The 36th Canadian Conference on Artificial Intelligence

PAC-Bayesian Learning of Aggregated Binary Activated Neural Networks with Probabilities over Representations

Louis Fortier-Dubois†,†, Benjamin Leblanc†, Gaël Letarte†, François Laviolette†, Pascal Germain†
† Département d’informatique et de génie logiciel, Université Laval

Abstract

Considering a probability distribution over parameters is known as an efficient strategy to learn a neural network with non-differentiable activation functions. We study the expectation of a probabilistic neural network as a predictor by itself, focusing on the aggregation of binary activated neural networks with normal distributions over real-valued weights. Our work leverages a recent analysis derived from the PAC-Bayesian framework that derives tight generalization bounds and learning procedures for the expected output value of such an aggregation, which is given by an analytical expression. While the combinatorial nature of the latter has been circumvented by approximations in previous works, we show that the exact computation remains tractable for deep but narrow neural networks, thanks to a dynamic programming approach. This leads us to a peculiar bound minimization learning algorithm for binary activated neural networks, where the forward pass propagates probabilities over representations instead of activation values. A stochastic counterpart that scales to wide architectures is proposed.

Keywords: Statistical learning, PAC-Bayes, binary activated neural networks, representation learning

1. Introduction

The computation graphs of deep neural networks (a.k.a. architectures) are challenging to analyze, due to their multiple composition of non-linearities [1], overparametrization [2] and highly non-convex learning objective [3, 4]. Studying simpler models seems a sensible strategy to gain insight on neural network behaviour and state performance guarantees [e.g. 5, 6]. Our work starts from one possible simplification, obtained by considering the binary activation function, meaning that each neuron outputs only one bit of information instead of the many bits needed to represent a real number. The use of neural networks involving binary weights, with or without binary activation [7–9], has been suggested for reducing their resource consumption, and these may be especially useful in view of using a pre-trained network for forward propagation on embedded systems, but this is not our primary objective. We aim to foster an atypical vision of neural networks, where binary activated networks with real-valued parameters are viewed as elementary pieces of an ensemble, that we study as a whole.

Our work is motivated by the analysis of Letarte, Germain, Guedj, and Laviolette [10] and Biggs and Guedj [11], rooted in the PAC-Bayes theory [12]: they propose a learning objective for aggregation of binary activated networks derived from a high-confidence generalization bound, and they empirically show that minimizing this objective provides a predictor with both tight and theoretically sound guarantees. They also derived an analytical expression for the expected output value of binary activated networks sampled from Gaussian distributions. Being differentiable, this expression enables gradient descent optimization, and is to be added to methods to train networks with non-differentiable activation functions [13–15]. However, in order to preserve valid PAC-Bayes guarantees and be able to train large neural networks, Letarte et al. [10] rely on an approximation: neurons on the same layer all treat their inputs as if they were independent draws of the same probability distribution, when in fact all

* louis.fortier-dubois.1@ulaval.ca

This article is © 2023 by author(s) as listed above. The article is licensed under a Creative Commons Attribution (CC BY 4.0) International license (https://creativecommons.org/licenses/by/4.0/legalcode), except where otherwise indicated with respect to particular material included in the article. The article should be attributed to the author(s) identified above.
the inputs must correspond to the same draw.\textsuperscript{1} Not only does this make the algorithm output values that are slightly straying from the true aggregation expectation, it also fatally increases the PAC-Bayes bound for deeper architectures. Lately, Biggs and Guedj \cite{11} revisited the PAC-Bayes aggregation of neural networks, notably providing lower-variance approximation schemes; doing so, they exhibited that the forward propagation function of Letarte et al. can be rewritten in order to remove the above-mentioned independence assumption. Starting from this result, we conduct the major part of our study stepping away from all approximations.

Hence, our first contribution highlights that the exact expectation of an aggregation of binary activated networks is computable in time exponential in the width of the network, and linear in its depth. The originality of our proposed learning algorithm relies on computing probabilities of occurrences of the hidden layer representations. Doing so, not only our algorithm allows us to obtain non-vacuous PAC-Bayes bounds for very deep binary activated networks, but reveals itself as an interesting prediction mechanism. Noteworthy, we show that once the parameters are optimized, the prediction on a new example is achievable with a time complexity that remains constant relatively to the network depth. Our second contribution consists in the analysis of a compact scheme of our resulting predictors, having a constant computing time regarding the network width, and the dichotomy between the first contribution consists in the analysis of a compact scheme of our resulting predictors, having a constant computing time regarding the network width, and the dichotomy between the first contribution consists in the analysis of a compact scheme of our resulting predictors, having a constant computing time regarding the network width, and the dichotomy between the first two contributions, we present a stochastic version with sub-exponential time complexity regarding the network width.

