Mitigating the Diminishing Effect of Elastic Weight Consolidation

Canasai Kruengkrai  Junichi Yamagishi
National Institute of Informatics, Japan
{canasai,jyamagishi}@nii.ac.jp

Abstract
Elastic weight consolidation (EWC, Kirkpatrick et al. 2017) is a promising approach to addressing catastrophic forgetting in sequential training. We find that the effect of EWC can diminish when fine-tuning large-scale pre-trained language models on different datasets. We present two simple objective functions to mitigate this problem by rescaling the components of EWC. Experiments on natural language inference and fact-checking tasks indicate that our methods require much smaller values for the trade-off parameters to achieve results comparable to EWC.

1 Introduction
New training data may arrive after we have spent considerable time training our model on the data at hand. A simple method for exploiting both new and old training data is to mix them and retrain the model from scratch. However, this mix-and-retrain method is neither always practical nor economical, especially in academic environments where computational resources are limited.

Sequential training is a potential alternative approach but faces a difficult challenge called catastrophic forgetting in which the performance on old data drastically drops when we train a model on new data. There exists a line of work that has addressed this challenge (Rusu et al., 2016; Li and Hoiem, 2018; Kirkpatrick et al., 2017; Mallya et al., 2018; He and Jaeger, 2018; Zhang et al., 2020). In this paper, we are particularly interested in elastic weight consolidation (EWC, Kirkpatrick et al. 2017), which has been shown to be helpful for domain adaptation (Saunders et al., 2019; Thompson et al., 2019).

EWC adds a regularization term to the objective function to ensure that the model works well on both new and old data. We empirically find that EWC requires unexpectedly large values for the trade-off parameter ($\lambda$) between the regularizer and the loss to be effective when applying to pre-trained language models. Figure 1 shows such a phenomenon in which EWC has no effect in preventing catastrophic forgetting of the prior dataset (MNLI) when increasing $\lambda$ to $10^5$ and yields the highest average accuracy at $10^7$.

We propose two simple objective functions for mitigating the diminishing effect of EWC. Our objective functions rely on rescaling the components of EWC. Specifically, the first objective function involves taking the square root of the regularization term, while the second one involves using the absolute value of the gradient instead of the squared gradient. Both of our objective functions can reduce the values of the trade-off parameter $\lambda$ by three to seven orders of magnitude while producing results similar to those of the original EWC.

1Our code is available at https://github.com/nii-yamagishilab/ewc.
2 Background

2.1 Problem formulation

We consider a supervised learning problem in which the task is to map an input \( x \in X \) to a label \( y \in Y \). We need to train a model \( h_\theta : X \rightarrow Y \) with parameters \( \theta \in \mathbb{R}^d \). Given a dataset \( D = \{(x_i, y_i)\}_{i=1}^M \), we typically estimate \( \theta \) on the basis of empirical risk minimization (ERM, Vapnik 1992):

\[
J_{\text{ERM}}(\theta) = \frac{1}{M} \sum_{(x,y)\in D} \mathcal{L}(h_\theta(x), y),
\]

(1)

where \( \mathcal{L} \) is the negative log likelihood loss:

\[
\mathcal{L}(h_\theta(x), y) = - \sum_{y\in Y} \mathbb{1}\{\hat{y} = y\} \log p_\theta(\hat{y}|x).
\]

Our base model \( h_\theta \) is a neural network containing a multilayer perceptron (MLP) on top of a pre-trained language model (e.g., BERT). Thus, we define \( p_\theta(\hat{y}|x) = \text{softmax}(h_\theta(x)) \), where \( h_\theta = \text{MLP}(\text{BERT}(x)) \). The model parameters \( \theta \) include those in the MLP and BERT.

2.2 Elastic weight consolidation

Elastic weight consolidation (EWC, Kirkpatrick et al. 2017) is based on a Bayesian framework that seeks to approximate the posterior distribution of \( \theta \) conditional on two datasets. Let \( D \) and \( D^0 \) denote the current and prior datasets, respectively. We express the posterior distribution as:

\[
p(\theta|D, D^0) = \frac{p(\theta, D, D^0)}{p(D, D^0)},
\]

\[
= \frac{p(D|\theta, D^0)p(\theta, D^0)}{p(D, D^0)},
\]

\[
= \frac{p(D|\theta)p(\theta|D^0)p(D^0)}{p(D)p(\theta|D^0)},
\]

\[
\propto p(D|\theta)p(\theta|D^0),
\]

