On the generalization of bayesian deep nets for multi-class classification

Yossi Adi 1 Yaniv Nemcovsky 2 Alex Schwing 3 Tamir Hazan 2

Abstract

Generalization bounds which assess the difference between the true risk and the empirical risk have been studied extensively. However, to obtain bounds, current techniques use strict assumptions such as a uniformly bounded or a Lipschitz loss function. To avoid these assumptions, in this paper, we propose a new generalization bound for Bayesian deep nets by exploiting the contractivity of the Log-Sobolev inequalities. Using these inequalities adds an additional loss-gradient norm term to the generalization bound, which is intuitively a surrogate of the model complexity. Empirically, we analyze the effect of this loss-gradient norm term using different deep nets.

1. Introduction

Deep neural networks are ubiquitous across disciplines and often achieve state of the art results. Albeit deep nets are able to encode highly complex input-output relations, in practice, they do not tend to overfit (Zhang et al., 2016). This tendency to not overfit has been investigated in numerous works on generalization bounds. Indeed, many generalization bounds apply to composite functions specified by deep nets. However, most of these bounds assume that the loss function is bounded or Lipschitz. Unfortunately, this assumption excludes plenty of deep nets and Bayesian deep nets that rely on the popular negative log-likelihood (NLL) loss.

In this work we introduce a new PAC-Bayesian generalization bound for unbounded loss functions with unbounded gradient-norm, i.e., non-Lipschitz functions. This setting is closer to present-day deep net training, which uses the unbounded NLL loss and requires to avoid large gradient values during training so as to prevent exploding gradients. To prove the bound we utilize the contractivity of the log-Sobolev inequality (Ledoux, 1999). It enables to bound the moment-generating function of the model risk. Our PAC-Bayesian bound adds a novel complexity term to existing PAC-Bayesian bounds: the expected norm of the loss function gradients computed with respect to the input. Intuitively this norm measures the complexity of the loss function, i.e., the model. In our work we prove that this complexity term is sub-gamma when considering linear models with the NLL loss, or more generally, for any linear model with a Lipschitz loss function. We also derive a bound for any Bayesian deep net, which permits to verify empirically that this complexity term is sub-gamma. See Figure 1.

This new term, which measures the complexity of the model, augments existing PAC-Bayesian bounds for bounded or Lipschitz loss functions which typically consist of two terms: (1) the empirical risk, which measures the fitting of the posterior over the parameters to the training data, and (2) the KL-divergence between the prior and the posterior distribu-

Figure 1. The proposed bound as a function of $\lambda$ for both ResNet (top) and a Linear model (bottom). Notice, this suggests that the random variables $L_D(w) - L_S(w)$ for both ResNet and Linear models are sub-gamma (see Definition 1 and Theorem 1). We obtain the results for ResNet using CIFAR-10 dataset and for the Linear model using MNIST dataset. The parameter for the sub-gamma fit are $v = 1.0$ for both models and $c = 1e^{-5}$ for ResNet and $c = 1e^{-4}$ for the Linear model.
tions over the parameters, which measures the complexity of learning the posterior when starting from the prior over the parameters.

2. Related work

Generalization bounds for deep nets were explored in various settings. VC-theory provides both upper bounds and lower bounds to the network’s VC-dimension, which are linear in the number of network parameters (Bartlett et al., 2017b; 2019). While VC-theory asserts that such a model should overfit as it can learn any random labeling (e.g., Zhang et al. (2016)), surprisingly, deep nets generally do not overfit.

Rademacher complexity allows to apply data dependent bounds to deep nets (Bartlett & Mendelson, 2002; Neyshabur et al., 2015; Bartlett et al., 2017a; Golowich et al., 2017; Neyshabur et al., 2018). These bounds rely on the loss and the Lipschitz constant of the network and consequently depend on a product of norms of weight matrices which scales exponentially in the network depth. Wei & Ma (2019) developed a bound that considers the gradient-norm over training examples. In contrast, our bound depends on average quantities of the gradient-norm and thus we answer an open question of Bartlett et al. (2017a) about the existence of bounds that depend on average loss and average gradient-norm, albeit in a PAC-Bayesian setting. PAC-Bayesian bounds that use Rademacher complexity have been studied by Kakade et al. (2009); Yang et al. (2019).

Stability bounds may be applied to unbounded loss functions and in particular to the negative log-likelihood (NLL) loss (Bousquet & Elisseeff, 2002; Rakhlin et al., 2005; Shalev-Shwartz et al., 2009; Hardt et al., 2015; Zhang et al., 2016). However, stability bounds for convex loss functions, e.g., for logistic regression, do not apply to deep nets since they require the NLL loss to be a convex function of the parameters. Alternatively, Hardt et al. (2015) and Kuzborskij & Lampert (2017) estimate the stability of stochastic gradient descent dynamics, which strongly relies on early stopping. This approach results in weaker bounds for the non-convex setting. Stability PAC-Bayesian bounds for bounded and Lipschitz loss functions were developed by London (2017).

