Detecting Bias in Transfer Learning Approaches for Text Classification

Irene Li
Department of Computer Science
Yale University
irene.li@yale.edu

Abstract

Classification is an essential and fundamental task in machine learning, playing a cardinal role in the field of natural language processing (NLP) and computer vision (CV). In a supervised learning setting, labels are always needed for the classification task. Especially for deep neural models, a large amount of high-quality labeled data are required for training. However, when a new domain comes out, it is usually hard or expensive to acquire the labels. Transfer learning could be an option to transfer the knowledge from a source domain to a target domain. A challenge is that these two domains can be different, either on the feature distribution, or the class distribution for the nature of the samples. In this work, we evaluate some existing transfer learning approaches on detecting the bias of imbalanced classes including traditional and deep models. Besides, we propose an approach to bridge the gap of the domain class imbalance issue.

1 Introduction

Machine learning has been widely applied to multiple applications in a variety of industries. Supervised machine learning is an essential type of algorithm where both data and the corresponding labels are required when doing the process of learning. Classification, as a very fundamental supervised machine learning task, plays an important role in many applications like face recognition and sentiment analysis (Le and Nguyen, 2015). However, a large amount of labeled data is often required when working with the supervised classification task, especially for deep neural networks. When it is difficult or expensive to get enough labeled data, transfer learning (Pan and Yang, 2009) is considered to be an approach to solve this issue which tries to transfer any existing knowledge to a new domain.

Existing research has been targeting on how to improve model performance when applying transfer learning techniques from a source domain to a target domain. In the real world, there are some differences in the source and target domain. We focus on the domain class imbalance (DCI) issue, where we have different ratios of the samples for classes in two domains. For instance, imagine a binary classification problem, we have 50/50 (Pos/Neg) balanced samples in the source domain, but we may have 30/70 in the target domain. In this case, if a classifier predict all the samples to be negative cases, it can still achieve an accuracy of 0.7. But in some extreme situations like in the medical domain, we also want to examine the accuracy for the positive cases. Most of the works have shown that there is an average improvement like an average accuracy and F1 score improvement on all classes. Fewer efforts were made to check the improvements for each class, especially for some rare classes. In this work, we aim to provide some analysis on the robustness of deep transfer learning models in text classification task with a domain class imbalanced setting. This work is inspired by (Weiss and Khoshgoftaar, 2016), where they performed tests on some traditional transfer learning algorithms under this setting with the lack of analysis for deep models.

1.1 Related Work

Most related works learn feature matching and instance reweighting for the two domains. Recent work by (Long et al., 2014) proposed a novel Transfer Joint Matching (TJM) method to model them in a unified optimization problem which is focusing reducing the domain difference by jointly matching the features
and re-weighting the instances across domains. This method substantially improved cross-domain image recognition baseline. Another way is to learn a good feature representation shared by both two domains. (Pan et al., 2010) proposed a new learning method to learn the shared representation called transfer component analysis (TCA). TAC learns some transferable feature components in a Reproducing Kernel Hilbert Space (RKHS) using Maximum Mean Discrepancy (MMD). Then in the shared feature space, some standard machine learning method can be used to do the classification task. Similarly, (Long et al., 2015) brought this framework into a deep neural network, achieving satisfying results in classification on images.

Adversarial learning methods are proved to be more robust when working with deep neural network models. In a recent work by (Tzeng et al., 2017), a model was proposed to combine discriminative modeling, untied weight sharing, and a GAN loss, call Adversarial Discriminative Domain Adaptation (ADDA). Their results achieved a state-of-the-art unsupervised adaptation results in a classic image classification task. We will provide more details in the following section.

The mentioned related works are mostly for CV applications, such methods are also possible to be adapted into NLP applications like sentiment classification.

2 Task Definition and Preliminaries

For simplicity, first we define these notations: indices $s$ and $t$ indicate Source and Target domains. Source domain samples are $X_s = \{x_{s1}, x_{s2}, \ldots, x_{sn}\}$ and the labels are $Y_s = \{y_{s1}, y_{s2}, \ldots, y_{sn}\}$; similarly, target domain samples are $X_t = \{x_{t1}, x_{t2}, \ldots, x_{tm}\}$ and the labels are $Y_t = \{y_{t1}, y_{t2}, \ldots, y_{tm}\}$. In our unsupervised transfer learning setting, the $Y_t$ are invisible to the model in the training stage, but $Y_s$ and $Y_t$ share the same label sets $Z = \{z_1, z_2, ..., z_l\}$.