2. Background and notation

We focus our study on the task of binary classification, using binary activated multilayer (BAM) neural networks, \textit{i.e.}, networks where each neuron either outputs \(-1\) or \(+1\), using the sign function: \(\text{sgn}(x) = -1\) if \(x < 0\), \(+1\) otherwise. We consider fully connected BAMs of \(L \in \mathbb{N}^+\) layers of size \(d_k \in \mathbb{N}^+\), \(\forall k \in \{1, 2, \ldots, L\}\), and inputs of size \(d_0 \in \mathbb{N}^+\). We fix \(d_L = 1\), whose output is the classification output of the whole network. We call \(L\) the depth of the network, \(d_k\) the width of the \(k\)th layer, and \(\max_{k \in \{1, 2, \ldots, L\}} d_k\) the width of the network. The sequence \(\langle d_k \rangle_{L \in 0}^L\) constitutes a (fully connected) architecture. Unlike in binary neural networks \textit{e.g.} \cite{7}, the parameters of a BAM are not constrained to be binary, but only activations are binary-valued. We thus have weights \(W_k \in \mathbb{R}^{d_k \times d_{k-1}}\) and biases \(b_k \in \mathbb{R}^{d_k}\), for \(k \in \{1, 2, \ldots, L\}\). That being said, in the remaining, the equations will be stated without loss of generality in terms of the weights \(W_k\) only. Therefore, a BAM \(B\) is totally defined by the tuple \(B := \langle W_k \rangle_{k \in 1}^L\). See Fig. 1a for an example of architecture. The 0\textsuperscript{th} layer is the input layer, the 1\textsuperscript{st} one is the leading hidden layer, any \(k\)th layer, with \(1 < k < L\), is simply called a hidden layer and the \(L\)th one is the output layer. Following the premises of Letarte et al. \cite{10}, we consider a distribution over BAMs, which we call an aggregation of BAMs.

\textbf{Definition 1.} An aggregation of BAMs with mean parameters \(B_M\), denoted \(A(B_M)\), is given by an isotropic Gaussian probability distribution over all parameters, centered in \(B_M\).

The BAM forward propagation process consists of computing the following function for an input \(x \in \mathbb{R}^{d_0}\), where \(\text{sgn}\) is defined element-wise:

\[
F_B(x) = \text{sgn}(W_L \text{sgn}(W_{L-1} \text{sgn}(\ldots \text{sgn}(W_1 x) \ldots))).
\]

In other words, the output of a BAM \(B\) is \(F_B(x) := F_B^L(x)\), given the recursive equations

\[
F_B^k(x) = \begin{cases} 
\text{sgn}(W_1 x) & \text{if } k = 1, \\
\text{sgn}(W_k F_B^{k-1}(x)) & \text{otherwise}.
\end{cases}
\]

\textsuperscript{1}This recalls the \textit{mean-field approximation} performed by Soudry, Hubara, and Meir \cite{9} for learning binary activated networks in a Bayesian setting.
Beside, the output of an aggregation of BAMs is the expected output of a BAM drawn from the (continuous) parameters distribution:

\[ F_{A(B_M)}(x) = E_{B \sim A(B_M)} F_B(x). \]  

(2.1)

Such aggregation of BAMs is our main object of study. Note that the forthcoming Section 4 is dedicated to a PAC-Bayesian treatment where \( A(B_M) \) is considered as a posterior distribution. In line with the (PAC-)Bayesian literature, we call the single BAM network \( B_M \) the Maximum-A-Posterior (MAP) predictor.

3. The aggregation output

We present a recursive formulation to compute the exact aggregation output, denoted \( F_{A(B_M)}(x) \), which is differentiable end-to-end. The formulation is equivalent to the one of Biggs and Guedj [11, Eq. (9)], but is expressed in order to highlight the probabilities of representations for each layer, which is the cornerstone of our analysis.

Given a fixed representation (an input vector \( a \in \mathbb{R}^d \)), the expected output of a single neuron with sign activation over an isotropic Gaussian distribution centered on \( w \in \mathbb{R}^d \) is

\[ E_{v \sim N(w, I)} \text{sgn}(v \cdot a) = \text{erf} \left( \frac{w \cdot a}{\sqrt{2}||a||} \right), \]

where \( \text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt \) is the Gauss error function. However, as the input vector of a neuron relies on the distribution of weights on the previous layers, the representation itself is a random vector. A neuron outputs a value \( s \in \{-1, 1\} \) with probability

\[ \Pr(f_w(a) = s) = \frac{1}{2} + \frac{s}{2} \text{erf} \left( \frac{w \cdot a}{\sqrt{2}||a||} \right). \]  

(3.1)

Thus, the probability of observing a specific representation \( s = (s_1, \ldots, s_{d_k}) \in R_k \) (with \( R_k := \{-1, 1\}^{d_k} \)) at layer \( k \) can be expressed in a recursive manner, having the events...
\[ a_k^s := F_B^k(x) = s \] and \[ a_{k-1}^s := F_B^{k-1}(x) = s : \]

\[
Pr(a_k^s) = \begin{cases} 
\prod_{i=1}^{d_k} \left( \frac{1}{2} + \frac{s^i}{2} \text{erf} \left( \frac{W_i \cdot x}{\sqrt{2||x||}} \right) \right) & \text{if } k = 1, \\
\sum_{s \in R_{k-1}} \Pr(a_k^s | a_{k-1}^s) \Pr(a_{k-1}^s) & \text{otherwise.} 
\end{cases}
\]

The base case of the above recursion refers to the leading hidden layer \( F_B^1 \). The probability of observing a representation \( s \in R_1 \) on this first hidden layer given an input \( x \) amounts to be the product of the probability associated with the \( d_1 \) individual neuron values (Eq. 3.1).