PAC-Bayesian bounds were recently applied to deep nets (McAllester, 2013; Dziugaite & Roy, 2017; Neyshabur et al., 2017). In contrast to our work, those related works all consider bounded loss functions. An excellent survey on PAC-Bayesian bounds was provided by Germain et al. (2016). Alquier et al. (2016) introduced PAC-Bayesian bounds for linear classifiers with the hinge-loss by explicitly bounding its moment generating function. Alquier et al. (2012) provide an analysis for PAC-Bayesian bounds with Lipschitz functions. Our work differs as we derive PAC-Bayesian bounds for non-Lipschitz functions. Work by Germain et al. (2016) is closer to our setting and considers PAC-Bayesian bounds for the quadratic loss function. In contrast, our work considers the multi-class setting, and non-linear models. PAC-Bayesian bounds for the NLL loss in the online setting were put forward by Takimoto & Warmuth (2000); Banerjee (2006); Bartlett et al. (2013); Grünwald & Mehta (2017). The online setting does not consider the whole sample space and therefore is simpler to analyze in the Bayesian setting.

PAC-Bayesian bounds for the NLL loss function are intimately related to learning Bayesian inference (Germain et al., 2016). Recently many works applied various posteriors in Bayesian deep nets. Gal & Ghahramani (2015); Gal (2016) introduce a Bayesian inference approximation using Monte Carlo (MC) dropout, which approximates a Gaussian posterior using Bernoulli dropout. Srivastava et al. (2014); Kingma et al. (2015) introduced Gaussian dropout which effectively creates a Gaussian posterior that couples between the mean and the variance of the learned parameters and explored the relevant log-uniform priors. Blundell et al. (2015); Louizos & Welling (2016) suggest to take a full Bayesian perspective and learn separately the mean and the variance of each parameter.

3. Background

Generalization bounds provide statistical guarantees on learning algorithms. They assess how the learned parameters $w$ of a model perform on test data given the model’s result on the training data $S = \{(x_1, y_1), \ldots, (x_m, y_m)\}$, where $x_i$ is the data instance and $y_i$ is the corresponding label. The performance of the parametric model is measured by a loss function $\ell(w, x, y)$. The risk of this model is its average loss, when the data instance and its label are sampled from the true but unknown distribution $D$. We denote the risk by $L_D(w) = \mathbb{E}_{(x,y) \sim D}\ell(w, x, y)$. The empirical risk is the average training set loss $L_S(w) = \frac{1}{m} \sum_{i=1}^m \ell(w, x_i, y_i)$.

PAC-Bayesian theory bounds the expected risk $\mathbb{E}_{w \sim q}L_D(w)$ of a model when its parameters are averaged over the learned posterior distribution $q$. The parameters of the posterior distribution are learned from the training data $S$. In our work we start from the following PAC-Bayesian bound:

**Theorem 1** (Alquier et al. (2016)). Let $KL(q||p) = \int q(w) \log(q(w)/p(w))dw$ be the KL-divergence between two probability density functions $p, q$. For any $\lambda > 0$, for any $\delta \in (0,1]$ and for any prior distribution $p$, with probability at least $1 - \delta$ over the draw of the training set $S$, the following holds simultaneously for any posterior distribution $q$: $\mathbb{E}_{w \sim q}[L_D(w)] \leq \mathbb{E}_{w \sim q}[L_S(w)] + \frac{C(\lambda, p) + KL(q||p) + \log(1/\delta)}{\lambda}$, (1)
where

\[ C(\lambda, p) = \log \mathbb{E}_{w \sim p, S \sim D}[e^{\lambda(L_D(w) - L_S(w))}]. \]  

Unfortunately, the complexity term \( C(\lambda, p) \) of this bound is impossible to compute for large values of \( \lambda \), as we show in our experimental evaluation. To deal with this complexity term, Alquier et al. (2016); Germain et al. (2016); Boucheron et al. (2013) consider the sub-Gaussian assumption, which amounts to the bound \( C(\lambda, p) \leq \frac{\lambda^2 v}{2(1 - \lambda c)} \) for any \( \lambda \in \mathbb{R} \) and some variance factor \( v \). This assumption is also referred to as the Hoeffding’s lemma, which is related to Hoeffding’s lemma that is usually applied in PAC-Bayesian bounds to loss functions that are uniformly bounded by a constant, i.e., for any \( w, x, y \) simultaneously.

Unfortunately, many loss functions that are used in practice are unbounded. In particular, the NLL loss function is unbounded even in the multi-class setting when \( y \) is discrete. For instance, consider a fully connected deep net, where the input vector of the \( k \)-th layer is a function of the parameters of all previous layers, i.e., \( x_k(W_0, \ldots, W_{k-1}) \). The entries of \( x_k \) are computed from the response of its preceding layer, i.e., \( W_{k-1}x_{k-1} \), followed by a transfer function \( \sigma(\cdot) \), i.e., \( x_k = \sigma(W_{k-1}x_{k-1}) \). Since the NLL is defined as \( -\log p(y|x, w) = -(W_kx_k)_y + \log(\sum_y e^{(W_kx_k)_y}) \), the NLL loss increases with \( r \) and is unbounded when \( r \to \infty \) if the rows in \( W_k \) consist of the vector \( r_1 \).