There are two main differences between source and target domain data. Firstly, the marginal data distributions are different, thus $P(X_s) \neq P(X_t)$. That means the features would be different for these two domains. If we take a classifier trained on source domain and directly apply it into the target, we will have a performance drop. Secondly, the sample class ratios in training sets are different. We define the sample class ratio to be the distribution of the ratio of each class. To formulate, we choose $R_s = \{r_{s1}, r_{s2}, \ldots, r_{sl}\}$ to be sample class ratio of source domain, and $R_t = \{r_{t1}, r_{t2}, \ldots, r_{tl}\}$ for target domain. Note that this work focus on a class imbalanced setting, in our experiments, for each domain, we choose the ratios to be different for each class. Also we want a domain class imbalanced setting which means $R_s \neq R_t$.

2.1 Word Embeddings

Proposed by (Mikolov et al., 2013), word embeddings are dense word vectors as the presentations while preserving the semantics of the words. Usually, they can be pre-trained using free text without any labels. The dimension of the dense vectors are pre-defined and then trained using the skip-gram model or cbow model (Mikolov et al., 2013). In this work, we will pre-train the word vectors as our input to other models.

2.2 Generative Adversarial Networks (GANs)

GANs (Goodfellow, 2016) have been widely applied in various applications and tasks and achieving promising results. It is a generalized model which contains two main components: discriminator $D$ and generator $G$. The task for the generator $G$ is to generate some cases to fool the discriminator $D$ that these cases are from real data distribution $P_{data}$. Then the discriminator $D$ is to try its best to recognize if input cases are coming from $P_{data}$. The generator $G$ takes noise variables $p_z(z)$ as input to generate sample cases. Finally, we will learn the distribution of $G$ to be $P_y$, which we are expecting it to be close to $P_{data}$. In general, it can be defined as a two-player minimax game with a value function $V(G, D)$:

$$
\min_G \max_D V(D, G) = \mathbb{E}_{x \sim P_{data}}[\log D(x)] + \mathbb{E}_{z \sim P_z(z)}[\log(1 - D(G(z)))]
$$

(1)
2.3 ADDA Model

As mentioned before, in transfer learning tasks, the data distributions are different. As the source domain data could be obtained more easily, we have a good understanding of its distribution \( P(X_s) \). Then we apply a feature extractor \((M_s)\) for the raw inputs, then the distribution becomes \( P(M_s(X_s)) \) which is known already once the feature extractor \((M_s)\) is well-learned with the labels provided. Then the task is, can we learn a feature extractor for the target samples \((M_t)\) while the labels are missing? In this section, we introduce the idea of applying GAN to solve this issue.

The base model we choose is the Adversarial Discriminative Domain Adaptation (ADDA) model proposed by (Tzeng et al., 2017), as shown in Figure 1. The model was proposed to solve an unsupervised image classification task, where they have images from two domains: digit images with colorful background (source images) and hand written digit images without background (target images).

The first step is to pre-train a classifier \(C\) using the source data where labels are provided. It is essential to learn the features of the training samples. The choice is to apply a Convolutional Neural Network (CNN) (Krizhevsky et al., 2012) model before feeding into the classifier \(C\) as a feature extractor \((M_s)\) for the source domain. In this step, the loss function is a typical classification loss, thus the optimization problem will be:

\[
\min_{M_s, C} \mathcal{L}_{\text{cls}}(X_s, Y_s) = \\
- \mathbb{E}_{(x_s, y_s) \sim (X_s, Y_s)} \sum_{k=1}^{K} 1[k = y_s] \log C(M_s(x_s))
\] (2)

