

---

# Binary Ensemble Neural Network: More Bits per Network or More Networks per Bit?

---

**Shilin Zhu**

Computer Science  
University of California San Diego  
La Jolla, CA 92093  
shz338@eng.ucsd.edu

**Xin Dong**

Computer Science  
Harvard University  
Cambridge, MA 02138  
xindong@g.harvard.edu

**Hao Su**

Computer Science  
University of California San Diego  
La Jolla, CA 92093  
haosu@eng.ucsd.edu

## Abstract

Binary neural networks (BNN) have been studied extensively since they run dramatically faster at lower memory and power consumption than floating-point networks, thanks to the efficiency of bit operations. However, contemporary BNNs whose weights and activations are both single bits suffer from severe accuracy degradation. To understand why, we investigate the representation ability, speed and bias/variance of BNNs through extensive experiments. We conclude that the error of BNNs are predominantly caused by the intrinsic instability (training time) and non-robustness (train & test time). Inspired by this investigation, we propose the Binary Ensemble Neural Network (BENN) which leverages ensemble methods to improve the performance of BNNs with limited efficiency cost. While ensemble techniques have been broadly believed to be only marginally helpful for strong classifiers such as deep neural networks, our analyses and experiments show that they are naturally a perfect fit to boost BNNs. We find that our BENN, which is faster and much more robust than state-of-the-art binary networks, can even surpass the accuracy of the full-precision floating number network with the same architecture.

## 1 Introduction

Deep Neural Networks (DNNs) have achieved great impact to broad disciplines in academia and industry [52, 34]. Recently, the deployment of DNNs are transferring from high-end cloud to low-end devices such as mobile phones and embedded chips, serving general public with many real-time applications, such as drones, miniature robots, and augmented reality. Unfortunately, these devices typically have limited computing power and memory space, thus cannot afford DNNs to achieve important tasks such as object recognition involving significant matrix computation and memory usage.

Binary Neural Network (BNN) is among the most promising techniques to meet the desired computation and memory requirement. BNNs [27] are deep neural networks whose weights and activations have only two possible values (e.g., -1 and +1) and can be represented by a single bit. Beyond the obvious advantage of saving storage and memory space, the binarized architecture admits only bitwise operations, which can be computed extremely fast using digital logic units [19] such as ALU with much less power consumption than floating-point unit (FPU).

Despite the significant gain in speed and space, however, current BNNs suffer from notable accuracy degradation when applied to challenging tasks such as ImageNet classification. To mitigate the gap, previous researches in BNNs have been focusing on designing more effective optimization algorithms to find better local minima of the quantized network weights. However, the task is highly non-trivial, since gradient-based optimization that used to be effective to train DNNs now becomes tricky to implement. This is because gradient of BNNs cannot be computed exactly due to the quantized network weights and the discontinuous step activation functions.

Instead of tweaking network optimizers, we strive to explore what have caused the performance gap, by a systematic experimental investigation into the representation power, speed, bias, variance, stability, and robustness of BNNs. The investigations imply that BNNs suffer from severe intrinsic instability and nonrobustness issues regardless of network parameter values. The observation further indicates that the drawbacks of BNNs are not likely to be resolved by solely improving the optimization techniques; instead, it is mandatory to cure the BNN function, particularly to reduce the prediction variance and improve the robustness to noises.

Inspired by the analysis, in this work, we propose Binary Ensemble Neural Network (BENN). Though the basic idea is as straight-forward as to simply aggregate multiple BNNs by boosting or bagging, the statistical properties of the ensembled classifiers become much nicer: not only the bias and variance are reduced, more importantly, the robustness to noises at test time is significantly improved. All the experiments suggest that BNNs and ensembled methods are a perfectly natural fit. Using architectures of the same connectivity (a variant of Network in Network [37]), we find that *boosting only 4 BNNs would be able to even surpass the baseline DNN with real weights*. This is by far the fastest, most accurate, and most robust results achieved by binarized networks.

To the best of our knowledge, this is the first work to bridge BNNs with ensemble methods. Unlike traditional BNN improvements that have computational complexity of  $\gtrsim O(K^2)$  by using  $K$ -bit per weights [58] or  $K$  bases in total [40], the complexity of BENN is reduced to  $O(K)$ . Compared with [58, 40], BENN also enjoys better bitwise operation parallelizability. With trivial parallelization, the complexity can be reduced to  $O(1)$ . We believe that BENN can shed light on more research along this idea to achieve extremely fast yet robust computation by networks.

## 2 Related Work

**Quantized and binary neural networks:** People have found that there is no need to use full-precision parameters and activations and can still preserve the accuracy of a neural network using  $k$ -bit fixed point numbers, as stated by [18, 22, 56, 8, 36, 39, 43, 51, 44]. The first approach is to use low-bitwidth numbers to approximate real ones proposed by [28], which is called quantized neural networks (QNNs). [60, 59] also proposed ternary neural networks. Although recent advances such as [58] can achieve competitive performance compared with full-precision models, they cannot fully speed it up because we still cannot perform parallelized bitwise operation with bitwidth larger than one. [27] is the very recent work that binarizes all the weights and activations, which was the birth of BNN. They have demonstrated the power of BNNs in terms of speed, memory use and power consumption. But recent works such as [53, 11, 20, 10] also reveal the strong accuracy degradation and mismatch issue during the training when BNNs are applied in complicated tasks such as ImageNet ([12]) recognition, especially when the activation is binarized. Although some work like [40, 45, 13] have offered reasonable solutions to approximate full-precision neural network, much more computation and tricks on hyperparameters are still needed to implement compared with BENN. Since they either use  $K$ -bitwidth quantization or  $K$  binary bases, the computational complexity cannot get rid of  $O(K^2)$  if  $O(1)$  is required for 1-bit single BNN, while BENN can achieve  $O(K)$  and even  $O(1)$  if multiple threads are naturally paralleled. Also, many of current literatures tried to minimize the distance between binary and real-value parameters. But empirical assumptions such as Gaussian parameter distribution are usually required in order to get a priori for each BNN or just keep the sign same as suggested by [40], otherwise the non-convex optimization is hard to deal with. By contrast, BENN can be a general framework to achieve the goal and has strong potential to work

even better than full-precision networks, without involving any more hyperparameters than a single BNN (except the number of ensemble rounds).

**Ensemble techniques:** To avoid simply relying on a single powerful classifier, the ensemble strategy can improve the accuracy of given learning algorithm combining multiple weak classifiers as summarized by [6, 9, 42]. The two most common strategies are bagging by [5] and boosting by [47, 17, 46, 24], which were proposed many years ago and have strong statistical foundation. They have roots in a theoretical framework PAC model by [54] which was the first to pose the question of whether weak learners can be ensembled into a strong learner. Bagging predictors are proved to reduce variance while boosting can reduce both bias and variance, and their effectiveness have been proved by many theoretical analysis. Traditionally ensemble was used with decision trees, decision stumps, random forests and achieved great success thanks to its desirable statistical properties. In recent years people did not pay much attention to them because neural network is not a weak classifier anymore thus ensemble can unnecessarily increase the model complexity. However, when applied to weak binary neural networks, we found it generates new insights and hopes, and BENN is a natural outcome of such perfect combination. In this work, we build our BENN on the top of variant bagging, AdaBoost by [15, 48], LogitBoost by [17] and can be extended to many more variants of traditional ensemble algorithms. We hope this work can revive these intelligent approaches and bring their life back into modern neural networks.

