Intra Order-Preserving Functions for Calibration of Multi-Class Neural Networks

Predicting calibrated confidence scores for multi-class deep networks is important for avoiding rare but costly mistakes. A common approach is to learn a post-hoc calibration function that transforms the output of the original network into calibrated confidence scores while maintaining the network’s accuracy. However, previous post-hoc calibration techniques work only with simple calibration functions, potentially lacking sufficient representation to calibrate the complex function landscape of deep networks. In this work, we aim to learn general post-hoc calibration functions that can preserve the top-$k$ predictions of any deep network. We call this family of functions intra order-preserving functions. We propose a new neural network architecture that represents a class of intra order-preserving functions by combining common neural network components. Additionally, we introduce order-invariant and diagonal sub-families, which can act as regularization for better generalization when the training data size is small. We show the effectiveness of the proposed method across a wide range of datasets and classifiers. Our method outperforms state-of-the-art post-hoc calibration methods, namely temperature scaling and Dirichlet calibration, in several evaluation metrics for the task.

1 Introduction

Deep neural networks have demonstrated impressive accuracy in classification tasks, such as image recognition [8, 28] and medical research [10, 3]. These exciting results have recently motivated engineers to adopt deep networks as default components in building decision systems; for example, a multi-class neural network can be treated as a probabilistic predictor and its softmax output can provide the confidence scores of different actions for the downstream decision making pipeline [6, 2, 21]. While this is an intuitive idea, recent research has found that deep networks, despite being accurate, can be overconfident in their predictions, exhibiting high calibration error [20, 7, 11]. In other words, trusting the network’s output naively as confidence scores in system design could cause undesired consequences: a serious issue for applications where mistakes are costly, such as medical diagnosis and autonomous driving.

A promising approach to address the miscalibration is to augment a given network with a parameterized calibration function, such as extra learnable layers. This additional component is tuned post-hoc using a held-out calibration dataset, so that the effective full network becomes calibrated [7, 14, 16, 15, 27, 35]. In contrast to usual deep learning, the calibration dataset here is typically

*Equal Contribution.
We identify necessary and sufficient conditions for describing intra order-preserving functions, study their differentiability, and propose a novel neural network architecture that can represent complex intra order-preserving function through common neural network components. From practical point of view, we devise a new post-hoc network confidence calibration technique using different intra order-invariant sub-families. Because a post-hoc calibration function keeps the top-$k$ class prediction if and only if it is an intra order-preserving function, learning the post-hoc calibration function within the intra order-preserving family presents a solution to the dilemma between accuracy and flexibility faced in the previous approaches. We conduct several experiments to validate the benefits of learning.
with these new functions for post-hoc network calibration. The results demonstrate improvement over various calibration performance metrics, compared with the original network, temperature scaling [7], and Dirichlet calibration [14].

2 Problem Setup

We address the problem of calibrating neural networks for \( n \)-class classification. Let define \([n] := \{1, \ldots, n\}\), \( \mathcal{Z} \subseteq \mathbb{R}^d \) be the domain, \( \mathcal{Y} = [n] \) be the label space, and let \( \Delta_n \) denote the \( n-1 \) dimensional unit simplex. Suppose we are given a trained probabilistic predictor \( \phi_o : \mathbb{R}^d \rightarrow \Delta_n \) and a small calibration dataset \( \mathcal{D}_c \) of i.i.d. samples drawn from an unknown distribution \( \pi \) on \( \mathcal{Z} \times \mathcal{Y} \). For simplicity of exposition, we assume that \( \phi_o \) can be expressed as the composition \( \phi_o := \mathsf{sm} \circ g \), with \( g : \mathbb{R}^d \rightarrow \mathbb{R}^n \) being a non-probabilistic \( n \)-way classifier and \( \mathsf{sm} : \mathbb{R}^n \rightarrow \Delta_n \) being the softmax operator, i.e. \( \mathsf{sm}_i(x) = \frac{\exp(x_i)}{\sum_j \exp(x_j)} \), for \( i \in \mathcal{Y} \), where the subscript \( i \) denotes the \( i \)th element of a vector. When queried at \( z \in \mathcal{Z} \), the probabilistic predictor \( \phi_o \) returns \( \arg \max_i \phi_o_i(z) \) as the predicted label and \( \max_i \phi_o_i(z) \) as the associated confidence score. (The top-\( k \)-prediction is defined similarly.) We say \( g(z) \) is the logits of \( z \) with respect to \( \phi_o \).

Given \( \phi_o \) and \( \mathcal{D}_c \), our goal is to learn a post-hoc calibration function \( f : \mathbb{R}^n \rightarrow \mathbb{R}^n \) such that the new probabilistic predictor \( \phi := \mathsf{sm} \circ f \circ g \) is better calibrated and keeps the accuracy (or similar performance concepts like top-\( k \) accuracy) of the original network \( \phi_o \). That is, we want to learn new logits \( f(g(z)) \) of \( z \). As we will discuss, this task is non-trivial, because while learning \( f \) might improve calibration, doing so could also risk over-fitting to the small dataset \( \mathcal{D}_c \) and damaging accuracy. To make this statement more precise, below we first review the definition of perfect calibration [7] and common calibration metrics and then discuss challenges in learning \( f \) with \( \mathcal{D}_c \).

