Avoiding catastrophic forgetting in mitigating model biases in sentence-pair classification with elastic weight consolidation

James Thorne
Department of Computer Science
University of Cambridge
jt719@cam.ac.uk

Andreas Vlachos
Department of Computer Science
University of Cambridge
av308@cam.ac.uk

Abstract

The biases present in training datasets have been shown to be affecting models for a number of tasks such as natural language inference (NLI) and fact verification. While fine-tuning models on additional data has been used to mitigate such biases, a common issue is that of catastrophic forgetting of the original task. In this paper, we show that elastic weight consolidation (EWC) allows fine-tuning of models to mitigate biases for NLI and fact verification while being less susceptible to catastrophic forgetting. In our evaluation on fact verification systems, we show that fine-tuning with EWC Pareto dominates standard fine-tuning, yielding models lower levels of forgetting on the original task for equivalent gains in accuracy on the fine-tuned task. Additionally, we show that systems trained on NLI can be fine-tuned to improve their accuracy on stress test challenge tasks with minimal loss in accuracy on the MultiNLI dataset despite greater domain shift.

1 Introduction

A number of recent works have illustrated shortcomings in the sentence-pair classification models that are used for Natural Language Inference (NLI) and fact verification that arise from limited or biased training data: Naik et al. (2018) demonstrated that phenomena such as the presence of negation or a high degree of lexical overlap, induce misclassifications on models trained on the MultiNLI dataset (Williams et al., 2018); Poliak et al. (2018) and Gururangan et al. (2018) identified an over-sensitivity to one of the two inputs in sentence-pair classification: biases introduced during the construction of the instances are exploited by models to learn associations between one of the two sentences and the label without considering the other – known as hypothesis-only bias.

Mitigating these biases is especially pertinent in the task of fact verification: predicting whether a claim is supported or refuted by evidence. It is critical that evidence is correctly taken into account when labeling an instance or generating an explanation to the end-user. A common model for fact verification (Pomerleau and Rao, 2017; Thorne et al., 2018) is text-pair classification between a claim and evidence retrieved from a trusted source (Nie et al., 2018; Yoneda et al., 2018; Hanselowski et al., 2018, inter alia).

To mitigate these undesirable behaviors caused by biases in the training data, Liu et al. (2019a) fine-tune models with a small targeted number of labeled instances exposing the bias to “inoculate” the models. In a different approach, Suntwal et al. (2019) delexicalize instances – replacing tokens with placeholders, preventing classifiers from exploiting mutual information between domain-specific noun-phrases and class labels. Belinkov et al. (2019) mitigate biases through adversarial training, penalizing the model for encoding a hypothesis-only bias. Finally, Schuster et al. (2019) re-weight the loss of instances during training guided by the mutual information between tokens and the instance labels.

Debiasing models is a multi-objective optimization problem where original task accuracy and is often sacrificed in favor of accuracy on a different evaluation set. With fine-tuning, the success is dependent both on the model capacity and the domain shift between the original and fine-tuning data (Liu et al., 2019a): using data that differs greatly from the original task results in a reduction in accuracy on the original task, a behavior called catastrophic forgetting (French, 1999).

In this paper, we show that regularizing fine-tuning with Elastic Weight Consolidation (Kirkpatrick et al., 2017, EWC) minimizes catastrophic forgetting by penalizing weight updates to pa-
parameters crucial to the original task when fine-tuning. We evaluate models trained on two datasets, MultiNLI and FEVER, and demonstrate that fine-tuning with EWC on stress-test data (Naik et al., 2018) and symmetric counterfactual instances (Schuster et al., 2019) mitigates model bias while yielding significantly lower reductions in accuracy compared to standard fine-tuning for a number of popular model architectures.

