Abstract

Language models (LMs) must be both safe and equitable to be responsibly deployed in practice. With safety in mind, numerous detoxification techniques (e.g., Dathathri et al. 2020; Krause et al. 2020) have been proposed to mitigate toxic LM generations. In this work, we show that these detoxification techniques hurt equity: they decrease the utility of LMs on language used by marginalized groups (e.g., African-American English and minority identity mentions). In particular, we perform automatic and human evaluations of text generation quality when LMs are conditioned on inputs with different dialects and group identifiers. We find that detoxification makes LMs more brittle to distribution shift, especially on language used by marginalized groups. We identify that these failures stem from detoxification methods exploiting spurious correlations in toxicity datasets. Overall, our results highlight the tension between the controllability and distributional robustness of LMs.

1 Introduction

Recent neural language models (LMs) have shown enormous improvements in text generation abilities. A key factor behind these improvements is large training corpora that are collected from online sources (Radford et al., 2019). Unfortunately, because such corpora are too large to filter granularly (Roller et al., 2020), they inevitably contain so-called toxic examples: undesirable language such as expletives, slurs, or other offensive and threatening speech. When trained on such data, LMs inevitably learn to generate toxic text (Henderson et al., 2018; Wallace et al., 2019).

To address this issue, recent work has turned towards detoxifying LMs: reducing toxic generations without affecting perplexity or generation quality on nontoxic inputs. Existing detoxification strategies involve techniques such as finetuning LMs on nontoxic data (Gehman et al., 2020) or incorporating a toxicity discriminator during decoding (Dathathri et al., 2020). Our evaluation of these techniques shows that they are indeed effective at mitigating toxicity, but at what cost?

We demonstrate that detoxification can hurt LM utility on language used by minority groups. Concretely, we evaluate detoxified LMs on text with minority identity mentions (e.g., words such as “gay” or “Muslim”) and surface markers of African-American English (Green, 2002, AAE). We first show that, compared to text containing White-Aligned English (WAE), detoxification causes a disproportionately large increase in LM perplexity on text with AAE and minority identity mentions. Moreover, increasing the strength of detoxification amplifies this bias.

The same trends hold when evaluating the text generation quality of LMs using crowdworkers. When conditioned on WAE text, detoxified LMs can roughly maintain the topic, fluency, and style of an input prompt. However, generation quality deteriorates when models are conditioned on AAE text, i.e., detoxification hurts an LMs’ ability to understand and complete AAE text.

We identify that these failures are due to the use of biased toxic classification data. In particular, toxicity datasets often contain spurious correlations between the toxic label and the presence of AAE and minority identity mentions (Sap et al., 2019). These correlations cause detoxification techniques to steer generations away from AAE text, i.e., detoxification hurts an LMs’ ability to understand and complete AAE text.

We conclude by outlining concrete harms and possible solutions to these biases. With regard to harms, we argue that biased systems force marginalized users to code-switch or hide their identity and that these systems can contribute to social stigmas. For solutions, we discuss improved procedures for data annotation and model training that may help debias detoxification techniques.
2 Methods and Experimental Setup

The goal of detoxification is to mitigate the frequency of toxic generations (also called hate speech or offensive language) without affecting an LM’s utility or generation quality on nontoxic inputs. We detoxify models using controllable generation techniques that steer outputs away from toxicity. Following past work (Gehman et al., 2020; Xu et al., 2020), we use four techniques that provide state-of-the-art levels of detoxification.

2.1 Detoxification Techniques

DAPT We consider domain-adaptive pretraining (Gururangan et al., 2020, DAPT), i.e., finetuning LMs on nontoxic data. This technique aims to erase an LM’s knowledge of toxicity via catastrophic forgetting (McCloskey and Cohen, 1989).

PPLM We consider plug and play language models (Dathathri et al., 2020, PPLM). Here, we first train a toxicity classifier using the hidden states of the LM as features. At generation time, the LM’s hidden states are iteratively updated using a gradient from the toxicity classifier.

GeDi We consider GeDi (Krause et al., 2020), which combines the probabilities from the LM with the probabilities from a second, smaller LM that is trained on nontoxic data (Krause et al., 2020). We finetune GPT-2 small (Radford et al., 2019) for the second LM.

