Calibration with Bias-Corrected Temperature Scaling Improves Domain Adaptation Under Label Shift in Modern Neural Networks

Avanti Shrikumar†
Stanford University
avanti@stanford.edu

Anshul Kundaje†
Stanford University
akundaje@stanford.edu

† co-corresponding authors

Abstract

Label shift refers to the phenomenon where the marginal probability \(p(y)\) of observing a particular class changes between the training and test distributions while the conditional probability \(p(x|y)\) stays fixed. This is relevant in settings such as medical diagnosis, where a classifier trained to predict disease based on observed symptoms may need to be adapted to a different distribution where the baseline frequency of the disease is higher. Given calibrated estimates of \(p(y|x)\), one can apply an EM algorithm to correct for the shift in class imbalance between the training and test distributions without ever needing to calculate \(p(x|y)\). Unfortunately, modern neural networks typically fail to produce well-calibrated probabilities, compromising the effectiveness of this approach. Although Temperature Scaling can greatly reduce miscalibration in these networks, it can leave behind a systematic bias in the probabilities that still poses a problem. To address this, we extend Temperature Scaling with class-specific bias parameters, which largely eliminates systematic bias in the calibrated probabilities and allows for effective domain adaptation under label shift. We term our calibration approach "Bias-Corrected Temperature Scaling". On experiments with CIFAR10, we find that EM with Bias-Corrected Temperature Scaling significantly outperforms both EM with Temperature Scaling and the recently-proposed Black-Box Shift Estimation.

1 Introduction

Imagine we train a classifier in a developed country to predict whether or not a person is diseased given observed symptoms, and we deploy this classifier in a developing country in the hopes that it will improve access to healthcare. If the prevalence of the disease in the developing country is considerably higher than in the developed country, the classifier might systematically misdiagnose people in the developing country as not having the disease. How can we adapt the classifier to cope with the difference in the baseline prevalence of the disease between the two countries?

Formally, let \(y\) denote our labels (e.g. whether or not a person is diseased), and let \(x\) denote the observed symptoms. Let the joint distribution \((x, y)\) in the developed country be denoted as \(P\), and let the distribution in the developing country (where we do not have access to the labels \(y\)) be denoted as \(Q\). How can we adapt a classifier trained to estimate \(p(y|x)\) such that it works on \(Q\)? Absent any assumptions about the nature of the shift between \(P\) and \(Q\), this problem is intractable. However, if we believe that the disease generates similar symptoms in both countries, we can assume that \(p(x|y) = q(x|y)\), and that the shift in the joint distribution \(q(x, y)\) is due to a shift in the label proportion \(q(y)\) (formally, \(q(x, y) = p(x|y)q(y)\)). This is known as label shift or prior probability shift [Amos, 2008], and it corresponds to anti-causal learning (i.e. predicting the cause \(y\) from
Label shift is in contrast to a phenomenon called covariate shift, which is more appropriate for causal learning (i.e., predicting effects $y$ from their causes $x$). Under co-variate shift, it is assumed that $p(y|x) = q(y|x)$, and that changes in the joint distribution $q(x, y)$ are caused by a shift in $q(x)$ (i.e. $q(x, y) = q(x)p(y|x)$). Under the covariate shift assumption, there is less need to adapt $p(y|x)$ to work on distribution $q$ because $p(y|x) = q(y|x)$, although there may be computational benefits to adaptation [Amos, 2008]. The covariate shift assumption is not appropriate for the anti-causal setting. For example, childhood leukemia is more common among children raised in highly sterile environments [McKie, 2018]. All other things equal, a child presenting a particular set of symptoms $x$ is more likely to have leukemia if they were also raised in a highly sterile environment (i.e. $q(y|x)$ is not static, but rather depends on the prior proportion of $q(y)$ in sterile vs. non-sterile environments).