(2)

where we assume that \( D \) and \( D^0 \) are conditionally independent in the third line and ignore the constant in the last line. Taking the log on both sizes of Eq. (2), we have:

\[
\log p(\theta|D, D^0) = \log p(D|\theta) + \log p(\theta|D^0). \quad (3)
\]

The first term on the right-hand side corresponds to the log likelihood of \( D \), which can be computed using Eq. (1). The second term is intractable but can be approximated using a second-order Taylor expansion of the KL-divergence around the parameters of the previously trained model, \( \theta^0 \):

\[
\log p(\theta|D^0) \approx \frac{1}{2} \Delta \theta^T H \Delta \theta, \quad (4)
\]

where \( \Delta \theta = \theta - \theta^0 \) and \( H \) is the expected negative Hessian of the posterior distribution (Pascual and Bengio, 2014). Computing \( H \) is impractical. Kirkpatrick et al. (2017) proposed approximating \( H \) using the diagonal of the Fisher information matrix. Let \( \text{diag}(f) \) be the diagonal matrix with diagonal \( f \). We estimate \( f \) with the average of the squared gradient across some \( N \) subsamples \( S^0 \):

\[
f = \frac{1}{N} \sum_{(x,y)\in S^0} (\nabla_{\theta_0} \mathcal{L}(h_\theta(x), y))^2. \quad (5)
\]

Replacing \( H \) with \( \text{diag}(f) \), we can simplify Eq. (4) as:

\[
\log p(\theta|D^0) \approx \frac{1}{2} \sum_{j=1}^d f_j (\theta_j - \theta^0_j)^2. \quad (6)
\]

Applying Eqs. (1) and (6) to Eq. (3), we obtain the EWC objective:

\[
J_{\text{EWC}}(\theta) = J_{\text{ERM}}(\theta) + \frac{\lambda}{2} \sum_{j=1}^d f_j (\theta_j - \theta^0_j)^2, \quad (7)
\]

where \( \lambda \) is the trade-off parameter.

3 Proposed method

As shown in Figure 1, EWC requires extremely large values of \( \lambda \) to be effective. We analyze the components of EWC and find that this problem arises from the Fisher approximation in Eq. (5). The diagonal element \( f_j \) corresponds to the \( j^{\text{th}} \) element of the squared gradient with respect to \( \theta_j \). Since its training had already converged, the values of the gradient are typically small. When we square such a small decimal and combine it with the squared difference between the current and prior parameters, the final value can be vanishingly small.\(^2\) We find that this issue is neither affected by datasets nor pre-trained language models. In Appendix A, we further investigate this issue on another pre-trained language model.

We propose scaling up the Fisher approximation by taking the square root to resolve the issue above. We define the square root of EWC (REWC) as:

\[
J_{\text{REWC}}(\theta) = J_{\text{ERM}}(\theta) + \lambda \sqrt{A} + \epsilon, \quad (8)
\]

\(^2\)For example, in the MNLI \( \Rightarrow \) FEVER experiment, we find that 85.9% of non-zero \( f_j \) are less than 1e-10.
Figure 2: Accuracy vs. trade-off parameter $\lambda$ of our REWC and AEWC. Both methods begin to affect accuracy with much lower $\lambda$ (i.e., $10^2$ and $10^{-1}$ for REWC and AEWC, respectively) while maintaining average accuracies similar to EWC.

where $A = \sum_{j=1}^{d} f_j(\theta_j - \theta_0)^2$, and $\epsilon$ is a small value (e.g., $10^{-8}$) for preventing the derivative of the square root at 0.

Another solution is to use the absolute value of the gradient instead of the squared gradient. We define:

$$g = \frac{1}{N} \sum_{(x,y) \in S^0} |\nabla_{\theta} L(h_{\theta}(x), y)|. \tag{9}$$

Note that $\text{diag}(g)$ is positive semi-definite (like $\text{diag}(f)$) because all of its eigenvalues are greater than or equal to 0. Replacing the squared difference with the absolute difference yields our absolute EWC (AEWC):

$$J_{AEWC}(\theta) = J_{ERM}(\theta) + \lambda \sum_{j=1}^{d} g_j |\theta_j - \theta_0^j|. \tag{10}$$

Figure 2 shows the results of REWC and AEWC based on the same setting as in Figure 1.