### 3 Why Making BNNs Work Well is Challenging?

Despite the speed and space advantage of BNN, its performances is still far inferior to the real valued counterparts. There are at least two possible reasons: First, functions representable by BNNs may have some inherent flaws; Second, current optimization algorithms are still unable to find good local minima and may be further improved. While most researchers have been working on developing better optimization methods, we suspect that BNNs may have some fundamental flaws. The following investigation reveals the fundamental limitations of BNN-representable functions experimentally.

Because all weights and activations are binary, an obvious fact is that BNNs can only represent a subset of discrete functions, being strictly weaker than real networks that are universal continuous function approximators [26]. What are not so obvious are two serious limitations of BNNs: the robustness issue w.r.t. input perturbations, and the stability issue w.r.t. training data sampling at training time. Classical learning theory tells us that both robustness and stability are closely related to the generalization error of a model [57, 4].

**Robustness Issue:** In practice, we observe much more severe overfitting effects of BNNs than real networks. We conjecture that the generalization issue is closely relevant to the robustness of BNNs. Robustness is defined as the property that if a testing sample is “similar” to a training sample, then the testing error is close to the training error [57]. To verify our hypothesis, we compute the following quantity to compare real-value DNN, BNN, and our BENN model as described in Sec 4:

$$\mathbb{E}_w \mathbb{E}_{\Delta x} \|f(x + \Delta x; w) - f(x; w)\|^2 \quad (1)$$

where  $f$  is the network and  $w$  is the network weight. Firstly, we randomly sample real-value weights  $w \sim \mathcal{N}(0, \mathbb{I})$  as suggested by literatures to get a DNN  $f_r$  with weights  $w_r$  and binarize it to get a BNN  $f_b$  with binary weights  $w_b$ . We also binarize  $w$  in BENN and get  $w_{benn}$ . We normalize each input image in CIFAR-10 to the range of  $[-1, 1]$ . Then we inject the input perturbation  $\Delta x$  on each example by a Gaussian noise with different variances (up to 0.1, see Appendix), run a forward pass on both networks, and measure the expected  $l_2$  norm of the change on the output distribution. The  $l_2$  norm of DNN, BNN and QNN in first 100 rounds is shown in Fig.1(left) with perturbation variance 0.01. Results show that BNNs always have larger output change, concluding that they are always more susceptible to input perturbation, and BNN does worse than QNN with more bits. We also see that having more bits at activations improves BNN’s robustness significantly, while having more bits on weights has marginal improvement. Thus the activation binarization seems to be the bottleneck. Secondly, we train a real-value network  $f_r$  and a BNN  $f_b$  using XNOR-Net [45] rather than direct sampling. We also include our designed BENN  $f_{benn}$  in comparison. Then we perform the same Gaussian input perturbation  $\Delta x$ , run forward pass, and collect the change of classification error  $\mathcal{L}$  on CIFAR-10 as:

$$\mathbb{E}_{\Delta x} |\mathcal{L}(f(x + \Delta x)) - \mathcal{L}(f(x))| \quad (2)$$

Results in Fig.1(middle) indicates that BNNs are still more sensitive to noises even if it is well optimized. Although people have shown that weights in BNN still have nice statistical properties as

in [1], the conclusion can change dramatically if both weights and activations are binarized while input is perturbed.

**Stability Issue:** BNNs are known to be hard to optimize due to problems such as gradient mismatch and non-smoothness of activation function. [36] has shown that stochastic rounding converges to within  $O(\Delta)$  accuracy of the minimizer in expectation where  $\Delta$  denotes quantization resolution, assuming the error surface is convex. However, the community has not fully understood the non-convex error surface of BNN and how it interacts with different optimizers such as SGD or ADAM [33]. One explanation of such instability is the non-smoothness of the function output w.r.t. the binary network parameters, because the input to each layer is also binarized numbers by the activation function of the previous layer. In other words, in BNN’s function family, not only each function is non-smooth w.r.t. the input, but also it is non-smooth w.r.t. parameters. Fig. 1 (right) shows the accuracy oscillation within 20 epochs after we train BNN/QNN with 300 epochs, and results show that we should at least have QNN with weights and activations both 4-bit in order to stabilize the network. As a comparison, BENNs with 5 and 32 ensembles have already achieved amazing stability.

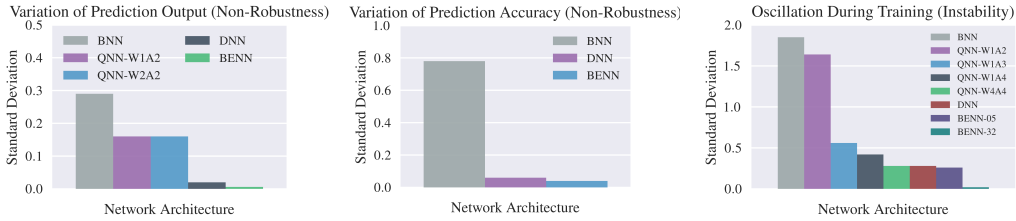


Figure 1: **Left:** BNN has large output variation (robustness issue). **Middle:** BNN has large variation of prediction accuracy (robustness issue). **Right:** BNN has large test accuracy variation during training (instability issue). BENN can cure these problems. Here, the perturbation variance is 0.01.

## 4 Binary Ensemble Neural Network

In this section, we illustrate our BENN using bagging and boosting strategies, respectively.

**Deterministic Binarization:** We adopt the widely used deterministic binarization as  $x_b = \text{Sign}(x)$  to quantize network weights and activations, which is preferred to leverage hardware accelerations. However, back-propagation becomes challenging since the derivative is zero almost everywhere except for the stepping point. In this work, we borrow the common strategy called "straight-through estimator" (STE), during back-propagation as  $\frac{\partial J}{\partial x} = \frac{\partial J}{\partial x_b} I_{|x| \leq 1}$ .

### 4.1 BENN-Bagging

The key idea of bagging is to average weak classifiers that are trained from i.i.d samples of the training set. To train each BNN classifier, we sample  $M$  examples independently with replacement from the training set  $\mathcal{D}$ . We do this  $K$  times to get  $K$  BNNs, denoted as  $b^1, \dots, b^K$ .

At test time, we aggregate the opinions from these  $K$  classifiers and decide among  $C$  classes. We propose two ways of aggregating the outputs. One is to choose the label that most BNNs agree with (hard decision), while the other is to choose the best label after aggregating their softmax probabilities (soft decision).