The general case refers to the subsequent hidden layers \( (F_B^2, \ldots, F_B^L) \). The probability of observing a representation \( s \in R_k \) is decomposed into the sum of the \( 2^{d_{k-1}} \) probabilities of observing the representation \( \bar{s} \in R_{k-1} \) on the previous hidden layer (obtained recursively) and the conditional probability (obtained from Eq. (3.1), using the fact that \( ||\bar{s}||^2 = d_{k-1} \)):

\[
Pr(a_k^s | a_{k-1}^\bar{s}) = \prod_{i=1}^{d_k} \left[ \frac{1}{2} + \frac{s^i}{2} \text{erf} \left( \frac{W_i \cdot \bar{s}}{\sqrt{2d_{k-1}}} \right) \right].
\]

Finally, assuming the output layer is only one neuron wide, the exact output of the aggregation can be computed with: \( F_{A(B^L)}(x) = \mathbb{E}_{B \sim \mathcal{A}(B^L)} F_B(x) = Pr(F_B^L(x) = 1) - Pr(F_B^L(x) = -1) \).

By contrast, the proposed PBGNet algorithm of Letarte et al. [10, Eq. (16)] computes \( F_{PBG}^k(x) \) using the following equations (equivalent to the ones above only when \( L \leq 2 \)):

\[
F_{PBG}^k(x) = \begin{cases} 
\text{erf} \left( \frac{W_1 \cdot x}{\sqrt{2||x||}} \right) & \text{if } k = 1, \\
\sum_{\bar{s} \in R_{k-1}} \text{erf} \left( \frac{W_k \cdot \bar{s}}{\sqrt{2d_{k-1}}} \right) \prod_{i=1}^{d_k} \left[ \frac{1}{2} + \frac{s^i}{2} \text{erf} \left( \frac{W_i \cdot \bar{s}}{\sqrt{2d_{k-1}}} \right) \right]^i & \text{otherwise.}
\end{cases}
\]

This comes down to outputting at each layer only the expectation of the BAM representation given the expectation of the previous layer, instead of our complete probability distribution. Their method therefore deletes information at each layer since the expectation does not carry the correlation between each individual neuron output. This approximation recalls the mean-field one, on which the Bayesian analysis of binary activated networks of Soudry, Hubara, and Meir [9] relies. We avoid such approximations, and we compute \( F_{A(B^L)}(x) \) by a dynamic programming approach, described next.

**Dynamic program.** Abusing notation a little, when writing \( [g(s)]_{s \in R} \) we assume all \( s \) are taken in lexicographical order. Hence, posing

\[
\Psi_k = \prod_{i=1}^{d_k} \left( \frac{1}{2} + \frac{s^i}{2} \text{erf} \left( \frac{W_i \cdot \bar{s}}{\sqrt{2d_{k-1}}} \right) \right)_{s \in R_k, \bar{s} \in R_{k-1}}, \tag{3.2}
\]

one can obtain straightforwardly the probability vector \( \mathbf{P}_k = [Pr(F_{PBG}^k(x)|s)]_{s \in R_k} \) by computing \( \Psi_k \cdot \mathbf{P}_{k-1} \). Starting with

\[
\mathbf{P}_1(x) = \prod_{i=1}^{d_1} \left( \frac{1}{2} + \frac{s^i}{2} \text{erf} \left( \frac{W_i \cdot \bar{s}}{\sqrt{2d_{k-1}}} \right) \right)_{s \in R_1}, \tag{3.3}
\]

and computing \( \mathbf{P}_k \) for \( k \in \{2, 3, \ldots, L\} \) in ascending order, we can therefore compute the exact expectation of a BAM \( B \sim A \) in time exponential in \( B \)'s width, yet linear in its depth.

The previous formulas lead to what stands as the forward propagation process of our new neural network, which we name ABNet for **Aggregation of Binary activated Networks**. From parameters \( B_M \), it computes \( F_{A(B_M)}(x) \). The computation graph of ABNet is illustrated by Fig. 1b. The width of hidden layers \( k < L \) are of exponential size \( 2^{dk} \) relatively to the width \( d_k \) of the BAM networks it aggregates. Each layer of ABNet outputs a probability
distribution over all possible configurations of the underlying BAM. The next layer then multiplies those probabilities by the conditional probabilities $\Psi$, which is just a reorganization of the weights and is totally independent of the input $x$. As a result, ABNet applies only linear functions on hidden and output layers; an observation we discuss further in Section 5.