Definition 1. For a distribution \( \pi \) on \( \mathcal{Z} \times \mathcal{Y} \) and a probabilistic predictor \( \psi : \mathbb{R}^d \rightarrow \Delta_n \), let random variables \( z \in \mathcal{Z} \), \( y \in \mathcal{Y} \) be distributed according to \( \pi \), and define random variables \( \hat{y} := \arg \max_i \psi_i(z) \) and \( \hat{p} := \psi_o(z) \). We say \( \psi \) is perfectly calibrated with respect to \( \pi \), if for any \( \hat{p} \in [0, 1] \), it satisfies \( \text{Prob}(\hat{y} = y | \hat{p} = \hat{p}) = \hat{p} \).

Note that \( z, y, \hat{y}, \hat{p} \) are correlated random variables. Therefore, Definition 1 essentially means that, if \( \psi \) is perfectly calibrated, then for any \( \hat{p} \in [0, 1] \), the true label \( y \) and the predicted label \( \hat{y} \), with a probability exactly \( \hat{p} \) in the events where \( z \) satisfies \( \max_i \psi_i(z) = \hat{p} \).

In practice, learning a perfectly calibrated predictor is unrealistic, so we need a way to measure the calibration error. A common calibration metric is called Expected Calibration Error (ECE) [23]:

\[
\text{ECE} = \frac{1}{M} \sum_{m=1}^{M} |B_m| \left( \text{acc}(B_m) - \text{conf}(B_m) \right).
\]

This equation is calculated in two steps: First the confidence scores of samples in \( \mathcal{D}_c \) are partitioned into \( M \) equally spaced bins \( \{B_m\}_{m=1}^{M} \). Second the weighted average of the differences between the average confidence \( \text{conf}(B_m) = \frac{1}{|B_m|} \sum_{i \in B_m} \hat{p}^i \) and the accuracy \( \text{acc}(B_m) = \frac{1}{|B_m|} \sum_{i \in B_m} 1(y^i = \hat{y}^i) \) in each bin is computed as the ECE metric, where \( |B_m| \) denotes the size of bin \( B_m \). \( 1 \) is the indicator function, and the superscript \( i \) indexes the sampled random variable. In addition to ECE, other calibration metrics have also been proposed [7][25][1][17]; e.g., Classwise-ECE [14] and Brier score [1] are proposed as measures of classwise-calibration. All the metrics for measuring calibration have their own pros and cons. Here, we consider the most commonly used metrics for measuring calibration and leave their analysis for future work.

While the calibration metrics above measure the deviation from perfect calibration in Definition 1, they are usually not suitable loss functions for optimizing neural networks, e.g., due to the lack of continuity or non-trivial computation time. Instead, the calibration function \( f \) in \( \phi = \mathsf{sm} \circ f \circ g \) is often optimized indirectly through a surrogate loss function (e.g. the negative log-likelihood) defined on the held-out calibration dataset \( \mathcal{D}_c \). [7].

2.1 Importance of Inductive Bias

Unlike regular deep learning scenarios, here the calibration dataset \( \mathcal{D}_c \) is relatively small. Therefore, controlling the capacity of the hypothesis space of \( f \) becomes a crucial topic [7][15][14]. There is typically a trade-off between preserving accuracy and improving calibration: Learning \( f \) could...
improve the calibration performance, but it could also change the decision boundary of $\phi$ from $\phi_o$, decreasing the accuracy. While using simple calibration functions may be applicable when $\phi_o$ has a simple function landscape or is already close to being well calibrated, such a function class might not be sufficient to calibrate modern deep networks with complex decision boundaries as we will show in the experiments in Section 6.

The observation above motivates us to investigate the possibility of learning calibration functions within a hypothesis space that can provably guarantee preserving the accuracy of the original network $\phi_o$. The identification of such functions would address the previous dilemma and give precisely the needed structure to ensure generalization of calibration when the calibration dataset $D_c$ is small.

3 Intra Order-Preserving Functions

In this section, we formally describe this desirable class of functions for post-hoc network calibration. We name them intra order-preserving functions. Learning within this family is both necessary and sufficient to keep the top-$k$ accuracy of the original network unchanged. We also study additional function structures on this family (e.g. limiting how different dimensions can interact), which can be used as regularization in learning calibration functions. Last, we discuss a new neural network architecture for representing these functions.

