Interpreting Bias in the Neural Networks: A Peek Into Representational Similarity

Gnyanesh Bangaru*
VNRVJIET
Hyderabad-90, T.S, India
cgnyanesh@gmail.com

Lalith Bharadwaj Baru*
IHub-Data, IIIT Hyderabad
Hyderabad-08, T.S, India
lalithbharadwaj313@gmail.com

Kiran Chakravarthula*
VNRVJIET
Hyderabad-90, T.S, India
kiran_c@vnrvjiet.in

Abstract

Neural networks trained on standard image classification data sets are shown to be less resistant to data set bias. It is necessary to comprehend the behavior of the objective function that might correspond to superior performance for data with biases. However, there is little research on the selection of the objective function and its representational structure when trained on data set with biases.

In this paper, we investigate the performance and internal representational structure of convolution-based neural networks (e.g., ResNets) trained on biased data using various objective functions. We specifically study similarities in representations, using Centered Kernel Alignment (CKA), for different objective functions (probabilistic and margin-based) and offer a comprehensive analysis of the chosen ones.

According to our findings, ResNets representations obtained with Negative Log Likelihood ($\mathcal{L}_{\text{NLL}}$) and Softmax Cross-Entropy ($\mathcal{L}_{\text{SCE}}$) as loss functions are equally capable of producing better performance and fine representations on biased data. We note that without progressive representational similarities among the layers of a neural network, the performance is less likely to be robust.

1 Introduction

Deep neural networks that have been trained with a huge amount of data pertaining to multiple classes have provided the most robust performance. Techniques like Domain-Adaptation and Transfer Learning are meant to be widely used, as they help to derive better transferable features to gain considerable performance. The prime objective of a neural network is to interpret the data over providing accurate performance and whereas training these neural networks in a controlled setting [21] leads them to perform poorly on unseen data, especially in the case of data with biases.

Moreover, the usage of pre-trained models produces biased results as the sought-after ImageNet tends to learn certain gender, racial and multiple inter-sectional biases as addressed by Kate Crawford et al. [7] and Ryan et al. [23]. A study, addressed in this work [8], states that by the present time, 85% of AI projects tend to produce erroneous results due to the presence of bias and loss of fairness in the existing data and algorithms. The learning progression of deep learning paradigm is turning to baffle model’s interpretability and make the models amiss.

Fortunately, certain optimization techniques for neural networks are been designed to address the representational bias problem. Further, an evaluation strategy for comprehending the relationship between feature spaces of multiple dimensions has been developed [2, 17, 24].

*These authors have equally contributed and Lalith has done this work while studying at VNRVJIET.
The representations learned through these neural networks are predominant towards providing prodigious performance whereas they are concealed w.r.t to their internal layer-based interpretation. This majorly leads the models to underperform on such data with biases.

Specifically, it is thus very crucial to interpret the reason behind such a learning mechanism to tackle the problem of bias. In this process, we address the following questions: What may be an ideal objective function for the biased data? What sort of representations do neural networks learn in due course, after being exposed to such data? How are the internal representations of neural networks impacted by altering the data samples (align and conflict)? Finally, how interpretable are the representations that are trained using biased data?

Contributions The contributions of this work are listed as,

1. Our Analysis suggests that $L_{NLL}$, and $L_{SCE}$ objective functions could contribute for a best performance with data with biases.

2. We have illustrated the internal representational structure of each model using CKA and conclude that, training a neural network with $L_{NLL}$ or $L_{SCE}$ loss attained better performance with progressive similarity across the layers.

2 Related Works

| Dataset Kind | Dataset Name | Classes | Train-Val-Test |
|--------------|--------------|---------|----------------|
| Biased       | C-MNIST      | 10      | 55k-5k-10k     |
| Biased       | CIFAR-C      | 10      | 45k-4.8k-10k   |
| Biased       | B-FFHQ       | 2       | 19.2k-1k-1k    |

Table 1: The above table illustrates data sets containing biased samples. ‘NA’ is specified to denote the absence of samples for that particular split.

Simon et al. [15] provides deeper insights into the transferability of representations when exposed to various loss functions, but this work majorly focuses on probabilistic objectives. Kim et al. [12] proposes a novel regularized loss function to unlearn the target bias in the data, based on mutual information obtained from InfoGANs [6], and a gradient reversal layer. Over time, it helps in reducing the pernicious effects of bias in data. Adeli et al. [1] proposes a dual-objective adversarial training loss function to learn traits that show the least statistical dependence and the maximum percipience with protected bias. We first examine the empirical performance of the objective functions by classifying them into two groups: (a) probabilistic, and (b) margin-based variations. Later, we examine the significance of particular objective functions that offer representation structure with strong generalizability and transferability.