**Stochastic version.** ABNet has many interesting theoretical properties, but the necessity of computing the probability of every combination of neuron outputs at a given layer makes it too cumbersome for practical applications. We propose a stochastic version of ABNet, which keeps its property of avoiding the mean field approximation while limiting the computation complexity with regard to the width to a quadratic one. Note that the stochastic versions of ABNet and PBGNet are truly different: while the former propagates probabilities over representations, the latter relies on forward and backward passes alike standard neural networks. This is achievable by picking a constant number $n$ of representations $R'_k$ uniformly from $R_k$ at layer $k$, computing only the occurring probability of those $n$ representations (replacing representation sets $R_k$ by their uniformly drawn counterparts $R'_k$ in Equations 3.2 and 3.3), and normalizing at each layer by dividing $P_k$ by $\sum_{s_k \in R'_k} P_k [s_k]$.

**Complexity.** Assuming every layer has the same width $d$ at each layer, the complexity of PBGNet is $O(L^2d^2)$ (or $O(Lnd^2)$ for its stochastic counterpart, with $n$ samples), while the complexity of ABNet is $O(L2^d d^2)$ (or $O(Ln^2d^2)$ for the stochastic version). See Fig. 2 for an empirical study of computing times. A salient fact is that stochastic versions scale much better on wide architectures (Fig. 2a).

4. Bounding and optimizing the generalization loss

Initiated by McAllester [12], the PAC-Bayes theory allows one to bound the generalization error of a learned predictor without requiring a validation set, under the sole assumption that data is sampled in an iid way from the unknown distribution $D$.

To be eligible for a PAC-Bayesian treatment, predictors must be expressed through a posterior probability distribution over a predefined class of hypotheses. Even though neural networks are not naturally defined as such, many valuable analyses have been proposed by applying a PAC-Bayesian theory to stochastic variants of deterministic neural networks [17–21] by considering perturbations (typically Gaussian distributed noise) on the weights. This strategy can be applied to any neural network topology and activation functions, but the generalization bounds do not apply to the underlying deterministic (non-perturbed)
Given a prior in data (2) The KL divergence of Equation (4.2), acting as a regularization term, does give the same as a distribution over (finite) BAM networks (Eq 2.1), the PAC-Bayesian bound applies to the output of ABNet. The forthcoming Theorem 2 provides high confidence upper bound for the generalization loss of a learned ABNet, defined as \( \mathcal{L}_D(F_A) = \mathbb{E}_{(x,y) \sim D} \ell(F_A(x), y) \), where \( \ell(y', y) = \frac{1}{2} (1 - yy') \in [0, 1] \) is the linear loss for the binary classification problem. The two main quantities involved in the computation of the bound are the empirical loss on the learning sample \( S = \{(x_i, y_i)\}_{i=1}^n \sim D^n \),
\[
\hat{\mathcal{L}}_S(F_A) = \frac{1}{n} \sum_{i=1}^n \ell(F_A(x_i), y_i),
\]
and the Kullback-Leibler (KL) divergence between the learned parameters (posterior distribution) \( B = (W_k)_{k=1}^L \) and a reference (prior distribution) \( B^p = (W_k^p)_{k=1}^L \) which is independent of the training data. By using isotropic Gaussians for both the prior and the posterior, the KL divergence is easily obtained with
\[
\text{KL}(B\|B^p) = \frac{1}{2} \sum_{k=1}^L \|W_k - W_k^p\|^2.
\]

The PAC-Bayes theorem below is borrowed from Letarte et al. [10], which itself is a variation from a seminal result from Catoni [24], but has the major advantage to directly deal with the trade-off between the empirical loss and the KL divergence (i.e., the value of \( C \) in Equation (4.3) is the one minimizing the bound).

**Theorem 2.** Given a data independent prior distribution \( B^p \) and \( \delta \in (0, 1) \), with probability at least \( 1 - \delta \) over a realization of the learning sample \( S \sim D^n \), then, for all posterior \( B \):
\[
\mathcal{L}_D(F_A) \leq \inf_{C > 0} \left\{ \frac{1}{1 - e^{-\delta}} \left( 1 - \exp \left[ -C \hat{\mathcal{L}}_S(F_A) - \frac{1}{n} \left( \text{KL}(B\|B^p) + \ln \left( \frac{2n}{\delta} \right) \right) \right] \right\}.
\]

A salient feature of the PAC-Bayesian bounds is that they are uniformly valid (with probability at least \( 1 - \delta \)) for the whole family of posterior. This is particularly suited for the design of a bound minimization algorithm, as the right-hand side of Equation (4.3) suggests an objective to minimize, and is providing a generalization guarantee even when the optimization procedure does not converge to a global minimum. Thus, we propose to train the ABNet architecture by minimizing the bound given in Theorem 2 by stochastic gradient descent. That is, the following objective is optimized according to parameters \( B \) and \( C > 0 \):
\[
\frac{1}{1 - e^{-\delta}} \left( 1 - \exp \left[ -C \hat{\mathcal{L}}_S(F_A) - \frac{1}{n} \left( \text{KL}(B\|B^p) + \ln \left( \frac{2n}{\delta} \right) \right) \right] \right).
\]