The main advantage brought by bagging is to reduce the variance of a single classifier. This is known to be extremely effective for deep decision trees which suffer from high variance, but only marginally helpful to boost the performance of neural networks, since networks are generally quite stable. Interestingly, though less helpful to real-value networks, bagging is effective to boost BNNs since the instability issue is severe for BNNs due to gradient mismatch and strong discretization noise as stated in Sec.3.

### 4.2 BENN-Boosting

Boosting is another important tool to ensemble classifiers. Instead of just aggregating the predictions from multiple independently trained BNNs, boosting combines multiple weak classifiers in a sequen-

Table 1: Analysis of Theoretically Computational Complexity. (F-full-precision,  $Q_k$ -k-bit quantization, B-binary)

Network	Weights	Activation	Operations	Memory Saving	Computation Saving
Standard DNN	F	F	+, -, $\times$	1	1
[10, 29, 35, 60, 59],...	B	F	+, -	$\sim 32x$	$\sim 2x$
[58, 28, 56, 2],...	$Q_k$	$Q_k$	+, -, $\times$	$\sim \frac{32}{k}x$	$< \frac{58}{k^2}x$
[40],...	$k \times B$	$k \times B$	+, -, XNOR, bitcount	$\sim \frac{32}{k}x$	$\sim \frac{58}{k^2}x$
[45] and ours	B	B	XNOR, bitcount	$\sim 32x$	$\sim 58x$

tial manner and can be viewed as a stage-wise gradient descent method optimized in the function space. Boosting is able to reduce both bias and variance of individual classifiers.

There are many variants of boosting algorithms and we choose the AdaBoost algorithm for its popularity. Suppose classifier  $k$  has hypothesis  $b^k : X \rightarrow \mathbb{R}$ , weight  $\alpha_k$  and output distribution  $p^k$ , we can denote the aggregated classifier as  $B^K : X \rightarrow \mathbb{R}$  and its aggregated output distribution  $P^K$ . Then AdaBoost minimizes the following exponential loss:

$$J(B^K) = \sum_i e^{-Y^T P^K} = \sum_i e^{-Y^T (P^{K-1} + \alpha_k p^k)}$$

where  $Y = (y_1, \dots, y_C)^T$  and  $i$  denotes index of training example. In addition, BENN can work with any other boosting methods such as LogitBoost and XGBoost.

**Reweighting Principle** The key idea of boosting algorithm is to make the current classifier pay more attention to misclassified samples by previous classifiers but less attention to those that have already been classified correctly. Reweighting is the most common way of budgeting attention based on the historical results. There are essentially two ways to accomplish this goal:

- Reweighting on sampling probabilities: Suppose initially each training example  $i$  is assigned  $\pi = u_i = 1/M$  uniformly, so each sample gets equal chance to be picked. After each round, we reweight the sampling probability according to the classification confidence.
- Reweighting on loss/gradient: We may also incorporate  $u_i$  into gradient, so that BNN updates parameters with larger step size on misclassified examples as  $\nabla'_w J(b^k)_i \leftarrow \lambda \cdot (\alpha_k p^k_y)(u_i) \cdot \nabla_w J(b^k)$ , where  $\lambda$  is the learning rate. However, this approach is less effective experimentally for BNNs, and we conjecture that it exaggerates the gradient mismatch problem.

### 4.3 Test-time Complexity

A 1-bit BNN with the same connectivity as the original full-precision 32-bit neural networks can save  $\sim 32x$  memory. In reality, BNN can achieve  $\sim 58x$  speed up on the current generation of 64-bit CPUs and may be further improved with special hardware such as FPGA. Some existing works only binarize the weights but leave activations full-precision, which practically only results in  $\gtrsim 2x$  speed up. As for BENN with  $K$  rounds, each BNN's inference is independent thus the total memory saving is  $\sim 32/Kx$ . As for boosting, we can further scale down the size of each BNN to save more computations and memory usage. To sum up, existing approaches have complexity  $O(K^2)$  with  $K$ -bit QNN [58] or use  $K$  binary bases [40], because they cannot avoid the bit collection operation to generate a number, although their fix-point computation is much more efficient than float-point computation. If  $O(1)$  is the time complexity of the boolean operation, then BENN reduces the quadratic complexity to  $O(K)$  with  $K$  ensembles but still maintains the very satisfying accuracy and stability as stated above. We can even make the inference in  $O(1)$  for ensemble models if multiple threads can be supported. A complete comparison is shown in Table 1.

## 5 Theoretical Analysis

Given a real valued DNN  $f_w$  with a set of parameters  $w \sim N(0, \sigma_w^2)$ , a BNN  $f_{w_b}$  with binarized parameters  $w_b$ , input vector  $x \sim N(0, 1)$  (after Batch Normalization) and perturbation  $\Delta x \sim N(0, \sigma^2)$ , and a BENN  $f_{w_{\text{benn}}}$  with  $K$  ensembles, we want to compare their robustness w.r.t. the input perturbation. Here we analyze the variance of output change before and after perturbation. This is

because the output change has zero mean and its variance reflects the distribution of output variation. More specifically, larger variance means increased variation of output w.r.t. input perturbation.

Assume  $f_w, f_{w_b}, f_{w_{\text{benn}}}$  are outputs before non-linear activation function of a single neuron in an one-layer network, we have the output variation of real-value DNN:

$$f_w(x + \Delta x) - f_w(x) = w \odot (x + \Delta x) - w \odot x = w \odot \Delta x$$

whose distribution has variance  $\sigma_r^2 = |w|\sigma_w^2\sigma^2$ , where  $|w|$  denotes number of input connections for this neuron and  $\odot$  denotes inner product. This is because summation of multiple independent distributions (due to inner product  $\odot$ ) has variance summed as well. Some modern non-linear activation function  $g(\cdot)$  like ReLU will not change the inequality of variances (i.e., if  $\sigma_{f_a}^2(x) > \sigma_{f_b}^2(x)$ , then  $\sigma_{g(f_a(x))}^2 > \sigma_{g(f_b(x))}^2$ ), thus we can ignore them in the analysis to keep it simple.