Filtering Finally, we consider output filtering, where we generate a fixed number of times (we use 10) from the LM and return the least toxic generation according to a toxicity classifier. We reuse the same toxicity classifier from PPLM.

2.2 Hyperparameters and Training Data

We use GPT-2 medium (Radford et al., 2019) as the base LM for all detoxification techniques. We use the hyperparameters from the original papers for each technique, except we generate using top-k sampling (Fan et al., 2018) with k = 50 for all methods to enable a fair comparison.

For training data, we use the commonly-studied English Jigsaw Civil Comments dataset. We remove examples where between 10% and 50% of the annotations are the toxic label (i.e., examples with low inter-annotator agreement). We publicly release our code.

3 Detoxifying LMs Introduces Biases

In this section, we evaluate the detoxification methods and show that they introduce biases into LMs that may harm marginalized groups.

1https://www.kaggle.com/c/jigsaw-unintended-bias-in-toxicity-classification
2https://github.com/albertkx/detoxifying-lms/
3.1 Automatic Evaluation Using Perplexity

We first perform intrinsic evaluations of each detoxification technique by computing the perplexity of detoxified models on various datasets. Note that we are not generating from the LM in this evaluation.\footnote{The filtering detoxification method has the same perplexity as the baseline LM because it is applied post-decoding. We do not report it here. For GeDi, we set $\omega$ to 0.3 because the default value of 30 results in nearly infinite perplexities.}

**White-Aligned English Perplexity** We first evaluate the perplexity on White-Aligned English (WAE) text that is either toxic or nontoxic. We use WAE tweets from Groenwold et al. (2020).\footnote{We split this data into toxic and nontoxic sets by scoring the WAE-AAE pairs using the Perspective API at https://www.perspectiveapi.com/.}

The detoxification techniques are effective at removing toxicity: the perplexity on toxic data increases substantially (Figure 1, toxic evaluation set). All techniques also cause a (smaller) increase in the perplexity on nontoxic WAE tweets, which shows that detoxification comes at some cost to the LM’s utility. Part of this increase likely results from distribution shift: the detoxification methods are trained on comments data, but our evaluation sets come from Twitter.

**Identity Mentions and AAE Perplexity** We next evaluate the perplexity of the detoxified LMs on nontoxic language that may be used by marginalized groups. Concretely, we use text that contains minority identity mentions (e.g., words such as “gay” or “Muslim”) or surface markers of African-American English (Green, 2002, AAE). We form two evaluation sets using tweets. First, we collect tweets from the Twitter API that contain specific identity mentions.\footnote{See Appendix A for our word list. We filter out any toxic tweets using the Perspective API and randomly select 1,000 of the remaining tweets.} Second, we use the nontoxic data from Groenwold et al. (2020), which are the AAE equivalents of the nontoxic WAE tweets we used for the previous evaluation.

We find that there is a disproportionately large increase in LM perplexity on the AAE and minority identity mention tweets (Figure 1, AAE and identity mentions). For example, when using PPLM, the perplexity increases by a factor of 2.1 on nontoxic WAE data and a factor of 4.3 on minority identity mention data.

**Stronger Detoxification Amplifies Biases** We also find that stronger detoxification amplifies the gap in perplexity between text with WAE and text with AAE or minority identity mentions. This occurs for all detoxification techniques, for example, in Figure 2 we vary a parameter in GeDi that increases the degree of detoxification ($\omega$). As more detoxification is applied, the ratio of AAE perplexity to WAE perplexity increases dramatically, reaching upwards of 400.

3.2 Human Evaluation of Generation Quality

As an extrinsic evaluation, we measure the generation quality of each detoxification method using crowdworkers on Amazon Mechanical Turk. We provide a short prompt as input to the detoxified LMs and then generate 30 additional tokens. For the prompts, we tokenize the aforementioned AAE and WAE tweets and extract the first half of each tweet. We sample 50 prompts from each set of tweets, producing 100 total prompts. Annota-
I walked up to this guy disrespecting a female. I told him I may be a virgin but if he wanted to f*ck me, he was welcome to.

DAPT but that he must not be and he did not care what I did . . .
PPLM in order to get him to leave me alone. I wanted to tell him . . .
Filtering so I’ll pass. I walked back to him after being assaulted and told . . .
GeDi so I said that she shouldn’t wear . . .