The second step is the adversarial adaptation training process. The goal for this part is to fix the feature extractor for the source domain \((M_s)\) which is learned in the first step, and learn the one for the target domain \((M_t)\). The main idea is use the GAN (Goodfellow, 2016) framework. Then the Target CNN or the feature extractor for the target domain \((M_t)\) acts like a generator which tries to generate similar samples with the source images, and it takes the original target images as the input. Then a discriminator \((D)\) is set to determine weather the images come from source or target by outputting domain labels. In other words, we will try to approximate the distribution from target \(P(M_t(X_t))\) to the known distribution from source \(P(M_s(X_s))\). In this step, \((M_t)\) will be learned, which acts like a mapping function from the target images to source images, and then the pre-trained classifier \(C\) can be adapted to the target domain images. The optimization function for the adversarial loss here can be found below. In this stage, \((M_s)\) is fixed while learning \((M_t)\).
The last step is the testing stage where we predict labels for the target images. We take the learned target CNN feature extractor $M_t$ from step two and the pre-trained classifier $C$ from step one to do classification.

3 Distance-based Backpropagation ADDA Model (DBA)

Inspired by the work of (Shen et al., 2018) and (Wang et al., 2019), it is possible to improve the model by instance re-weighting. The main idea is, we can give more weights to the instances from the target domain if they are quite similar to the instances from source domain. We can apply distance-based method to guide the process of backpropagation during training. The original stochastic gradient descent (SGD) is defined as:

$$\theta \leftarrow \theta - \alpha \nabla_{\theta} J(\theta; x^i, y^i)$$

(5)

where we have $\alpha$ as the learning rate, and the SGD step is applied during each mini-batch with $k$ instances (we set $k = 10$ in all of our experiments). Then the distance-based backpropagation is defined as:

$$\theta \leftarrow \theta - \alpha \sum_{i=1}^{k} w_i \nabla_{\theta} J(\theta; x^i, y^i)$$

(6)

where $w_i$ is the weight to each instance $x_i$.

Now we show how to calculate the instance weights. The distance-based backpropagation aims to give more weights to the instances which are very close to each other from target and source domains. Here, we take the outputs of a mini batch after the feature extractors $M_s(x_s)$ and $M_t(x_t)$, and for each instance $x_{i,t}$ from target domain, the weight is defined as:

$$w_i = \frac{1}{\tau \text{Dist}(M_t(x_i) - M_t(x_{i,t}))}$$

(7)

where $\tau$ is a partition function to make sure all weights (within a single mini batch) sum up to be 1. We decide the distance metric between each target domain instance output (a vector) and the output from source domain $M_s(x_s)$ (as a matrix) later. If the distance is small, then we should give more weight to that instance. It is possible to apply other distance metrics as well.

Then the distance-based backpropagation will be applied only for the target feature extractor part. We keep the source feature extractor to be optimized via the original SGD.

4 Experiments

The original ADDA model was proposed to solve image classifications. As we are targeting on text classification task, we will choose the input to be word embeddings and CNN model to deal with the input sentences (Zhang and Wallace, 2015). As mentioned before, we truncate each sentence to be 140 words, and each word embedding has a dimension of 128, then we make it as a 2-D matrix as an image-like input to CNN. As illustrated in figure 2, when the word embeddings are fed into the model, then we have a convolutional layer following by a pooling layer. In the end, there is a fully-connected layer and a softmax layer to predict the labels.

Besides, when choosing the base model for feature extractors $M_s$ and $M_t$, it is also possible to apply Long short-term memory networks (LSTM) (Hochreiter and Schmidhuber, 1997), but we may leave this out since CNN is already proved to be well-performed.
Our desired algorithmic result would be a potential improvement on this existing ADDA model with an imbalanced training sample testing with text classification job. The original experimental results by (Tzeng et al., 2017) did not include a model performance for this particular setting. One possible idea is to apply weights for individual samples while doing the adversarial adaptation training process. More specifically, both \( E_{x_s} \sim X_s \) and \( E_{x_t} \sim X_t \) in Equation 3 can be adjusted by the class ratios. For example, if the ratio is 90/10 for Pos/Neg, we may add more weights for the samples of Neg class for fairness and prevent some bias.

4.1 Implementation

Adapted code from https://github.com/corenel/pytorch-adda, implemented in PyTorch. Some bugs are fixed, and applied loading texts in stead of images. For simple baseline results, implemented from scratch. Use libraries include NLTK\(^1\) for natural language processing, and scikit-learn\(^2\) for machine learning methods.