Although this objective may appear similar to the ones of previous PAC-Bayes analyses, the proposed ABNet objective differs in two noticeable ways:

1. The predictor output, and therefore the empirical loss of Equation (4.1), corresponds to the exact BAM expectation and is computed thanks to the forward propagation routine of ABNet, instead of the more classical computational graph of Letarte et al. [10] or the approximation scheme of Biggs and Guedj [11].
2. The KL divergence of Equation (4.2), acting as a regularization term, does give the same penalty to weights of every layer in ABNet for networks of depth \( L \geq 2 \). In contrast, the corresponding term in PBGNet [10] penalizes weights by a growing factor according to the layer depth.

---

2 Following the common practice [10, 11, 18, 21], we chose an SGD random initialization as \( B^p \).
5. Compacting the ABNet

Recall from Section 3 that the aggregation output can be computed by the matrix product $F_A(B)(x) = \{1, -1\} \cdot (\Psi_L(\Psi_{L-1}(\ldots \Psi_3(\Psi_2 P_1(x) \ldots)))$, with $(\Psi_k)_{k=2}^{L}$ and $P_1(x)$ computed from parameters $B = (W_k)_{k=1}^{L}$ according to Equations (3.2) and (3.3). From this point of view, ABNet simply computes a linear function of the leading hidden layer representation $P_1(x)$, highlighting a limitation of all binary (and discrete-valued) activated neural networks. Indeed, all matrices $\Psi_k$ are solely based on the weights and do not rely on the input layer. Since there is no activation function between hidden layers, dot product associativity allows us to state the following.

**Proposition 3.** The output of an aggregation of BAMs $A(B)$, where $B$ has leading hidden layer width of $d_1$ and arbitrary width for other hidden layers, can be obtained by forward propagating in a compact (with regard to depth) neural network having a leading hidden layer of width $2^{d_1}$ with erf activation and an output layer of width 1 with identity activation:

$$F_A(x) = H \cdot P_1(x),$$

where $P_1(x)$ is a vector of $2^{d_1}$ elements defining a probability distribution on the outputs of the leading hidden layer of $B$ on $x$, and $H \in [-1, 1]^{2^{d_1}}$ is a vector giving the expected output of the rest of the network given the output of the first layer, such that

$$H = [1, -1] \cdot \Psi_L \cdot \Psi_{L-1} \cdot \ldots \cdot \Psi_3 \cdot \Psi_2 .$$

Since only $P_1(x)$ changes in function of $x$, for fixed weights one can numerically precompute $H := [h_s]_{s \in R_1}$ once and for all $x$. In the underlying BAM this is analogous to precomputing the output for every representation outputted by the leading hidden layer. Every entry of $H$ is a real number between $-1$ and 1 since it represents an expectation on a BAM output. This observation leads us to the following corollary.

**Corollary 4.** Notwithstanding the fact that the underlying BAM architecture can be arbitrarily deep, the aggregation output can always be expressed in the following shallow form, with $h_s \in [-1, 1]$: 

$$F_A(x) = \sum_{s \in R_1} h_s \prod_{i=1}^{d_1} \left( \frac{1}{2} + \frac{s^i}{2} \text{erf} \left( \frac{W_i \cdot x}{\sqrt{2} \| x \|} \right) \right) .$$

Thus, forward propagation of ABNet can be computed in time constant with regard to $L$.

We call the algorithm that computes Equation (5.3) the **Compact ABNet**. See Fig. 1c for a visual representation. Interestingly, the PAC-Bayes generalization bound of Theorem 2 is not obtainable directly from the Compact ABNet parameters. Therefore, our bound minimization algorithm requires the ABNet architecture. Noteworthy, our empirical experiments (Section 6, Fig. 4) show that training deeper ABNet can achieve better generalization than a shallower architecture, even when both share a Compact architecture of the same size. Compacting our stochastic version is also possible. Since the dot product must be executed on fixed $R_s$, the drawn samples must be predetermined and remain the same at each inference; this leads to a very concise classifier which performs just as well as the last learned Stochastic ABNet. As can be seen on Fig. 2b, compact networks are much faster at inference time than their deep equivalent, as their complexity does not increase with depth.

Our original approach of propagating probabilities over representations is what brings the light on the compactability phenomenon. It is a well-known result that any function can be approximated to an arbitrary level of accuracy with a neural network having as few as one hidden layer, given that the layer is wide enough [25]. It has also been shown that a shallow "student" network can learn to mimic a deep "teacher" network to reach the same performance level [1]. However, typical neural networks do not allow such an explicit
For all \( x \), the probabilities of outputting a specific representation at the leading hidden layer, obtained from \( P_1(x) \), multiplied by the expected output for each of these regions, given by \( H \).

The aggregation output \( F_{A(B_M)}(x) \) for all \( x \), obtained by summing over representations. Using \( ABNet \) as a classifier, one can simply use \( \text{sgn}(F_{A(B_M)}(x)) \) as the prediction for an input \( x \).