## 5.1 Activation Binarization

Suppose  $w$  is real valued but only input binarized (denote as  $f_w^b$ ), the activation binarization (-1 and +1) has threshold 0, then the output variation is:

$$f_w^b(x + \Delta x) - f_w^b(x) = w \odot \text{sign}(x + \Delta x) - w \odot \text{sign}(x)$$

whose distribution has variance  $\sigma_{A_b}^2 = |w|\sigma_w^2\sigma_{\text{sign}(x+\Delta x)-\text{sign}(x)}^2$ . This is because  $\text{sign}(x) \in \{-1, +1\}$  so the inner product is just the summation of  $|w|$  independent distributions, each having variance  $\sigma_{\text{sign}(x+\Delta x)-\text{sign}(x)}^2$ . Note that  $\text{sign}(x + \Delta x) - \text{sign}(x)$  only has three possible values, namely, 0, -2 and +2. We compute each of them as follows:

$$\begin{aligned} \Pr(\text{sign}(x + \Delta x) - \text{sign}(x) = 2) &= \Pr(x < 0 \text{ AND } x + \Delta x > 0) \\ &= \Pr(\Delta x > -x | x < 0) \Pr(x < 0) \\ &= \int_{-\infty}^{0^-} \left[ \int_{-x}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(\Delta x)^2}{2\sigma^2}} d(\Delta x) \right] \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx \\ \Pr(\text{sign}(x + \Delta x) - \text{sign}(x) = -2) &= \Pr(x > 0 \text{ AND } x + \Delta x < 0) \\ &= \Pr(\Delta x < -x | x > 0) \Pr(x > 0) \\ &= \int_{0^+}^{\infty} \left[ \int_{-\infty}^{-x} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(\Delta x)^2}{2\sigma^2}} d(\Delta x) \right] \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx \\ \Pr(\text{sign}(x + \Delta x) - \text{sign}(x) = 0) &= 1 - \Pr(\text{sign}(x + \Delta x) - \text{sign}(x) = \pm 2) \end{aligned}$$

and its variance can be computed by:

$$\begin{aligned} \sigma_{A_b}^2 &= |w|\sigma_w^2 \left\{ \mathbb{E}[(\text{sign}(x + \Delta x) - \text{sign}(x))^2] - \mathbb{E}^2[(\text{sign}(x + \Delta x) - \text{sign}(x))] \right\} \\ &= |w|\sigma_w^2 \left\{ \mathbb{E}[(\text{sign}(x + \Delta x) - \text{sign}(x))^2] \right\} \end{aligned}$$

since  $\mathbb{E}[(\text{sign}(x + \Delta x) - \text{sign}(x))] = 0$ . Unfortunately this integral does not have analytical formula, we use numerical method to obtain  $\Pr(\text{sign}(x + \Delta x) - \text{sign}(x) = \pm 2)$ . Therefore, the variance is:

$$\sigma_{A_b}^2 = B|w|\sigma_w^2, \sigma_r^2 = R|w|\sigma_w^2$$

where  $B(= \sigma_{\text{sign}(x+\Delta x)-\text{sign}(x)}^2)$  and  $R(= \sigma^2)$  can be found in Table 2. When  $\sigma < 1$ , robustness of BNN is worse than DNN's. As for BENN-Bagging with  $K$  ( $K > 1$ ) ensembles, the output change has variance:

$$\sigma_{\text{benn}}^2 = K\sigma_{A_b}^2 \cdot \frac{1}{K^2} = \frac{\sigma_{A_b}^2}{K} = \frac{B}{K}|w|\sigma_w^2 < \sigma_{A_b}^2$$

thus BENN-Bagging has better robustness than BNN. If  $K > \frac{\sigma_{A_b}^2}{\sigma_r^2} = \frac{B}{R}$ , then BENN-Bagging can have even better robustness than DNN.

## 5.2 Weight Binarization



If we binarize  $w$  to  $w_b$  but keeping the activation real-valued, the output variation follows:

$$f_{w_b}(x + \Delta x) - f_{w_b}(x) = \text{sign}(w) \odot \Delta x$$

with variance  $\sigma_{W_b}^2 = |w| \sigma_{\text{sign}(w)}^2 \sigma^2 = |w| \sigma^2$ . Thus whether weight binarization will hurt robustness or not depends on whether  $\sigma_{\text{sign}(w)}^2 = 1 > \sigma_w^2$  holds or not. In particular, the robustness will not decrease if  $\sigma_w^2 = 1$ . BENN-Bagging has variance  $\sigma_{\text{benn}}^2 = \frac{1}{K} |w| \sigma^2$ . So if  $K > \frac{1}{\sigma_w^2}$ , then BENN-Bagging is better than DNN.

Table 2: Relation between B, R and  $\sigma$

$\sigma$	B	R
1.5	<b>1.25</b>	2.25
1.0	1.0	1.0
0.5	0.59	<b>0.25</b>
0.1	0.13	<b>0.01</b>
0.01	0.013	<b>0.0001</b>
0.001	0.0013	<b>0.000001</b>

### 5.3 Extreme Binarization

If both activation and weight are binarized (denote as  $f_{w_b}^b$ ), the output variation:

$$f_{w_b}^b(x + \Delta x) - f_{w_b}^b(x) = \text{sign}(w) \odot [\text{sign}(x + \Delta x) - \text{sign}(x)]$$

has variance  $\sigma_{E_b}^2 = |w| \sigma_{\text{sign}(w)}^2 (\sigma_{\text{sign}(x + \Delta x) - \text{sign}(x)}^2) = B |w|$  which is just the combination of Sec.1.1 and Sec.1.2. BENN-Bagging has variance  $\sigma_{\text{benn}}^2 = \frac{B}{K} |w|$ , which is more robust than DNN when  $K > \frac{\sigma_{E_b}^2}{\sigma_r^2} = \frac{B}{R \sigma_w^2}$ .

The above analysis results in the following theorem:

**Theorem 1** Given a activation binarization, weight binarization or extreme binarization one-layer network introduced above, input perturbation is  $\Delta x \sim N(0, \sigma^2)$ , then the output variation obeys:

1. If only activation is binarized, BNN has worse robustness than DNN when perturbation  $\sigma < 1$ . BENN-Bagging is guaranteed to be more robust than BNN. BENN-Bagging with  $K$  ensembles is more robust than DNN when  $K > \frac{B}{R}$ .
2. If only weight is binarized, BNN has worse robustness than DNN when  $\sigma_w < 1$ . BENN-Bagging is guaranteed to be more robust than BNN. BENN-Bagging with  $K$  ensembles is more robust than DNN when  $K > \frac{1}{\sigma_w^2}$ .
3. If both weight and activation are binarized, BNN has worse robustness than DNN when  $\sigma_w < 1$  and perturbation  $\sigma < 1$ . BENN-Bagging is guaranteed to be more robust than BNN. BENN-Bagging with  $K$  ensembles is more robust than DNN when  $K > \frac{B}{R \sigma_w^2}$ .

### 5.4 Multiple Layers Scenario

All the above analysis is for one layer models before and after activation function. The same conclusion can be extended to multiple layers scenario with Theorem 2.