On all experiments on the FEVER task, fine-tuning mitigated model biases, increasing the absolute accuracy of a BERT model on the symmetric dataset by at least 10%. Without EWC, the original task accuracy reduced from 87% to 79% whereas with EWC, accuracy was reduced to 82%. Experimentally, we find the Pareto frontier of fine-tuning with EWC dominates the Pareto frontier of fine-tuning without it, indicating that higher gains on the fine-tuning task can be attained at the same cost to the original task when using EWC.

Similar patterns were observed when fine-tuning MultiNLI models with NLI stress-test data. Without EWC, absolute accuracy on the original task fell by 32% for both the DA and ESIM models when fine-tuning on the ‘antonym’ challenge set. Incorporating EWC minimized catastrophic forgetting to a 3% absolute reduction in accuracy for DA and 9% for the ESIM.

2 Mitigating biases with fine-tuning

Fine-tuning adapts the weights of a model trained on one task through further training to improve generalization on another task. The assumption underpinning its success (Luong and Manning, 2015) is that while the initial training of the model results in parameters that generalize well on another task (typically due to a larger training dataset available for the first task and its similarity between with the second one), accuracy can be further improved by fine-tuning them for the second task, typically by training on a small amount of data specific to it. This technique is commonly used in mitigating model biases (Liu et al., 2019a), where the data for the original task, while useful in model training, they often contain biases, which are dealt with by further training the model on instances targeting these biases.

While fine-tuning often addresses model biases, it can result in model parameters over-adjusting to the bias targeting instances and reducing the accuracy on the original task, referred to as catastrophic forgetting (French, 1999). One way to mitigate this issue is to regularize the updates to the parameters so that they do not deviate too much from those learned in the original task, which is also a motivation in multi-task training (Ruder, 2017).

Elastic Weight Consolidation (Kirkpatrick et al., 2017, EWC) penalizes parameter updates according to the sensitivity of the model to them in the original task. The model sensitivity is estimated by the Fisher information matrix, which describes the model’s expected sensitivity to a change in parameters, and near the (local) minimum of the loss function used for training is equivalent to the second-order derivative

\[ F = \mathbb{E}_{x \sim \mathcal{D}_{\text{original}}} \left[ \nabla^2 \log p(y|x; \theta) \right]. \]

In EWC, the Fisher information is used to elastically scale the cost of updating parameters \( \theta \) from the original value \( \theta^* \), controlled by the \( \lambda \) hyper-parameter, as follows:

\[
\mathcal{L}(\theta) = \mathcal{L}_{\text{FT}}(\theta) + \sum_i \frac{\lambda}{2} F_{i,i} (\theta_i - \theta_i^*)^2
\]

For efficient training, we use the empirical Fisher (Martens, 2014): diagonal elements are approximated through squaring first-order gradients from a sample of instances, recomputed before each epoch. If the Fisher information is not used (i.e. fixing \( F_{i,i} = 1 \)), this penalty is equivalent to L2 regularization, which we also compare against.

3 Experimental setup

We show through empirical evaluation that EWC mitigates catastrophic forgetting, preserving accuracy on the original task data, in two tasks: reducing hypothesis-only bias in fact verification systems and inoculating NLI classifiers against stress-tests exposing their biases. We first train models for each task without taking any steps to mitigate bias and compare the effect of EWC when fine-tuning to no regularization, L2 regularization and naively merging the challenge instances into the training data.

Mitigating hypothesis only bias in fact verification: We train models using sentence-pair instances extracted from the FEVER dataset released by Thorne et al. (2018). For the supported and refuted we use the evidence present in the dataset, and the NotEnoughInfo class, random
The pre-trained models are fine-tuned using 708 instances from the symmetric data released by Schuster et al. (2019). The symmetric dataset was constructed from a sample of the FEVER instances with SUPPORTED and REFUTED labels where the claims were retained but the evidence was replaced with a counterfactual statement that would negate the label – mitigating the hypothesis-only bias by reducing the mutual information between claims and labels. Following Schuster et al. (2019)'s evaluation, we train two ESIM variants (Chen et al., 2016), and a BERT (Devlin et al., 2019). As RoBERTa (Liu et al., 2019b) has been shown to be more robust to adversarial training (Bartolo et al., 2020), we also include this in our evaluation.

