

Efficacy of Bayesian Neural Networks in Active Learning

Vineeth Rakesh
Interdigital AI Lab
USA

vineethrakesh@gmail.com

Swayambhoo Jain
Interdigital AI Lab
USA

swayambhoo.jain@gmail.com

Abstract

Obtaining labeled data for machine learning tasks can be prohibitively expensive. Active learning mitigates this issue by exploring the unlabeled data space and prioritizing the selection of data that can best improve the model performance. A common approach to active learning is to pick a small sample of data for which the model is most uncertain. In this paper, we explore the efficacy of Bayesian neural networks for active learning, which naturally models uncertainty by learning distribution over the weights of neural networks. By performing a comprehensive set of experiments, we show that Bayesian neural networks are more efficient than ensemble based techniques in capturing uncertainty. Our findings also reveal some key drawbacks of the ensemble techniques, which was recently shown to be more effective than Monte Carlo dropouts.

1. Introduction

Although machine learning techniques have achieved a major breakthrough in recent years, their performance comes at a cost of acquiring large volumes of training data. This is especially true for supervised deep learning models that demand a substantial amount of labeled data to achieve a reasonable performance. For applications that require expert knowledge such as medical and biological images, labels are extremely hard and expensive to obtain. Active learning (AL) aims to mitigate this problem by smartly selecting data points to label (from an expert) from a large pool of unlabeled data to improve model performance. This sampling is typically based on some *acquisition function* (AF) which provides a score for each unlabeled data that signifies its level of importance. While there are many approaches to implementing AF [1, 2], uncertainty-based based approaches are shown to be the most effective [3, 4, 5, 6].

Bayesian neural network (BNN) naturally models uncertainty by learning a probability distribution over the neural network weights. Therefore, for a given input, as we take

multiple realizations of the network, the variance captured by the weights is reflected as the variation in the output, which in-turn models uncertainty. BNNs learn by applying a prior distribution over weights and performing variational inference to approximate the posterior distribution. In [7], the authors proved that applying dropout to neural networks is equivalent to a BNN. This theory was further leveraged by proposing Monte Carlo Dropout (MCD) for uncertainty estimation in AL [5]. In a recent work, [6] showed that ensemble of neural networks (EN) outperform MCD when it comes to uncertainty estimation; thus, proving to be the choice for active learning. Consequentially, it is natural to assume EN to perform better than BNN since MCD is equivalent to BNN. *However, dropout neural networks form a special class of BNN where the posterior distribution is a special case of spike-and-slab distribution. Contrary to this, BNNs allow for a broader class of prior and posterior distributions on weights.*

In this paper, we re-establish the efficacy of BNNs in active learning over ensembles and MCD by using a more general scaled normal prior based BNN proposed in [8]. The scaled normal prior is a continuous relaxation of the *spike-and-slab* distribution and subsumes Dropout as a special case. Through extensive experiments on multiple datasets namely, MNIST, Fashion MNIST, CIFAR10 and CIFAR100 and a regression dataset on housing price prediction we show that the scaled normal prior based BNN provides more robust and efficient active learning over EN and MCD. We perform several experiments to demonstrate the pros and cons of BNN over EN and MCD. For each round of active learning, the models are trained using two different settings: (1) re-use the trained state of the model from previous round and retrain on the newly appended datapoints (termed as *continual training*) and (2) reset the model parameters and retrain from scratch. Our results show that BNN performs significantly better than EN in terms of classification accuracy when it comes to continual training. In fact, the performance of EN is worse than MCD which can be attributed to overfitting and catastrophic forgetting. That being said, when retrained from scratch, BNN and EN per-

form on a similar level, which is still an advantage for BNN since estimating uncertainty using ensembles is a costly process. We found that EN requires about five ensembles in order to achieve good active learning performance. This implies, training of five different i.i.d networks and storing the trained state of every single network instance. BNN on other hand, achieves similar yet a more robust performance with a trade-off of just doubling parameter size of conventional neural network.

Besides illustrating the overall effectiveness of BNN for active learning, we answer the following questions: (1) do acquisition functions behave the same for Bayesian, ensemble and MC dropouts? (2) how does model capacity affect the outcome, do BNNs with lower model capacity perform worse than EN (or MCD)? (3) are BNNs better than EN when predicting challenging class labels? Inspired by the performance of BNNs, we also propose a computationally efficient uncertainty estimation method for fully connected dense layers with ReLU non-linearity. Since AL involves repeated uncertainty estimation over large unlabeled dataset, efficient uncertainty estimation is of huge practical importance. In the proposed method, instead of taking multiple instantiations of neural networks to estimate the uncertainty, we perform just one forward pass. In this forward pass, at each neuron, we approximate the probability distribution parametrically. We show that this algorithm is capable of achieving performances that is on-par with the traditional uncertainty estimation in BNN.

To the best of our knowledge, we are the first to perform comprehensive empirical analysis to demonstrate the efficacy of BNNs for active learning. While most existing research limit themselves to experiments on small architectures and dataset, ours does not have such constraints.

2. Related Work

Active learning has been explored extensively in classical machine learning literature [9]. Much of the focus of classical literature has been on the high dimensional data arising in the context of linear models such as support vector machine [10, 11, 12]. That being said, recently, there has been a significant interest in AL for deep neural networks (DNNs). While there are many ways to perform AL in DNNs, uncertainty-based sampling techniques are the preferred choice due to their ease of implementation and computational efficiency. Uncertainty in the output of neural networks can be estimated using (a) Bayesian neural networks or (b) ensemble of neural networks.

A popular technique for AL using BNNs is called Monte Carlo dropout which was first proposed in [5]. The basic idea is to pass the new unlabeled data through the DNNs multiple times while retaining the dropout layer. This results in different realizations at the output of the DNNs. These realizations can be used to estimate the uncertainty in

output using various measures such as entropy or the variance ratio. The estimated uncertainty can then be utilized for acquiring new unlabeled data points thus performing active learning.

