LEARNING TO BALANCE WITH INCREMENTAL LEARNING

Anonymous authors
Paper under double-blind review

ABSTRACT

Classification tasks require balanced distribution of data in order to ensure the learner to be trained to generalize over all classes. In realistic settings, however, the number of instances vary substantially among classes. This typically leads to a learner that promotes bias towards the majority group due to its dominating property. Therefore, methods to handle imbalanced data is crucial for alleviating distributional skews and fully utilizing the under-represented data. We propose a novel training method, Sequential Targeting, that forces an incremental learning setting by splitting the data into mutually exclusive subset and adaptively balancing the data distribution as tasks develop. To address problems that arise within incremental learning, we apply dropout and elastic weight consolidation with our method. It is demonstrated in a variety of experiments on both text and image dataset (IMDB, CIFAR-10, MNIST) and has proven its superiority over traditional methods such as oversampling and under-sampling.

1 INTRODUCTION

In a real-world application setting, it is rarely the case where the discrete distribution of the data is perfectly balanced. It is common for real-world data to be skewed to majority classes when the minority class is often the class of interest. Skewed data distribution is explicitly addressed in anomaly detection as it is a matter of high interest in various fields including disease, fraud and malware detection [Rao et al. (2006); Wei (2013); Cieslak et al. (2006)]. Since correctly classifying under-represented classes is equally important as classifying majority classes, if not more so, methods to temper the model from biasing towards certain classes are of great importance. In order to develop an intelligent classifier, approaches to generalize over different distributional tasks are getting increasingly important and being extensively researched.

Learning from imbalanced data inevitably brings bias toward frequently observed classes. Data-level manipulation tries to under-sample majority classes or over-sample minority classes. But these methods have a tendency to discard valuable information from observations of majority classes or over-fit to limited data, especially as the imbalance level gets severe.

We propose a novel training architecture, Sequential Targeting (ST), which handles the data imbalance problem without manipulating the data by forcing an incremental learning setting. ST divides the entire training data set into mutually exclusive partitions, adaptively balancing the data distribution among tasks. The split data is then sorted in similarity with the target distribution and used to train a balanced learner. In order to address catastrophic forgetting [French, 1999], which is an inevitable phenomenon when training a learner in a sequential fashion, we utilize different methods [Kirkpatrick et al. (2016); Goodfellow et al. (2013)] to stabilize the knowledge attained from the previous tasks. This allows the learner to pay more focus on the newly adapted data distribution while not forgetting the representation from previous tasks.

We validate the effectiveness of our method with experiments conducted on both text and image data. Different data imbalance levels as well as proportion of the minority classes were experimented. Experimental results show that Sequential Targeting outperforms previous approaches, with notable gap especially in extremely imbalanced cases. Furthermore, Sequential Targeting proves to be compatible with both traditional data-level methods and recent algorithm-level approaches.

Our contribution in this paper is as follows:
We introduce a novel method addressing the data imbalance problem by splitting the data and incrementally training a learner to perform a balanced learning by paying equal attention to the minority data as to the majority. The learner’s initial focus on the majority class is compensated by the redistributed task that comes sequentially, resulting in an overall increase of performance.

Incremental learning techniques have been utilized to prevent catastrophic forgetting on tasks encountered before. The novelty of our method stands since we applied incremental learning to address the data imbalance problem.

We propose a novel method that is compatible with previous methods addressing the data imbalance problem. Best performance is shown when utilized together.

2 RELATED WORKS

Balancing Methods  Previous researchers have proposed data-level methods as well as algorithm-level methods that address the data imbalance problem. Data-level techniques such as SMOTE and its variants [Chawla et al. (2002); Han et al. (2005)] attempt to alleviate the level of imbalance by manipulating the training data. Cluster based oversampling [Puntumapon et al. (2016)] attempts to cluster the data into groups using k-means algorithm and apply oversampling to each cluster, which proves to reduce within-class imbalance and between-class imbalance. SMOTEboosting [Chawla et al. (2003)] applies SMOTE before every round of boosting and provides more samples of misclassified set for weak learners often including the minority class samples.

Alternatively, algorithm-level methods [Krawczyk (2016); Sheng & Ling (2006)], commonly implemented with a weight or cost schema, modify the underlying learner or its output to reduce bias towards the majority group. Algorithm-level methods modify the structure of the decision process of how much to focus on under-represented samples. This could be implemented by assigning cost matrix as a penalty [Fernando et al., 2017]. Moreover, loss functions could be modified, such as in the case of focal loss [Lin et al. (2017)], which reshapes the standard cross entropy loss such that it penalizes the loss assigned to well-classified instances.