In our experimental validation in Section 5 we show that the unboundedness of the NLL loss results in a complexity term \( C(\lambda, p) \) that is not sub-Gaussian.

This complexity term \( C(\lambda, p) \) influences the value of \( \lambda \), which controls the convergence rate of the bound, as it weighs the complexity terms \( C(\lambda, p) \) and \( KL(q||p) \) by \( \frac{\lambda}{c} \). Therefore, a tight bound requires \( \lambda \) to be as large as possible. However, since \( \lambda \) influences \( C(\lambda, p) \) exponentially, one needs to make sure that \( C(\lambda, p) < \infty \). In such cases one may use sub-gamma random variables (Alquier et al., 2016; Germain et al., 2016; Boucheron et al., 2013):

**Definition 1.** The random variable \( L_D(w) - L_S(w) \) is called sub-gamma if the complexity term \( C(\lambda, p) \) in Theorem 1 satisfies \( C(\lambda, p) \leq \frac{\lambda^2 v}{2(1 - \lambda c)} \) for every \( \lambda \) such that \( 0 < \lambda < 1/c \).

In Corollary 1 we prove that the complexity term \( C(\lambda, p) \) is sub-gamma when considering linear models with the NLL loss, or more generally, for any linear model with a Lipschitz loss function. In Corollary 2 we derive a bound on \( C(\lambda, p) \) for any Bayesian deep net, which permits to verify empirically that \( C(\lambda, p) \) is sub-gamma.

### 4. PAC-Bayesian bounds for smooth loss functions

Our main theorem below shows that for smooth loss functions, the complexity term \( C(\lambda, p) \) is bounded by the expected gradient-norm of the loss function with respect to the data \( x \). This property is appealing since the gradient-norm contracts the network’s output, as evident in its extreme case by the vanishing gradients property. In our experimental evaluation we show how this contractivity depends on the depth of the network and the variance of the prior and its affect on the generalization of Bayesian deep nets.

**Theorem 2.** Consider the setting of Theorem 1 and assume \((x, y) \sim D, x \) given \( y \) follows the Gaussian distribution and \( \ell(w, x, y) \) is a smooth loss function (e.g., the negative log-likelihood loss). Let \( M(\alpha) \triangleq \mathbb{E}_{(x, y) \sim D} e^{\alpha \ell(w, x, y)} \). Then \( C(\lambda, p) \leq \)

\[
\log \mathbb{E}_{w \sim p} e^{2\lambda \mathbb{E}_{(x, y) \sim D} \|\nabla_x \ell(w, x, y)\|^2} \leq \frac{\lambda^2}{2c} \mathbb{E}_{(x, y) \sim D} e^{2\alpha \ell(w, x, y)}
\]  

Our proof technique to show the main Theorem uses the log-Sobolev inequality for Gaussian distributions (Ledoux, 1999) as we illustrate next.

**Proof.** The proof consists of three steps. First we use the statistical independence of the training samples to decompose the moment generating function

\[
\mathbb{E}_{S \sim D} [e^{\lambda(L_D(w) - L_S(w))}] = e^{\lambda L_D(w)} M\left(\frac{\lambda}{m}\right)^m.
\]  

Next we consider the moment generating function \( M\left(\frac{\lambda}{m}\right) \triangleq \mathbb{E}_{(x, y) \sim D} e^{\frac{\lambda}{m} \ell(w, x, y)} \) in its log-space, i.e., by considering the cumulant generating function \( K(\alpha) \triangleq \frac{1}{\alpha} \log M(\alpha) \) and obtain the following equality:

\[
M\left(\frac{\lambda}{m}\right) = e - \frac{\lambda}{m} L_D(w) - \frac{\lambda}{m} J_0 \frac{\alpha M(\alpha) - M(\alpha) \log M(\alpha)}{\alpha^2 M(\alpha)} d\alpha.
\]  

Finally we use the log-Sobolev inequality for Gaussian distributions, \( \alpha M'(\alpha) - \alpha^2 M(\alpha) \log M(\alpha) \leq 0 \) and complete the proof through some algebraic manipulations.

The first step of the proof results in Eq. (4). To derive it we use the independence of the training samples:

\[
\mathbb{E}_{S \sim D} [e^{\lambda(L_D(w) - L_S(w))}] = e^{\lambda L_D(w)} \mathbb{E}_{S \sim D} [e^{\lambda \sum_{i=1}^m \ell(w, x_i, y_i)}] = e^{\lambda L_D(w)} \prod_{i=1}^m \mathbb{E}_{(x_i, y_i) \sim D} [e^{\frac{\lambda}{m} \ell(w, x, y)}] = e^{\lambda L_D(w)} \left( \mathbb{E}_{(x, y) \sim D} [e^{\frac{\lambda}{m} \ell(w, x, y)}] \right)^m.
\]

On the generalization of bayesian deep nets
The first equality holds since \( e^{\lambda L_D(w)} \) is a constant that is independent of the expectation \( S \sim D^m \). The last equality holds since \((x_i, y_i) \sim D\) are identically distributed.