On the other hand, ensemble based uncertainty estimation involves having an ensemble of neural networks which typically have same architecture but trained with different random initialization [4]. Uncertainty is estimated by passing unlabeled examples through individual ensembles and their outputs are then used to estimate the uncertainty. It was shown in [6] that ensemble methods outperforms the Monte Carlo dropout-based estimation. This performance is primarily attributed to the higher capacity and diversity in the ensemble models as compared to different realizations of neural networks in dropout based networks. While there are some studies that leverage BNNs for active learning [4, 13, 14, 15], they have a few or all of the following shortcomings: (1) experiments are restricted to simple architectures with a few dense or convolutional neural network (CNN) layers (2) evaluation is restricted to basic datasets such as MNIST (3) no comparison of BNNs with ensemble models (4) claim to use BNNs, but actually use Monte Carlo dropouts as approximation to BNNs.

3. Active Learning Via Bayesian Neural Networks

Bayesian neural network: For a given dataset $\mathcal{D} = \{(\mathbf{x}_i, \mathbf{y}_i)\}_{i=1}^D$, Bayesian neural networks involves calculation of the distribution of weights given the training data $p(\mathbf{w}|\mathcal{D})$. The predictive distribution for a test data \mathbf{x} can be obtained by marginalizing \mathbf{w} as follows: $p(\mathbf{y}|\mathbf{x}, \mathcal{D}) = \int p(\mathbf{y}|\mathbf{x}, \mathbf{w})p(\mathbf{w}|\mathcal{D})d\mathbf{w}$. This is equivalent to *averaging predictions from an ensemble of neural networks* weighted by the posterior probabilities of their parameters \mathbf{w} . However, exact computation of the posterior is intractable, therefore, we resort to variational inference. That is, we wish to approximate $p(\mathbf{w}|\mathcal{D}) = p(\mathcal{D}|\mathbf{w})p(\mathbf{w})/p(\mathcal{D})$ by positing an approximate posterior $q_\phi(\mathbf{w})$ of variational parameters ϕ . The problem then reduces to optimizing the evidence-lower-bound (ELBO) defined as follows:

$$\mathcal{L}(\phi) = \underbrace{\mathbb{E}_{q_\phi(\mathbf{w})}[\log p(\mathcal{D}|\mathbf{w})]}_{(a)} + \underbrace{\text{KL}[q_\phi(\mathbf{w})||p(\mathbf{w})]}_{(b)} \quad (1)$$

where term (a) is the data-dependent likelihood term, and (b) is the regularizer that measures the KL divergence between the posterior and prior. For prior we use the scaled normal prior proposed in [8] in which the scales z follow a log-uniform prior: $p(z) \propto |z|^{-1}$. For a given layer weight matrix $\mathbf{W} \in \mathbf{R}^{m \times n}$ for a fully connected layer of neural network with input dimension n and output dimension m

the scales of shared across input dimension as

$$p(\mathbf{W}, \mathbf{z}) \propto \prod_{j=1}^n \frac{1}{|z_j|} \prod_{i,j}^{m,n} \mathcal{N}(w_{ij}|0, z_j^2). \quad (2)$$

The main rationale behind scaled normal prior is that it is continuous relaxation of the *spike-and-slab* distribution. Dropout which is the basis of MCD based active learning is a special case of *spike-and-slab* distribution [8] and we hope to get better performance with the scaled normal prior. We consider the following joint approximate posterior

$$q_\phi(\mathbf{W}, \mathbf{z}) = \prod_j^n \mathcal{N}(z_j|\mu_{z_j}, \sigma_{z_j}^2) \prod_{i,j}^{m,n} \mathcal{N}(w_{ij}|z_j\mu_{ij}, z_j^2\sigma_{ij}^2), \quad (3)$$

and the corresponding ELBO is given by:

$$\mathcal{L}(\phi) = \mathbb{E}_{q_\phi(\mathbf{z})} q_\phi(\mathbf{W}|\mathbf{z}) [\log p(\mathcal{D}|\mathbf{W})] - \mathbb{E}_{q_\phi(\mathbf{z})} [\text{KL}(q_\phi(\mathbf{W}|\mathbf{z})||p(\mathbf{W}|\mathbf{z})) - \text{KL}(q_\phi(\mathbf{z})||p(\mathbf{z}))]. \quad (4)$$

The KL divergences can be replaced with the closed form expressions

$$\text{KL}(q_\phi(\mathbf{W}|\mathbf{z})||p(\mathbf{W}|\mathbf{z})) = \frac{1}{2} \sum_{i,j}^{m,n} \log \frac{e^{\sigma_{ij}^2 + \mu_{ij}^2 - 1}}{\sigma_{ij}^2},$$

$$\text{KL}(q_\phi(z)||p(z)) \approx \sum_j^n k_1 \left(1 - \gamma(k_2 - k_3 \alpha_j) - \frac{m(\alpha_j)}{2k_1} \right),$$

where $\alpha_j = -\log(\sigma_{z_j}^2/\mu_{z_j}^2)$, $\gamma(\cdot)$ and $m(\cdot)$ are the sigmoid and soft-plus functions respectively and the constants $k_1 = 0.63576$, $k_2 = 1.87320$, $k_3 = 1.48695$ [16].

From practical implementation point-of-view this scaled normal prior BNN is easier to implement as compared to other prior. By virtue of the closed form KL-divergences the ELBO in (4) can be optimized within the framework of standard stochastic gradient ascent. In addition to this, during test time it can implemented as a single feedforward pass where we replace \mathbf{W} at layer with its mean $\tilde{\mathbf{W}} = \mathbf{M}_W \text{diag}(\mu_z)$ where \mathbf{M}_W is the matrix of means μ_{ij} and μ_z is the vector of means μ_{z_j} .