3.1 Setup: Sorting and Ranking

We begin by defining sorting functions and ranking in preparation for the formal definition of intra order-preserving functions. Let $\mathbb{P}^n \subset \{0, 1\}^{n \times n}$ denote the set of $n \times n$ permutation matrices. Sorting can be viewed as a permutation matrix; Given a vector $x \in \mathbb{R}^n$, we say $S : \mathbb{R}^n \to \mathbb{P}^n$ is a sorting function if $y = S(x)x$ satisfies $y_1 \geq y_2 \geq \cdots \geq y_n$. In case there are ties in the input vector $x$, the sorting matrix can not be uniquely defined. To resolve this, we use a pre-defined tie breaker vector which is used as a tie breaking protocol. We say a vector $t \in \mathbb{R}^n$ is a tie breaker if $t = Pr$, for some $P \in \mathbb{P}^n$, where $r = [1, \ldots, n]^	op \in \mathbb{R}^n$. Tie breaker pre-assigns priorities to indices of the input vector and is used to resolve ties. For instance, $S_1 = [1 \ 0 \ 0]$ and $S_2 = [0 \ 1 \ 0]$ are the unique sorting matrices of input $x = [0, 0]^	op$ with respect to tie breaker $t_1 = [1, 2]^	op$ and $t_2 = [2, 1]^	op$, respectively. We say two vectors $u, v \in \mathbb{R}^n$ share the same ranking if $S(u) = S(v)$ for any tie breaker $t$.

3.2 Intra Order-Preserving Functions

We define the intra order-preserving property with respect to different coordinates of a vector input.

Definition 2. We say a function $f : \mathbb{R}^n \to \mathbb{R}^n$ is intra order-preserving, if, for any $x \in \mathbb{R}^n$, both $x$ and $f(x)$ share the same ranking.

The output of an intra order-preserving function $f(x)$ maintains all ties and strict inequalities between elements of the input vector $x$. Namely, for all $i, j \in [n]$, we have $x_i > x_j$ (or $x_i = x_j$) if and only if $f_i(x) > f_j(x)$ (or $f_i(x) = f_j(x)$). For example, a simple intra order-preserving function is the temperature scaling $f(x) = x/t$ for some $t > 0$. Another common instance is the softmax operator.

Clearly, applying an intra order-preserving function as the calibration function in $\phi = \text{sm} \circ f \circ g$ does not change top-$k$ predictions between $\phi$ and $\phi_o = \text{sm} \circ g$.

Next, we provide a necessary and sufficient condition for constructing continuous, intra order-invariant functions. This theorem will be later used to design neural network architectures for learning calibration functions. Note that for a vector $v \in \mathbb{R}^n$ and an upper-triangular matrix of ones $U$, $Uv$ is the reverse cumulative sum of $v$ (i.e. $(Uv)_i = \sum_{j=1}^n v_j$).

Theorem 1. A continuous function $f : \mathbb{R}^n \to \mathbb{R}^n$ is intra order-preserving, if and only if $f(x) = S(x)^{-1}Uw(x)$ with $U$ being an upper-triangular matrix of ones and $w : \mathbb{R}^n \to \mathbb{R}^n$ being a continuous function such that

- $w_i(x) = 0$, if $y_i = y_{i+1}$ and $i < n$,
- $w_i(x) > 0$, if $y_i > y_{i+1}$ and $i < n$,
- $w_n(x)$ is arbitrary,

where $y = S(x)x$ is the sorted version of $x$.
The proof is deferred to Appendix. Here we provide as sketch as to why Theorem 1 is true. Since \( w_i(x) \geq 0 \) for \( i < n \), applying the matrix \( U \) on \( w(x) \) results in a sorted vector \( Uw(x) \). Thus, applying \( S(x)^{-1} \) further on \( Uw(x) \) makes sure that \( f(x) \) has the same ordering as the input vector \( x \). The reverse direction can be proved similarly. For the continuity, observe that the sorting function \( S(x) \) is piece-wise constant with discontinuities only when there is a tie in the input \( x \). This means that if the corresponding elements in \( Uw(x) \) are also equally valued when a tie happens, the discontinuity of the sorting function \( S \) does not affect the continuity of \( f \) inherited from \( w \).

### 3.3 Order-Invariant and Diagonal Sub-families

Different classes in a classification task typically have shared characteristics. Therefore, calibration functions sharing properties across different classes can work as a suitable inductive bias in learning. Here we use this idea to define two additional structures interesting to intra order-preserving functions: order-invariant and diagonal properties. Similar to the purpose of the previous section, we will study necessary and sufficient conditions for functions with these properties.

First, we study the concept of order-invariant functions.

**Definition 3.** We say a function \( f : \mathbb{R}^n \to \mathbb{R}^n \) is order-invariant, if \( f(Px) = Pf(x) \) for all \( x \in \mathbb{R}^n \) and permutation matrices \( P \in \mathbb{P}^n \).

For an order-invariant function \( f \), when two elements \( x_i \) and \( x_j \) in the input \( x \) are swapped, the corresponding elements \( f_i(x) \) and \( f_j(x) \) in the output \( f(x) \) are also swapped. In this way, the mapping learned for the \( i \)th class can also be used for the \( j \)th class. Thus, the order-invariant family shares the calibration function between different classes while allowing the output of each class be a function of all other class predictions.

We characterize in the theorem below the properties of functions that are both intra order-preserving and order-invariant (an instance is the softmax operator). It shows that, to make an intra order-preserving function also order-invariant, we just need to feed the function \( w \) in Theorem 1 with the sorted input \( y = S(x)x \) instead of \( x \). This scheme makes the learning of \( w \) easier since it always sees sorted vectors (which are a subset of \( \mathbb{R}^n \)).