4.2 Evaluation Metrics

The goal is to finalize a classifier \( C \) which has the ability to do classification on the target domain data \( X_t \). Average accuracy and F1 scores will be reported among all the classes. Accuracy is defined as the correct number of samples classified divided by the total number of samples. F1 score is defined as:

\[
F_1 = \left( \frac{\text{recall}^{-1} + \text{precision}^{-1}}{2} \right)^{-1} = 2 \cdot \frac{\text{precision} \cdot \text{recall}}{\text{precision} + \text{recall}}.
\]

(8)

Also we check the scores for individual class. To be more specific, we define the accuracy for each class to be: the number of correct samples classified by \( C \) divided by the total number of samples in that class. Similarly, we will compare F1 score for each class. By comparing the performance of different models, we are expecting an improvement in both accuracy and F1 score.

4.3 Datasets

We did experiments on the Multi-Domain Sentiment Dataset\(^3\), which contains four domains of the labeled reviews. Each domain contains 1000 positive and 1000 negative user reviews.

\(^1\)https://www.nltk.org/
\(^2\)https://scikit-learn.org/stable/
\(^3\)https://www.cs.jhu.edu/~mdredze/datasets/sentiment/
Table 1: Baseline methods

| Method | Src acc | Tgt acc | Src f1 (p) | Src f1 (n) | Tgt f1 (p) | Tgt f1 (n) |
|--------|---------|---------|------------|------------|------------|------------|
| LR     | 0.8250  | 0.7294  | 0.8204     | 0.8293     | 0.7283     | 0.7291     |
| NB     | 0.5938  | 0.5412  | 0.6011     | 0.5850     | 0.5314     | 0.5456     |
| RF     | 0.7446  | 0.6592  | 0.7569     | 0.7304     | 0.6784     | 0.6343     |

5 Results and Analysis

Simple Baseline methods We tried with simple TFIDF (term frequency–inverse document frequency) features as the input to three traditional classifiers: logistic regression (LR), random forest (RF), naive Bayesian (NB). Table 1 shows the baseline results when we applied balanced training, please note that these are average results. Since in this method, we do not have a progress of adaptation, so column Src acc gives the accuracy for training and testing on the source domain, while Tgt acc gives the accuracy for training on source but testing on target data. We also provide F1 scores for both positive (marked as (p)) and negative (marked as (n)) class. From the results, we can see that logistic regression (LR) performs much better than the other two classifiers, so we will then compare other model results with this method.

LR-discriminator Model To compare with the ADDA model, it is better to keep the model structure, which is shown in Figure 1. So we then replaced the CNN feature extractor with a traditional linear network structure and kept other layers. Specifically, the linear feature extractor is defined as:

\[ x' = xA^T + b \]  (9)

where matrix A and vector b are trainable parameters. We use this linear layer to do feature extraction when the inputs are TFIDF features, and each token is represented by its ID. To prevent overfitting, the dimensions of each layer shrink into smaller numbers. We show the results for balanced training in Table 3 (LR-Dis). The In column shows the results for training and testing in source domain, while Out column provides results for training in source but testing in target domain, and Adapted is after adaptation and tested in target domain. The columns f1(p) and f1(n) illustrate F1 scores for positive and negative class for each corresponding method. However, this setting is not suitable for this task as most of the accuracy are lower than random guess (0.5). The bold values are the ones higher than random guess, but there is no significant improvement. A possible reason is overfitting, as the training accuracy can be 0.9.

Deep Adaptation Adversarial Model Results with the ADDA model are shown in Table 3 marked as ADDA in the method column. Similarly, we show the accuracy in different training settings: balanced training, 1:10 (pos:neg), 3:10(pos:neg), 5:10(pos:neg) and 7:10(pos:neg). It is desired that adapted results are higher than out-domain results (bold values). We give in domain and out domain accuracy and f1 scores for both classes, as well as the results after adapting.

Optimizer and Distance Metric To select a better distance metric for calculating the weight in Equation 7 and a good optimizer, we compare Euclidean distance (EC) and Cosine similarity (Cosine) in Table 2, as well as two optimizers: stochastic gradient descent (SGD) (Bottou, 2010) and Adam (Adam) (Kingma and Ba, 2014). It shows that by applying Adam optimizer and Cosine similarity, we could have a slightly better transferred results with a higher accuracy and f1 scores for both positive and negative class. We only show results for the experimental setting from dvd domain to the other three classes for comparison.