Acquisition functions: Once the model is trained on a small dataset, we use acquisition functions (AF) to fetch the most uncertain datapoints. In a recent work [6], the authors experimented with several acquisition functions and found entropy [17] and variation-ratio to be the best candidates [18]. Therefore, we use these two metrics as our choice of AF. A BNN trained for multi-class classification problem of C classes maps a given data vector \mathbf{x} to a C dimensional vector containing the probability of various classes in its components. For a given unlabelled data vector \mathbf{x} the entropy is calculated by T forward passes, each time with new

weight realization \mathbf{W}_t from the trained posterior. First, the T outputs vectors are averaged to obtain the probability for a given class c as $\hat{p}(y = c|\mathbf{x}) = 1/T \sum_t p(y = c|\mathbf{x}, \mathbf{W}_t)$ where \mathbf{W}_t is the t^{th} realization of weights obtained from the trained posterior. Next, with these probability estimates the entropy can be calculated as follows:

$$H(y|\mathbf{x}) = - \sum_c \hat{p}(y = c|\mathbf{x}) \log(\hat{p}(y = c|\mathbf{x})). \quad (5)$$

The variation ratio can be calculated as $v = 1 - f_m/T$ where f_m is the number of predictions falling into the modal class category.

Active learning algorithm: With the Bayesian neural networks and acquisition functions defined, we now describe our active learning methodology in Algorithm 1. The procedure starts by training the model with some seed sample \mathcal{S} (line 11). The size of this sample could be anywhere between 2-5 percent of the training set (depending on the complexity of data), we call this step as *seed training*. At each round $r \in R$, we add k new samples by calling the active learning functions (line 13). The function first removes the chosen sample \mathcal{S} from the main dataset \mathcal{D} and creates T instances of networks by sampling weights that was learned during the training phase. Each instance is tested on unseen data points to obtain ensemble of outputs (lines 4-7). Depending on the type of AF (i.e., variation-ratio or entropy), the uncertainty over ensembles is calculated and the new data-points are chosen based on the largest uncertainty score. Once the model is trained on newly appended data points, the algorithm proceeds by validating on the held-out training dataset \mathcal{D}_v (line 16). Note that it is not necessary to use the validation data \mathcal{D}_v and it is entirely optional. We assumed that even in active learning setting, we can afford using a very small percentage of unseen data for validation. In the subsequent rounds, the best weights from the previous round are loaded (i.e., based on the validation set) and the algorithm resumes performing AL and re-training. Unlike [6], after each round we *do not retrain the model from scratch*. In our experiments, we found that retraining from scratch does not perform as well as re-using weights from previous rounds and re-training.

Accelerating uncertainty estimation: As discussed earlier while the scaled normal prior BNN allows inference in a single feedforward pass but for the uncertainty estimation passing it still requires a given unlabelled example passed through multiple realization weights using the trained posterior. This is computationally expensive and we alleviate this by approximating the probability distribution of the input to the last layer directly. Equipped with this distribution we propose to directly generate the random realizations of the input before last layer non-linearity and use those to estimate the uncertainty.

For the scaled normal posterior in (3) the analytical ex-

pression for the distribution is challenging due to the non-linear transformations in the neural network and dependencies due to structure of layers such as convolution layers. To illustrate this, consider a simple linear transformation of \mathbf{x} by matrix $\mathbf{W} \in \mathbb{R}^{m \times n}$, bias vector $\mathbf{b} \in \mathbb{R}^m$ given by $\mathbf{y} = \mathbf{W}\mathbf{x} + \mathbf{b}$ where \mathbf{W} follows the posterior in (3). Each entry of \mathbf{y} is a sum of n independent random variables with scaled normal distribution as $y_i = \sum_{j=1}^n W_{ij}x_j + b_i$. Considering the fact that a typical neural network has multiple layers and non-linearities, the calculation of analytical distribution is non-trivial. However, under the assumption that y_i is Gaussian, the mean and variance of y_i after passing through ReLU non-linearity is analytically tractable. Based on this, for a multi-layer neural network comprising of L dense layers we can obtain the distribution of components vectors before the non-linearity from the distribution of layer input. Suppose weights of l^{th} layer are represented by $\mathbf{W}^l \in \mathbb{R}^{n^l \times n^{l+1}}$ where n^{l+1}, n^l are the input and output dimension of this layer. Then the expectation and variance of components of the vector $\mathbf{y}^l = \mathbf{W}^l \mathbf{x}^{l-1} + \mathbf{b}^l$ can be obtained terms of first and second order moments of components of \mathbf{x}^{l-1} as follows

$$\mathbb{E}[y_i^l] = \sum_{j=1}^{n^l} \mathbb{E}[w_{ij}^l] \mathbb{E}[x_j^{l-1}] + b_i^l, \quad (6)$$

$$\begin{aligned} \mathbb{V}[y_i^l] &= \sum_{j=1}^{n^l} \mathbb{E}[(w_{ij}^l)^2] \mathbb{E}[(x_j^{l-1})^2] \\ &\quad - \mathbb{E}[x_j^{l-1}]^2 \mathbb{E}[w_{ij}^l]^2, \end{aligned} \quad (7)$$

where $\mathbb{E}[w_{ij}^l]^2 = (\sigma_{z_j}^2 + \mu_{z_j}^2)(\sigma_{i_j}^2 + \mu_{i_j}^2)$. Further, the input to next layer is obtained passing \mathbf{y}^l through a ReLU non-linearity as $\mathbf{x}^l = \text{ReLU}(\mathbf{y}^l)$. We assume that non-linearity until the last layer is ReLU. Finally, assuming that components of \mathbf{y}^l are Gaussian with mean and variance computed as above, the mean and variance of components of \mathbf{x}^l are given below

$$\mathbb{E}[x_i^l] = \mathbb{E}[y_i^l] \Phi(\delta_i^l) + \mathbb{V}[y_i^l] f(-\delta_i^l), \quad (8)$$

$$\begin{aligned} \mathbb{E}[(x_i^l)^2] &= \left(\mathbb{E}[y_i^l]^2 + \mathbb{V}[y_i^l] \right) \Phi(\delta_i^l) \\ &\quad + \sqrt{\mathbb{E}[y_i^l]^2 \mathbb{V}[y_i^l]} f(\delta_i^l) \end{aligned} \quad (9)$$

where $\delta_i^l = \mathbb{E}[y_i^l] / \sqrt{\mathbb{V}[y_i^l]}$, Φ and f are c.d.f. and p.d.f. of standard Gaussian distribution. Using above equations (6) to (9) the mean and variance at the input before non-linearity of each layer can be computed iteratively till the last layer \mathbf{y}^L . Equipped with this information the uncertainty can then be computed by directly generating \mathbf{y}^L and then passing them through the last layer's non-linearity.