**Theorem 2.** A continuous, intra order-preserving function \( f : \mathbb{R}^n \to \mathbb{R}^n \) is order-invariant, if and only if \( f(x) = S(x)^{-1}Uw(y) \), where \( U, w, \) and \( y \) are in Theorem 1.

Another structure of interest here is the diagonal property.

**Definition 4.** We say a function \( f : \mathbb{R}^n \to \mathbb{R}^n \) is diagonal, if \( f(x) = [f_1(x_1), \ldots, f_n(x_n)] \) for \( f_i : \mathbb{R} \to \mathbb{R} \) with \( i \in [n] \).

In the context of calibration, a diagonal calibration function means that different class predictions do not interact with each other in \( f \). Defining diagonal family is mostly motivated by the success of temperature scaling method \( ^{[7]} \), which is a linear diagonal intra order-preserving function. Therefore, although diagonal intra order-preserving functions may sound limiting in learning calibration functions, they still represent a useful class of functions.

The next theorem relates diagonal intra order-preserving functions to increasing functions.

**Theorem 3.** A continuous, intra order-preserving function \( f : \mathbb{R}^n \to \mathbb{R}^n \) is diagonal, if and only if \( f(x) = [f_1(x_1), \ldots, f_n(x_n)] \) for some continuous and increasing function \( f : \mathbb{R} \to \mathbb{R} \).

Compared with general diagonal functions, diagonal intra order-preserving automatically implies that the same function \( f \) is shared across all dimensions. Thus, learning with diagonal intra order-preserving functions benefits from parameter-sharing across different dimensions, which could drastically decrease the number of parameters.

Finally, below we show that functions in this sub-family are also order-invariant and inter order-preserving. Note that inter and intra order-preserving are orthogonal definitions. Inter order-preserving is also an important property for calibration functions, since this property guarantees that \( f_i(x) \) increases with the original class logit \( x_i \). The set diagram in Fig. 2 depicts the relationship among different intra order-preserving families.

**Definition 5.** We say a function \( f : \mathbb{R}^n \to \mathbb{R}^n \) is inter order-preserving if, for any \( x, y \in \mathbb{R}^n \) such that \( x \geq y \), \( f(x) \geq f(y) \), where \( \geq \) denotes elementwise comparison.
we follow the calibration literature [30, 7, 14] and use the negative log likelihood (NLL) loss, i.e.,

\[ \ell(y, \sigma(\mathbf{z})) = -\log(\text{softmax}(\mathbf{z})) \]

with respect to the parameters of \( m \) which only needs \( f \) when we set \( w = f \). To ensure Theorems 1 and 2 describe general representations of intra order-preserving functions through a vector \( \theta \) and set \( w = f \). Use the NLL loss in all the experiments to study the benefit of learning \( \ell \):

\[ \ell(D) = \frac{1}{N} \sum_{i=1}^{N} \ell(y_i, \sigma(\mathbf{z})) + \frac{1}{2} \| \theta \|^2, \]

where \( \ell \) is a positive function such that \( \sigma(a) = 0 \) only when \( a = 0 \), and \( m_i \) is a strictly positive function. It is easy to verify that this parameterization of \( w \) satisfies the requirements on \( w \) stated in Theorem 1. However, we note that this class of functions cannot represent all possible \( w \) stated in Theorem 1. In general, the speed \( w_i(x) \) converges to 0 can be a function of \( x \), but in the proposed factorization above, the rate of convergence to zero is a function of only two elements \( y_i \) and \( y_{i+1} \). Fortunately, such a limitation does not substantially decrease the expressiveness of \( f \) in practice, because the subspace where \( w_i \) vanishes has zero measure in \( \mathbb{R}^n \) (i.e. subspaces where there is at least one tie in \( x \in \mathbb{R}^n \)).

By Theorem 1 and Theorem 2, the proposed architecture in Fig. 2 ensures \( f(x) \) is continuous in \( x \) as long as \( \sigma(y_i - y_{i+1}) \) and \( m_i(x) \) are continuous in \( x \). In the appendix, we show that this is true when \( \sigma \) and \( m_i \) are continuous functions. Additionally, we prove that when \( \sigma \) and \( m \) are continuously differentiable, \( f(x) \) is also directionally differentiable with respect to \( x \). Note that the differentiability to the input is not a requirement to learn the parameters of \( m \) with a first order optimization algorithm which only needs \( f \) to be differentiable with respect to the parameters of \( m \). The latter condition holds in general, since the only potential sources of non-differentiable \( f \), \( S(x)^{-1} \) and \( y \) are constant with respect to the parameters of \( m \). Thus, if \( m \) is differentiable with respect to its parameters, \( f \) is also differentiable with respect to the parameters of \( m \).

3.4 Practical Considerations

Theorems 1 and 2 describe general representations of intra order-preserving functions through a function \( w \) that satisfies certain non-negative constraints. Inspired by these theoretical results, we propose a neural network architecture, Fig. 3 to represent exactly a family of intra order-preserving functions.