3 Setup

Terminology The input data is represented as $X \in \{x^{(1)}, x^{(2)}, ..., x^{(n)}\}$ where $n$ is the total number of samples. The encoder $Enc(.)$ is used to extract features from a given input $X$. The features extracted from the encoder are presented as $f_v \leftarrow Enc(X)$; where $f_v \in \{f_v^{(1)}, f_v^{(2)}, ..., f_v^{(n)}\}$. The dimensions of the feature vector vary by changing the encoder. As most of the experiments were carried out using a supervised framework, the data sets do have certain ground truth labels, and these are represented as $Y \in \{y^{(1)}, y^{(2)}, ..., y^{(n)}\}$. The activation functions, sigmoid and softmax, are indicated by $\sigma(a_i) = 1/(1 + e^{-a_i})$ and $S(a_i) = e^{a_i} / \sum_j e^{a_j}$, respectively. The loss (objective) function, is denoted by $L(.)$ and the suffixes indicate its specified variant. The norms $\|a\|_1$ and $\|a\|_2$ indicate Manhattan and Euclidean norms respectively.

Models In this work, we use ResNet18 to understand convolution-type representations. ResNet18 is used for all of the data, which are illustrated in Table[1]. We have considered standard ResNets with global average pooling. The fully connected layers for ResNet18 are [512-c] (Where c denotes the number of classes). Intermediate dropout layers are used with a drop rate of 40% and a set constant for all data sets to have a fair evaluation.

Suppose, $a \in \mathbb{R}^n$ then, $\|a\|_1 = \sum_i |a_i| : \|a\|_2 = \sqrt{\sum_i a_i^2}$
Training and fine-tuning  To train each model we utilized Adam \[13\] as an optimizer with a standard learning rate of $10^{-3}$ and a weight decay of $10^{-5}$. For all of the executions, we trained each model from scratch. We fed 512 samples in batches to neural networks by varying the objective functions. The early stopping criterion is embedded with the patience of 12 epochs to ensure the model does not over-fit with excessive training. The results reported in Tables \[3\] are produced without any augmentations (except normalisation) and pre-trained weights.

Datasets  As mentioned, for bias data classification, we have utilized the data set provided by Lee et al. \[10\] where they aim to solve the bias problem by providing 3 different biased datasets: Colored MNIST, Corrupted CIFAR, and Biased FFHQ. From the provided datasets, we have analysed all of these datasets. Each data set consists of various diversity ratios in order to tackle the problem of bias. In which, bias is reduced by providing diverse bias-conflicting samples i.e. align and conflict divisions in the data set. The partition of data conflict is based on a percentage of diversity and we have used 5% diversity, among the varying diversity ratios. The number of diverse samples in that particular bias-conflicting data set is more compared to that of 0.5% and 1% i.e., in colored MNIST bias-conflicting samples are considered to have more images with differently colored digits whereas in 0.5% and 1% we have less diversity of bias-conflicting samples.

4 Experimentation

The choice of the objective function to train a deep neural network, on specified data remains a question. Janocha et al. \[10\] provided a theoretical justification and conducted experiments on MNIST pointing out the importance of $L_1$ and $L_2$ not just as regularizers, but as objective functions for better generalisations. Hui et al. \[9\] empirically proves that square loss with a little parametric tuning would produce significant results for most tasks of natural language processing (NLP) and automatic speech recognition (ASR). Hui et al. \[9\] specifically mentioned that the proposed square loss is not brittle for randomised initialisation. A recent analysis by Simon et al. \[14\] provides insights noting that the representations acquired to classify certain tasks with more margin-based objective functions calculate the error that approximates the underlying probabilities for representations acquired from an encoder (ResNet). In this paper, we include three probabilistic objectives and they are detailed in Table \[2\]. First, the Softmax cross-entropy \([5]\) ($L_{SCCE}$), a highly used objective, is obtained by applying softmax activation in the final layer of the neural network, and this feed is minimised by the negative log-likelihood ($L_{NLL}$). Next, Binary cross-entropy ($L_{BCE}$) is obtained by applying sigmoid activation ($\sigma(\cdot)$) at the final layer of neural networks and this information is minimised by NLL.

| Loss | Equation |
|------|----------|
| $L_{SCCE}$ | $(y_i \neq \hat{y}_i) \sum_c |y_i - \sigma(f(x_i))|$ |
| $L_{BCE}$ | $(y_i \neq \hat{y}_i) \sum_c y_i \log(\sigma(f(x_i))) + (1 - y_i) \log(1 - \sigma(f(x_i)))$ |
| $L_1$ | $\sum_i |y_i - S(f(x_i))|$ |
| $L_2$ | $\sum_i |y_i - S(f(x_i))|^2$ |
| $L_{BCE}$ | $\sum_i |y_i - \sigma(f(x_i))|$ |

Table 2: The above table illustrates all the objective functions that are experimented with in this work.