Algorithm 1: Uncertainty-based smart data sampling

```

1 Inputs: Training dataset  $\mathcal{D}$ , validation dataset  $\mathcal{D}_v$ , test dataset  $\mathcal{D}_t$ , seed
   dataset  $\mathcal{S}$ , model  $\mathcal{M}$ , number of epochs  $E$ , mini batch size  $b$ , number of
   rounds  $R$ , acquisition size  $k$ , number of instances  $T$ .
2 ActiveSubSelectData (typ)
3    $\mathcal{D} \leftarrow \mathcal{D} - \mathcal{S}$ 
4    $ENO \leftarrow []$  (array to hold ensemble outputs)
5   for  $j \in T$  do
6      $\mathcal{M}_s \sim \mathcal{M}(\mathbf{w})$  (sample from a weight instance)
7      $ENO \leftarrow$  append the model output  $\mathcal{M}_s(\mathcal{D})$ 
8    $new \leftarrow$  get uncertainty of  $ENO$  with eq(5) if typ is "Entropy" else
     use variation-ratio  $v$ 
9    $new \leftarrow$  sort  $new$  and get top- $k$  datapoints with the most
     uncertainty
10   $\mathcal{S} \leftarrow \mathcal{S} \cup new$ 
11 Train( $\mathcal{M}$ ) with seed sample
12 for each  $r \in R$  do
13   ActiveSubSelectData("Entropy/Variation-Ratio")
14   for each  $e \in E$  do
15     Train( $\mathcal{M}$ ) on  $\mathcal{S}$ 
16      $v_{loss} \leftarrow$  Evaluate( $\mathcal{M}$ ) on  $\mathcal{D}_v$  and get validation loss
17     if EarlyStoppingCriteria( $v_{loss}$ ): break
18    $\mathcal{M} \leftarrow$  Load best weights based on  $\mathcal{D}_v$  (if continual training)
19 Test( $\mathcal{M}$ ) on  $\mathcal{D}_t$ 

```

4. Experiments

Starting from simple multi-layer perceptrons to deep CNN models we perform several experiments to understand the effectiveness and shortcomings of BNNs over EN and MCD. Our objective is to analyze BNNs from the following perspective: (1) overall efficiency in acquisition of new data points (2) robustness of BNNs during minimal retraining (i.e., retraining by reusing the trained model from previous round) and (3) impact of model capacity, and ensemble size. In addition to this, we also show the outcome of the proposed accelerated uncertainty estimation over dense neural networks.

Dataset and models: The experiments are performed on four image classification datasets and one regression dataset. For classification, we chose MNIST, Fashion MNIST (FMNIST) [19], CIFAR10 and CIFAR100 [20]. For regression, we chose the housing price prediction dataset introduced by [21]. It consists of 535 unique houses sampled from the state of California. Each house is represented by both visual and textual data with the visual features representing the front side of the house, the kitchen, the bedroom and the bathroom. The following neural network architectures are used in this paper (for detailed description please refer Appendix 6.1). (a) *LeNetD2*: a simple densely connected network with 300 and 100 neurons in the first and second layer respectively, (b) *LeNet5* [22]: consists of 2 CNN layers followed by a classifier network with three dense layers, (c) *AlexNet Light (ANL)*: this is simplified version of the Alexnet architecture that is similar to the K-CNN used in [6]. It has 4 CNN layers followed by two dense layers, (d) *VGG*: there are several variations of VGG.

For our experiments, we use VGG19 [23] with 16 CNN layers followed by the classifier network, and (e) *Densenet*: we use Densenet121 [24] with a growth rate of 32. The Bayesian versions of these models were implemented from scratch. At the time of writing, there are no standardized module for Pytorch¹ that can seamlessly convert a conventional neural network to its Bayesian counterpart. The complete active learning library consisting of all the models and experiments performed in this paper will be publicly hosted via Github².

Active learning setting: Our training procedure was explained in Algorithm 1. Depending on the model complexity and the dataset, the number of rounds R is set anywhere between 40 to 80. The number of data-points added during each round (i.e., k) varies from 5 to 250. The number of neural network instances (NNI) to compute uncertainty (i.e., the variable T) is set as 15 for Densenet and 25 for all other neural networks. For BNN, the instances are created by sampling from the posterior distribution of weights and for MCD, the dropouts are activated during the active learning phase (but turned off during testing phase). Similar to [6], for EN, the number of NNI are set as 5 and the weights are initialized using the default Pytorch setting, which follows Kaiming uniform distribution. The details of neural network architecture, dataset, epochs, acquisition size, etc., are summarized in Table 1. Experiments are performed by either reusing the state of the model from previous round and retraining, termed as *continual training* (CT) or completely resetting the model and *retraining from scratch* (RFS). In CT, in each new round, models are trained for a significantly lower number of epoch, typically around 30-50, depending on the type of model and dataset. On the contrary, in RFS the number of epochs range anywhere between 100-200, which makes the training time much greater than CT.

Evaluation metrics: For classification task, the following metrics are used (1) *Top-1 Accuracy*: is the ratio between the number of correct predictions and the total number of predictions. We take the class that corresponds to the highest probability (i.e., from the softmax layer) as the predicted label, (2) *Pr*: precision is the fraction of true positives among the retrieved instances, and (3) *F1*: F1 is the harmonic mean of the precision and recall, where recall is defined as the fraction of the total relevant instances (i.e., both true positives and true negatives) that were retrieved.