The main idea in Fig. 3 is to parameterize \( w \) through a composition of smaller functions. For \( i < n \), we set \( w_i(x) = \sigma(y_i - y_{i+1})m_i(x) \), where \( \sigma : \mathbb{R} \to \mathbb{R} \) is a positive function such that \( \sigma(a) = 0 \) only when \( a = 0 \), and \( m_i \) is a strictly positive function. It is easy to verify that this parameterization of \( w \) satisfies the requirements on \( w \) in Theorem 1. However, we note that this class of functions cannot represent all possible \( w \) stated in Theorem 1. In general, the speed \( w_i(x) \) converges to 0 can be a function of \( x \), but in the proposed factorization above, the rate of convergence to zero is a function of only two elements \( y_i \) and \( y_{i+1} \). Fortunately, such a limitation does not substantially decrease the expressiveness of \( f \) in practice, because the subspace where \( w_i \) vanishes has zero measure in \( \mathbb{R}^n \) (i.e. subspaces where there is at least one tie in \( x \in \mathbb{R}^n \)).

By Theorem 1 and Theorem 2, the proposed architecture in Fig. 2 ensures \( f(x) \) is continuous in \( x \) as long as \( \sigma(y_i - y_{i+1}) \) and \( m_i(x) \) are continuous in \( x \). In the appendix, we show that this is true when \( \sigma \) and \( m_i \) are continuous functions. Additionally, we prove that when \( \sigma \) and \( m \) are continuously differentiable, \( f(x) \) is also directionally differentiable with respect to \( x \). Note that the differentiability to the input is not a requirement to learn the parameters of \( m \) with a first order optimization algorithm which only needs \( f \) to be differentiable with respect to the parameters of \( m \). The latter condition holds in general, since the only potential sources of non-differentiable \( f \), \( S(x)^{-1} \) and \( y \) are constant with respect to the parameters of \( m \). Thus, if \( m \) is differentiable with respect to its parameters, \( f \) is also differentiable with respect to the parameters of \( m \).

4 Implementation

Given a calibration dataset \( D_c = \{(x^i, y^i)\}_{i=1}^{N} \) and a calibration function \( f \) parameterized by some vector \( \theta \), we define the empirical calibration loss as

\[ \ell(y, \sigma(\mathbf{z})) = -\log(\text{softmax}(\mathbf{z})) \]

where \( x^i = g(z^i) \), \( \ell : \mathcal{Y} \times \mathbb{R}^n \to \mathbb{R} \) is a classification cost function, and \( \lambda \geq 0 \) is the regularization weight. Here we follow the calibration literature [30, 7, 14] and use the negative log likelihood (NLL) loss, i.e.,

\[ \ell(y, f(x)) = -\log(\text{softmax}(f(x))) \]

where \( \text{softmax} \) is the softmax operator and \( \text{softmax}_g \) is its \( g \)th element. We use the NLL loss in all the experiments to study the benefit of learning \( f \) with different structures. The study of other loss functions for calibration is outside the scope of this paper.

To ensure \( f \) is within the intra order-preserving family, we restrict \( f \) to have the structure in Theorem 1 and set \( w_i(x) = \sigma(y_i - y_{i+1})m(x) \), as described in Section 3.4. We parameterize function \( m \) by a generic multi-layer neural network and utilize the softplus activation \( s^+(a) = \log(1 + \exp(a)) \).
on the last layer when strict positivity is desired and represent $\sigma$ as $\sigma(a) = |a|$. For example, when $m_i(x)$ is constant, our architecture recovers the temperature scaling scheme [7].

The order-invariant version in Theorem 2 can be constructed similarly. The only difference is that the neural network that parameterizes $m$ receives instead the sorted input. Fig. 3 illustrates the architecture of these models.

The diagonal intra order-preserving version in Theorem 3 is formed by learning an increasing function shared across all logit dimensions. We use the official implementation of proposed architecture in [31] that learns monotonic functions with unconstrained neural networks.

5 Related Work

Many different post-hoc calibration methods have been studied in the literature [27, 7, 14, 16, 15, 17]. Their main difference is in the parametric family of the calibration function. In Platt scaling [27], scale and shift parameters $a, b \in \mathbb{R}$ are used to transform the scalar logit output $x \in \mathbb{R}$ i.e. $f(x) = ax + b$ of a binary classifier. Temperature scaling [7] is a simple extension of Platt scaling for multi-class calibration in which only a single scalar temperature parameter is learned. Dirichlet calibration [14] allows learning within a richer linear functions family $f(x) = Wx + b$, where $W \in \mathbb{R}^{n \times n}$ and $b \in \mathbb{R}^n$ but the learned calibration function may also change the decision boundary of the original model; Kull et al. [14] suggested regularizing the off-diagonal elements of $W$ to avoid overfitting. Similar to our work, the concurrent work in Zhang et al. [39] also give special attention to order preserving transformations for calibration. However, their introduced functions are less expressive than the ones presented in this work. Earlier works like isotonic regression [36], histogram binning [35], and Bayesian binning [36] are also post-hoc calibration methods.