The second step of the proof results in Eq. (5). It relies on the relation of the moment generating function and the cumulant generating function \( M(\frac{\lambda}{m}) = \hat{m}_k(\frac{\lambda}{m}) \). The fundamental theorem of calculus asserts \( K(\frac{\lambda}{m}) = K(0) = \int_0^{1/m} K'(\alpha) \, d\alpha \), while \( K'(\alpha) \) refers to the derivative at \( \alpha \).

We then compute \( K'(\alpha) \) and \( K(0) \):

\[
K'(\alpha) = \frac{\alpha M'(\alpha) - M(\alpha) \log M(\alpha)}{\alpha^2 M(\alpha)}, \quad (10)
\]

\[
K(0) = \lim_{\alpha \to 0^+} \frac{\log M(\alpha)}{\alpha} = -L_D(w). \quad (11)
\]

The second equality follows from l'Hopital rule: \( \lim_{\alpha \to 0^+} \log M(\alpha) = \lim_{\alpha \to 0^+} \frac{M'(\alpha)}{M(\alpha)} \) and recalling that \( M(0) = 1 \) and \( M'(0) = -L_D(w) \).

The third and final step of the proof begins with applying the log-Sobolev inequality in Eq. (6) for Gaussian distributions. Combining it with Eq. (5) leads to the inequality \( \frac{\alpha}{m} \leq \int_0^{\frac{1}{m}} e^{\frac{\alpha}{m} L_D(w) + \frac{\alpha^2}{2} \int_0^{\frac{1}{m}} 2 e^{-\alpha e^{(w,x,y)}} \alpha^2 \| \nabla_x e^{(w,x,y)} \|^2 \, d\alpha} \).

\[
e^{-\frac{\alpha}{m} L_D(w)} e^{\frac{\alpha^2}{2} \int_0^{\frac{1}{m}} e^{-\alpha e^{(w,x,y)}} \alpha^2 \| \nabla_x e^{(w,x,y)} \|^2 \, d\alpha}. \quad (13)
\]

This is compelling because the \( e^{-\lambda L_D(w)} \) term in the above inequality cancels with the term \( e^{\lambda L_D(w)} \) in Eq. (4). This shows theoretically why the complexity term mostly depends on the gradient-norm. This observation also concludes the proof after rearranging terms. □

The above theorem can be extended to settings for which \( x \) is sampled from any log-concave distribution, e.g., the Laplace distribution, cf. Gentil (2005). For readability we do not discuss this generalization here.

Eq. (4) hints at the infeasibility of computing the complexity term \( C(\lambda, p) \) directly for large values of \( \lambda \); since the loss function is non-negative, the value of \( e^{\lambda L_D(w)} \) grows exponentially with \( \lambda \), while \( e^{\frac{\lambda}{m}} \approx \frac{\lambda}{m} \) diminishes to zero exponentially fast. These opposing quantities make evaluation of \( C(\lambda, p) \) numerically infeasible. In contrast, our bound makes all computations in log-space, hence its computation is feasible for larger values of \( \lambda \), up to their sub-gamma interval \( 0 < \lambda < 1/\epsilon \), see Table 1.

Notably, the general bound in Theorem 2 is more theoretical than practical: to estimate it in practice one needs to avoid the integration over \( \alpha \). However, it is an important intermediate step to derive a practical bound for linear models with Lipschitz loss function, and a general bound for any smooth loss function as we discuss in the next two sections respectively.

### 4.1. Linear models

In the following we consider smooth loss functions over linear models in the multi-class setting, where \( x \in \mathbb{R}^d \) is the data instance, \( y \in \{1, \ldots, k\} \) are the possible labels and the loss function takes the form \( \ell(w, x, y) = \ell(Wx, y) \). We also assume that \( \ell(t, y) \) is a Lipschitz function, i.e., \( \| \nabla \ell(t, y) \| \leq L \). Included in these assumptions are the popular NLL loss \( \log(-\ell(p(x, y)|x = -\langle Wx, y \rangle + \log(\sum_y e^{\langle Wx, y \rangle}) \) that is used in logistic regression and the multi-class hinge loss \( \max_y \{ \langle Wx, y \rangle - \langle Wx, y \rangle \} \) that is used in support vector machines (SVMs).

**Corollary 1.** Consider smooth loss functions over linear models \( \ell(w, x, y) = \ell(Wx, y) \), with Lipschitz constant \( L \), i.e., \( \| \nabla \ell(t, y) \| \leq L \). Under the conditions of Theorem 2 with Gaussian prior distribution \( p \sim N(0, \sigma_p) \) and variance \( \sigma_p^2 \) for which \( \lambda \leq \sqrt{\frac{m}{8}} / L \sigma_p \), we obtain \( C(\lambda, p) \leq kd \log(2) \).

**Proof.** This bound is derived by applying Theorem 2. We begin by realizing the gradient of \( \ell(Wx, y) \) with respect to \( x \). Using the chain rule, \( \nabla_x \ell(Wx, y) = W^\top \nabla_{Wx} \ell(Wx, y) \).