Our Model We then apply cosine similarity and Adam optimizer as our final choice in our proposed model. Compared with other baseline models in Table 3, we show that our model Our performs better in the adapted results among all the other models.

We now compare the F1 scores of both positive and negative classes in Figure 3, where x-axis shows the class with ratio group and y-axis gives the F1 scores. For example, 1:10 gives the positive class under the ratio of 1:10, and the Neg beside it indicates the negative class with the same ratio. We can see that, in a reasonable training setting, especially for 3:10, 5:10 and 7:10, our proposed model has a better F1 score in the minor class, but nearly the same F1 score with the other class. While under a fair training...
setting, the ADDA model performs well in both classes. While given such a small number of training and testing example, the distance metric maybe not that accurate, especially for a small batch size, which may have some impact for calculating the gradients.

### 6 Conclusion and Future Work

We show that our proposed Distance-based Backpropagation model has the ability and potential to preventing class bias, with more unbalanced training data, the better our model perform.

However, from our results, we show that directly applying method works in small datasets, while small datasets without pre-trianed word embeddings will easily tend to overfit. The future work is to extend our method to larger scale datasets, and it is also possible to do more analysis on other optimizers. Besides, more work can be done in solving unbalanced training issue. Our proposed approach is possible to be applied in this following manner: we assign a larger weight $w_i$ to minor class instances, and Equation 7 then becomes:

Table 2: Comparison of SGD and Adam, Euclidean distance and Cosine similarity.

| Method   | Ratio | In  | H(p) | H(n) | Out | H(p) | H(n) | Adapted | H(p) | H(n) |
|----------|-------|-----|------|------|-----|------|------|---------|------|------|
| Baseline | 10:10 | 0.7211 | 0.7262 | 0.7149 | 0.6433 | 0.6460 | 0.6363 | - | - | - |
| LR       | 0.5150 | 0.4991 | 0.5261 | 0.5047 | 0.4928 | 0.5130 | 0.5033 | 0.4926 | 0.5103 |
| ADDA     | 0.7592 | 0.7535 | 0.7612 | 0.6660 | 0.6738 | 0.6440 | 0.6705 | 0.6673 | 0.6723 |
| Our      | 0.7604 | 0.7517 | 0.7668 | 0.6703 | 0.6723 | 0.6625 | 0.6703 | 0.6724 | 0.6626 |

| Baseline | 1:10  | 0.5044 | 0.6666 | 0.0337 | 0.5032 | 0.6662 | 0.0279 | - | - | - |
| LR       | 0.5067 | 0.6521 | 0.1489 | 0.5015 | 0.6495 | 0.1354 | 0.5017 | 0.6516 | 0.1236 |
| ADDA     | 0.5000 | 0.6667 | 0.0000 | 0.5007 | 0.6673 | 0.0000 | 0.5007 | 0.6673 | 0.0000 |
| Our      | 0.5000 | 0.6667 | 0.0000 | 0.5007 | 0.6673 | 0.0002 | 0.5007 | 0.6673 | 0.0002 |

| Baseline | 3:10  | 0.5399 | 0.6750 | 0.1953 | 0.5208 | 0.6633 | 0.1474 | - | - | - |
| LR       | 0.5038 | 0.6151 | 0.2990 | 0.5009 | 0.6120 | 0.2989 | 0.5014 | 0.6171 | 0.2834 |
| ADDA     | 0.5275 | 0.6789 | 0.1015 | 0.5155 | 0.6732 | 0.0625 | 0.5104 | 0.6712 | 0.0418 |
| Our      | 0.5279 | 0.6794 | 0.1022 | 0.5213 | 0.6751 | 0.0834 | 0.5213 | 0.6751 | 0.0834 |