Aside from the aforementioned performance metrics, it is also important to know the calibration of our models since a high accuracy does not imply good calibration and vice versa [25]. Therefore, for classification tasks, we use *expected calibration error* (ECE) [26] as the metric of choice. ECE approximates the level of calibration by parti-

Dataset	Model	Epoch(CT/RFS)	#Rnd	Aq Size
F/MNIST	LenetD2	30/100	40	1K/100/4K
F/MNIST	Lenet5	30/100	40	100/100/4K
CIFAR10	VGG16	50/200	80	1K/250/20K
CIFAR100	VGG16	50/200	80	1K/250/20K
Housing	LenetD2	50	40	50/5/200

Table 1: Settings of active learning experiments for various datasets. The acquisition size (*Aq Size*) is the number of new data-points added in each round and *#Rnd* is the number of rounds. *Aq Size* is divided into 3 parts (separated by /), where the first indicates seed sample size, the second is the # datapoints added in each round and the third is the total acquisition size across all rounds.

tioning predictions into M equally-spaced bins and taking a weighted average of the bin’s accuracy/confidence difference. More precisely,

$$ECE = \sum_{m=1}^M \frac{|B_m|}{n} |acc(B_m) - conf(B_m)| \quad (10)$$

where n is the total number of samples and B_m indicates a group of samples whose prediction confidence falls into a certain interval. $acc(B_m)$ is the ground truth accuracy and $conf(B_m)$ is predicted probability (termed as confidence) of B_m . For regression task, we use the *coefficient of determination* R^2 , which is a measure of the closeness of the predicted model relative to the actual model [27]. R^2 is defined as $1 - SSE/SST$, where $SSE = \sum_{i=1}^n (\hat{y}_i - y_i)^2$ and $SST = \sum_{i=1}^n (\bar{y} - y_i)^2$, \hat{y}_i is the predicted value of i and \bar{y} is the observed average.

4.1. Results

Performance on shallow neural networks: We begin by looking at the accuracy performance of BNN and other baselines over LeNetD2 and Lenet5 architectures. In Figure 1, x-axis is the number of samples at each round, which is indicated as ($\times 100$). For instance at $x = 5$, we have added 500 samples and round 0 marks the beginning of the active learning procedure. Each model is followed by a hyphen and a letter, which indicates the type of acquisition function. For example, *E* is entropy and *VR* is variation ratio. For representation purpose we do not show random sampling, but in our experiments they substantially trailed behind every acquisition function. Overall, across all models, VR tends to outperform entropy when it comes to acquisition functions. Nonetheless, this difference is more pronounced during the first half of rounds, during the final rounds the difference becomes quite narrow. This shows that EN tends to improve its acquisition quality when it sees more data. When it comes to MNIST, BNN and EN perform on a similar level, while MCD trails behind. However, due to the simplicity of dataset, the difference in performance is not that discernible. For FMNIST, which is a more challenging dataset,

¹Models were implemented using Pytorch(pytorch.org) and Numpy(numpy.org) libraries

²github.com/VRM1/ActiveLearning

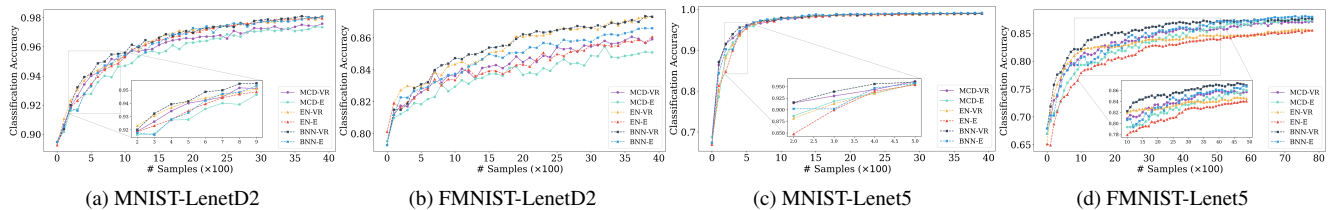


Figure 1: Active learning performance on LeNetD2 and LeNet5 architecture with *CT* setting. For MNIST, BNN and EN perform on a similar level, while MCD trails behind. For FMNIST, BNN clearly outperforms the rest and although EN performs similar to MCD upto round 10, it clearly starts to trail behind EN and surprisingly even loses to MCD.

we start to see some interesting differences. In LeNetD2 (Figure 1 (b)), while the performance of BNN and EN are on-par with each other (for VR), BNN seems to yield better results for entropy. In LeNet5 (Figure 1 (d)) although EN performs similar to BNN upto round 10, BNN clearly produces better accuracy than all other models upto round 50. Additionally, we observe EN’s accuracy lagging quite significantly behind the rest after about 30 rounds. This was quite surprising to us since in [6], the authors claim EN to perform better than MCD. Upon further investigation, we found that the poor performance of EN (compared to MCD) is *only observed with CT*. In the upcoming experiments, we will show the results on both CT and RFS.

Performance on Cifar10: The active learning performance of ANL and VGG is represented in Figure 2 (a)-(d). The results unravel some important characteristics of the models. First, when it comes to CT, BNNs performance is significantly better than both EN and MCD, especially for VGG. Here, BNN achieves about 75% and MCD about 67% accuracy, but similar to previous results (i.e., LeNet5) EN clearly under performs with just 55%. A possible reason for this outcome could be the lack of regularization. ENs are full capacity models without any dropouts and we observe quite substantial overfitting during CT setting. This in-turn result in making incorrect decisions when acquiring new data points during the active learning phase. Another reason could be catastrophic forgetting, which is a well known problem in continual training of neural networks [28, 29]. BNN on the other hand seems to be more robust to such perturbations. That being said, when retraining from scratch EN starts to outperform MCD as it doesn’t overfit the data acquired in previous rounds, which aligns with the recent study [6]. For ANL (Figure 2 (b)) we clearly see EN outperforming MCD, however, BNN still achieves better performance. When it comes to VGG (Figure 2 (c)) we don’t find any distinct performance gaps between all three models. Overall, when retrained from scratch, all models perform better compared to CT, but we observe a lot more variations in the accuracy scores, while in CT the increase in accuracy is quite smooth.