Hence, we obtain for the gradient norm \( \| \nabla_x \ell(Wx, y) \| \leq \| \nabla \ell(Wx, y) \| \| W^\top \| \leq L^2 \sum_{y=1}^k \sum_{j=1}^d w_{y,j}^2 \leq L^2 \sum_{y=1}^k \sum_{j=1}^d w_{y,j}^2 \).

Plugging this result into Eq. (3) we obtain the following bound for its exponent:

\[
\mathbb{E}_{(x,y) \sim D} \left[ \| \nabla_x \ell(w, x, y) \|^2 \right] \leq \lambda L_D(w) = \lambda L \log \left( \frac{1}{m} \right).
\]

Thus, for \( \lambda = \sqrt{\frac{m}{8}} / L \sigma_p \), the ratio in the integral equals one and the integral \( \int_0^\frac{\lambda}{m} e^{-\alpha} \, d\alpha = \frac{\lambda}{m} \). Combining these results we obtain:

\[
C(\lambda, p) \leq \log \left( \mathbb{E}_{w \sim p} e^{\frac{2x^2 L^2}{m} \sum_{y,j} w_{y,j}^2} \right).
\]

Finally, whenever \( \lambda L \sigma_p \leq \sqrt{\frac{m}{8}} \) we follow the Gaussian integral and derive the bound

\[
\mathbb{E}_{w \sim p} e^{\frac{2x^2 L^2}{m} \sum_{y,j} w_{y,j}^2} \leq \left( \frac{m}{m - 8L^2 \sigma_p^2} \right)^{kd}.
\]

□
The above corollary provides a PAC-Bayesian bound for classification using the NLL loss, and shows $C(\lambda, p)$ is sub-gamma in the interval $0 < \lambda < \sqrt{2m}/L\sigma_p$. Interestingly, it can achieve a rate of $\lambda = m$, albeit with variance of the prior of $1/m$. In our experimental evaluation we show that it is better to achieve lower rate, i.e., $\lambda = \sqrt{m}$ while using a prior with a fixed variance, i.e., $\sigma_p \approx 0.1$. The above bound also extends the result of Alquier et al. (2016) for binary hinge-loss to the multi-class hinge loss (cf. Alquier et al. (2016), Section 6). Unfortunately, the above bound cannot be applied to non-linear loss functions, since their gradient-norm is not bounded, as evident by the exploding gradients property in deep nets.

4.2. Non-linear models

In the following we derive a generalization bound for on-average bounded loss functions and on-average bounded gradient-norms.

**Corollary 2.** Consider smooth loss functions that are on-average bounded, i.e., $\mathbb{E}_{(x,y) \sim D}[\ell(w, x, y)] \leq b$. Under the conditions of Theorem 2, for any $0 < \lambda \leq m$ we obtain

$$C(\lambda, p) \leq \log \mathbb{E}_{w \sim p} e^{\frac{2\lambda^2 b}{m} \mathbb{E}_{(x,y) \sim D} \|\nabla_x \ell(w, x, y)\|^2}.$$  

(19)

**Proof.** This bound is derived by applying Theorem 2 and bounding $\int_0^1 e^{-\alpha \ell(w, x, y)} d\alpha \leq e^b$. We derive this bound in three steps:

- From $\ell(w, x, y) \geq 0$ we obtain $e^{-\alpha \ell(w, x, y)} \leq 1$.
- We lower bound $M(\alpha) \geq M(1)$ for any $0 \leq \alpha \leq \lambda/m$: First we note that $0 < \lambda \leq m$, therefore we consider $0 \leq \alpha \leq 1$. Also, since $\ell(w, x, y) \geq 0$ the function $e^{-\alpha \ell(w, x, y)}$ is monotonically decreasing in $\alpha$ within the unit interval, i.e., for $0 \leq \alpha_1 \leq \alpha_2 \leq 1$ there holds $e^{-(\alpha_2 - \alpha_1)\ell(w, x, y)} \geq e^{-(\alpha_2 - \alpha_1)\ell(w, x, y)}$ and consequently $M(\alpha) \geq M(1)$ for any $\alpha \leq 1$.
- The assumption $\mathbb{E}_{(x,y) \sim D}[\ell(w, x, y)] \geq -b$ and the monotonicity of the exponential function result in the lower bound $e^{\mathbb{E}_{(x,y) \sim D}[\ell(w, x, y)]} \geq e^{-b}$. From convexity of the exponential function, $M(1) = \mathbb{E}_{(x,y) \sim D} e^{-\ell(w, x, y)} \geq e^{\mathbb{E}_{(x,y) \sim D}[\ell(w, x, y)]}$ and the lower bound $M(1) \geq e^{-b}$ follows.

Combining these bounds we derive the upper bound

$$\int_0^1 e^{-\alpha \ell(w, x, y)} d\alpha \leq \int_0^1 e^{-\alpha}\frac{1}{e^{\lambda/p}} d\alpha = e^b,$$

and the result follows.