Using the \( BAM \) classifier from the MAP \( F_{B_M}(x) \), the decision boundary is less expressive.

Figure 3. Predictions of an \( ABNet \) and its underlying \( BAM \) with architecture \( ⟨2, 2, 2, 1⟩ \), i.e., with two-dimensional inputs and two hidden layers of two neurons, on a toy dataset.

construction that maps an initially (non-linear) deep structure to a shallow form. The result of Proposition 3 is a curiosity that is worth analyzing further. Remarkably, there is a clear dichotomy between the roles of \( P_1(x) \) and \( H \): the former transforms data points into a probability distribution over the leading hidden layer representations, whereas the latter gives the aggregation output for each of those representations. Put otherwise, the first layer serves as an embedding and the rest of the layers operate as a classifier. Fig. 3 illustrates the particularity of the prediction mechanism of \( ABNet \).

**The leading hidden layer.** Equation (5.1) implies that the leading hidden layer defines regions in the input space. All subsequent hidden layers together express the output value of these regions. Fig. 3a shows how those regions divide the input space on the toy problem. Each region is associated with one of the four leading hidden layer binary representation.

Each neuron of the leading hidden layer of a \( BAM \) defines a hyperplane in the input space, where inputs on one side are mapped to \(-1\), and \(1\) on the other side. Considering all regions that are enclosed between the hyperplanes yields up to \(2^{d_1} \) regions, corresponding to the \(2^{d_1} \) output representations \( R_1 \). Many of those regions may stray very far from the actual data. For example, in Fig. 3a the region corresponding to representation \((1, -1)\) exists on the other side of where the two planes meet, which is far from any existing data.

**Additional hidden layers.** The vector \( H \) represents by extension a function from \((-1, 1)^{d_1} \) to \([-1, 1] \). Its role is to determine what sign should be outputted for each region defined by the leading hidden layer, with a confidence term. Its content is not arbitrary since it must be obtained from the weights of the subsequent hidden layers as in Equation (5.2). Depth therefore adds expressivity to \( BAM \) aggregations by allowing regions created by the leading hidden layer to output uncorrelated signs, with more or less confidence.

As illustrated by Figures 3c–d, taking the output of \( ABNet \) is not equivalent as taking the output of its associated \( MAP \). For the same parameters, the aggregation allows more complex

---

3By considering the few most important region, one could potentially interpret \( ABNet \) predictions more easily than for classical neural networks. We consider this question as future work, and refer the reader to Montúfar, Pascanu, Cho, and Bengio [26] for a study of regions in the broader context of neural networks with continuous activations.
regions than BAMs, taking advantage that an input can belong to several regions, with certain probabilities; there exist points $x$ and parameters $B_M$ for which $\text{sgn}(F_A(B_M)(x)) \neq F_{B_M}(x)$. For instance, many incorrectly classified $-1$ data points in Fig. 3d fall within the correct region in Fig. 3c because ABNet can compensate the proximity to the central $+1$ region with a lesser proximity with two $-1$ regions. It is therefore worthy to use the aggregation as a predictor by itself instead of its MAP, for its expressive power. Indeed, Zhu, Dong, and Su [27] observe that ensemble methods on binary neural networks confer stability with regard to input and parameter perturbations, which leads to better generalization.

6. Numerical experiments

We evaluated our proposed approach ABNet by following the experimental framework of Letarte, Germain, Guedj, and Laviolette [10], on the same six binary classification datasets: $ads$ and $adult$ from the UCI repository [16], along with four MNIST [28] binary variants $mnistLH$ (labels $\{0, 1, 2, 3, 4\}$ form the "Low" class, and $\{5, 6, 7, 8, 9\}$ the "High" class), $mnist17$, $mnist49$ and $mnist56$ (only examples labeled respectively $1&7$, $4&9$, and $5&6$ are retained).\(^4\) As the exact versions of PBGNet and ABNet are limited by their exponential complexity regarding their width, we explored narrow network architectures (widths $d \in \{2, 4, 8\}$) and wider architectures (widths $d \in \{10, 50, 100\}$) accessible only to stochastic versions, all for 1 to 3 hidden layers. All experiments were repeated with 5 different random train/test dataset splits and weights initializations. Networks parameters are optimized using Adam [29] for the following learning rate values: $\{0.1, 0.01, 0.001, 0.0001\}$. Training is performed for 100 epochs with early stopping after 20 epochs without improvement.

We first compare ABNet to its direct counterpart PBGNet [10], both directly optimizing the PAC-Bayesian generalization bound during learning, with the prior distribution defined by the network weights random initialization. We also explore the minimization of the empirical loss with the variants ABNet$^\ell$ (Eq. 4.1) and PBGNet$^\ell$, where 20% of the training data is used as a validation set for model selection.