Calibration characteristics: When it comes to measuring robustness of machine learning models, relying solely on performance metrics such as accuracy is not sufficient. In our experiments, the calibration score is measured as expected calibration error (ECE) using equation (10). In Figure 2 (e)-(h), the y-axis is the ECE and the x-axis is the elapsed round number. For instance, for both ANL and VGG since the active learning is performed until round 80 (Figure 2 (a)-(d)), 25% implies the 20th round of the corresponding experiment. From calibration plots, we observe that ENs have the best out-of-the-box ECE scores followed by MCD. Although BNN offers great performance in terms of accuracy, they seem to be quite poorly calibrated. Thankfully, calibration is a post-training step and there are several ways to calibrate a model such as histogram binning and temperature scaling; in this paper we adopt the later. The ECE of the calibrated BNN model is shown as the blue bar. It is important to note that even though we have significantly reduced the calibration error, the accuracy of BNN still remains unaltered.

Performance on Cifar100: From Figure 3, one can observe that even for larger neural networks such as Densenets, BNN produces significantly better accuracy compared to MCD and EN. As for EN, it looks like as the neural networks become more complex, the CT methodology starts to substantially cripple the performance. When RFS both BNN and EN have similar performance, while MCD trails behind.

Performance on regression dataset: The robust performance of BNN is not just restricted to classification, but also extends to regression. Figure 4 shows the performance of BNN in terms of R^2 on housing price prediction. For this dataset, we used the LeNetD2 architecture where the input layer is a feature vector that is from by concatenating the image and descriptive text features of the individual houses [21]. For this dataset, we start with a seed sample of 50 and in each round we add five new data points that is selected via active learning. Here there is no major performance difference between BNN and EN, but MCD clearly under performs. Additionally, when it comes to BNN there

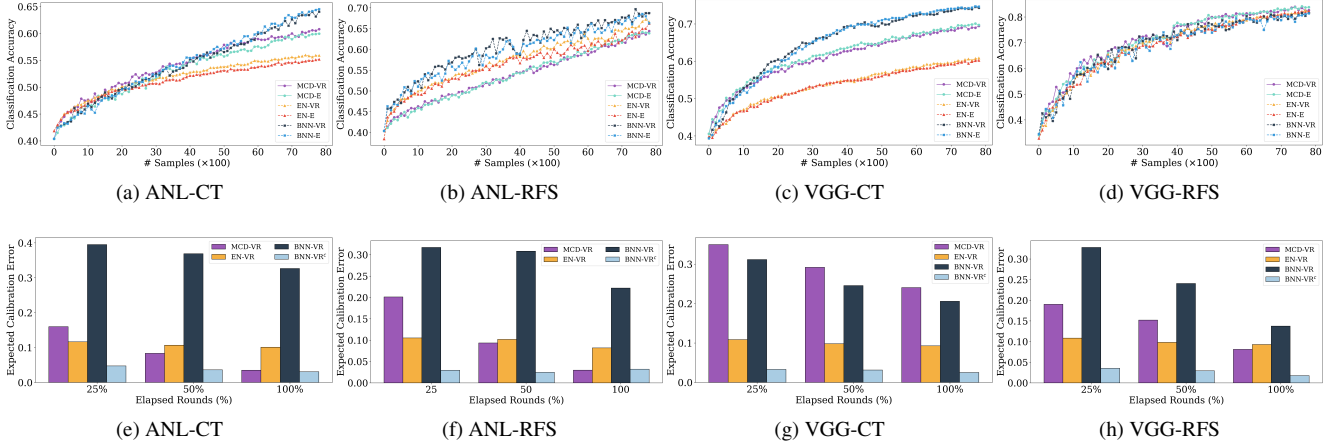


Figure 2: Active learning performance of ANL and VGG over Cifar10 – classification accuracy and model calibration. BNN yields a more robust performance when compared to EN and MCD, irrespective of the training methodology (a)-(d), while EN suffers quite significantly in the CT setting. When retraining from scratch, EN gets a major boost in performance and just slightly lags behind BNN for ANL and performs on par with BNN on VGG. Unfortunately, BNN suffers from poor calibration (e)-(h), but it can be quite easily corrected. The calibrated model BNN-VR^c is shown as the light blue bar.

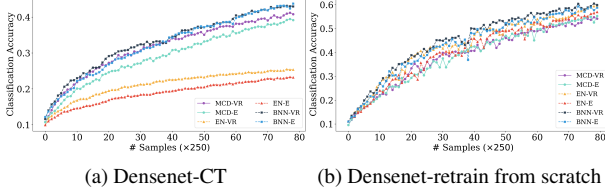


Figure 3: Active learning performance of Densenets on Cifar100 dataset. Similar to the results on Cifar10, BNN produces a more robust performance than EN and MCD whether it is CT or retraining from scratch.

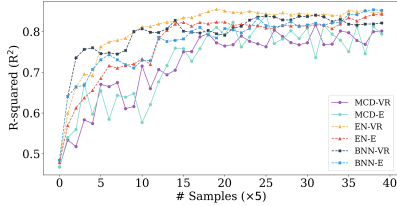


Figure 4: Housing price prediction dataset using LenetD2. There is no major performance difference between BNN and EN, but MCD clearly underperforms.

seems to be a lot more variance in R^2 score in each round, while EN tends to be smoother.

4.2. Ablation Study

We perform data-centric and model-centric ablation studies to get a deeper understanding of BNN’s performance.