The above derivation upper bounds the complexity term $C(\lambda, p)$ by the expected gradient-norm of the loss function, i.e., the flow of its gradients through the architecture of the model. It provides the means to empirically show that $C(\lambda, p)$ is sub-gamma (see Section 5.3). In particular, we show empirically that the rate of the bound $\lambda$ can be as high as $m$, dependent on the gradient-norm. This is a favorable property, since the convergence of the bound scales as $1/\lambda$. Therefore, one would like to avoid exploding gradient-norms, as this effectively harms the true risk bound. While one may achieve a fast rate bound by forcing the gradient-norm to vanish rapidly, practical experience shows that vanishing gradients prevent the deep net from fitting the model to the training data when minimizing the empirical risk. In our experimental evaluation we demonstrate the influence of the expected gradient-norm on the bound of the true risk.

5. Experiments

In this section we perform an experimental evaluation of the our PAC-Bayesian bounds, both for linear models and non-linear models. We begin by verifying our assumptions:

(i) The PAC-Bayesian bound in Theorem 1 cannot be computed for large values of $\lambda$. (ii) Although the NLL loss is unbounded, it is on-average bounded. Next, we study the behavior of the complexity term $C(\lambda, p)$ for different architectures, both for linear models and deep nets. We show that the random variable $L_D(w) - L_S(w)$ is sub-gamma, namely that $C(\lambda, p) \leq \frac{\lambda^2 u}{2(1-\lambda/c)}$ for every $\lambda$ such that $0 < \lambda < 1/c$. Importantly, we show that $1/c$ which relates to the rate of convergence of the bound is determined by the architecture of the deep net. Lastly, we demonstrate the importance of $C(\lambda, p)$ in the learning process, balancing the three terms of (i) the empirical risk; (ii) the KL divergence; and (iii) the complexity term.

**Implementation details.** We use multilayer perceptrons (MLPs) for the MNIST and Fashion-MNIST dataset (Xiao et al., 2017). We use convolutional neural networks (CNNs) the CIFAR-10 dataset. In all models we use the ReLU acti-
Figure 3. Verifying the assumption in Corollary 2 that the loss function is on-average bounded, i.e., $\mathbb{E}_{(x,y) \sim D} \ell(w, x, y) \leq b$. We tested this assumption on MNIST (left), Fashion-MNIST (middle), using MLPs and CIFAR10 (right) using CNNs. The loss is on-average bounded, while being dependent on the variance of the prior. For variance up to 0.1, the loss is on-average bound is about 1.

Figure 4. Estimating $\mathbb{E}_{(x,y) \sim D} \left[ \| \nabla_x \ell(w, x, y) \|^2 \right]$ as a function of the different variance levels for the prior distribution $p$. Results are reported for MNIST (left), Fashion-MNIST (middle), using MLPs and CIFAR10 (right) using CNNs. The linear model has the largest expected gradient-norm, since the Lipschitz condition considers the worst-case gradient-norm, see Corollary 1. The gradient-norm gets smaller as a function of the depth, due to the vanishing gradient property. As a result, deeper nets can have faster convergence rate, i.e., use larger values of $\lambda$ can be used in the generalization bound.

Figure 5. The proposed bound as a function of $\lambda$ for MLP models using two, three, four, and five layers, depicted from left to right, (the left figure is for two layers, the second left is for three layers and so on). Notice, this suggests that the random variables $L_D(w) - L_S(w)$ for all presented MLP models are sub-gamma. We obtain the results for all models using the MNIST dataset. The parameter for the sub-gamma fit is $c = 1e-5$ for all models using different scaling factors.

We start by empirically demonstrating the numerical instability of computing the complexity term $C(\lambda, p)$ in Eq. 2. This numerical instability occurs due to the exponentiation of the random variables, namely $e^{N(L_D(w) - L_S(w))}$, which
Figure 6. Our bound on $C(\lambda, p)$ as a function of variance levels for the prior distribution over the models parameters, for $\lambda = \sqrt{m}$ (top) and $\lambda = m$ (bottom). One can see that the bound gets larger when the variance of the prior increases. This plot conforms the practice of Bayesian deep nets that set the variance of the prior up to 0.1. Notice, the five layers for the $\lambda = m$, it get value only for variance of 0.1, below that value the bound is zero, and above that value the bound explodes.

quickly goes to infinity as $\lambda$ grows. We estimated Eq. 2 over MNIST, for 5 MLPs of depth $d = 1, ..., 5$, where MLP of depth 1 is a linear model. For a fair comparison we changed layers’ width to reach roughly the same number of parameters in each model (except for the linear case). For these architectures evaluated $C(\lambda, p)$ for different values of $\lambda$, using variance of 0.1 over the prior distribution. The results are depicted in Figure 2. One can see that we are able to compute the complexity term $C(\lambda, p)$ for $\lambda \leq 25$ and even to smaller $\lambda$ for the linear model ($\lambda \leq 5$). Standard bounds for MNIST require $\lambda$ to be in the interval $\sqrt{m} < \lambda < m$, where $m$ is the training sample size ($m = 60,000$ for MNIST). We observe that while computing $C(\lambda, p)$ the term $e^{\lambda L_2(w)}$ goes to infinity while $e^{-\lambda L_2(w)}$ goes to zero, and they are not able to balance each other. In our derivation this is solved by looking at the gradient to emphasize their change, see Eq. (13).