Mitigating model limitations in NLI stress tests: Liu et al. (2019a) observed catastrophic forgetting when fine-tuning DA (Parikh et al., 2016) and ESIM (Chen et al., 2016) models trained on MultiNLI (Williams et al., 2018) with the numerical-reasoning and antonym stress tests released by Naik et al. (2018). The stress test data were generated by modifying MultiNLI instances with templates and WordNet substitutions respectively. Following the same experimental setup, we fine-tune DA and ESIM models trained on MultiNLI and evaluate fine-tuning on stress-test data with and without EWC.

Experimental methodology For both tasks, each model was trained using default architectures and hyper-parameters adopted by the community using the AllenNLP implementations (Gardner et al., 2017). We trained 5 models with different random initializations until convergence allowing us to report the mean and standard deviation of the models’ accuracy. For fine-tuning, the learning rate, regularization penalties (for EWC and L2), and number of epochs were selected through 5-fold cross-validation using the development split of the fine-tuning datasets.

| Model          | Baseline | Merged | FineTuned | FineTune+L2 | FineTune+EWC |
|----------------|----------|--------|-----------|-------------|--------------|
| ESIM+GloVe     | 79.94 ± 0.4 | 79.57 ± 0.4 | 70.78 ± 1.1 | 73.29 ± 0.4 | 74.64 ± 0.7  |
| ESIM+ELMo      | 80.15 ± 0.2 | 80.33 ± 0.8 | 76.45 ± 0.8 | 73.72 ± 0.6 | 78.09 ± 0.4  |
| BERT Base      | 86.88 ± 0.5 | 86.87 ± 0.5 | 78.82 ± 0.9 | 79.90 ± 1.4 | 82.23 ± 1.1  |
| RoBERTa Base   | 88.12 ± 0.3 | 88.11 ± 0.1 | 82.51 ± 1.5 | 83.14 ± 1.4 | 85.12 ± 1.1  |

Table 1: Fine tuning FEVER NLI classifiers with symmetric data without (FineTuned column) and with (FT+EWC) elastic weight consolidation.
through adjusting the learning rate and regularization strength hyper-parameters. Regularizing with EWC Pareto dominates (Figure 1) standard fine-tuning for both the ESIM and BERT models, showing that, with EWC, equivalent gains on the symmetric task can be attained with a lower reduction in accuracy on the original FEVER task than standard fine-tuning.

Merging the instances from the symmetric dataset with the FEVER training data yielded modest improvements on the symmetric task without harming the original FEVER task accuracy. We attribute this to the impact of these 700 instances being diluted by the 145,000 training instances for the FEVER task. For the RoBERTa model, accuracy on the symmetric task increases to 87.03%. Although this does not exceed the accuracy of any of the fine-tuned models, it is not significantly worse than the FT+EWC treatment ($p = 0.06$).

4.2 Natural Language Inference

Without regularization, we found that the procedural generation of these instances induces different patterns and biases that models exploited the cost of the forgetting the original task if fine-tuned without regularization. In our experiments incorporating EWC (see Figure 2), the models are ‘inoculated’ against the patterns in the stress-test data – improving accuracies for the two challenges from 33% for both models to above 70% – but catastrophic forgetting is minimized. EWC was most effective for the ‘antonym’ challenge which had the largest domain shift from the original data due to all instances being labelled as contradiction as without regularization, the model just learned to predict the majority label.