4 Experiments

4.1 Datasets

We evaluated the objective functions described in §2 and §3 on natural language inference and fact-checking tasks. We used six datasets pre-processed by Schuster et al. (2021) as follows:

**MNLI** (Williams et al., 2018) is a multi-genre natural language inference dataset. The task is to determine the inference relation between two sentences. Schuster et al. (2021) converted the original labels {"entailment", "contradiction", "neutral"} into {"supported", "refuted", "not enough info"}.

**FEVER** (Thorne et al., 2018) (Fact Extraction and VERification) verifies whether a claim is supported or refuted by an evidence sentence, or decides whether there is insufficient information to make a decision.

**VITC** (Schuster et al., 2021) introduces the notion of contrastive evidence to FEVER. Given a claim, two evidence sentences that are nearly identical but with different labels are created. Thus, the task becomes more challenging than that of FEVER. The dataset contains both real and synthetic examples. We used only the real ones in our experiments.

**ADVERSARIAL** (Thorne et al., 2019) is derived from the FEVER 2.0 shared task, containing adversarially created claims that aim to induce erroneous predictions to the FEVER-trained models.

**SYMMETRIC** (Schuster et al., 2019) is another dataset that challenges the FEVER-trained models. It contains synthetically created claim-evidence pairs designed to break models that often make predictions using claims only without taking evidence sentences into account.

**TRIGGERS** (Atanasova et al., 2020) contains adversarial claims generated by using GPT-2 (Radford et al., 2019) given the original claims and triggers, which are words that cause the model to flip its prediction.

We selected $\lambda$ that yields the highest average accuracy on the development (dev) sets. To avoid a bias towards more populated datasets (e.g., VITC), we created our balanced dev sets by randomly selecting 9,000 examples from each of the original dev sets. Since the dev and test sets of MNLI are identical, we split 9,000 examples from the training set to form the dev set and used the test set for the final evaluation. Table 1 shows our dataset statistics.
<table>
<thead>
<tr>
<th>Dataset</th>
<th>Train</th>
<th>Dev</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNLI</td>
<td>383,702</td>
<td>9,000</td>
<td>9,832</td>
</tr>
<tr>
<td>FEVER</td>
<td>178,059</td>
<td>9,000</td>
<td>11,710</td>
</tr>
<tr>
<td>ViT-C</td>
<td>248,953</td>
<td>9,000</td>
<td>34,481</td>
</tr>
<tr>
<td>Adversarial</td>
<td>–</td>
<td>–</td>
<td>766</td>
</tr>
<tr>
<td>Symmetric</td>
<td>–</td>
<td>–</td>
<td>712</td>
</tr>
<tr>
<td>Triggers</td>
<td>–</td>
<td>–</td>
<td>186</td>
</tr>
</tbody>
</table>

Table 1: Dataset statistics in our experiments. Bottom three datasets contain only test sets adversarially created for testing robustness of fact-checking models.

### 4.2 Training details

We implemented our base model described in §2.1 using Hugging Face’s Transformers library (Wolf et al., 2020). Specifically, the model consists of a two-layer MLP and BERT-base. Let $x$ be the input sequence (i.e., a pair of sentences in our datasets). BERT-base encodes $x$ into a sequence of hidden state vectors. Following common practice, we used the first hidden state vector of the special classification token (i.e., [CLS]) to represent $x$ and fed it to the MLP followed by a softmax function.

For all experiments, we used Adafactor optimizer (Shazeer and Stern, 2018) with a gradient clipping of 1.0. Our effective batch size is 256.3 For standard training, we randomly initialized the model parameters with $\mathcal{N}(0, 0.02)^4$, except for those of BERT-base. We trained each model for three epochs with a learning rate of 2e-5.

For sequential training, we randomly selected 1% of examples from $D^0$ to represent $S^0$ in Eq. (5). We also varied the subsample size from 0.1% to 10% but did not observe significant changes in performance. We initialized the current model parameters using the prior ones (i.e., $\theta^0 \rightarrow \theta$). Determining a learning rate can be challenging. We used a method analogous to the learning rate decay technique (Ng, 2017). Let $\alpha_0$ be the initial learning rate and $r$ be the number of prior training runs. We computed the learning rate $\alpha$ for the current training run as:

$$\alpha = \frac{1}{1 + (\text{decay\_rate} \times r) \alpha_0}. \quad (11)$$

For example, consider the case of further training the MNLI-trained model on the FEVER dataset, where $\alpha_0 = 2e-5$ and $r = 1$. We set decay_rate to 1e-2 for all sequential training experiments. Using Eq. (11), the learning rate $\alpha$ for the current run decreases to 1.98e-5. We conducted all the experiments on NVIDIA Tesla A100 GPUs.