In contrast to post-hoc calibration methods, several researches proposed to modify the training process to learn a calibrated network in the first place. Data augmentation methods [30, 34] overcome overfitting by enriching the training data with new artificially generated pseudo data points and labels. Mixup [38] creates pseudo data points by computing the convex combination of randomly sampled pairs. Cutmix [34] uses a more efficient combination algorithm specifically designed for image classification in which two images are combined by overlaying a randomly cropped part of the first image on the second image. In label smoothing [26, 22], the training loss is augmented to penalize high confidence outputs. To discourage overconfident predictions, [29] modifies the original NNL loss by adding a cross-entropy loss term with respect to the uniform distribution. Similarly, [18] adds a calibration regularization to the NLL loss via kernel mean embedding.

Bayesian neural networks [5, 20] derive the uncertainty of the prediction by making stochastic perturbations of the original model. Notably, [5] uses dropout as approximate Bayesian inference. [20] estimates the posterior distribution over the parameters and uses samples from this distribution for Bayesian model averaging. These methods are computationally inefficient since they typically feed each sample to the network multiple times.

6 Experiments

We evaluate the performance of intra order-preserving (OP), order-invariant intra order-preserving (OI), and diagonal intra order-preserving (DIAG) families in calibrating the output of various im-
Table 1: ECE (with $M = 15$ bins) on various image classification datasets and models with different calibration methods. The subscript numbers represent the rank of the corresponding method on the given model/dataset. The accuracy of the uncalibrated model is shown in parentheses. The number in parentheses in DIR, MS, and UNCONSTRAINED methods show the change in accuracy for each method.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>Uncal</th>
<th>TS</th>
<th>DIR</th>
<th>MS</th>
<th>DIA</th>
<th>OI</th>
<th>OP</th>
<th>UNCONSTRAINED</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFAR10</td>
<td>ResNet 110</td>
<td>0.0451 (0.936%)</td>
<td>0.0113</td>
<td>0.0108 (0.13%)</td>
<td>0.0106 (0.18%)</td>
<td>0.0062 (0.061%)</td>
<td>0.0170 (0.04%)</td>
<td>0.0192 (0.04%)</td>
<td></td>
</tr>
<tr>
<td>CIFAR10</td>
<td>Wide ResNet 32</td>
<td>0.0341 (0.957%)</td>
<td>0.0078</td>
<td>0.0086 (0.35%)</td>
<td>0.0074 (0.35%)</td>
<td>0.0165 (0.064%)</td>
<td>0.0075 (0.07%)</td>
<td>0.0087 (0.01%)</td>
<td></td>
</tr>
<tr>
<td>CIFAR10</td>
<td>DenseNet 40</td>
<td>0.0560 (0.924%)</td>
<td>0.0095</td>
<td>0.0110 (0.15%)</td>
<td>0.0099 (0.17%)</td>
<td>0.0069</td>
<td>0.0116</td>
<td>0.0128</td>
<td>0.0125 (0.05%)</td>
</tr>
<tr>
<td>SVHN</td>
<td>ResNet 152 (SU)</td>
<td>0.0086 (0.981%)</td>
<td>0.0061</td>
<td>0.0086 (0.95%)</td>
<td>0.0060 (0.98%)</td>
<td>0.0057</td>
<td>0.0116</td>
<td>0.0118</td>
<td>0.0016 (0.03%)</td>
</tr>
<tr>
<td>SVHN</td>
<td>ResNet 152 (SU)</td>
<td>0.0184 (0.916%)</td>
<td>0.0126</td>
<td>0.0282 (0.32%)</td>
<td>0.0142 (0.18%)</td>
<td>0.0105</td>
<td>0.0111</td>
<td>0.0120</td>
<td>0.0114 (0.04%)</td>
</tr>
<tr>
<td>CIFAR100</td>
<td>ResNet 110</td>
<td>0.1878 (0.838%)</td>
<td>0.0147</td>
<td>0.0186 (0.15%)</td>
<td>0.0258 (0.28%)</td>
<td>0.0172</td>
<td>0.0126</td>
<td>0.0174</td>
<td>0.0421 (0.61%)</td>
</tr>
<tr>
<td>CIFAR100</td>
<td>DenseNet 40</td>
<td>0.2161 (0.707%)</td>
<td>0.0098</td>
<td>0.0111 (0.15%)</td>
<td>0.0220 (0.48%)</td>
<td>0.0075</td>
<td>0.0098</td>
<td>0.0154</td>
<td>0.0099 (0.12%)</td>
</tr>
<tr>
<td>CARS</td>
<td>ResNet 101 (pre)</td>
<td>0.0692 (0.935%)</td>
<td>0.0447</td>
<td>0.0464 (0.16%)</td>
<td>0.0396 (0.56%)</td>
<td>0.0101</td>
<td>0.0240</td>
<td>0.0193</td>
<td>0.0052 (0.47%)</td>
</tr>
<tr>
<td>CARS</td>
<td>ResNet 101</td>
<td>0.0321 (0.852%)</td>
<td>0.0321</td>
<td>0.0245 (0.35%)</td>
<td>0.0345 (1.17%)</td>
<td>0.0206</td>
<td>0.0225</td>
<td>0.0236</td>
<td>0.0786 (3.76%)</td>
</tr>
<tr>
<td>BIRDS</td>
<td>ResNet 50 (pre)</td>
<td>0.1443 (0.935%)</td>
<td>0.0431</td>
<td>0.0436 (0.16%)</td>
<td>0.0387 (1.16%)</td>
<td>0.0192</td>
<td>0.0174</td>
<td>0.0204</td>
<td>0.0206 (4.21%)</td>
</tr>
<tr>
<td>ImageNet</td>
<td>ResNet 152</td>
<td>0.0065 (76.2%)</td>
<td>0.0288</td>
<td>0.0342 (1.01%)</td>
<td>0.0567 (1.18%)</td>
<td>0.0087</td>
<td>0.0092</td>
<td>0.0143</td>
<td>0.1297 (93.47%)</td>
</tr>
<tr>
<td>ImageNet</td>
<td>DenseNet 161</td>
<td>0.0572 (77.1%)</td>
<td>0.0198</td>
<td>0.0376 (1.05%)</td>
<td>0.0443 (1.47%)</td>
<td>0.0101</td>
<td>0.0123</td>
<td>0.0168</td>
<td>0.1180 (6.17%)</td>
</tr>
<tr>
<td>ImageNet</td>
<td>ResNet 50 (large)</td>
<td>0.0610 (83.1%)</td>
<td>0.0713</td>
<td>0.0389 (0.60%)</td>
<td>0.0217 (0.35%)</td>
<td>0.0117</td>
<td>0.0084</td>
<td>0.0130</td>
<td>0.0016 (4.85%)</td>
</tr>
</tbody>
</table>