Even if our primary focus is on the learning of a BAM aggregation, the optimization procedure of PBGNet and ABNet may be used to learn a single BAM, as it is not itself learnable with standard gradient descent methods. We thus compare the Maximum-A-Posteriori (MAP) networks of both aggregated methods to three algorithms of the literature for learning neural networks with binary weights and/or activations: Expectation Backpropagation [9] (EBP) with real-valued weights and binary activations, Binarized Neural Network [8] (BNN) with both binary weights and activations, and BinaryConnect [7] (BC) with binary weights.

\(^4\)We conducted PBGNet experiments using the publicly available source code of Letarte et al. [10]. We did not perform experiments using the approximation scheme of Biggs and Guedj [11] as their code has not been made public. Moreover, the experiments of the latter were performed solely on $mnistLH$ dataset, showing similar accuracy than PBGNet for a similar architecture.

Figure 4. Impact of depth for PBGNet (dashed) and ABNet (solid) on test errors and bound values according to the width for mnistLH datasets. Results correspond to means and standard deviations over 5 repetitions.
<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>Narrow architectures</th>
<th>Wide architectures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>$L-1$ $d$ Bound</td>
<td>$Error_{test}$</td>
</tr>
</tbody>
</table>
| ads     | PBGNet & ABNet | 3 2 0.192 0.140 0.141 ± 0.012 0.141 | 3 10 0.213 0.140 0.141 ± 0.010 0.141 | 3 2 0.192 0.140 0.141 ± 0.012 0.141 | 2 10 0.216 0.140 0.141 ± 0.010 0.141 | | 3 4 0.887 0.015 0.026 ± 0.003 0.026 | 2 50 1.000 0.12 0.13 ± 0.005 0.025 | 2 2 0.003 0.040 ± 0.008 0.054 | 3 10 0.005 0.033 ± 0.006 0.049 | \ | BC | 1 4 - 0.025 0.031 ± 0.004 0.031 | 1 10 - 0.021 0.032 ± 0.005 0.032 | | \ | BNN | 1 8 - 0.037 0.038 ± 0.004 0.038 | 1 100 - 0.029 0.032 ± 0.005 0.032 | | \ | adult | PBGNet & ABNet | 3 4 0.723 0.135 0.149 ± 0.002 0.156 | 3 10 0.360 0.141 0.154 ± 0.002 0.151 | 3 10 0.143 0.154 ± 0.002 0.151 | 2 10 0.360 0.141 0.154 ± 0.002 0.151 | | ABNet | 3 4 0.780 0.132 0.149 ± 0.003 0.150 | 1 10 0.143 0.154 ± 0.002 0.151 | 1 10 0.143 0.154 ± 0.002 0.151 | | EBP | 1 8 - 0.145 0.152 ± 0.003 0.166 | 2 100 - 0.049 0.186 ± 0.001 0.189 | | \ | BC | 1 8 - 0.142 0.151 ± 0.002 0.151 | 1 50 - 0.160 0.164 ± 0.001 0.164 | | \ | BNN | 1 2 - 0.180 0.182 ± 0.017 0.182 | 1 100 - 0.157 0.165 ± 0.002 0.165 | | | mnist17 | PBGNet & ABNet | 3 2 0.036 0.005 0.006 ± 0.001 0.006 | 1 10 0.041 0.005 0.006 ± 0.001 0.006 | 3 10 0.041 0.005 0.006 ± 0.001 0.006 | 2 10 0.041 0.005 0.006 ± 0.001 0.006 | | ABNet | 3 2 0.036 0.005 0.006 ± 0.001 0.006 | 1 10 0.041 0.005 0.006 ± 0.001 0.006 | 1 10 0.041 0.005 0.006 ± 0.001 0.006 | | EBP | 1 8 - 0.000 0.006 ± 0.001 0.006 | 2 10 - 0.000 0.005 ± 0.000 0.005 | | \ | BNN | 1 8 - 0.000 0.008 ± 0.001 0.008 | 1 100 - 0.004 0.007 ± 0.001 0.007 | | \ | mnist49 | PBGNet & ABNet | 1 2 0.136 0.036 0.036 ± 0.004 0.036 | 1 10 0.149 0.037 0.037 ± 0.004 0.036 | 1 10 0.149 0.037 0.037 ± 0.004 0.036 | 1 10 0.149 0.037 0.037 ± 0.004 0.036 | | ABNet | 1 2 0.136 0.036 0.036 ± 0.004 0.036 | 1 10 0.147 0.038 0.037 ± 0.004 0.036 | 1 10 0.147 0.038 0.037 ± 0.004 0.036 | | EBP | 3 8 1.000 0.004 0.017 ± 0.003 0.017 | 3 10 1.000 0.024 0.029 ± 0.003 0.027 | 3 10 1.000 0.024 0.029 ± 0.003 0.027 | | \ | BNN | 3 8 - 0.020 0.033 ± 0.003 0.034 | 3 50 - 0.001 0.021 ± 0.004 0.026 | | \ | mnist56 | PBGNet & ABNet | 1 2 0.084 0.021 0.023 ± 0.006 0.023 | 1 10 0.090 0.023 0.025 ± 0.003 0.024 | 1 10 0.090 0.023 0.025 ± 0.003 0.024 | 1 10 0.090 0.023 0.025 ± 0.003 0.024 | | ABNet | 1 2 0.084 0.021 0.023 ± 0.006 0.023 | 1 10 0.090 0.023 0.025 ± 0.003 0.024 | 1 10 0.090 0.023 0.025 ± 0.003 0.024 | | EBP | 3 8 1.000 0.004 0.011 ± 0.003 0.011 | 1 10 0.097 0.003 0.008 ± 0.002 0.038 | 1 10 0.097 0.003 0.008 ± 0.002 0.038 | | \ | BNN | 3 8 - 0.001 0.010 ± 0.004 0.015 | 2 10 - 0.000 0.019 ± 0.004 0.021 | | \ | mnistLH | PBGNet & ABNet | 1 8 0.186 0.091 0.092 ± 0.036 0.093 | 1 10 0.167 0.058 0.059 ± 0.010 0.060 | 1 10 0.167 0.058 0.059 ± 0.010 0.060 | 1 10 0.167 0.058 0.059 ± 0.010 0.060 | | ABNet | 3 8 0.162 0.056 0.058 ± 0.002 0.059 | 2 10 0.187 0.087 0.088 ± 0.006 0.087 | 2 10 0.187 0.087 0.088 ± 0.006 0.087 | | EBP | 3 8 0.099 0.025 0.042 ± 0.006 0.043 | 3 10 0.095 0.050 0.060 ± 0.005 0.058 | 3 10 0.095 0.050 0.060 ± 0.005 0.058 | | \ | BNN | 3 8 - 0.016 0.043 ± 0.002 0.082 | 1 100 - 0.011 0.027 ± 0.001 0.032 | | \ | but ReLU activations. Experiments involving EBP, BNN or BC are performed using fully connected networks, following the procedure used for ABNet and PBGNet.