### 4.3 Results

Table 2 shows the results of various settings on the test sets. For sequential training, conducting experiments on all combinations takes time and considerable resources. Thus, we chose only a representative order for the datasets in accordance with their publication times. Since the MNLI and FEVER datasets were published at the same time, we decided to start with MNLI due to its generality.

We considered the mix-and-retrain method ($\cup$) with ERM as the topline setting. Unsurprisingly, this method yields the best performance on the prior datasets. The sequential training method ($\Rightarrow$) with ERM (i.e., vanilla fine-tuning) encounters severe catastrophic forgetting on the prior datasets. Our REWC and AEWC effectively reduce the values of $\lambda$. AEWC requires the lowest $\lambda$ among the three objective functions. The performances of all the methods seem comparable on average, but each yields a different trade-off in accuracy between the prior and current datasets. Regarding the training time, AEWC is faster than REWC/EWC (though not significant) because its computation is simpler.

Figure 3: Accuracy vs. trade-off parameter $\lambda$ of EWC and AEWC without $f_j$ and $g_j$, respectively.

---

3 We used gradient accumulation with 8 batches of 32.
4 This is the default setting in Transformers.
We omitted the prior dataset (MNLI). However, take the prior parameters into account. To examine the benefit of gradient information, we conducted ablation studies on EWC between the current and prior parameters. The gradient component helps suggest which parameter is important. To examine the benefit of gradient information, we conducted ablation studies on EWC and AEWC in the MNLI ⇒ FEVER experiment. We omitted $f_j$ and $g_j$ from Eqs. (7) and (10), respectively. The remaining regularization terms resemble the squared $\ell_2$-norm and the $\ell_1$-norm that take the prior parameters into account.

As seen in Figure 3, without the gradient component, both methods need lower $\lambda$ to affect the accuracy of the prior dataset (MNLI). However, improvements on the prior dataset are marginal (~1%) before reaching the optimal average accuracy compared to the original EWC and AEWC (~4%). Table 3 shows the ablation results on the test sets, indicating that omitting the gradient component yields lower accuracies on the prior dataset. These results confirm that the gradient component is indeed helpful.

### 4.4 Discussion

We can interpret the EWC family as a weighted sum of the squared (or absolute) differences between the current and prior parameters. The gradient component helps suggest which parameter is important. To examine the benefit of gradient information, we conducted ablation studies on EWC and AEWC in the MNLI ⇒ FEVER experiment. We omitted $f_j$ and $g_j$ from Eqs. (7) and (10), respectively. The remaining regularization terms resemble the squared $\ell_2$-norm and the $\ell_1$-norm that take the prior parameters into account.

As seen in Figure 3, without the gradient component, both methods need lower $\lambda$ to affect the accuracy of the prior dataset (MNLI). However, improvements on the prior dataset are marginal (~1%) before reaching the optimal average accuracy compared to the original EWC and AEWC (~4%). Table 3 shows the ablation results on the test sets, indicating that omitting the gradient component yields lower accuracies on the prior dataset. These results confirm that the gradient component is indeed helpful.

### 5 Conclusion

Without realizing the diminishing effect of EWC, we may fine-tune a pre-trained language model with a conventional range of hyperparameters and find no effect in combating catastrophic forgetting. We identified a possible cause of this issue and suggested two alternative objective functions, REWC and AEWC, that yield results comparable to the original EWC. Exploring more efficient ways for choosing an optimal $\lambda$ is part of our future work.

### Acknowledgments

This work is supported by JST CREST Grants (JPMJCR18A6 and JPMJCR20D3) and MEXT KAKENHI Grants (21H04906), Japan.
References


We verified the diminishing effect of EWC on another pre-trained language model, A Lite BERT (ALBERT, Lan et al. 2020). Figure 4 shows the results of sequential training: MNLI ⇒ FEVER. We can still see the diminishing effect of the original EWC, while our REWC and AEWC reduce the value of \( \lambda \) by three and six orders of magnitude and produced similar results.

Figure 4: Accuracy vs. trade-off parameter \( \lambda \) on the balanced dev sets of MNLI and FEVER using ALBERT-base (Lan et al., 2020). EWC, REWC, and AEWC achieve highest average accuracies with \( \lambda = 10^6, 10^3, \) and \( 10^0 \), respectively.