4.1 Probabilistic Objectives

Probabilistic objective functions calculate the error that approximates the underlying probabilities for representations acquired from an encoder (ResNet). In this paper, we include three probabilistic objectives and they are detailed in Table \[2\]. First, the Softmax cross-entropy ($L_{SCCE}$), a highly used objective, is obtained by applying softmax activation in the final layer of the neural network, and this feed is minimised by the negative log-likelihood ($L_{NLL}$). Next, Binary cross-entropy ($L_{BCE}$) is obtained by applying sigmoid activation ($\sigma(\cdot)$) at the final layer of neural networks and this information is minimised by NLL.

Primarily, the $L_{BCE}$ loss function is used for binary classification problems but, a recent work empirically proves that its implication on multi-class would lead to better performance \[3\] by applying the one-vs-rest strategy. Finally, the likelihood provides the joint probability of the sample distribution and minimises the negative logarithm of the obtained likelihood \[4\].
Figure 1: This figure illustrates CKA visualizations for all the objective functions on B-FFHQ, C-MNIST, and C-CIFAR data. Each tile of the plot consists of a color, indicating the correlation of representations i.e., the similarity of each layer representation. For these, corresponding color map is provided on the right side of each image tile. For visualizing CKA, we considered all the layers of the neural network (ResNet18) including activation, normalization, and fully-connected layers. The matrix is formed by comparing the features acquired by each layer of the ResNet18 with itself.

4.2 Margin-based Objectives

Margin-based objective functions calculate the error by discriminating the representations extracted from an encoder (ResNet). Similarly to probabilistic objectives, we include three margin-based objectives, which are detailed in Table 2. First, the mean absolute error ($L_1$ objective function) finds the Manhattan distance between the two representations. We acquire the theoretical motivation of Janocha et al. [10] that $L_1$ would reduce the sparseness in the representations. Rather than directly discriminating the representations in the final layer, we use softmax to ensure appropriate learning without saturation of partial derivatives.

Similar to $L_1$, we use $L_2$ to find the Euclidean distance between two representations (final layer). Lastly, Hui et al. [9] rescaled SoS to be more robust by providing two parameters $\alpha, \beta$. Injection of these parameters resulted in a decent performance for the NLP and ASR tasks, but was poorly performed on the computer vision tasks. For experimentation, we have chosen $\alpha, \beta = 1$, and this reduces to standard SoS.

4.3 Empirical Analysis

Now, let us understand the empirical performance of these objective functions trained on all variants of the data detailed in Table 3. A detailed mode of training, choice of neural networks, data sets and hyperparameters are neatly detailed in the Setup section. In most of the cases, $L_{NLL}$ was able to achieve top accuracy scores. But, $L_{SCE}$ obtained the highest accuracy for B-FFHQ and $L_2$ performed standalone; $L_{NLL}$ was able to compete closely with $L_{NLL}$. Hence, aggregating these results, it is strongly recommended that using probabilistic loss functions ($L_{SCE}$ and $L_{NLL}$) to obtain decent performance on most of the biased data. The empirical performance attained by these objective functions is well-understood but, the question arises with the internal representations of the model trained on these data and for this we comprehend the underlying the representational structure.

4.4 Representational Analysis

The Centered Kernel Alignment (CKA) was devised to understand the representation structure of artificial neural networks. It is well established in the literature that CKA [15] acquires qualitative representations compared to PwCCA [18] and SVCCA [20]. CKA not only captures the correspondence between the representations of a neural network but also allows us to compute the similarity between pairs of layers.
Table 3: The table below provides the empirical performance of the individual objective functions for the generic, bias, and OOD data. The experiments were carried out without any augmentations and did not use learnt weights (ImageNet1K or ImageNet21K) for the training models. These experiments were conducted three times for each objective function for a fair evaluation. The tabulated mean and standard deviation (mean ± std) in each cell depicts the accuracy scores obtained after experimenting thrice with the ‘test’ data. **Bold** and **underline** represent the accuracy scores of **first** and **second** best performing models, respectively.