Catastrophic Forgetting  Researchers have investigated methods to circumvent catastrophic forgetting, a phenomenon of a learner forgetting about the previously learned task when encountered with another task. One of the major approaches is to use an ensemble of networks, each trained with individual tasks [Rusu et al., 2016]. However, this approach has a complexity issue. Alternatively, Fernando et al. (2017) proposed an ensemble approach which attempts to fix the parameters learned from the previous task and train new parameters on consecutive tasks. This method has successfully reduced complexity issues, but performance suffers from the lack of trainable parameters. Goodfellow et al. (2013), on the other hand, investigated catastrophic forgetting in neural networks and showed that applying dropout substantially helps overcome this phenomenon without any apparent downfalls. This accounts to the increased optimal size of the parameters with dropout applied, thereby increasing the capacity of the learner and reducing generalization error.

Recent studies have focused on developing a regularization term that buffers the model from forgetting the previously trained information. Elastic weight consolidation (EWC) [Kirkpatrick et al., 2016] is one of the most conspicuous works in this field. EWC algorithm, which implements modified regularization term that consolidates knowledge across tasks, imposes restriction on the model to slow down updating certain important parameters from the previous task.

EWC considers neural network training from a probabilistic perspective. Optimizing the network parameters $\theta$ is equivalent to finding their most feasible values given some data $D$. We can compute this conditional probability $p(\theta|D)$ from the prior probability of the parameters $p(\theta)$ and the probability of the data $p(D|\theta)$ by using Bayes’ rule:

$$\log p(\theta|D) = \log p(D|\theta) + \log p(\theta) - \log p(D)$$  

(1)

By assuming that the data is split into two independent parts, one defining the previous task $D_{prev}$ and the other current task $D_{curr}$, we can rearrange the equation by applying Bayesian update rule:
log p(θ|D_\text{curr}) = log p(D_\text{curr}|θ) + log p(θ|D_\text{prev}) − log p(D_\text{curr})  \quad (2)

The prior distribution learned from previous dataset is further enriched by the data given at the current task. Due to the intractability of the posterior distribution, EWC poses an assumption on the prior distribution to follow a Gaussian distribution with the mean as θ^{*}\text{prev}_i and the Fisher information matrix, F, of the previous task as the precision. In order to minimize the loss of information, the objective function is defined as follows:

\[ L(θ) = L_\text{curr}(θ) + \sum_i λ^2 F_i(θ_i − θ^{*}\text{prev}_i)^2 \quad (3) \]

where \( L_\text{curr}(θ) \) sets the loss for the current task, λ sets the importance of the previous task and \( i \) labels each parameter.

3 SEQUENTIAL TARGETING

We first introduce a broad overview of the novel training architecture: Sequential Targeting. Next, we show how this method has been applied to address the data imbalance problem.

3.1 MATCHING THE TARGET DISTRIBUTION

We propose a novel model architecture of forced incremental learning on imbalanced setting. The term forced incremental learning has rarely, if ever, been used since incremental learning is a much complicated task. In incremental learning, the new data is referred to as different task in this paper. The task is consistently provided therefore the learner needs to be constantly updated on the new task. Because of catastrophic forgetting, learners perform much better when trained with an individual task than continually being updated with multiple tasks. In spite of this phenomenon, we have proven it is beneficial to force an incremental learning setting where the given data distribution varies substantially from the target data distribution, such as in the case of data imbalance. The target distribution, denoted as \( P_T \), is the idealistic data distribution in which the learner would perform the best if trained on.

Our method effectively improves the model by dividing a given task, \( D_\text{total} \), into multiple tasks, \( D_1, D_2, ..., D_k \), so that \( \bigcup D_i = D_\text{total} \) and \( \bigcap D_i = \emptyset \). Each task is partitioned into varying distributions: \( P_1, P_2, ..., P_k \). The learner is sequentially trained on these tasks in the order of similarity with the target distribution, which is measured with KL-divergence. The following has to hold:

\[ D_{\text{KL}}(P_T||P_\text{prev}) > D_{\text{KL}}(P_T||P_\text{curr}), \text{ where } P_i \xrightarrow{\mathcal{D}} P_T \quad (4) \]

Using a single learner over all tasks, we incrementally condition on the maximum performance from the previous task and stabilize the learned parameters on the current task. As explained in equation [2] the learner’s parameters from the previous task distribution is used to train on the current task distribution. KL divergence explains the discrepancy between the task distribution and the target distribution. As tasks proceed, the data distribution approximates the target distribution. At last, the task becomes identical to the target distribution ensuring \( D_{\text{KL}}(P_T||P_k) \approx 0 \).