**Theorem 2** Given a activation binarization, weight binarization or extreme binarization  $L$ -layer network (without batch normalization for generalization) introduced above, input perturbation is  $\Delta x \sim N(0, \sigma^2)$ , then the accumulated perturbation of ultimate network output obeys:

1. For DNN, ultimate output variation is  $\sigma_r^2 \leq \sigma^2 \prod_{l=1}^L |w_l| \sigma_{w_l}^2$ .
2. For activation binarization BNN, ultimate output variation is  $\sigma_{A_b}^2 \leq B \prod_{l=1}^L |w_l| \sigma_{w_l}^2$ .
3. For weight binarization BNN, ultimate output variation is  $\sigma_{W_b}^2 \leq \sigma^2 \prod_{l=1}^L |w_l|$ .
4. For extreme binarization BNN, ultimate output variation is  $\sigma_{E_b}^2 \leq B \prod_{l=1}^L |w_l|$ .
5. Theorem 1 holds for multiple layers scenario.

People have not fully understood the effect of variance reduction in boosting algorithms and some debates still exist in literature [7, 17], given that classifiers are not independent with each other.

Table 3: Network Configurations on CIFAR-10 (W-weights, A-activation, Params-number of parameters in network)

Config	Weight	Activation	Size	Params
SBNN (Semi-BNN)	First and last layer:32-bit	First and last layer:32-bit	100%	100%
EBNN (Extreme-BNN)	All layers:1-bit	All layers:1-bit	100%	100%
QBNN (Quantized-BNN)	All layers:1-bit	All layers:Q-bit	100%	100%
IBNN (Except-Input-BNN)	All layers:1-bit	First layer: 32-bit	100%	100%
S/E/IBNN-Tiny	-	-	50%	25%
S/EBNN-Nano	-	-	10%	1%

However, our experiments show that BENN-boosting can also reduce variance in our situation, which is consistent with [16, 17]. The theoretical analysis on BENN-boosting is left for future work.

If we switch  $x$  and  $w$ , replace input perturbation  $\Delta x$  with parameter perturbation  $\Delta w$  in the above analysis, then the same conclusion holds for parameter perturbation (stability issue). To sum up, BNN often can be worse than DNN in terms of robustness and stability, and our method BENN can cure these problems.

## 6 Warm-Restart Training for BENNs

To accelerate the training of new network classifier in BENN, we initialize the weights of the new classifier by cloning the weights from the most recently trained classifier. We name this training scheme as *warm-restart training*. Compared with another obvious training scheme to randomly initialize the weights of each new classifier, this warm-restart training can largely reduce training time. Additionally, we also observe that warm restart is able to deliver higher aggregated performance after the convergence is reached. We conjecture that the knowledge of those unseen data for the new classifier has been transferred from the inherited weights and is helpful to increase the discriminability of the new classifier.

**Implementation Details** We train BENN on the image classification task with CNN block structure containing a batch normalization layer, a binary activation layer, a binary convolution layer, a non-binary activation layer (e.g., sigmoid, ReLU) and a pooling layer. To compute the gradient of sign step function  $sign(x)$ , we use the same approach suggested by STE. Similar to binarization in the forward pass, we can binarize the gradient in the backward pass. When updating the parameters, we use real-value weights otherwise the tiny step size will be ignored after deterministic binarization, and maintaining accurate parameter update is proved to be essential for stochastic gradient descent. In this work, we train each BNN using standard and warm-restart training. Unlike the previous works which always keep the first and last layer full-precision, we train BENN with 7 different architecture configurations as shown in Table 3.

## 7 Experimental Results

We evaluate our algorithm on CIFAR-10 and ImageNet with a variant of Network-In-Network and AlexNet. The descriptions of our major baselines are included in Table 4. We use BENN-XX-YY to denote BENN from YY weak classifiers with ensemble method XX, and B-XBNN to denote the best single BNN under configuration XBNN from Table 3.

### 7.1 Insights Generated from CIFAR-10

In this section, we show the large performance gain using BENN on CIFAR-10 and summarize some insights. Each BNN is retrained by 100 epochs before ensemble and each full-precision network is trained by 300 epochs to obtain the best accuracy for reference. Here, we use a variant of Network-In-Network (NIN) for CIFAR-10 (see Appendix for the architecture), but BENN can be applied on any other state-of-the-art architectures and binarizing methods.

**Single BNN versus BENN:** The most important result is that BENN can achieve much better accuracy and stability than a single BNN with negligible sacrifice in speed. Experiments across all configurations show that BENN has the accuracy gain ranging from 4.21% to 24.16% (across different configurations, see Appendix) over BNN on CIFAR-10. If each BNN is weaker (e.g., EBNN), the gain over BNN will increase as shown in Fig.2. This verifies that BNN is indeed a good weak classifier for ensembles. Surprisingly, BENN outperforms full-precision neural network in SBNN after 32 ensembles by up to 1.52%. Note that in order to have the same memory usage as a



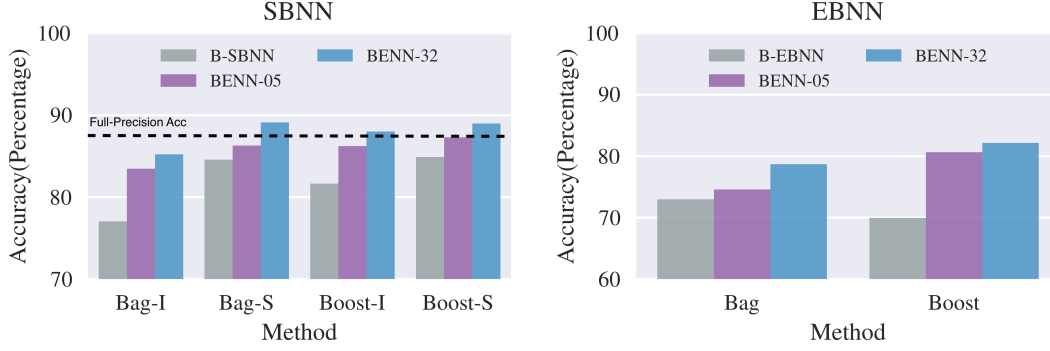


Figure 2: **Left:** Both bagging and boosting can increase the test accuracy significantly with more ensembles. It can even achieve better accuracy than its full-precision counterpart. **Right:** Boosting

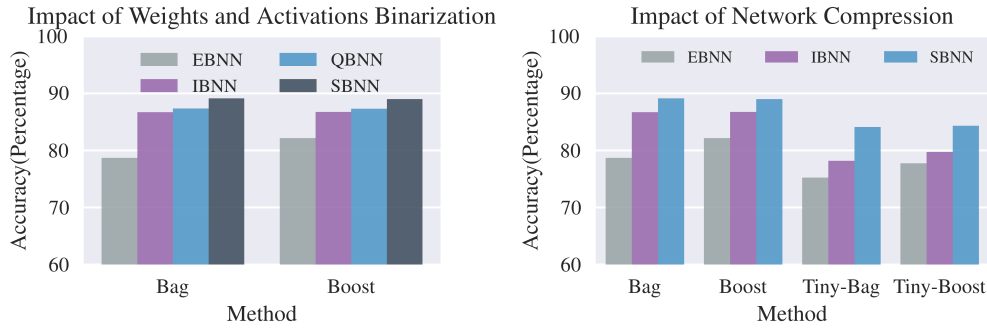


Figure 3: **Left:** After ensemble, the accuracy increases with more bits for activations, and BENN can work pretty well as long as the input image is not binarized. **Right:** Reducing model size causes accuracy degradation on single BNN, and we need more ensembles to make BENN close to the full-precision counterpart. Preserving the first and last layer full-precision helps a lot.

