causes the model to start getting wrong more often in the learning process. However, the result is ultimately better than the baseline model. The UserIdentifier model makes the least amount of these mistakes in the learning process, but this does not translate into better quality as measured by the F1-score. HuBi-Medium is also the
**Figure 2**: The original Data Maps method for data samples across different modalities. Depending on the model used, data division between hard-to-learn, ambivalent and easy-to-learn changed.

only model for which variability decreases relative to baseline in the vast majority of samples, indicating that the personalization component for this model significantly affects the rate at which the model converges to a local optimum, after which there is little variation in subsequent epochs.
Figure 3: Results of the Differential Data Maps for data samples.

Furthermore, interesting results can be observed in the DDC variant, in which the training data are aggregated after users; see Figure 4. Each point on the graph represents cases annotated by a particular person, and the place on the graph indicates the shift of the personalized model results relative to the baseline. In addition, we added information indicating the entropy of the user’s ratings in the set. The UserIdentifier model for all dimensions of offensiveness resulted
Figure 4: Results of the Differential Data Maps for data samples aggregated by users.

In increased correctness and variability for most users. The lower the entropy of user ratings, the higher the correctness. In the UserID model for dimensions in which a large group of users has variability lower than the baseline (insult, sentiment), we observe no significant differences between the baseline and personalized models. Finally, for HuBi-Medium, the lack of significant differences is strongly correlated with the largest increase in confidence. In addition, it can be
seen that for all dimensions, we observe a significant decrease in variability, with confidence decreasing most strongly for users with high entropy and mostly increasing for users with low entropy.

8. Conclusions and Future Work

In this article, we presented a novel evaluation method called Differential Dataset Cartography. It allows for pairwise visual comparison of model performance. During experiments, we have shown interesting findings provided by our new method. However, further analysis could help identify more insights that could not be obtained from the raw metric values.

The experiments show that including the user context results in significantly improved performance compared to the baseline model. The evaluation metrics show that the HuBi-Medium model outperformed other architectures in most tasks. However, using DDM provided an additional perspective for analyzing the model behavior. Our method emphasized the difference in user representations and the nature of training each of the personalized architectures. It also provided additional information on how each architecture gathers knowledge about users.

Moreover, by aggregating the DDM by users, we explored how much knowledge the model can extract from a specific user. This shows another aspect of human perception – we can discover how difficult it is to learn the preferences of a single person from the model point of view. This can be used as additional feedback relevant during the annotation process to estimate how much data we need about a particular user to learn their perspective effectively. Furthermore, a precise user learning difficulty estimate can be helpful during the architecture design process, which should consider awareness of the general difficulty level of the task.

In future work, we will conduct more experiments using other datasets to obtain more knowledge about the behavior of personalized models. In addition, we want to analyze in detail the samples that form the clusters that can be observed in the DDM charts. This will help to understand the impact of specific samples on the model efficiency. The code for all methods and experiments is publicly available in CLARIN-PL repository⁴.

Acknowledgments

This work was financed by (1) the European Regional Development Fund as a part of the 2014-2020 Smart Growth Operational Programme, project no. POIR.01.01.01-00-0288/22 (JK); POIR.04.02.00-00C002/19 (JB, KK), (2) the statutory funds of the Department of Artificial Intelligence, Wroclaw University of Science and Technology.

References


⁴https://github.com/CLARIN-PL/personalized-nlp/releases/tag/2023-aaai-defactify