Saerens et al. [2002] showed that, given estimates of $p(y)$ and $p(y|x)$, a simple EM-based algorithm can be applied to estimate $q(y)$ under the label shift assumption without needing to estimate $p(x|y)$. However, because estimates of $p(y|x)$ derived from modern neural networks are often poorly calibrated, this strategy can sometimes fail to accurately estimate $q(y)$. Even though Temperature Scaling [Guo et al. [2017] can reduce the expected calibration error of modern neural networks, we find that it can still result in probabilities that are systematically biased, which can pose a problem for the EM-based algorithm. To address this, we extend Temperature Scaling with class-specific bias parameters, and term the resulting approach Bias-Corrected Temperature Scaling. On experiments with CIFAR10, we find that our method consistently outperforms both the recently proposed Black-Box Shift Estimation [Lipton et al. [2018] as well as EM applied in the absence of Bias-Corrected Temperature Scaling.

2 Previous Work

Label shift has several antecedents in the literature. Zhang et al. [2013] proposed an approach based on Kernel Mean Matching, but this approach was found to scale poorly with dataset size and underperformed on high-dimensional data [Lipton et al. [2018]. Saerens et al. [2002] proposed an EM algorithm for estimating the shift in the class prior probabilities between the training and test distributions. The algorithm has the following update steps:

\[
\hat{q}^{(0)}(y = i) = \hat{p}(y = i)
\]

\[
\hat{q}^{(s)}(y = i|x_k) = \frac{\hat{q}^{(s)}(y = i) \hat{p}(y = i|x_k)}{\sum_{j=1}^{N} \hat{q}^{(s)}(y = j) \hat{p}(y = j|x_k)}
\]

\[
\hat{q}^{(s+1)}(y = i) = \frac{1}{N} \sum_{k=1}^{N} \hat{q}^{(s)}(y = i|x_k)
\]

Here, $\hat{p}(y = i)$ is our estimate of the prior probability of observing class $i$ on the training set, $\hat{q}^{(s)}(y = i)$ is the estimate in EM step $s$ of the prior probability of observing class $i$ on the testing set, $\hat{p}(y = i|x_k)$ is the conditional probability of observing class $i$ given features $x_k$ on the training set, $\hat{q}^{(s)}(y = i|x_k)$ is the conditional probability in EM step $s$ of observing class $i$ given features $x_k$ on the testing set, and $N$ is the number of examples in the testing set. Because there is no need to estimate $p(x|y)$ in any step of the EM procedure, the algorithm can scale to high-dimensional datasets. We use this algorithm in our work.

Lipton et al. [2018] proposed Black-Box Shift Estimation, which defines $[w]_i = \frac{\hat{q}(y = i)}{\hat{p}(y = i)}$. Let $f$ be a function that accepts an input and returns the model’s predicted class, $x_k$ denote an example from a held-out portion of the training set, and $x_k'$ denote an example from the testing set. The empirical
estimate of \( w \), denoted as \( \hat{w} \), is computed as follows:

\[
\hat{u}_{g_i} = \sum_k \frac{1}{m} \mathbb{1}\{f(x'_k) = i\}
\]

\[
\hat{C}_{g_i,y_j} = \frac{1}{n} \sum_k \mathbb{1}\{f(x_k) = i \text{ and } y_k = j\}
\]

\[
\hat{w} = \hat{C}_{g,y}^{-1} \hat{u}_g
\]

Because the approach above is not guaranteed to produce positive values for all elements of \( \hat{w} \), any negative elements of \( \hat{w} \) are set to 0 after they are estimated. Domain adaptation is then performed by retraining the model on the entire training set distribution with examples upweighted in accordance with \( \hat{w} \). Note that this approach requires a portion of the training set to be held out during the initial training phase in order to accurately estimate the confusion matrix \( \hat{C}_{g,y} \) (the entire training set is used during the retraining phase).