**Antonym challenge:** Both the DA and ESIM models were sensitive to fine-tuning, attaining near perfect accuracy. The challenge data only contains instances labeled contradiction: the large domain shift from the MultiNLI dataset causes catastrophic forgetting in both the DA and ESIM models when fine-tuning. For the DA, accuracy on MultiNLI fell from 71.6% to 33.7%, and for the ESIM accuracy fell from 77.9% to 43.6%. With a low EWC penalty, both models attained > 99% accuracy on the challenge data, but MultiNLI accuracy only fell to 54.4% for the DA and 60.2% for the ESIM. With a higher EWC penalty the stress-test accuracy was 93.0% for the DA and 98.5% for the ESIM. Accuracy on MultiNLI fell to 66.2% and 68.6% for the two models respectively. While Liu et al. (2019a) do not show empirical evaluation for this challenge, their paper remarks that fine-tuning on data with a limited number of patterns is not informative due to models learning to predict the majority label. This is avoided with EWC.

**Numerical reasoning challenge:** The changes in accuracy were less extreme than the antonym challenge. The DA model achieved an accuracy on the stress-test challenge of 82.15% without EWC and 70.5% with EWC. The value reported by Liu et al. (2019a) was 77% but analysis also showed that a rule-based classifier could attain a score of 82.05% exploiting the terms ‘less than’ and ‘more than’ appearing in the hypothesis. Without EWC, the DA classifier learns this pattern at the cost of forgetting the original task: MultiNLI accuracy fell from 71.6% to 58.2%, whereas, with EWC it only fell to 68.5%. For the ESIM, the accuracy on the stress-test was 85.2% without EWC and 80.6%
with it. MultiNLI accuracy fell from 77.9% to 75.4% without EWC and 76.8% with EWC. Liu et al. (2019a) reported that fine-tuning ESIM reduced accuracy on MultiNLI from 78% to 71% to score 91% on the stress test.

5 Discussion

EWC has previously been successfully applied to neural machine translation (NMT), where Thompson et al. (2019) and Saunders et al. (2019) minimize catastrophic forgetting when adapting the domain of models through fine-tuning. Modelling debiasing as domain adaptation with EWC was successful in mitigating gender bias in NMT by Saunders and Byrne (2020).

When fine-tuning the NLI and fact verification models, EWC was also effective in minimizing catastrophic forgetting. All fine-tuning datasets exhibited a domain-shift from the original training data: for the antonym NLI dataset, all instances were labelled as CONTRADICTON and for the FEVER task, the symmetric dataset (Schuster et al., 2019) only contained instances for the SUPPORTED and REFUTED classes, with no instances for the NOENOUGHINFO class.

The FEVER dataset has a hypothesis-only bias (Schuster et al., 2019). This is indicated in Table 2 where training a model on only the claims and ignoring evidence yields an accuracy of 61.5%. If there was no mutual information between claims (without evidence) and labels, this should be 33%. The availability of counterfactual data meant that it was possible to experiment with fine-tuning as a mitigation strategy. However, this type of debiased data is not available for other sentence-pair fact verification tasks. While LiarPlus (Alhindi et al., 2018) and MultiFC (Augenstein et al., 2019) both have a similar task signature with claims and additional information provided as text, the text is not evidential (i.e. not containing a premise that would support or refute the claim). Instead, the additional text in these datasets serves as explanation and related information. This is indicated by experimental results in Table 2 where classification models have higher accuracy than a text-pair classification when only using the claim text. Future work will consider how biases in these datasets could be mitigated, dependent on the availability of counterfactual data.

| Dataset         | Accuracy (%) |
|-----------------|--------------|
| Liar-Plus       | 28.74        |
| Liar-Plus (binary) | 72.59       |
| MultiFC         | 46.02        |
| FEVER (3-way)   | 61.50        |
| FEVER (2-way)   | 79.09        |
| Claim Only      | 20.48        |
| Sentence Pair   | 70.48        |
|                 | 44.83        |
|                 | 88.93        |
|                 | 92.24        |

Table 2: Validation accuracy for claim-only vs sentence pair classification for fact verification datasets trained on RoBERTa

6 Conclusions

In this paper, we showed that many model architectures for sentence pair classification propagate the biases that are captured in the datasets that are used to train the model, replicating results by (Gururangan et al., 2018) and (Poliak et al., 2018). While previous work by (Liu et al., 2019a) show that fine-tuning models is one way to remove bias, in some cases where the data distributions differ, this removal of bias comes at the expense of catastrophic forgetting. We showed that an elastic weight consolidation penalty is sufficient to minimize catastrophic forgetting when using fine-tuning to mitigate biases in sentence pair classification tasks.