In Corollary 2 we assume that although the loss is unbounded, it is on-average bounded, meaning $E_{(x, y) \sim \mathcal{D}}(\ell(w, x, y)) \leq b$. We tested this assumption on MNIST, Fashion-MNIST using MLPs of depth $d = 1, ..., 5$ and CIFAR10 using CNNs of depth $d = 2, ..., 5$, where for in the CNN models $d$ is the number of convolutional layers, and we include a max pool layer after each convolutional layer. In all CNN models we include an additional output layer to be a fully connected one. To span the possible weights we sampled them from a normal prior distribution with different variance. The results appear in Figure 3. We observe that the loss is on-average bounded by 10, while being dependent on the variance of the prior. Moreover, for variance up to 0.1, the on-average loss bound is about 1 and its affect on the complexity term $C(\lambda, p)$ is minimal. Notice, although the expected loss is increasing for high variance levels, these are not being used for initialize deep nets, considering common initialization techniques.

5.2. Complexity of Neural Nets

Next we turn to estimate our bounds of $C(\lambda, p)$, both for the linear models and nonlinear models, corresponding to Corollary 1 and Corollary 2. We use the same architectures as mentioned above. The bound on $C(\lambda, p)$ is controlled by the expected gradient-norm $E_{(x, y) \sim \mathcal{D}}(\|\nabla_x \ell(w, x, y)\|^2)$. Figure 4 presents the expected gradient-norm as a function of different variance levels for the prior distribution $p$ over the models parameters. For the linear model we used the bound in Corollary 1. One can see that the linear model has the largest expected gradient-norm, since the Lipschitz condition considers the worst-case gradient-norm. One also can see that the deeper the network, the smaller its gradient-norm. This is attributed to the gradient vanishing property. As a result, deeper nets can have faster convergence rate, i.e., use larger values of $\lambda$ in the generalization bound, since the vanishing gradients creates a contractivity property that stabilize the loss function, i.e., reduces its variability. However, this comes at the expanse of the expressivity of the deep net, since vanishing gradients cannot fit the training data in the learning phase. This is demonstrated in the next experiment.

Figure 6 presents the bound on $C(\lambda, p)$ as a function of the variance levels for the prior distribution over the models parameters. One can see that the bound gets larger when the variance of the prior increases. Another thing to note is that the bound is often explodes when the variance is larger than 0.3. This conforms with Corollary 1, which $C(\lambda, p)$ is unbounded for variance larger than 0.3. This plot conforms the practice of Bayesian deep nets that set the variance of the prior up to 0.1.

5.3. Sub-Gamma Approximation

In Section 4.1 we proved that the proposed bound is sub-gamma for the linear case. Unfortunately, such proof can not be directly applied to the non-linear case. Hence, we empirically demonstrate that the proposed bound over $C(\lambda, p)$
On the generalization of bayesian deep nets

Table 1. We optimize MLP models of different depth levels, where one corresponds to the linear model, two corresponds to two layers and so on. We report the avg. test loss, avg. train loss, bound on $C(\lambda, p)$, and the KL value for the MNIST dataset.