**Narrow architectures.** The PAC-Bayesian inspired models with empirical loss minimization (PBGNet & ABNet) obtain competitive error rates (similar to the results achieved by BC using ReLU activations and binary weights). However, the empirical loss minimization procedure lead to non-informative generalization bounds values. When considering the bound for optimization and model selection for PBGNet and ABNet, selected network architectures are smaller with usually a single hidden layer, as the objective function contains a regularization term on the weight values (see Eq. 4.4), and the error rates grow while bound values improve to a relevant level. Also, bound minimization algorithms are far
less prone to overfitting than traditional optimization schemes, as their training errors are remarkably close to their testing errors (recall that PBGNet and ABNet are equivalent for one hidden layer). On the larger and harder dataset mnistLH, the narrow ABNet achieves better error rate and bound value than PBGNet by selecting a deeper architecture thanks to its less penalizing KL divergence regularization. On the performances of the MAP induced BAM networks, error rates are usually similar or slightly higher than their aggregated counterpart, implying these approaches are suitable algorithms to learn BAM networks.

**Wide architectures.** For all algorithms and most datasets, obtained results for wide and narrow binary neural networks are surprisingly similar. This reveals that constraining ABNet’s width to compute the exact aggregation output is not a major caveat. In particular, when one seeks tight PAC-Bayesian guarantees, lower complexity of narrow models should be favored. That being said, the proposed stochastic training for ABNet enables scaling to wider networks. While achieving most of the time comparable results to the stochastic PBGNet, the obtained risk on the large mnistLH dataset suggests that the approximation scheme of ABNet may not be as effective as the exact computation.

**Deep architectures.** A key improvement of ABNet over PBGNet is the KL divergence computation which is not hindered by a growing factor penalizing the weights according to the network depth. This property should allow ABNet to learn deeper networks with tighter generalization bounds, which we investigated on the mnistLH dataset by extending the main experiment up to 8 hidden layers. Results are presented in Figure 4 where the difference of behaviour between the models is clearly highlighted. For a small number of hidden layers, the performances are similar, but as the number of hidden layer grows, bound values for PBGNet sharply rise and test error rates degrade significantly. On the other hand, bound values are relatively stable for ABNet, indicating its potential to learn deep neural network architectures (the minimum bound is achieved for 3 hidden layers of width 4, which adequately indicates the best test error).

7. Conclusion

Many desirable properties stem from considering a PAC-Bayesian analysis of aggregations over binary activated networks. Like the previous approaches on which we build [10, 11], our proposed learning algorithm gives a sensible way to optimize the parameters of such networks, and provides tight bounds on the generalization error of deep architectures. The originality of our work lies in the focus on the exact computation of aggregation of narrow networks, for which we derive an atypical training scheme based on the propagation of probabilities over hidden layer representations. We further extend the analysis to expose the dichotomy between the first layers versus the others. We believe the latter observation is a sensible tool to understand the expressivity conferred by a network's architecture. Pursuing this research direction could contribute to a line of work [30–32] studying the role of depth in neural networks, but in the context of model aggregation. An interesting perspective is to consider more complex distributions over the network parameters.

**References**