32-bit full-precision network, we constrain the ensemble up to 32 rounds if no network compression is involved. If more ensembles are available, BENN can perform even better.

We also measure the stability of the classifier within 20 epochs. The results in Fig.4(right) indicate that picking the best single BNN can indeed reduce the oscillation, because this maximization operation has regularization effect. Moreover, BENN can reduce the variance up to 90% if ensemble 5 rounds and up to 99% after 32 rounds. This is because the statistical property of ensemble framework makes BENN become a graceful way to ensure high stability.

**Bagging versus boosting:** It is known that bagging can only reduce the variance of the predictor, while boosting can reduce both bias and variance. The results in Fig.2(right), Fig.3(right) and Fig.4(left) show that boosting starts to outperform bagging in Tiny configurations by up to 2.51% and Nano configurations by up to 13.38%, and the gap increases with more ensemble rounds. Thus we believe that compared with bagging, boosting can reduce the variance as well, but it continues to reduce bias with more BNNs.

**The impact of single BNN's size:** If each BNN has enough complexity with low bias but high variance caused by binarization, then bagging is better approach than boosting, because we can train bagged weak BNNs in parallel but we can only train boosting in sequential, although they can both be paralleled during inference. However when each BNN has large bias, then boosting is much better choice as we already seen. The results in Fig.3(right) show that BENN can cure the accuracy degradation after compression. More specifically, the Tiny configuration generates gap as 7.71% for SBNN, 5.0% for EBNN, 12.18% for IBNN before ensemble. After ensemble, these gaps decrease to 4.8%, 4.41% and 7.0%. Surprisingly, 50% compression only reduces the accuracy of full-precision network by 1.18%, which means binarization significantly worsen the performance and single BNN is much more sensitive to network size. We believe one possible next step is to only compress the network except the first layer, where we first embed our image in high-dimensional binary space and then use efficient binary operations.

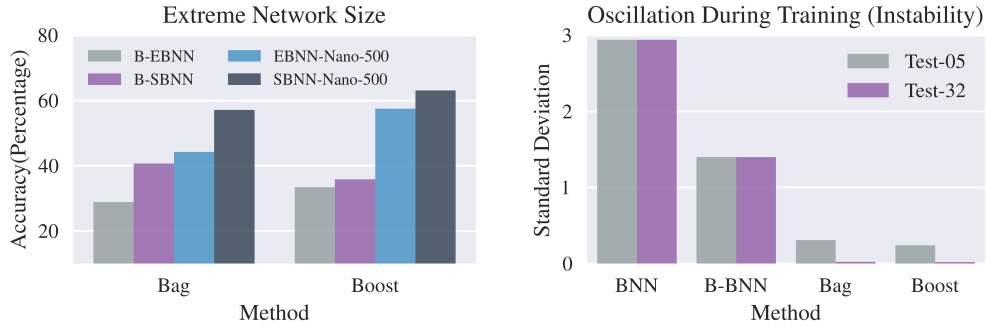


Figure 4: **Left:** We ensemble 500 rounds after we compress the model aggressively, and BENN can have large gain compared with single BNN. **Right:** BENN effectively reduces the oscillation during training and resolves the instability issue of BNN.

**Standard versus Warm-restart training:** Standard bagging and boosting use independent training, which will forget the knowledge learned so far, while warm-restart training will make bagging and boosting remember what has been learned. Fig.2(left) shows that warm-restart training will always perform better up to 3.9% for bagging and 2.95% for boosting after same number of training epochs. This means gradually adapting to more examples may be a better choice. We believe this is an interesting phenomenon but it needs more justification by studying theory of convergence by adjusting number of epochs and learning rate.

**The effect of number of bits:** Higher bitwidth results in lower variance and bias at the same time. This can be seen in Fig.3(left) where we make activations 2-bit. QBNN (Q=2) and IBNN have comparable accuracy after ensemble, but much better than EBNN and worse than SBNN. This indicates that the gain of having more bits is mostly due to better features from the input image, since input binarization is a real pain for neural networks. Surprisingly, BENN can still achieve more than 80% accuracy under such pain on EBNN.

**The effect of first and last layer:** Almost all the existing works in BNN assume the full precision of the first and last layer, since binarization on these two layers will cause severe accuracy degradation. We also spot this phenomenon by EBNN, SBNN and IBNN in Fig.3(left). The performance drop between EBNN and SBNN is 11.9% and 3.98%. But after ensemble, these gaps are squeezed to 6.98% and 2.36%. This indicates BENN can squeeze the performance gap caused by binarization of the first and last layer. For BENN, we can make all weak BNNs share the same full-precision weights of these two special layers after some pre-training, and we can only apply BENN to those intermediate layers. In this way, we can further reduce the memory usage.

## 7.2 Compare with the state-of-the-art on ImageNet

We believe BENN is one of the best neural network structures for network acceleration. To demonstrate the effectiveness of BENN, we compare our algorithm with state-of-the-arts on ImageNet recognition task (ILSVRC2012) using AlexNet. Specifically, we compare BENN with full-precision network, DoReFa-Net (k-bit quantized weight and activation), XNOR-Net (binary weight and activation), BNN (binary weight and activation) and BinaryConnect (binary weight). We also tried ABC-Net (k binary bases for weight and activation) but the network

does not even converge on NIN architecture (with accuracy only around  $\sim 37\%$ ) during optimization using CIFAR-10. Note that accuracy of BNN and BinaryConnect on AlexNet are reported by [45] instead of original authors. For DoReFa-Net and XNOR-Net, we use the best reported accuracy by original authors with 1-bit weight and activation. Our BENN is retrained with only 2~3 epochs for each ensemble round, given a well pre-trained model to use. As shown in Table 4, BENN-Boosting can surpass full-precision AlexNet by only 5 ensemble rounds, and can further boost to 58.34% after

Table 4: Comparison with state-of-the-arts on ImageNet using AlexNet (W-weights, A-activation)

Method	W	A	Top-1
Full-Precision[34, 45]	32	32	56.6%
XNOR-Net [45]	1	1	44.2%
DoReFa-Net[58]	1	1	43.6%
BinaryConnect[10, 45]	1	32	35.4%
BNN[27, 45]	1	1	27.9%
BENN-Bag-5 (ours)	1	1	54.56%
BENN-Boost-5 (ours)	1	1	57.28%
BENN-Bag-8 (ours)	1	1	55.81%
<b>BENN-Boost-8 (ours)</b>	1	1	<b>58.34%</b>

8 ensembles. We can also see the difference between bagging and boosting in terms of bias/variance reduction. This indicates that for most modern neural networks, we do not need to re-train single BNN for many epochs in each round, which can save a lot of time during training.