References

Tariq Alhindi, Savvas Petridis, and Smaranda Muresan. 2018. Where is Your Evidence: Improving Fact-checking by Justification Modeling. In Proceedings of the First Workshop on Fact Extraction and VERification (FEVER), pages 85–90, Brussels, Belgium. Association for Computational Linguistics.

Isabelle Augenstein, Christina Lioma, Dongsheng Wang, Lucas Chaves Lima, Casper Hansen, Christian Hansen, and Jakob Grue Simonsen. 2019. MultiFC: A Real-World Multi-Domain Dataset for Evidence-Based Fact Checking of Claims. In Proceedings of EMNLP-IJCNLP, Hong Kong, China. Association for Computational Linguistics.

Max Bartolo, Alastair Roberts, Johannes Welbl, Sebastian Riedel, and Pontus Stenetorp. 2020. Beat the AI: Investigating Adversarial Human Annotations for Reading Comprehension.

Yonatan Belinkov, Adam Poliak, Stuart Shieber, Benjamin Van Durme, and Alexander Rush. 2019. On Adversarial Removal of Hypothesis-only Bias in Natural Language Inference. In Proceedings of the Eighth Joint Conference on Lexical and Computational Semantics (*SEM 2019), pages 256–262, Minneapolis, Minnesota. Association for Computational Linguistics.
Qian Chen, Xiaodan Zhu, Zhenhua Ling, Si Wei, Hui Jiang, and Diana Inkpen. 2016. Enhanced LSTM for Natural Language Inference. In Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics, page 1657-1668, Vancouver, Canada.

Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2019. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers), Minneapolis, Minnesota.

Robert M French. 1999. Catastrophic forgetting in connectionist networks. Trends in Cognitive Sciences, 3(4):128–135.

Matt Gardner, Joel Grus, Mark Neumann, Oyvind Tafjord, Pradeep Dasigi, Nelson Liu, Matthew Peters, Michael Schmitz, and Luke Zettlemoyer. 2017. AllenNLP: A Deep Semantic Natural Language Processing Platform.

Suchin Gururangan, Swabha Swayamdipta, Omer Levy, Roy Schwartz, Samuel R Bowman, and Noah A Smith. 2018. Annotation Artifacts in Natural Language Inference Data.

Andreas Hanelowski, Hao Zhang, Zile Li, Daniil Sorokin, Benjamin Schiller, Claudia Schulz, and Iryna Gurevych. 2018. UKP-Athene: Multi-Sentence Textual Entailment for Claim Verification. In Proceedings of the First Workshop on Fact Extraction and VERification (FEVER), pages 103–108, Brussels, Belgium.

James Kirkpatrick, Razvan Pascanu, Neil Rabinowitz, Joel Veness, Guillaume Desjardins, Andrei A. Rusu, Kieran Milan, John Quan, Tiago Ramalho, Agnieszka Grabska-Barwinska, Demis Hassabis, Claudia Clopath, Dharshan Kumaran, and Raia Hadsell. 2017. Overcoming catastrophic forgetting in neural networks. Proceedings of the National Academy of Sciences of the United States of America, 114(13):3521–3526.

Nelson F. Liu, Roy Schwartz, and Noah A. Smith. 2019a. Inoculation by Fine-Tuning: A Method for Analyzing Challenge Datasets. pages 2171–2179.