To reduce the computational expense consumed by linear CKA, mini-batch CKA is applied by computing the mean of HSIC (Hilbert-Schmidt Independence Criterion) scores on selected mini-batches \( N \). This strategy is implemented straightforwardly as Thao et al. [19]. The mini-batch CKA is detailed as follows:

\[
    \text{CKA}^{mini} = \frac{\sum_{i=1}^{N} \text{HSIC}_i(\hat{X}_i, \hat{Y}_i)}{\sqrt{\sum_{i=1}^{N} \text{HSIC}_i(\hat{X}_i, \hat{X}_i)} \sqrt{\sum_{i=1}^{N} \text{HSIC}_i(\hat{Y}_i, \hat{Y}_i)}},
\]

where, \( \hat{X}_i = X_i X_i^T; \hat{Y}_i = Y_i Y_i^T \). These \( X_i \in \mathbb{R}^{n \times d_1} \) and \( Y_i \in \mathbb{R}^{n \times d_2} \) are activation matrices for \( i^{th} \) mini-batch of examples without replacement. We now try to analyse the representations using CKA for all the objective functions on the aforementioned data.

In Figure 1, when considering B-FFHQ data, the CKA representation matrix formed for \( \mathcal{L}_{\text{NLL}}, \mathcal{L}_{\text{BCE}} \) and \( \mathcal{L}_{\text{SCE}} \) seems to have similar characteristics. While considering the case for the C-MNIST data set, all the loss functions tend to form a small box-like structure at the ultimate layers (at the top right corner after 50\(^{th}\) layer). But, \( \mathcal{L}_{\text{NLL}}, \mathcal{L}_{\text{SoS}}, \) and \( \mathcal{L}_{\text{SCE}} \) seem to have uniformly distributed representation with decreasing similarity with the depth of the neural network. Finally, for C-CIFAR data the refined representation similarity is obtained for \( \mathcal{L}_{\text{SCE}}, \mathcal{L}_{\text{BCE}} \) and \( \mathcal{L}_2 \).

However, the performance for all the data is higher for Probabilistic objectives. Considering the case of \( \mathcal{L}_{\text{SoS}} \) objective, it is prone to have **block structured** representations on utmost all the data [19]. This structured block resembles the neural network as **overparameterised** model. The underlying reason is either that the model has fewer data samples or a deeper network. This can be surmounted by truncating the layers with identical representational similarity.

These indications are clear to note that, the objectives \( \mathcal{L}_{\text{SCE}} \) and \( \mathcal{L}_{\text{NLL}} \) not only provide decent empirical performance but capture fine representations with ResNets. Hence, from this interpretation we infer that, representations acquired by probabilistic objectives are comparatively better to provide good generalisations for diverse bias data sets.

---

\( ^3 \)To understand the CKA and its underlying significance we request the readers to go through the works [15][19].
5 Conclusion

By summarising the above, we infer that $L_{\text{NLL}}$ and $L_{\text{SCE}}$ objectives would be apt for data with biases. But while experimenting, it should be noted that the variance in accuracy must be minimalist to ensure robustness. Next, if the neural networks are exposed to biased data, generalisation is attained only when the layers of CKA matrices have a progressive dissimilarity with the depth of the network.

In the future, we see the potential requirement of data sets comprising samples with biases as big as ImageNet. Similarly, the representations acquired by the models are to be ensured with the least bias possible. We believe that, comprehending the representations acquired from biased data would aid researchers in providing a novel debiasing neural network or a bias mitigation strategy. Also we believe that, this CKA framework can be extended to study the detailed interpretability of the neural networks [11].

6 Ethical Aspects and Broader Impact

Inherent biases of the individuals who train AI models inevitably reflect in the models. Such inherent biases are due to psychological constructs, different types of biases, and the inter-working thereof [8]. In addition to the unintentional, implicit, and indirect nature of these inherent biases, the need to retain certain biases—such as demographic aspects of the data—needed to qualify the data increases the complexity in the overall bias. Unconventional training and evaluation methods may be necessary to de-bias the AI models and minimize human interventions, leading to the design and development of meta approaches to create ethical or responsible AI systems.

Since scientists and analysts routinely conclude, albeit based on evidence-based insights, biased data can be inherently misleading. The impact of such misinterpretation can be corrected through exposure, experience, and expertise when humans are involved in the interpretation. However, if the data itself is biased or only the interpretations of the data were presented by researchers, the danger of unconscious or even conscious biases cannot be ruled out entirely. While Smith’s book [22] is an elaborate example of how research methodologies are inherently designed with ignorance towards the subjects of study, subtler cases of bias can be innate to the ways data are sourced, stored, pre-processed, analyzed, and interpreted.