## 8 Discussion

**More bits per network or more networks per bit?:** We believe this paper brings up this important question. As for biological neural networks such as our brain, the signal between two neurons is more like a spike instead of high-range real-value signal. This implies that using real-value numbers may not be necessary in network but involves a lot of redundancies while wasting a lot of computing power. Our work converts the direction of "more bits per network" into "more networks per bit". BENN provides a hierarchical view, i.e., we build weak classifiers by aggregating the weakest single neurons to enrich more features, and build strong classifier by aggregating the weak classifiers by voting. We have shown that this hierarchical approach is more intuitive and natural to represent knowledge. Although the optimal ensemble structure is beyond the scope of this paper, we believe some structure searching techniques or meta-learning can be applied here. Moreover, the improvement on single BNN such as studying the error surface and resolving the curse of activation and gradient binarization is still essential for the success of BENN.

**BENN is hardware friendly:** Using BENN with  $K$  ensembles is better than using one  $K$ -bit classifier. Firstly,  $K$ -bit quantization still cannot get rid of fixed-point multiplication, while BENN can support bitwise operation. Secondly, people have shown that the complexity of a multiplier is proportional to the square of bitwidth, thus BENN simplifies the hardware design as well. Thirdly, BENN can use spike signals in the real chip instead of keeping the signal real-value all the time, which can save a lot of energy. Finally, unlike the recent literature which needs quadratic time to compute, BENN can be better parallelized on the real chip.

## 9 Conclusion and future work

In this paper, we proposed BENN, a novel neural network architecture which bridges BNN with ensemble methods. The experiments showed a large performance gain in terms of accuracy, robustness and stability. Our experiments also reveal some insights about trade-offs with number of bits, network size, and number of BNNs. We believe that by leveraging specialized hardware such as FPGA, BENN can be a new dawn for deploying large DNNs into mobile and embedded systems. This work also indicates that a single BNN's properties are still essential thus people need to work hard on both directions. In the future we will explore the power of BENN to reveal more insights about network bit representation and minimal network architecture (e.g., combine BENN with pruning), and BENN/hardware co-optimization. We also believe that a strong theoretical foundation is the most critical next step for BENN.

## References

- [1] Alexander G Anderson and Cory P Berg. The high-dimensional geometry of binary neural networks. *arXiv preprint arXiv:1705.07199*, 2017.
- [2] Sajid Anwar, Kyuyeon Hwang, and Wonyong Sung. Fixed point optimization of deep convolutional neural networks for object recognition. In *Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on*, pages 1131–1135. IEEE, 2015.
- [3] Yoshua Bengio, Nicholas Léonard, and Aaron Courville. Estimating or propagating gradients through stochastic neurons for conditional computation. *arXiv preprint arXiv:1308.3432*, 2013.
- [4] Olivier Bousquet and André Elisseeff. Stability and generalization. *Journal of machine learning research*, 2(Mar):499–526, 2002.
- [5] Leo Breiman. Bagging predictors. *Machine learning*, 24(2):123–140, 1996.
- [6] Leo Breiman. Bias, variance, and arcing classifiers. 1996.
- [7] Peter Bühlmann and Torsten Hothorn. Boosting algorithms: Regularization, prediction and model fitting. *Statistical Science*, pages 477–505, 2007.
- [8] Zhaowei Cai, Xiaodong He, Jian Sun, and Nuno Vasconcelos. Deep learning with low precision by half-wave gaussian quantization. *arXiv preprint arXiv:1702.00953*, 2017.

- [9] John G Carney, Pádraig Cunningham, and Umesh Bhagwan. Confidence and prediction intervals for neural network ensembles. In *Neural Networks, 1999. IJCNN'99. International Joint Conference on*, volume 2, pages 1215–1218. IEEE, 1999.
- [10] Matthieu Courbariaux, Yoshua Bengio, and Jean-Pierre David. Binaryconnect: Training deep neural networks with binary weights during propagations. In *Advances in neural information processing systems*, pages 3123–3131, 2015.
- [11] Matthieu Courbariaux, Itay Hubara, Daniel Soudry, Ran El-Yaniv, and Yoshua Bengio. Binarized neural networks: Training deep neural networks with weights and activations constrained to+ 1 or-1. *arXiv preprint arXiv:1602.02830*, 2016.
- [12] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. Imagenet: A large-scale hierarchical image database. In *Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on*, pages 248–255. IEEE, 2009.
- [13] Lei Deng, Peng Jiao, Jing Pei, Zhenzhi Wu, and Guoqi Li. Gated xnor networks: Deep neural networks with ternary weights and activations under a unified discretization framework. *arXiv preprint arXiv:1705.09283*, 2017.
- [14] Pedro Domingos. A unified bias-variance decomposition. In *Proceedings of 17th International Conference on Machine Learning*, pages 231–238, 2000.
- [15] Yoav Freund and Robert E Schapire. A decision-theoretic generalization of on-line learning and an application to boosting. In *European conference on computational learning theory*, pages 23–37. Springer, 1995.
- [16] Yoav Freund, Robert E Schapire, et al. Experiments with a new boosting algorithm. In *Icml*, volume 96, pages 148–156. Bari, Italy, 1996.
- [17] Jerome Friedman, Trevor Hastie, Robert Tibshirani, et al. Additive logistic regression: a statistical view of boosting (with discussion and a rejoinder by the authors). *The annals of statistics*, 28(2):337–407, 2000.
- [18] Yunchao Gong, Liu Liu, Ming Yang, and Lubomir Bourdev. Compressing deep convolutional networks using vector quantization. *arXiv preprint arXiv:1412.6115*, 2014.
- [19] Gokul Govindu, Ling Zhuo, Seonil Choi, and Viktor Prasanna. Analysis of high-performance floating-point arithmetic on fpgas. In *Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International*, page 149. IEEE, 2004.
- [20] Yiwen Guo, Anbang Yao, Hao Zhao, and Yurong Chen. Network sketching: Exploiting binary structure in deep cnns. *arXiv preprint arXiv:1706.02021*, 2017.
- [21] Suyog Gupta, Ankur Agrawal, Kailash Gopalakrishnan, and Pritish Narayanan. Deep learning with limited numerical precision. In *International Conference on Machine Learning*, pages 1737–1746, 2015.
- [22] Song Han, Huizi Mao, and William J Dally. Deep compression: Compressing deep neural networks with pruning, trained quantization and huffman coding. *arXiv preprint arXiv:1510.00149*, 2015.
- [23] Song Han, Jeff Pool, John Tran, and William Dally. Learning both weights and connections for efficient neural network. In *Advances in neural information processing systems*, pages 1135–1143, 2015.
- [24] Trevor Hastie, Saharon Rosset, Ji Zhu, and Hui Zou. Multi-class adaboost. *Statistics and its Interface*, 2(3):349–360, 2009.
- [25] Geoffrey Hinton. Neural networks for machine learning. In *Coursera*, pages 1135–1143, 2012.
- [26] Kurt Hornik, Maxwell Stinchcombe, and Halbert White. Multilayer feedforward networks are universal approximators. *Neural networks*, 2(5):359–366, 1989.
- [27] Itay Hubara, Matthieu Courbariaux, Daniel Soudry, Ran El-Yaniv, and Yoshua Bengio. Binarized neural networks. In *Advances in neural information processing systems*, pages 4107–4115, 2016.
- [28] Itay Hubara, Matthieu Courbariaux, Daniel Soudry, Ran El-Yaniv, and Yoshua Bengio. Quantized neural networks: Training neural networks with low precision weights and activations. *arXiv preprint arXiv:1609.07061*, 2016.
- [29] Kyuyeon Hwang and Wonyong Sung. Fixed-point feedforward deep neural network design using weights+ 1, 0, and- 1. In *Signal Processing Systems (SiPS), 2014 IEEE Workshop on*, pages 1–6. IEEE, 2014.