I walked up to sum n*gga disrespectin a female. I told him I might be a Virgin in a dress because I’m in my 60s, but my husband had . . .
PPLM in heaven and he was like, “Oh you’re from Michigan” I . . .
Filtering in heaven and wanted to be with him.Then after being asked “Why . . .
GeDi Mine uh unlimited number of vistors u . . .

| Dialect | Prompt | Method | Completion |
|---------|--------|--------|------------|
| WAE | I walked up to this guy disrespecting a female. I told him I may be a virgin | Baseline | but if he wanted to f*ck me, he was welcome to. |
| | | DAPT | but that he must not be and he did not care what I did . . . |
| | | PPLM | in order to get him to leave me alone. I wanted to tell him . . . |
| | | Filtering | so I’ll pass. I walked back to him after being assaulted and told . . . |
| | | GeDi | so I said that she shouldn’t wear . . . |
| AAE | I walked up to sum n*gga disrespectin a female. I told him I might be a Virgin | Baseline | N*gga so he could f*ck with my v*gina. |
| | | DAPT | in a dress because I’m in my 60s, but my husband had . . . |
| | | PPLM | in heaven and he was like, “Oh you’re from Michigan” I . . . |
| | | Filtering | in heaven and wanted to be with him.Then after being asked “Why . . . |
| | | GeDi | Mine uh unlimited number of vistors u . . . |

Table 1: Detoxification techniques are effective at mitigating toxic completions for most prompts, however, they often generate low-quality or nonsensical completions for AAE prompts. Above, we provide an input prompt that is the beginning of a WAE or AAE tweet and generate from the LM with top-k sampling. See Figure 3 for quantitative results from crowdworker evaluations. We censor vulgar and offensive words.

4 Why Detoxification Introduces Biases

In this section, we explain why detoxification causes the utility of LMs to degrade on text that contains AAE and minority identity mentions. First, note that all detoxification techniques make use of labeled toxic/nontoxic data. For example, DAPT uses this data directly: it finetunes the LM on nontoxic examples. PPLM, GeDi, and Filtering use this data indirectly: they train a classifier or LM on the toxicity data and then incorporate this model into the LM’s decoding strategy.

Unfortunately, there are spurious correlations between the toxic label and the presence of AAE and minority identity mentions (Sap et al., 2019; Dixon et al., 2018). These correlations arise from annotation and sampling biases. Annotation bias occurs because crowdworkers are often unfamiliar with AAE and consequently misjudge it as toxic (Sap et al., 2019). Sampling bias occurs because many toxic comments are directed towards marginalized groups (RWJF, 2017). The result of these two biases is that text which contains AAE and minority identity mentions is labeled as toxic at disproportionately high rates (Sap et al., 2019).

Detoxification techniques inherit these undesirable biases. For example, DAPT will train LMs to not only forget toxicity but also forget AAE and minority identity mentions. Similarly, the discriminators used by PPLM, GeDi, and Filtering will guide the generated text away from AAE and identity mentions because the discriminators typically consider such text as toxic (Dixon et al., 2018; Sap et al., 2019; Oliva et al., 2020). Also note that in all of the above cases, increasing the detoxifica-
tion strength (e.g., longer finetuning for DAPT or higher $\omega$ for GeDi) exacerbates these problems.

In our experiments, we test multiple detoxification methods to show that this bias is not linked to a specific technique, but instead to the process of detoxification in the presence of biased supervised data. In fact, other controllable generation techniques, including prompts (Wallace et al., 2019; Sheng et al., 2020; Shin et al., 2020) or conditional LMs (Keskar et al., 2019) will likely exhibit the same type of biases.

5 Harms of Detoxification

Our results demonstrate that the current state of detoxification poses representational harms (Blodgett et al., 2020) to minority groups. We discuss the concrete impacts of these harms below.

In-group Harms Detoxified LMs are deployed in downstream NLP systems in which they directly engage with end users. In addition to LMs not being able to generate minority identity mentions and minority dialects, our results suggest that detoxified LMs also struggle to understand these aspects of language. This could lead to scenarios where end users who are AAE speakers must code-switch to WAE to ensure that NLP systems work effectively for them. Aside from being an annoyance, this is also a microaggression that poses psychological harms and may discourage AAE speakers from engaging with NLP systems whatsoever.