The number of data splits, \( k \), and how each task is partitioned to have varying KL-divergence values are both highly dependent on what \( P_T \) is defined to be. We believe this training approach is the first of its kind, with the best of our knowledge.

3.2 ADAPTIVE BALANCING FOR DATA IMBALANCE

Imbalanced data setting tempers the model from learning extensively from under-represented instances. Therefore, it is crucial to enforce the learner to acquire knowledge equally among classes. In an idealistic setting, a learner is trained with equally represented dataset. However, in a realistic setting, imbalanced data includes some under-represented classes and the learner has difficulty
acquiring sufficient knowledge to generalize. Sequential Targeting enables balanced learning by redistributing the task to approach the target distribution as tasks develop.

It is idealistic to assume \( P_T \overset{d}{=} \text{Uniform}[0,p] \) in an imbalanced data setting therefore when \( p \) denotes the number of classes the target distribution is discrete uniform: \( \{ \frac{1}{p}, \frac{1}{p}, \ldots, \frac{1}{p} \} \). In our method, the training data is redistributed into two splits so that the last split is identical to the uniform distribution.

Figure 1: Comparison between baseline and Sequential Targeting

This training architecture lets the learner pay more focus to the under-represented data by manipulating the learning sequence. Sequentially training the learner to be exposed to increasing portion of minority class data benefits the overall performance. Moreover, applying dropout to the layers and implementing EWC during the transfer between tasks proves to help the learner maintain the knowledge acquired from the previous split.

4 Experiments

4.1 Evaluation Metrics and ratios

Accuracy is commonly used to measure the performance of a classification model. However, when it comes to skewed data, accuracy alone can be misleading and thus other appropriate metrics are needed to correctly evaluate the performance of the model. In this paper, we use precision, recall, and macro F1-score to objectively evaluate the model in a skewed data setting. Precision measures the percentage of actual positive among the number of positively predicted samples. Recall measures the percentage of the truly positive instances that was correctly predicted by the model. As precision and recall is in a trade-off relationship, selecting a learner that performs well on both metrics would be a reasonable policy. Macro F1-score combines both precision and recall as a harmonic mean weighted with equal importance on each class rather it be sparse or rich. In this paper, F1-score is used as the core metric for measuring performance.

Following the conventions of the previous research on imbalanced data [Buda et al. (2018); Johnson (2019)], we employ three distinct ratios used throughout the experiment to represent the imbalanced state of the data. One is the proportion of minority classes over majority classes \( \mu \):

\[
\mu = \frac{|\{i \in 0,1,\ldots,N : C_i \text{ is minority}\}|}{N}
\]

where \( C_i \) is the set of instances in class \( i \) and \( N \) is the total number of classes. Another parameter \( \rho \) is a ratio between the number of instances in majority classes and the number of instances in minority classes defined as follow:

\[
\rho = \frac{\{\max_i(C_i)\}}{\{\min_i(C_i)\}}
\]

The other parameter \( \eta \) is a parameter that compares the relative number of minority class instances among splits. For instance, if the first task consists of 100 samples in minority class and the second task consists of 50 samples, then \( \eta \) will be 2:1. We experienced various combinations of these three ratios and concluded that \( \eta \) does not have a significant effect on model performance. Therefore, the
number of instances of the minority classes between the splits is fixed as 1:1 throughout the whole experiment. Further consideration of $\eta$ can be found in the discussion section.

Figure 2 shows variation of $\mu$ and $\rho$ in the case of an idealist dataset and a realistic dataset.

4.2 Dataset and Neural Network Architecture

In this research, we performed experiments on IMDB, CIFAR-10, and MNIST datasets. The datasets were deliberately made into varying imbalanced states as shown in Table 1.

Table 1: Simulated Dataset in variations of $\rho$ and $\mu$.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>$\rho$</th>
<th>$\mu$</th>
<th>Class</th>
<th>Train Minority</th>
<th>Train Majority</th>
<th>Validation Minority</th>
<th>Validation Majority</th>
<th>Test Minority</th>
<th>Test Majority</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMDB</td>
<td>10</td>
<td>N/A</td>
<td>2</td>
<td>1,250</td>
<td>12,500</td>
<td>2,500</td>
<td>2,500</td>
<td>10,000</td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>N/A</td>
<td>2</td>
<td>625</td>
<td>12,500</td>
<td>2,500</td>
<td>2,500</td>
<td>10,000</td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>N/A</td>
<td>2</td>
<td>250</td>
<td>12,500</td>
<td>2,500</td>
<td>2,500</td>
<td>10,000</td>
<td>10,000</td>
</tr>
<tr>
<td>CIFAR-10</td>
<td>10</td>
<td>0.8</td>
<td>10</td>
<td>400</td>
<td>4,000</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>0.6</td>
<td>10</td>
<td>800</td>
<td>4,000</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>MNIST</td>
<td>10</td>
<td>0.8</td>
<td>10</td>
<td>500</td>
<td>5,000</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