- [30] Forrest N Iandola, Song Han, Matthew W Moskewicz, Khalid Ashraf, William J Dally, and Kurt Keutzer. Squeezenet: Alexnet-level accuracy with 50x fewer parameters and < 0.5 mb model size. *arXiv preprint arXiv:1602.07360*, 2016.
- [31] Sergey Ioffe and Christian Szegedy. Batch normalization: Accelerating deep network training by reducing internal covariate shift. *arXiv preprint arXiv:1502.03167*, 2015.
- [32] Minje Kim and Paris Smaragdis. Bitwise neural networks. *arXiv preprint arXiv:1601.06071*, 2016.
- [33] Diederik P Kingma and Jimmy Ba. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*, 2014.
- [34] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. In *Advances in neural information processing systems*, pages 1097–1105, 2012.
- [35] Fengfu Li, Bo Zhang, and Bin Liu. Ternary weight networks. *arXiv preprint arXiv:1605.04711*, 2016.
- [36] Hao Li, Soham De, Zheng Xu, Christoph Studer, Hanan Samet, and Tom Goldstein. Training quantized nets: A deeper understanding. In *Advances in Neural Information Processing Systems*, pages 5813–5823, 2017.
- [37] Min Lin, Qiang Chen, and Shuicheng Yan. Network in network. *arXiv preprint arXiv:1312.4400*, 2013.
- [38] Zhouhan Lin, Matthieu Courbariaux, Roland Memisevic, and Yoshua Bengio. Neural networks with few multiplications. *arXiv preprint arXiv:1510.03009*, 2015.
- [39] Darryl Lin, Sachin Talathi, and Sreekanth Annapureddy. Fixed point quantization of deep convolutional networks. In *International Conference on Machine Learning*, pages 2849–2858, 2016.
- [40] Xiaofan Lin, Cong Zhao, and Wei Pan. Towards accurate binary convolutional neural network. In *Advances in Neural Information Processing Systems*, pages 344–352, 2017.
- [41] Joachim Ott, Zhouhan Lin, Ying Zhang, Shih-Chii Liu, and Yoshua Bengio. Recurrent neural networks with limited numerical precision. *arXiv preprint arXiv:1608.06902*, 2016.
- [42] Nikunj Chandrakant Oza and Stuart Russell. *Online ensemble learning*. University of California, Berkeley, 2001.
- [43] Eunhyeok Park, Junwhan Ahn, and Sungjoo Yoo. Weighted-entropy-based quantization for deep neural networks. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017.
- [44] Antonio Polino, Razvan Pascanu, and Dan Alistarh. Model compression via distillation and quantization. *arXiv preprint arXiv:1802.05668*, 2018.
- [45] Mohammad Rastegari, Vicente Ordonez, Joseph Redmon, and Ali Farhadi. Xnor-net: Imagenet classification using binary convolutional neural networks. In *European Conference on Computer Vision*, pages 525–542. Springer, 2016.
- [46] Robert E Schapire and Yoram Singer. Improved boosting algorithms using confidence-rated predictions. *Machine learning*, 37(3):297–336, 1999.
- [47] Robert E Schapire. The boosting approach to machine learning: An overview. In *Nonlinear estimation and classification*, pages 149–171. Springer, 2003.
- [48] Robert E Schapire. Explaining adaboost. In *Empirical inference*, pages 37–52. Springer, 2013.
- [49] Daniel Soudry, Itay Hubara, and Ron Meir. Expectation backpropagation: Parameter-free training of multilayer neural networks with continuous or discrete weights. In *Advances in Neural Information Processing Systems*, pages 963–971, 2014.
- [50] Nitish Srivastava, Geoffrey Hinton, Alex Krizhevsky, Ilya Sutskever, and Ruslan Salakhutdinov. Dropout: A simple way to prevent neural networks from overfitting. *The Journal of Machine Learning Research*, 15(1):1929–1958, 2014.
- [51] Wonyong Sung, Sungho Shin, and Kyuyeon Hwang. Resiliency of deep neural networks under quantization. *arXiv preprint arXiv:1511.06488*, 2015.
- [52] Christian Szegedy, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, Andrew Rabinovich, et al. Going deeper with convolutions. *Cvpr*, 2015.

- [53] Wei Tang, Gang Hua, and Liang Wang. How to train a compact binary neural network with high accuracy? In *AAAI*, pages 2625–2631, 2017.
- [54] Leslie G Valiant. A theory of the learnable. *Communications of the ACM*, 27(11):1134–1142, 1984.
- [55] Li Wan, Matthew Zeiler, Sixin Zhang, Yann Le Cun, and Rob Fergus. Regularization of neural networks using dropconnect. In *International Conference on Machine Learning*, pages 1058–1066, 2013.
- [56] Jiaxiang Wu, Cong Leng, Yuhang Wang, Qinghao Hu, and Jian Cheng. Quantized convolutional neural networks for mobile devices. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 4820–4828, 2016.
- [57] Huan Xu and Shie Mannor. Robustness and generalization. *Machine learning*, 86(3):391–423, 2012.
- [58] Shuchang Zhou, Yuxin Wu, Zekun Ni, Xinyu Zhou, He Wen, and Yuheng Zou. Dorefa-net: Training low bitwidth convolutional neural networks with low bitwidth gradients. *arXiv preprint arXiv:1606.06160*, 2016.
- [59] Aojun Zhou, Anbang Yao, Yiwen Guo, Lin Xu, and Yurong Chen. Incremental network quantization: Towards lossless cnns with low-precision weights. *arXiv preprint arXiv:1702.03044*, 2017.
- [60] Chenzhuo Zhu, Song Han, Huizi Mao, and William J Dally. Trained ternary quantization. *arXiv preprint arXiv:1612.01064*, 2016.