Yinhan Liu, Myle Ott, Naman Goyal, Jingfei Du, Mandar Joshi, Danqi Chen, Omer Levy, Mike Lewis, Luke Zettlemoyer, and Veselin Stoyanov. 2019b. RoBERTa: A Robustly Optimized BERT Pretraining Approach.

Minh-thang Luong and Christopher D. Manning. 2015. Stanford Neural Machine Translation Systems for Spoken Language Domains. IWSLT-2015, pages 76–79.

James Martens. 2014. New insights and perspectives on the natural gradient method.

Aakanksha Naik, Abhilasha Ravichander, Norman Sadeh, Carolyn Rose, and Graham Neubig. 2018. Stress Test Evaluation for Natural Language Inference. In Proceedings of the 27th International Conference on Computational Linguistics, pages 2340–2353, Santa Fe.

Yixin Nie, Haonan Chen, and Mohit Bansal. 2018. Combining Fact Extraction and Verification with Neural Semantic Matching Networks.

Ankur P. Parikh, Oscar Täckström, Dipanjan Das, and Jakob Uszkoreit. 2016. A Decomposable Attention Model for Natural Language Inference. In Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing, pages 2249–2255, Austin, Texas. Association for Computational Linguistics.

Adam Poliak, Jason Naradowsky, Aparajita Haldar, Rachel Rudinger, and Benjamin Van Durme. 2018. Hypothesis Only Baselines in Natural Language Inference. In Proceedings of the Seventh Joint Conference on Lexical and Computational Semantics, pages 180–191, New Orleans, Louisiana. Association for Computational Linguistics.

Dean Pomerleau and Delip Rao. 2017. Fake News Challenge. \{url\{http://fakenewschallenge.org/\}\}.

Sebastian Ruder. 2017. An Overview of Multi-Task Learning in Deep Neural Networks. May.

Danielle Saunders and Bill Byrne. 2020. Reducing Gender Bias in Neural Machine Translation as a Domain Adaptation Problem. In Proceedings of the 58th meeting of the Association for Computational Linguistics, Seattle, WA. Association for Computational Linguistics.

Danielle Saunders, Felix Stahlberg, Adri de Gispert, and Bill Byrne. 2019. Domain Adaptive Inference for Neural Machine Translation. In Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, pages 222–228, Florence, Italy. Association for Computational Linguistics.

Tal Schuster, Darsh J Shah, Yun Jie Serene Yeo, Daniel Filizzola, Enrico Santus, and Regina Barzilay. 2019. Towards Debiasing Fact Verification Models. In Proceedings of EMNLP-IJCNLP, Hong Kong, China.

Sandeen Suntwal, Mathun Paul, Rebecca Sharp, and Mihai Surdeanu. 2019. On the Importance of Delexicalization for Fact Verification. pages 3411–3416.

Brian Thompson, Jeremy Gwinnup, Huda Khayrallah, Kevin Duh, and Philipp Koehn. 2019. Overcoming Catastrophic Forgetting During Domain Adaptation of Neural Machine Translation. (2018):2062–2068.

James Thorne, Andreas Vlachos, Christos Christodoulopoulos, and Arpit Mittal. 2018. FEVER: a large-scale dataset for Fact Extraction.
and VERification. In Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers), pages 809–819, New Orleans, Louisiana. Association for Computational Linguistics.

Adina Williams, Nikita Nangia, and Samuel Bowman. 2018. A Broad-Coverage Challenge Corpus for Sentence Understanding through Inference. In Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers), pages 1112–1122, New Orleans, Louisiana. Association for Computational Linguistics.

Takuma Yoneda, Jeff Mitchell, Johannes Welbl, Pontus Stenetorp, and Sebastian Riedel. 2018. UCL Machine Reading Group: Four Factor Framework For Fact Finding (HexaF). In Proceedings of the First Workshop on Fact Extraction and VERification (FEVER), pages 97–102, Brussels, Belgium.