Lipton et al. [2018] denote the version of BBSE described above as BBSE-hard. They also compare to a variant that they call BBSE-soft, which they describe as the case where where \( f \) outputs probabilities rather than hard classes. We interpreted this to mean that \( \hat{u}_{g_i} \) and \( \hat{C}_{g_i,y_j} \) are computed as follows:

\[
\hat{u}_{g_i} = \sum_k \frac{1}{m} f(x'_k)_i
\]

\[
\hat{C}_{g_i,y_j} = \frac{1}{n} \sum_k f(x_k)_i \mathbb{1}\{y_k = j\}
\]

In our experiments, we found that BBSE-soft used with an appropriate calibration method tended to outperform the original BBSE-soft and BBSE-hard (neither of which used calibration). In particular, we found that BBSE-soft with Bias-Corrected Temperature Scaling was particularly successful relative to the other BBSE variants.

3 Our Contributions

- We propose a new calibration approach called Bias-Corrected Temperature Scaling that corrects for systematic bias in the calibrated probabilities produced by Temperature Scaling.
- We propose combining recent work in label shift estimation with recent work in calibration to improve domain adaptation under label shift. In particular, we find that Bias-Corrected Temperature Scaling gives statistically significant improvements in domain adaptation over uncalibrated probabilities and regular Temperature Scaling when combined with EM [Saerens et al., 2002] or BBSE-soft [Lipton et al., 2018], with EM tending to be more successful that BBSE-soft after calibration. Note that BBSE requires the presence of a held-out set on which to compute the BBSE confusion matrix; this same held-out set can be used for calibration.
- We show that the weights from BBSE, when used with calibrated probabilities, can reliably produce improvements in accuracy without a need to retrain the model.

4 Methods

4.1 Bias-Corrected Temperature Scaling

Our recommended domain adaptation method is to use the EM algorithm of Saerens et al. [2002] in conjunction with a new calibration approach we propose called Bias-Corrected Temperature Scaling. The original Temperature Scaling algorithm [Guo et al., 2017] extends Platt Scaling [Platt, 1999] to the multiclass setting by introducing a temperature parameter \( T \) to the logit vector of the softmax.
function. Let \( z(x_k) \) be a function that returns the original logit vector. With temperature scaling, we have:

\[
p(y_i|x_k) = \frac{e^{z(x_k)_i/T}}{\sum_j e^{z(x_k)_j/T}}
\]

The parameter \( T \) is optimized with respect to the Negative Log Likelihood on a held-out portion of the training set, such as the validation set.

Guo et al. [2017] compared Temperature Scaling to an approach defined as vector-scaling, where a different temperature scaling parameter was used for each class along with class-specific bias parameters, namely:

\[
p(y_i|x_k) = \frac{e^{z(x_k)_i+W_i+b_i}}{\sum_j e^{z(x_k)_j+W_j+b_j}}
\]

The authors found that vector scaling had a tendency to overfit relative to Temperature Scaling and did not improve the expected calibration error. Unfortunately, in our experiments we found that Temperature Scaling alone often resulted in systematically biased estimates of \( p(y_i|x_k) \), which compromised the effectiveness of the EM algorithm. We therefore propose an intermediary between Temperature Scaling and Vector Scaling that we call Bias-Corrected Temperature Scaling, which we define as follows:

\[
p(y_i|x_k) = \frac{e^{z(x_k)_i/T+b_i}}{\sum_j e^{z(x_k)_j/T+b_j}} \tag{4}
\]

Like temperature scaling, the parameters \( T \) and \( b \) are optimized with respect to the Negative Log Likelihood on a held-out portion of the training set, such as the validation set. We find that Bias-Corrected Temperature Scaling corrects for systematic bias in the calibrated probabilities and improves the performance of EM-based domain adaptation.