**IMDB** is a text dataset, which contains 50000 movie reviews with binary labels (positive/negative). Reviews have been preprocessed, and each review is encoded as a sequence of word indexes. Three different imbalance ratios have been deliberately made ($\rho = 10, 20, 50$) to test how each method performs as the imbalance level worsens. The positive reviews are regarded as the positive class in our experiment. A CNN + LSTM model architecture was used for this task. After an initial embedding layer, a 1-dimension convolution layer is followed with a dropout layer ($dr = 0.2$). It is then followed by a Bidirectional LSTM and a Uni LSTM layer. Lastly, a 1-dimensional fully-connected layer ($dr = 0.2$) is followed by a sigmoid activation.

**CIFAR-10** is a image dataset that consists of 10 classes with 6000 training and 1000 test data for each class. We sampled from the original data with predetermined $\rho$ ratio ($\rho = 5, 10$) in order to experiment on an imbalanced setting. Since there are multiple classes in this dataset, two varied fraction of minority classes ($\mu = 0.8, 0.6$) were simulated and tested as well. Following the work of [Masko & Hensman (2015)] on CIFAR-10, we used a variant of CNN ([Lecun et al., 1998]). After applying two dimensional convolutional layer, ReLU activation is applied followed by maxpooling and a dropout layer ($dr = 0.5$). This procedure is repeated twice and three fully-connected layers with hidden node size of 120, 84, and 10 are utilized.

**MNIST** is a image dataset that consists of simple handwritten single digits. Each class of digits consists of 5500 training, 500 validation and 1000 test data. MNIST data is deliberately manipulated in order to match the predetermined $\rho$ and $\mu$ ratio ($\rho = 10$, $\mu = 0.8$). The model architecture used in MNIST data is a simple Multi-Layer Perception network which includes three consecutive fully-connected layers with hidden node size of 512, 512, and 10. A dropout layer with dropout rate 0.2 is implemented on each hidden layer. The activation function used in this architecture is ReLU.

**Experimental setup.** In our experiments, our proposed method has been extensively compared with two data-level methods, random oversampling (ROS) and random under-sampling (RUS). A naive duplicate sampling approach has been used for oversampling the minority data for simplicity. We
explored the full capability of Sequential Targeting by comparing multiple combinations with ROS and EWC. ROS is combined with ST by oversampling the first split; no sampling method is applied to the second split. For each configuration, five independent trial runs were trained with different initial weights. This setting ensures the effect of weight initialization to be ruled out in evaluating model performance. Among the five trials, the model with the highest validation score was used for evaluation. All the experimental settings including epochs, learning rate, and model architecture are fixed for each corresponding task.

4.3 Experiments

Table 2: Experimental results on IMDB

<table>
<thead>
<tr>
<th>Ratios</th>
<th>ρ = 10</th>
<th>ρ = 20</th>
<th>ρ = 50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metrics</td>
<td>F1</td>
<td>Precision</td>
<td>Recall</td>
</tr>
<tr>
<td>Baseline</td>
<td>0.7291</td>
<td>0.8572</td>
<td>0.6248</td>
</tr>
<tr>
<td>ROS</td>
<td>0.7548</td>
<td>0.702</td>
<td>0.8162</td>
</tr>
<tr>
<td>RUS</td>
<td>0.7921</td>
<td>0.7305</td>
<td>0.865</td>
</tr>
<tr>
<td>ST</td>
<td>0.7956</td>
<td>0.7499</td>
<td>0.8472</td>
</tr>
<tr>
<td>ST + EWC</td>
<td>0.8002</td>
<td>0.7181</td>
<td>0.9035</td>
</tr>
<tr>
<td>ST + EWC + ROS</td>
<td>0.8143</td>
<td>0.7984</td>
<td>0.8307</td>
</tr>
</tbody>
</table>

IMDB Results. Table 2 shows the experimental results on the IMDB dataset (Maas et al., 2011). We observe training the model with ST outperforms, if not on par with, traditional methods. Baseline is a setting where no deep learning techniques are employed therefore the learner is trained from the intrinsic imbalanced distribution. Results show a considerable increase in recall when ST is applied. This is because the model is able to predict more positive(minority) instances correctly since focus was put on the under-represented class. It is natural to expect a significant decrease in precision since the focus has been shifted away from the majority class. However, the drop is minimal when EWC is applied. This is because EWC helps the model to remember valuable information obtained during the training of the first split as the model is trained with the balanced second split. It was further observed that applying EWC, ROS, and ST together significantly outperforms other methods. Lastly, as the severity of data imbalance increases, the performance gap between applying ST and not applying grows substantially. In the case of ρ=10 and ρ=50, applying ROS together with ST and EWC shows the best performance in terms of F1-Score.