The current work emphasises the need to methodically improve the quality biased representations obtained from neural networks without proposing radical paradigm shifts in current methodologies. This work does not organically provide scope for misinterpretation of data or biased decisions made through data analytics. Furthermore, the work facilitates a better and more uniform representation of the data by reminding researchers to consciously consider the biased aspects of the data, which may be rather inconspicuous. A stronger motivation arises as Artificial Intelligence and Machine Learning continue to be used in various technology and social domains for diverse applications.

References

[1] Ehsan Adeli, Qingyu Zhao, Adolf Pfefferbaum, Edith V Sullivan, Li Fei-Fei, Juan Carlos Niebles, and Kilian M Pohl. Representation learning with statistical independence to mitigate bias. In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, pages 2513–2523, 2021.
[2] Hilal Asi, Yair Carmon, Arun Jambulapati, Yujia Jin, and Aaron Sidford. Stochastic bias-reduced gradient methods. Advances in Neural Information Processing Systems, 34, 2021.
[3] Lucas Beyer, Olivier J Hénaaff, Alexander Kolesnikov, Xiaohua Zhai, and Aäron van den Oord. Are we done with imagenet? arXiv preprint arXiv:2006.07159, 2020.
[4] Christopher M Bishop et al. Neural networks for pattern recognition. Oxford university press, 1995.
[5] John Bridle. Training stochastic model recognition algorithms as networks can lead to maximum mutual information estimation of parameters. Advances in neural information processing systems, 2, 1989.
[6] Xi Chen, Yan Duan, Rein Houthooft, John Schulman, Ilya Sutskever, and Pieter Abbeel. Infogan: Interpretable representation learning by information maximizing generative adversarial nets. Advances in neural information processing systems, 29, 2016.
[7] Kate Crawford. Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. Yale University Press, New Haven, 2021.
[8] Ray Eitel-Porter. Beyond the promise: implementing ethical ai. AI and Ethics, 1(1):73–80, 2021.
Like Hui and Mikhail Belkin. Evaluation of neural architectures trained with square loss vs cross-entropy in classification tasks. ICLR, 2021.

Katarzyna Janocha and Wojciech Marian Czarnecki. On loss functions for deep neural networks in classification. arXiv preprint arXiv:1702.05659, 2017.

Kohitij Kar, Simon Kornblith, and Evelina Fedorenko. Interpretability of artificial neural network models in artificial intelligence vs. neuroscience. arXiv preprint arXiv:2206.03951, 2022.

Byungju Kim, Hyunwoo Kim, Kyungsu Kim, Sungjin Kim, and Junmo Kim. Learning not to learn: Training deep neural networks with biased data. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pages 9012–9020, 2019.

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

Simon Kornblith, Ting Chen, Honglak Lee, and Mohammad Norouzi. Why do better loss functions lead to less transferable features? Advances in Neural Information Processing Systems, 34, 2021.

Simon Kornblith, Mohammad Norouzi, Honglak Lee, and Geoffrey Hinton. Similarity of neural network representations revisited. In International Conference on Machine Learning, pages 3519–3529. PMLR, 2019.

Jungsoo Lee, Eungyeup Kim, Juyoung Lee, Jiheyeon Lee, and Jaegul Choo. Learning debiased representation via disentangled feature augmentation. Advances in Neural Information Processing Systems, 34, 2021.

Yi Li and Nuno Vasconcelos. Repair: Removing representation bias by dataset resampling. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pages 9572–9581, 2019.

Ari Morcos, Maithra Raghu, and Samy Bengio. Insights on representational similarity in neural networks with canonical correlation. Advances in Neural Information Processing Systems, 31, 2018.

Thao Nguyen, Maithra Raghu, and Simon Kornblith. Do wide and deep networks learn the same things? uncovering how neural network representations vary with width and depth. ICLR, 2021.

Maithra Raghu, Justin Gilmer, Jason Yosinski, and Jascha Sohl-Dickstein. Svcca: Singular vector canonical correlation analysis for deep learning dynamics and interpretability. Advances in neural information processing systems, 30, 2017.

Jacob Russin, Randall C O Reilly, and Yoshua Bengio. Deep learning needs a prefrontal cortex. Work Bridging AI Cogn Sci, 107:603–616, 2020.

Linda Tuhiwai Smith. Decolonizing methodologies: Research and indigenous peoples. Bloomsbury Publishing, 2021.

Ryan Steed and Aylin Caliskan. Image representations learned with unsupervised pre-training contain human-like biases. Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, 2021.

Xingjian Zhen, Zihang Meng, Rudrasis Chakraborty, and Vikas Singh. On the versatile uses of partial distance correlation in deep learning. ArXiv, abs/2207.09684, 2022.