Performance on challenging class labels: When retraining from scratch, we see that the performance gap between

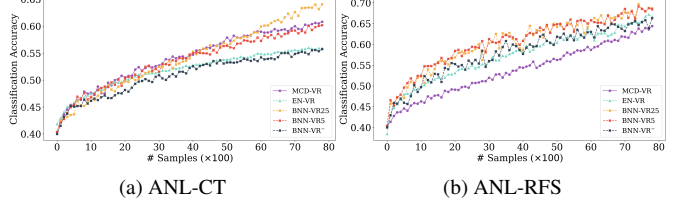


Figure 5: Impact of number of NNI and model capacity on Cifar10. BNN-VR25 indicates 25 network instances used to estimate the uncertainty, while BNN-VR5 implies five. BNN-VR⁻ is the ANL network with reduced capacity that matches those of MCD when dropouts are activated.

BNN and EN is quite narrow, especially on VGG (Figure 2(d)). Nonetheless, accuracy is a global score and when it comes to AL, it is important to measure the performance on labels that are hard to classify. Table 2 shows the precision and F1 measure of FMNIST and Cifar10 datasets for classes that are most challenging to predict. The corresponding accuracy plots can be seen from Figure 1(d) and Figure 2(d) respectively. Even though BNN and EN produce similar accuracy, for more challenging class labels, the former outshines the later. Across all selected rounds of active learning, both precision and F1 measures of BNN are clearly better than EN. This shows that BNN’s uncertainty estimation is more effective in acquiring datapoints that improve the model performance on challenging class labels.

Impact of NNI: The performance of AL is based on how robust is the uncertainty estimation. When it comes to BNN, a key factor that determines the goodness of estimation is

	Class	BNN-VR						EN-VR					
		25%		50%		100%		25%		50%		100%	
		Pr	F1	Pr	F1	Pr	F1	Pr	F1	Pr	F1	Pr	F1
Cifar10 (VGG)	Bird	51.2	47.9	63.8	67.1	79.3	76.9	48.8	46.2	62.8	63.4	75.7	75.2
	Cat	50.6	45.4	59.6	57.8	67.3	68.4	49.3	44.9	58.4	55.6	69	68.2
	Dog	36.4	44.0	62.7	65.1	77.8	77.2	54.1	58.2	60.9	64.9	74	74.9
FMNIST (Lenet5)	Pullover	74.7	75.3	81	79.8	81.8	80.2	71.4	72.4	74.4	75.2	78.3	77
	Shirt	57.1	62.8	62.7	64.5	66	66.3	56.6	56.2	61.9	60.5	62.7	63.4

Table 2: Precision and F1 score of BNN and EN on challenging class labels. The second row indicates the elapsed round and Pr indicates precision. Even though for VGG, EN and BNN have similar accuracy (Figure 2(d)), the precision and F1 measure on challenging labels indicate that performing AL via BNN leads to better results.

the number of NNI (i.e., lines 5-7 of Algorithm 1). A major advantage of EN over BNN (and MCD) is the low number of NNI that is needed to estimate uncertainty, which is set as five in our experiments. On the other hand, for BNNs we have 25 instances. Therefore, we wanted to test how good is BNN when the NNI is reduced to that of EN. The results of this experiment is shown in Figure 5. Here, one can observe that during CT, there is some performance dip but it is mostly towards the final rounds. On the other hand, for RFS, there is no noticeable loss in accuracy. We observed similar results even with entropy as the acquisition function. A possible reason for this outcome could be attributed to Bayesian’s ability to learn distribution over weights (instead of point estimate), which naturally models uncertainty during the training process (which EN and MCD lacks).

Impact of reduced model capacity: Besides NNI, another factor that determine the performance of AL is the model capacity. Both BCN and EN enjoy the benefit of being a full capacity model (during training). However, for MCD, due to dropouts a significant portion of neurons in dense and CNN layers remain inactive, which is one of main reasons for MCD’s inferior performance. In fact, [6] show that when ENs are capacity-limited, their performance drops roughly to that of MCD. To see this effect on BCN, we reduced the number of CNN filters and dense layers to that of MCD (i.e., 50% less for dense and 25% less for CNN). The outcome of this experiment is shown in Figure 5, where BNN-VR⁺ is the capacity-limited BCN. While we do see a noticeable performance dip when compared to the regular BNN, the accuracy still manages to be on-par with EN for both CT and RFS.

Performance of accelerated uncertainty estimation: Finally, we compare the performance of the proposed Bayesian accelerated uncertainty estimation learning (AUE) on LenetD2 architecture in Figure 6. It is interesting to see that for MNIST, our approximation is as effective as uncertainties estimated through iterative realizations of neural networks. For FMNIST (which is a more challenging dataset), AUE still produces respectable results. It is impor-

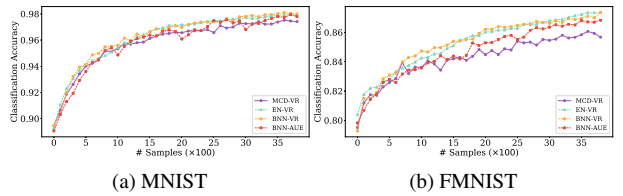


Figure 6: Active learning performance of iterative uncertainty estimation Vs accelerated uncertainty estimation (BNN-AUE) on MNIST and FMNIST datasets.

tant to note that iterative procedure creates multiple instantiations of the network and every instance needs to see the entire dataset to estimate uncertainty. Although, AUE cannot match the performance of the iterative approach, it significantly reduces the time taken to calculate the uncertainty and this might be a worthy trade-off between performance and speed.

5. Conclusion

In this paper, we analyzed Bayesian neural networks for active learning and showed that they are more efficient than ensemble and Monte Carlo dropouts in capturing uncertainty. Our experiments revealed the following characteristics of BNN: (a) BNNs are more robust when it comes to continual learning, and EN performs worse than MCD in this setting, (b) produces respectable uncertainty estimates even with reduced model capacity, and (c) produces better precision and F1 on difficult class labels compared to EN. To overcome the computation cost of repeated uncertainty estimation in active learning, we proposed an accelerated uncertainty estimation technique for dense layers.