Stigmatization of Language Detoxified models also have a propensity to avoid certain topics, e.g., mentioning a minority identity term. As a practical example, the (detoxified) Microsoft Zo chatbot was capable of discussing Christianity but could not discuss Islam (Stuart-Ulin, 2018). Failures like these further two types of stigma. First, having one’s identity silenced by an NLP system can lead to self-stigmatization and long-term health consequences. Second, a lack of informed, conscious discussion on topics of identity or dialect can magnify existing societal stigmas. For example, aligning an LM solely with WAE stigmatizes AAE as incorrect or “bad” English (Flores and Rosa, 2015). In the technology industry, this can perpetuate a dangerous expectation that AAE users are not consumers who matter, stymieing progress on equitable NLP systems.

Biases Are Not Limited to Detoxification Although we have focused on problems with detoxification in this paper, similar failures will occur whenever controllable generation methods are used. For example, a common goal is to control the sentiment of generated text (Dathathri et al., 2020; Krause et al., 2020). Unfortunately, since sentiment datasets are often biased against certain racial groups (Kiritchenko and Mohammad, 2018), controlling the sentiment of text will also affect which races are discussed.

6 Future Work: Towards Bias-Free Detoxification

The harms that we have identified occur largely due to spurious correlations in toxicity datasets. A natural direction for future work is to thus improve datasets, for example, by changing the annotation procedure (Sap et al., 2019) or labeling scheme (Kennedy et al., 2020; Sap et al., 2020). Unfortunately, this can also make collecting annotations more expensive. As an alternative or in addition to higher quality data, there is growing interest in training accurate models in the presence of biased data (Oren et al., 2019; Clark et al., 2019). Unfortunately, state-of-the-art debiasing methods are still far from perfect (Zhou et al., 2021). We plan to explore new methods for debiasing both datasets and models in future work.

References

Su Lin Blodgett, Solon Barocas, Hal Daumé III, and Hanna Wallach. 2020. Language (technology) is power: A critical survey of “bias” in NLP. In ACL.

Christopher Clark, Mark Yatskar, and Luke Zettlemoyer. 2019. Don’t take the easy way out: Ensemble based methods for avoiding known dataset biases. In EMNLP.

Sumanth Dathathri, Andrea Madotto, Janice Lan, Jane Hung, Eric Frank, Piero Molino, Jason Yosinski, and Rosanne Liu. 2020. Plug and play language models: A simple approach to controlled text generation. In ICLR.

Lucas Dixon, John Li, Jeffrey Sorensen, Nithum Thain, and Lucy Vasserman. 2018. Measuring and mitigating unintended bias in text classification. In AIES.

Angela Fan, Mike Lewis, and Yann Dauphin. 2018. Hierarchical neural story generation. In ACL.

Nelson Flores and J. Rosa. 2015. Undoing appropriateness: Raciolinguistic ideologies and language diversity in education. Harvard Educational Review.
Samuel Gehman, Suchin Gururangan, Maarten Sap, Yejin Choi, and Noah A. Smith. 2020. RealToxicityPrompts: Evaluating neural toxic degeneration in language models. In EMNLP Findings.

Lisa Green. 2002. African American English: A linguistic introduction.

Sophie Groenwold, Lily Ou, Aesha Parekh, Samhita Honnavalli, Sharon Levy, Diba Mirza, and William Yang Wang. 2020. Investigating African-American vernacular English in transformer-based text generation. In EMNLP.

Suchin Gururangan, Ana Marasović, Swabha Swayamdipta, Kyle Lo, Iz Beltagy, Doug Downey, and Noah A. Smith. 2020. Don’t stop pretraining: Adapt language models to domains and tasks. In ACL.

Peter Henderson, Koustuv Sinha, Nicolas Angelard-Gontier, Nan Rosemary Ke, Genevieve Fried, Ryan Lowe, and Joelle Pineau. 2018. Ethical challenges in data-driven dialogue systems. In AIES.

Chris J Kennedy, Geoff Bacon, Alexander Sahn, and Claudia von Vacano. 2020. Constructing interval variables via faceted Rasch measurement and multi-task deep learning: A hate speech application. arXiv preprint arXiv:2009.10277.