Table 3: Experimental results on image data

<table>
<thead>
<tr>
<th>Ratios</th>
<th>(CIFAR-10) ρ = 5 µ = 0.6</th>
<th>(CIFAR-10) ρ = 10 µ = 0.8</th>
<th>(MNIST) ρ = 10 µ = 0.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metrics</td>
<td>F1</td>
<td>Precision</td>
<td>Recall</td>
</tr>
<tr>
<td>Baseline</td>
<td>0.6695</td>
<td>0.6187</td>
<td>0.8794</td>
</tr>
<tr>
<td>ROS</td>
<td>0.8187</td>
<td>0.7956</td>
<td>0.8540</td>
</tr>
<tr>
<td>RUS</td>
<td>0.8263</td>
<td>0.8028</td>
<td>0.8567</td>
</tr>
<tr>
<td>ST</td>
<td>0.7916</td>
<td>0.7633</td>
<td>0.8329</td>
</tr>
<tr>
<td>ST + EWC</td>
<td>0.8033</td>
<td>0.7733</td>
<td>0.8403</td>
</tr>
<tr>
<td>ST + EWC + ROS</td>
<td>0.8298</td>
<td>0.8122</td>
<td>0.8532</td>
</tr>
</tbody>
</table>

CIFAR-10 and MNIST Results. Table 3 shows the results of experiments performed on the two image datasets. While MNIST (LeCun et al., 1998) is a simple handwritten digits dataset without color information, CIFAR-10 (Krizhevsky, 2012) is a relatively complicated image classification task with color information. The experimental results manifest larger gap exists when using ST on CIFAR-10 rather than on MNIST. This accounts to the relative simplicity of MNIST dataset which alleviates the shortcoming of skewed data during representation learning. This shows that ST greatly benefits the learner in a difficult setting where the the task difficulty and imbalance ratio is severe. The results show that a variant of our proposed method, ST with EWC and ROS, scores the best among other approaches in general.
5 Conclusion

Learning from imbalanced class inevitably brings bias toward frequently observed classes. Data-level manipulation tries to under-sample the majority classes or over-sample the minority classes. But these methods have a tendency to discard valuable information from observations of majority classes or overfit to sparse representation of minority classes, especially as the imbalance level gets higher. If the learning of a classification model is limited to maximizing the total accuracy over the entire data, models pay more attention to majority classes while neglecting the rest.

We propose Sequential Targeting, which effectively circumvents these issue by simply decomposing the data into k splits and sequentially training a learner in the decreasing order of KL divergence with the target distribution, which in the case of data imbalance problem is the discrete uniform distribution. Our architecture proves to be compatible with previous methods and outperforms existing methods when validated on imbalanced text and image classification tasks. Our model shows superiority in performance because of simultaneous increase in both precision and recall thereby improving the overall F1-score. We believe that our work makes a meaningful step towards the application of incremental learning on the data imbalance problem.

6 Discussion

Variations of $\eta$ ratio has been tested. However, it proves to be domain-dependent and most variations still outperformed previous methods. A fixed ratio of 1:1 was used throughout the experiment in this paper. However, in order to fully utilize ST, variations of different $\eta$ ratio should be tested for optimal performance.

In the case of ROS and RUS, ensemble methods could be utilized since data is randomly sampled. Each sample instance can be considered to train weak learners that can use max-voting schemes to create a single strong learner. Likewise, variations of $\eta$ ratio can be considered different samples train multiple weak learners. In further research, ensemble methods of ROS, RUS, and ST will be tested as well.

Lastly, since ST is compatible with algorithm-level methods, successful methods such as focal loss [Lin et al. 2017] and cost-sensitive deep neural network [Khan et al. 2015] are expected to increase overall performance if implemented together.

Acknowledgments

This work was funded by NAVER Corp.

References


Victor Sheng and Charles Ling. Thresholding for making classifiers cost sensitive. volume 1, 01 2006.