4.2 Suggestions for Estimating \( \hat{p}(y = i) \)

We discuss two approaches that could be taken to compute the prior probability \( \hat{p}(y = i) \) of observing class \( y = i \) for the initialization of the EM algorithm in Eqn. 2. The first, and most intuitive, is to set \( \hat{p}(y = i) \) to be the proportion of training set examples for which the label is \( i \). A second, slightly less obvious approach is to set \( \hat{p}(y = i) \) to be close to \( E_{x \sim p(x)} \hat{p}(y = i|x) \), where \( p(x) \) represents the training set distribution of \( x \). If \( \hat{p}(y = i|x) \) is unbiased, we would expect the two approaches to agree. However, depending on the calibration method used, this may not be the case. If \( \hat{p}(y = i) \neq E_{x \sim p(x)} \hat{p}(y = i|x) \), the EM algorithm may estimate a distribution shift even when the testing set is distributed identically to the training set. To see why, consider the first step of EM:

\[
\hat{q}^{(1)}(y = i) = \frac{1}{N} \sum_{k=1}^{N} \hat{q}^{(0)}(y = i|x_k)
\]

\[
= \frac{1}{N} \sum_{k=1}^{N} \hat{p}(y = i|x_k)
\]

This is computing an estimate of \( E_{x \sim q(x)} \hat{p}(y = i|x) \). If \( E_{x \sim p(x)} \hat{p}(y = i|x) \neq \hat{p}(y = i) \), then \( \hat{q}^{(1)}(y = i) \) is unlikely to equal \( \hat{p}(y = i) \) even when \( q(x) \) and \( p(x) \) have identical distributions. For this reason, we recommend setting \( \hat{p}(y = i) \) to be an estimate of \( E_{x \sim p(x)} \hat{p}(y = i|x) \), such as by averaging \( \hat{p}(y = i|x) \) over all \( x \) in a held-out portion of the training set (the use of a held-out set is helpful for avoiding the effects of overfitting). In order to perform a fair comparison between the different calibration methods (some of which produce biased calibrated probabilities), we have used this second approach in this paper (i.e. we averaged \( \hat{p}(y = i|x) \) over the validation set).

4.3 Improving Test-Set Accuracy Without Retraining

In the BBSE algorithm proposed in Lipton et al. [2018], domain adaptation is performed by retraining the classifier on training set examples that are upweighted according to the estimated class ratios
\[ \hat{w} \]. However, if predictions are calibrated, domain adaptation can also be performed by calculating \( q(y = i|x) \) in accordance with Eqn. 2 reproduced in simplified form below:

\[
\hat{q}(y = i|x) = \frac{w_i \hat{p}(y = i|x)}{\sum_{j=1}^{n} w_j \hat{p}(y = j|x)}
\] (5)

While the original BBSE algorithm is designed to work with uncalibrated and biased classifiers, it requires that the confusion matrix \( \hat{C}_{g,y} \) be computed on a held-out portion of the training set. This held-out portion could, in principle, be used to calibrate the probabilities, allowing Eqn. 5 to be applied to perform domain adaptation without retraining. This is helpful in situations where retraining the model is not feasible. However, it is important to note that retraining could still produce benefits by allowing the model to devote more modeling capacity to the more important parts of the input space.