| Baseline | 5:10  | 0.6046 | 0.6905 | 0.4372 | 0.5608 | 0.6663 | 0.3303 | - | - | - |
| LR       | 0.5025 | 0.5740 | 0.3982 | 0.5055 | 0.5766 | 0.4025 | 0.5029 | 0.5791 | 0.3902 |
| ADDA     | 0.6338 | 0.7280 | 0.4343 | 0.5850 | 0.6980 | 0.3241 | 0.5637 | 0.6919 | 0.2481 |
| Our      | 0.6296 | 0.7267 | 0.4163 | 0.5787 | 0.6960 | 0.3084 | 0.5786 | 0.6960 | 0.3083 |

| Baseline | 7:10  | 0.6997 | 0.7262 | 0.6392 | 0.6077 | 0.6710 | 0.4968 | - | - | - |
| LR       | 0.5146 | 0.5592 | 0.4583 | 0.5105 | 0.5494 | 0.4624 | 0.5071 | 0.5430 | 0.4600 |
| ADDA     | 0.7129 | 0.7646 | 0.6267 | 0.6258 | 0.6978 | 0.4824 | 0.6363 | 0.7095 | 0.5102 |
| Our      | 0.7242 | 0.7610 | 0.6633 | 0.6389 | 0.6890 | 0.5369 | 0.6389 | 0.6890 | 0.5370 |

Table 3: Final results.
\[ w_i = \begin{cases} \frac{n_p}{n_p + n_n} & \text{if } y_i \text{ is negative} \\ \frac{n_n}{n_p + n_n} & \text{if } y_i \text{ is positive} \end{cases} \]  

(10)

In this case, we will apply Equation 6 to both source and target feature extractor.

Acknowledgements

We thank Professor Nisheeth Vishnoi for useful discussions.

References

Léon Bottou. 2010. Large-scale machine learning with stochastic gradient descent. In Proceedings of COMPSTAT’2010, pages 177–186. Springer.

Ian Goodfellow. 2016. Nips 2016 tutorial: Generative adversarial networks. arXiv preprint arXiv:1701.00160.

Sepp Hochreiter and Jürgen Schmidhuber. 1997. Long short-term memory. Neural computation, 9(8):1735–1780.

Diederik P Kingma and Jimmy Ba. 2014. Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980.

Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. 2012. Imagenet classification with deep convolutional neural networks. Advances in neural information processing systems, 25:1097–1105.

Bac Le and Huy Nguyen. 2015. Twitter sentiment analysis using machine learning techniques. In Advanced Computational Methods for Knowledge Engineering, pages 279–289. Springer.

Mingsheng Long, Jianmin Wang, Guiguang Ding, Jiaguang Sun, and Philip S Yu. 2014. Transfer joint matching for unsupervised domain adaptation. In Proceedings of the IEEE conference on computer vision and pattern recognition, pages 1410–1417.

Mingsheng Long, Yue Cao, Jianmin Wang, and Michael Jordan. 2015. Learning transferable features with deep adaptation networks. In International conference on machine learning, pages 97–105. PMLR.

Tomas Mikolov, Ilya Sutskever, Kai Chen, Greg Corrado, and Jeffrey Dean. 2013. Distributed representations of words and phrases and their compositionality. arXiv preprint arXiv:1310.4546.

Sinno Jialin Pan and Qiang Yang. 2009. A survey on transfer learning. IEEE Transactions on knowledge and data engineering, 22(10):1345–1359.
Sinno Jialin Pan, Ivor W Tsang, James T Kwok, and Qiang Yang. 2010. Domain adaptation via transfer component analysis. *IEEE Transactions on Neural Networks*, 22(2):199–210.

Jian Shen, Yanru Qu, Weinan Zhang, and Yong Yu. 2018. Wasserstein distance guided representation learning for domain adaptation. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 32.

Eric Tzeng, Judy Hoffman, Kate Saenko, and Trevor Darrell. 2017. Adversarial discriminative domain adaptation. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 7167–7176.

Zhi Wang, Wei Bi, Yan Wang, and Xiaojiang Liu. 2019. Better fine-tuning via instance weighting for text classification. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 33, pages 7241–7248.

Karl R Weiss and Taghi M Khoshgoftaar. 2016. Investigating transfer learners for robustness to domain class imbalance. In *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 207–213. IEEE.

Ye Zhang and Byron Wallace. 2015. A sensitivity analysis of (and practitioners’ guide to) convolutional neural networks for sentence classification. *arXiv preprint arXiv:1510.03820*. 