Average Relative Error 1.00% 0.42% 0.4% 0.50% 0.27% 0.33% 0.41% 0.66%

Baseline. We compare the proposed function structures with temperature scaling (TS) [7], Dirichlet calibration with off-diagonal regularization (DIR) [14], and matrix scaling with off-diagonal regularization (MS) [14] as they are the current best performing post-hoc calibration methods. We also present the results of the original uncalibrated models (Uncal.) for comparison. To show the effect of intra order-preserving regularization, we also show the results of applying unconstrained multi-layer neural network without intra order-preserving constraint (UNCONSTRAINED). In cross-validation, we tune the architecture as well as regularization weight of UNCONSTRAINED and order-preserving functions. As we are using the same logit as [14], we report their results directly on CIFAR-10, CIFAR-100, and SVHN. However, since they do not present the results for CARS, BIRDS, and ImageNet datasets, we report their results of their official implementation on these datasets.

Results. Table 1 summarizes the results of our calibration methods and other baselines in terms of ECE and presents the average relative error with respect to the uncalibrated model. Overall, DIAG has the lowest average relative error followed by OI among the models and datasets presented in Table 1. OI is the best-performing method in 7 out of 14 experiments including ResNet 110 and Wide ResNet 32 models on CIFAR datasets as well as state-of-the-art PNASNet5 large model. DIAG family’s relative average error is half the MS and DIR methods and 15% less compared to Temp. Scaling. Although DIR and MS were able to maintain the accuracy of the original models in most of the cases by imposing off diagonal regularization, order-preserving family could significantly outperform them regarding the ECE metric. Finally, we remark that learning an unconstrained multi-layer neural network does not exhibit a good calibration performance and drastically hurts the accuracy in some datasets as shown in the last column of Table 1.

Fig. 4 illustrates the reliability diagrams of models trained on ResNet 152 (top row) and PNASNet5 large (bottom row). Weighted reliability diagrams are also presented to better indicate the differences regarding the ECE metric. Surprisingly, these diagrams show that the uncalibrated PNASNet5 large model is underconfident. The differences between the mappings learned by DIAG and temperature scaling on these models are illustrated on the right column. DIAG is capable of learning complex increasing functions while temperature scaling only scales all the logits. Compared with DIR and MS which learn a linear transformation, all intra order-preserving methods can learn non-linear transformations on the logits while decoupling accuracy from calibration of the predictions.

https://github.com/dirichletcal/experiments_dnn
Figure 4: Performance evaluations of ResNet 152 (Top Row) and PNASNet5 large (Bottom Row) on ImageNet dataset. (Left) Reliability diagrams. As suggested by [20] we show the difference between the estimated confidence and accuracy over $M = 15$ bins. The dashed grey lines represent the perfectly calibrated network at $y = 0$. Points above (below) the grey line show overconfident (underconfident) predictions in a bin. (Middle) Weighted reliability diagrams where bin values are weighted by data frequency distribution. Since the uncalibrated network has different distances to the perfect calibration in different bins, scaling by a single temperature will lead to a mix of underconfident and overconfident regions. Our order-preserving functions, on the other hand, have more flexibility to reduce the calibration error. (Right) Transformation learned by DIAG function compared to temperature scaling and uncalibrated model (identity map).