5 Experiments

We evaluated the efficacy of BBSE-hard, BBSE-soft and EM coupled to different calibration approaches. In our experiments, we trained ten CIFAR 10 models, each with a different random seed, using the architecture in [Geifman and El-Yaniv 2017]. The first 10K examples of the training set were reserved as a held-out validation set. Dirichlet shift was simulated on the testing set by sampling with replacement in accordance with class proportions generated by a dirichlet distribution with uniform \( \alpha \) values of 0.01, 0.1 or 1.0 (smaller values of \( \alpha \) result in more extreme label shift). Samples from the validation set were used for calibration, EM initialization and BBSE confusion matrix estimation. Performance was measured on the label-shifted testing set. In addition to exploring different degrees of dirichlet shift, we also investigated how the algorithms behaved when the number of samples used in the validation and testing set were varied. For example, in experiments with \( n = 500 \), only 500 samples from the validation set and 500 samples from the shifted testing set were presented to the domain adaptation and calibration algorithms. For each model, for a given \( \alpha \) and \( n \), 10 draws of the dirichlet distribution were performed, resulting in a total of 100 experi-
We have presented Bias-Corrected Temperature Scaling, a simple extension of Temperature Scaling that introduces class-specific bias parameters to correct for systematic bias in the calibrated probabilities. In experiments on CIFAR10, we show that domain adaptation with Bias-Corrected Temperature Scaling yields significant improvements compared to domain adaptation with no calibration or domain adaptation with regular Temperature Scaling. In particular, we find that EM with
Bias-Corrected Temperature Scaling is particularly effective, outperforming the recently-proposed Black-Box Shift Estimation. Future work might explore regularizing the EM update rules with conjugate priors to make them robust in the regime of very small dataset sizes, similar in spirit to the work of [Azizzadenesheli et al. 2019].

7 Software Availability

The label shift domain adaptation algorithms are implemented in https://github.com/kundajelab/abstention/blob/master/abstention/label_shift.py. Calibration approaches are implemented in https://github.com/kundajelab/abstention/blob/master/abstention/calibration.py.

8 Author Contributions

AS conceived of the method, designed & conducted experiments, and wrote the manuscript, with guidance and feedback from AK.

8.1 Acknowledgements

We thank the members of the Kundaje lab for discussion and feedback.
References

Storkey Amos. When training and test sets are different: Characterizing learning transfer. In Dataset
Shift in Machine Learning. The MIT Press, 2008.

Kamyar Azizzadenesheli, Anqi Liu, Fanny Yang, and Animashree Anandkumar. Regularized learn-
ing for domain adaptation under label shifts. In International Conference on Learning Representa-
tions, 2019. URL https://openreview.net/forum?id=rJl0r3R9KX

Y. Geifman and R. El-Yaniv. Selective Classification for Deep Neural Networks. ArXiv e-prints, 2017.

Chuan Guo, Geoff Pleiss, Yu Sun, and Kilian Q Weinberger. On calibration of modern neural
networks. June 2017.

Zachary Lipton, Yu-Xiang Wang, and Alexander Smola. Detecting and correcting for label shift
with black box predictors. In Jennifer Dy and Andreas Krause, editors, Proceedings of the 35th
International Conference on Machine Learning, volume 80 of Proceedings of Machine Learning
Research, pages 3122–3130, Stockholmsmässan, Stockholm Sweden, 10–15 Jul 2018. PMLR.
URL http://proceedings.mlr.press/v80/lipton18a.html

Robin McKie. For 30 years i’ve been obsessed by why children get leukaemia. now we have an
answer. The Guardian, December 2018.

John C Platt. Probabilistic outputs for support vector machines and comparisons to regularized
likelihood methods. In ADVANCES IN LARGE MARGIN CLASSIFIERS, 1999.

Marco Saerens, Patrice Latinne, and Christine Decaestecker. Adjusting the outputs of a classifier to
new a priori probabilities: a simple procedure. Neural Comput., 14(1):21–41, January 2002.

Bernhard Schoelkopf, Dominik Janzing, Jonas Peters, Eleni Sgouritsa, Kun Zhang, and Joris Mooij.
On causal and anticausal learning. June 2012.

Kun Zhang, Bernhard Schölkopf, Krikamol Muandet, and Zhikun Wang. Domain adaptation un-
der target and conditional shift. In Sanjoy Dasgupta and David McAllester, editors, Proceedings
of the 30th International Conference on Machine Learning, volume 28 of Proceedings of Machine
Learning Research, pages 819–827, Atlanta, Georgia, USA, 17–19 Jun 2013. PMLR. URL
http://proceedings.mlr.press/v28/zhang13d.html