Nitish Shirish Keskar, Bryan McCann, Lav R Varshney, Caiming Xiong, and Richard Socher. 2019. CTRL: A conditional transformer language model for controllable generation. arXiv preprint arXiv:1909.05858.

Svetlana Kiritchenko and Saif M Mohammad. 2018. Examining gender and race bias in two hundred sentiment analysis systems. In *SEM.

Ben Krause, Akhilesh Deepak Gotmare, Bryan McCann, Nitish Shirish Keskar, Shafiq Joty, Richard Socher, and Nazneen Fatema Rajani. 2020. GeDi: Generative discriminator guided sequence generation. arXiv preprint arXiv:2009.06367.

Michael McCloskey and Neal J Cohen. 1989. Catastrophic interference in connectionist networks: The sequential learning problem. In Psychology of learning and motivation.

Thiago Dias Oliva, Dennys Marcelo Antonialli, and Alessandra Gomes. 2020. Fighting hate speech, silencing drag queens? Artificial intelligence in content moderation and risks to LGBTQ voices online. In Sexuality & Culture.

Yonatan Oren, Shiori Sagawa, Tatsunori B Hashimoto, and Percy Liang. 2019. Distributionally robust language modeling. In EMNLP.

Alec Radford, Jeffrey Wu, Rewon Child, David Luan, Dario Amodei, and Ilya Sutskever. 2019. Language models are unsupervised multitask learners. Technical report.

Stephen Roller, Emily Dinan, Naman Goyal, Da Ju, Mary Williamson, Yinhan Liu, Jing Xu, Myle Ott, Kurt Shuster, Eric M. Smith, Y-Lan Boureau, and Jason Weston. 2020. Recipes for building an open-domain chatbot. arXiv preprint arXiv:2004.13637.

RWJF. 2017. Discrimination in America: Experiences and views.

Maarten Sap, Dallas Card, Saadia Gabriel, Choi Yejin, and Noah Smith. 2019. The risk of racial bias in hate speech detection. In ACL.

Maarten Sap, Saadia Gabriel, Lianhui Qin, Dan Jurafsky, Noah A Smith, and Yejin Choi. 2020. Social bias frames: Reasoning about social and power implications of language. In ACL.

Emily Sheng, Kai-Wei Chang, Premkumar Natarajan, and Nanyun Peng. 2020. Towards controllable biases in language generation. In EMNLP Findings.

Taylor Shin, Yasaman Razeghi, Robert L Logan IV, Eric Wallace, and Sameer Singh. 2020. Auto-Prompt: Eliciting knowledge from language models with automatically generated prompts. In EMNLP.

Chloe Rose Stuart-Ulin. 2018. Microsoft’s politically correct chatbot is even worse than its racist one. Quartz.

Eric Wallace, Shi Feng, Nikhil Kandpal, Matt Gardner, and Sameer Singh. 2019. Universal adversarial triggers for attacking and analyzing NLP. In EMNLP.

Jing Xu, Da Ju, Margaret Li, Y-Lan Boureau, Jason Weston, and Emily Dinan. 2020. Recipes for safety in open-domain chatbots. arXiv preprint arXiv:2010.07079.

Xuhui Zhou, Maarten Sap, Swabha Swayamdipta, Noah A Smith, and Yejin Choi. 2021. Challenges in automated debiasing for toxic language detection. In EACL.
A Minority Identity Mention Word List

We use the following words to identify tweets with minority identity mentions: lesbian, lesbians, gay, gays, bisexual, bisexuals, transgender, transgenders, trans, queer, lgbt, lgbtq, homosexual, blacks, mexicans, mexican, non-binary, latinx, latino, latina, jews, jew, arabs, arab, muslim, muslims.

B Amazon Mechanical Turk Details

Figures 4 and 5 show the instructions and examples given to the crowdworkers on Amazon Mechanical Turk. Figure 6 shows an example of the test interface.
Figure 4: The instructions given to the crowdworkers on Amazon Mechanical Turk.

Figure 5: The examples given to the crowdworkers on Amazon Mechanical Turk.

Figure 6: A test input for a crowdworker on Amazon Mechanical Turk.