In addition to ECE, which considers the top prediction, we also measure the NLL, Marginal Calibration Error [17], Classwise-ECE, and Brier score. As it is shown in Table 2, DIAG and OI have the best overall performance in terms of average relative error in most cases, while DIR is the top performing method in Classwise-ECE. Refer to the Appendix for discussions and the performance comparisons over all the datasets.

Table 2: Average relative error. Each entry shows the relative error compared to the uncalibrated model averaged over all the datasets. The subscripts represent the rank of the corresponding method on the given metric. See the Appendix for per dataset performance comparisons.

<table>
<thead>
<tr>
<th>Evaluation Metric</th>
<th>Uncal.</th>
<th>TS</th>
<th>DIR</th>
<th>MS</th>
<th>DIAG</th>
<th>OI</th>
<th>OP</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECE [17]</td>
<td>1.000†</td>
<td>0.420§</td>
<td>0.496§</td>
<td>0.508§</td>
<td>0.270†</td>
<td>0.343‡</td>
<td>0.410†</td>
</tr>
<tr>
<td>Debias ECE [17]</td>
<td>1.000†</td>
<td>0.357§</td>
<td>0.430§</td>
<td>0.409§</td>
<td>0.213†</td>
<td>0.248‡</td>
<td>0.396§</td>
</tr>
<tr>
<td>NLL</td>
<td>1.000†</td>
<td>0.766§</td>
<td>0.772§</td>
<td>0.768§</td>
<td>0.749†</td>
<td>0.751‡</td>
<td>0.765§</td>
</tr>
<tr>
<td>Marginal Calibration Error [17]</td>
<td>1.000†</td>
<td>0.750§</td>
<td>0.735§</td>
<td>0.996§</td>
<td>0.725†</td>
<td>0.778‡</td>
<td>0.898§</td>
</tr>
<tr>
<td>Classwise-ECE</td>
<td>1.000†</td>
<td>0.752§</td>
<td>0.704‡</td>
<td>0.734‡</td>
<td>0.729†</td>
<td>0.740‡</td>
<td>0.743§</td>
</tr>
<tr>
<td>Brier</td>
<td>1.000†</td>
<td>0.936‡</td>
<td>0.930§</td>
<td>0.936‡</td>
<td>0.924†</td>
<td>0.929‡</td>
<td>0.931‡</td>
</tr>
</tbody>
</table>

7 Conclusion

In this work, we introduce the family of intra order-preserving functions which retain the top-$k$ predictions of any deep network when used as the post-hoc calibration function. We propose a new neural network architecture to represent these functions, and new regularization techniques based on order-invariant and diagonal structures. In short, calibrating neural network with this new family of functions generalizes many existing calibration techniques, with additional flexibility to express the post-hoc calibration function. The experimental results show the importance of learning within the intra order-preserving family as well as support the effectiveness of the proposed regularization in calibrating multiple classifiers on various datasets.

We believe the applications of intra order-preserving family are not limited to network calibration. Other promising domains include, e.g., data compression, depth perception system calibration, and tone-mapping in images where tone-maps need to be monotonic. Exploring the applicability of intra order-preserving functions in other applications is an interesting future direction.
Broader Impact

Predicting calibrated confidence scores for multi-class deep networks is important for avoiding rare but costly mistakes. Trusting the network’s output naively as confidence scores in system design could cause undesired consequences: a serious issue for applications where mistakes are costly, such as medical diagnosis, autonomous driving, suspicious events detection, or stock-market. As an example, in medical diagnosis, it is vital to estimate the chance of a patient being recovered by a certain operation given her/his condition. If the estimation is overconfident/underconfident this will put the life of the patient at risk. Confidence calibrated models would enable integration into downstream decision-making systems, allow machine learning interpretability, and help gain the user trust. While this work focuses primarily on some of the theoretical aspects of the neural network calibration, it also proposes novel techniques to potentially improve broader set of applications where preserving the rank of set of inputs is desired e.g. tone-mapping in images where tone-maps need to be monotonic, depth perception system calibration, and data compression.

We need to remark that our research shows that methods perform differently under various calibration metrics. Unfortunately, discrepancy between different calibration metrics is not well understood and fully explored in the literature. We believe more insights into these inconsistencies would be valuable to the field. We report the performance under different calibration metrics to highlight these differences for the future research. This also means that integrating the proposed work or any other calibration method into decision making systems requires application specific considerations. Other than that, since this work is mostly on the theoretical aspect of improving calibration, we do not foresee any direct negative impacts.

Acknowledgments and Disclosure of Funding

We would like to thank Antoine Wehenkel for providing helpful instructions for his unconstrained monotonic networks. This research is supported in part by the Australia Research Council Centre of Excellence for Robotics Vision (CE140100016).

References


[34] Sangdoo Yun, Dongyoon Han, Seong Joon Oh, Sanghyuk Chun, Junsuk Choe, and Youngjoon Yoo. Cutmix: Regularization strategy to train strong classifiers with localizable features. In ICCV, pages 6023–6032, 2019.