References

- [1] Ozan Sener and Silvio Savarese. A geometric approach to active learning for convolutional neural networks. *arXiv preprint arXiv, 1708:1*, 2017. 1

- [2] Lin Yang, Yizhe Zhang, Jianxu Chen, Siyuan Zhang, and Danny Z Chen. Suggestive annotation: A deep active learning framework for biomedical image segmentation. In *International conference on medical image computing and computer-assisted intervention*, pages 399–407. Springer, 2017. 1
- [3] Yi Yang, Zhigang Ma, Feiping Nie, Xiaojun Chang, and Alexander G Hauptmann. Multi-class active learning by uncertainty sampling with diversity maximization. *International Journal of Computer Vision*, 113(2):113–127, 2015. 1
- [4] Balaji Lakshminarayanan, Alexander Pritzel, and Charles Blundell. Simple and scalable predictive uncertainty estimation using deep ensembles. In *Advances in neural information processing systems*, pages 6402–6413, 2017. 1, 2
- [5] Yarin Gal, Riashat Islam, and Zoubin Ghahramani. Deep bayesian active learning with image data. In *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pages 1183–1192. JMLR. org, 2017. 1, 2
- [6] William H Beluch, Tim Genewein, Andreas Nürnberger, and Jan M Köhler. The power of ensembles for active learning in image classification. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 9368–9377, 2018. 1, 2, 3, 4, 5, 6, 8
- [7] Yarin Gal and Zoubin Ghahramani. Dropout as a bayesian approximation: Representing model uncertainty in deep learning. In *international conference on machine learning*, pages 1050–1059, 2016. 1
- [8] Christos Louizos, Karen Ullrich, and Max Welling. Bayesian compression for deep learning. In *Advances in Neural Information Processing Systems*, pages 3288–3298, 2017. 1, 2, 3
- [9] Burr Settles. Active learning literature survey. Technical report, University of Wisconsin-Madison Department of Computer Sciences, 2009. 2
- [10] Alex Holub, Pietro Perona, and Michael C Burl. Entropy-based active learning for object recognition. In *2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pages 1–8. IEEE, 2008. 2
- [11] Ajay J Joshi, Fatih Porikli, and Nikolaos Papanikolopoulos. Multi-class active learning for image classification. In *2009 IEEE Conference on Computer Vision and Pattern Recognition*, pages 2372–2379. IEEE, 2009. 2
- [12] Xin Li and Yuhong Guo. Adaptive active learning for image classification. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 859–866, 2013. 2
- [13] Andreas Kirsch, Joost van Amersfoort, and Yarin Gal. Batchbald: Efficient and diverse batch acquisition for deep bayesian active learning. In *Advances in Neural Information Processing Systems*, pages 7026–7037, 2019. 2
- [14] Parmida Atighehchian, Frédéric Branchaud-Charron, and Alexandre Lacoste. Bayesian active learning for production, a systematic study and a reusable library. *arXiv preprint arXiv:2006.09916*, 2020. 2
- [15] Prateek Munjal, Nasir Hayat, Munawar Hayat, Jamshid Sourati, and Shadab Khan. Towards robust and reproducible active learning using neural networks. *arXiv*, pages arXiv–2002, 2020. 2
- [16] Dmitry Molchanov, Arsenii Ashukha, and Dmitry Vetrov. Variational dropout sparsifies deep neural networks. In *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pages 2498–2507. JMLR. org, 2017. 3
- [17] Claude E Shannon. A mathematical theory of communication. *Bell system technical journal*, 27(3):379–423, 1948. 3
- [18] Linton C Freeman. *Elementary applied statistics: for students in behavioral science*. John Wiley & Sons, 1965. 3
- [19] Han Xiao, Kashif Rasul, and Roland Vollgraf. Fashion-mnist: a novel image dataset for benchmarking machine learning algorithms. *arXiv preprint arXiv:1708.07747*, 2017. 4
- [20] Alex Krizhevsky, Geoffrey Hinton, et al. Learning multiple layers of features from tiny images. 2009. 4
- [21] Eman H Ahmed and Mohamed Moustafa. House price estimation from visual and textual features.(2016). *arXiv preprint cs.CV/1609.08399*, 2016. 4, 6
- [22] Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11):2278–2324, 1998. 4
- [23] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*, 2014. 5
- [24] Gao Huang, Zhuang Liu, Laurens Van Der Maaten, and Kilian Q Weinberger. Densely connected convolutional networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 4700–4708, 2017. 5
- [25] Chuan Guo, Geoff Pleiss, Yu Sun, and Kilian Q Weinberger. On calibration of modern neural networks. *arXiv preprint arXiv:1706.04599*, 2017. 5
- [26] Mahdi Pakdaman Naeini, Gregory F Cooper, and Milos Hauskrecht. Obtaining well calibrated probabilities using bayesian binning. In *Proceedings of the... AAAI Conference on Artificial Intelligence. AAAI Conference on Artificial Intelligence*, volume 2015, page 2901. NIH Public Access, 2015. 5
- [27] Nico JD Nagelkerke et al. A note on a general definition of the coefficient of determination. *Biometrika*, 78(3):691–692, 1991. 5
- [28] Ian J Goodfellow, Mehdi Mirza, Da Xiao, Aaron Courville, and Yoshua Bengio. An empirical investigation of catastrophic forgetting in gradient-based neural networks. *arXiv preprint arXiv:1312.6211*, 2013. 6
- [29] Ronald Kemker, Marc McClure, Angelina Abitino, Tyler Hayes, and Christopher Kanan. Measuring catastrophic forgetting in neural networks. *arXiv preprint arXiv:1708.02072*, 2017. 6