| Prior Variance | 0.0004 | 0.01  | 0.05  | 0.1   | 0.3   | 0.5   | 0.7   |
|----------------|--------|-------|-------|-------|-------|-------|-------|
| **One**        |        |       |       |       |       |       |       |
| Test Loss      | 0.753  | 0.442 | 0.277 | 0.271 | 0.324 | 0.408 | 0.677 |
| Train Loss     | 0.731  | 0.424 | 0.273 | 0.253 | 0.292 | 0.373 | 0.697 |
| Bound on $C(m, p)$ | 10.57 | 66.92 | inf   | inf   | inf   | inf   | inf   |
| Bound on $C(\sqrt{m}, p)$ | 0.0002 | 0.001 | 0.029 | 0.141 | 1.76  | 6.33  | 15.18 |
| KL             | 2027   | 10776 | 2561  | 1478  | 3886  | 7447  | 8995  |
| **Two**        |        |       |       |       |       |       |       |
| Test Loss      | 1.743  | 0.549 | 0.104 | 0.066 | 0.127 | 0.236 | 0.602 |
| Train Loss     | 1.752  | 0.569 | 0.095 | 0.038 | 0.056 | 0.155 | 0.425 |
| Bound on $C(m, p)$ | 0.0   | 0.014 | 0.540 | inf   | inf   | inf   | inf   |
| Bound on $C(\sqrt{m}, p)$ | 0.0   | 0.0   | 0.006 | 0.115 | 16.95 | inf   | inf   |
| KL             | 25848  | 30469 | 7369  | 7834  | 96976 | 166638| 244255|
| **Three**      |        |       |       |       |       |       |       |
| Test Loss      | 2.3    | 2.3   | 0.091 | 0.062 | 0.136 | 0.294 | 1.319 |
| Train Loss     | 2.3    | 2.3   | 0.078 | 0.027 | 0.067 | 0.268 | 1.173 |
| Bound on $C(m, p)$ | 0.0   | 0.0   | 0.002 | 31.99 | inf   | inf   | inf   |
| Bound on $C(\sqrt{m}, p)$ | 0.0   | 0.001 | 0.001 | 0.041 | 62.73 | inf   | inf   |
| KL             | nan    | 10776 | 9480  | 8215  | 95984 | 175134| 226237|
| **Four**       |        |       |       |       |       |       |       |
| Test Loss      | 2.3    | 2.3   | 0.083 | 0.067 | 0.132 | inf   | inf   |
| Train Loss     | 2.3    | 2.3   | 0.064 | 0.022 | 0.081 | inf   | inf   |
| Bound on $C(m, p)$ | 0.0   | 0.0   | 0.0   | 2.855 | inf   | inf   | inf   |
| Bound on $C(\sqrt{m}, p)$ | 0.0   | 0.0   | 0.0   | 0.012 | inf   | inf   | inf   |
| KL             | nan    | nan   | 10849 | 8239  | 113943| nan   | nan   |
| **Five**       |        |       |       |       |       |       |       |
| Test Loss      | 2.3    | 2.3   | 0.087 | 0.066 | 0.133 | inf   | inf   |
| Train Loss     | 2.3    | 2.3   | 0.055 | 0.019 | 0.101 | inf   | inf   |
| Bound on $C(m, p)$ | 0.0   | 0.0   | 0.0   | 0.204 | inf   | inf   | inf   |
| Bound on $C(\sqrt{m}, p)$ | 0.0   | 0.0   | 0.0   | 0.004 | inf   | inf   | inf   |
| KL             | nan    | nan   | 11800 | 9090  | 140305| nan   | nan   |

is indeed sub-gamma for various model architectures. For that we used the same models architectures as before using the MNIST dataset. Results are depicted in Figure 5. Notice, similar to the ResNet model, the proposed bound is sub-gamma in all explored settings using $c = 1e-5$ with different scaling factors.

5.4. Optimization

Lastly, in order to better understand the balance between all components composed the proposed generalization bound we optimize all five MLP models presented above using the MNIST dataset, and computed the average training loss, average test loss, KL divergence, and the bound on $C(\lambda, p)$, bound using $\lambda = m$ and $\lambda = \sqrt{m}$. We repeat this optimization process for various variance levels over the prior distribution over the model parameters. Results for the MNIST dataset are summarized in Table 1, more experimental results can be found in Section A.1 in the Appendix.

Results suggests that using variance levels of [0.05, 0.1] produce the overall best performance across all depth levels. This findings is consistent with our previous results which suggest that below this value the Bound goes to zero, hence make a good generalization on the expense of model performance. However, larger variance levels may cause the bound to explode and as a results makes the optimization problem harder.

Lastly, we analyzed the commonly used ResNet model (He et al., 2016). For that, we trained four different versions of the ResNet18 model: (i) standard model (ResNet); (ii) model with no skip connections (ResNetNoSkip); (iii) model with no batch normalizations (ResNetNoBN); and (iv) model without both skip connections and batch normalization layers (ResNetNoSkipNoBN). We optimize all models using CIFAR-10 dataset. Figure 7 visualizes the results. Consistently with previous findings, variance levels of 0.1 gets the best performance overall, both in terms of model test loss and the generalization.

Notice, ResNet and ResNetNoSkip achieve comparable performance in all measures. Additionally, when considering variance levels of 0.1 for the prior distribution, removing the batch normalization layers and including the skip-connections also gets comparable performance to ResNet and ResNetNoSkip. Similarly to Zhang et al. (2019), this
findings suggest that even without batch normalization layers models can converge using exact initialization. On the other hand while removing both batch normalization the and skip connections, models either explores immediately or suffer greatly from gradient vanishing. These results are consistent with previous findings in which batch normalization greatly improves optimization (Santurkar et al., 2018).

6. Discussion and Future Work

We present a new PAC-Bayesian generalization bound for deep Bayesian neural networks for unbounded loss functions with unbounded gradient-norm. The proof relies on bounding the log-partition function using the expected squared norm of the gradients with respect to the input. We prove that the proposed bound is sub-gamma for any linear model with a Lipschitz loss function and we verify it empirically for the non-linear case. Experimental validation shows that the resulting bound provides insights for better model optimization, prior distribution search and model initialization.

References

Alquier, P., Wintenberger, O., et al. Model selection for weakly dependent time series forecasting. *Bernoulli*, 18 (3):883–913, 2012.

Alquier, P., Ridgway, J., and Chopin, N. On the properties of variational approximations of gibbs posteriors. *Journal of Machine Learning Research*, 17(239):1–41, 2016.

Banerjee, A. On bayesian bounds. In *Proceedings of the 23rd international conference on Machine learning*, pp. 81–88. ACM, 2006.

Bartlett, P., Grunwald, P., Harremoës, P., Hedayati, F., and Kotłowski, W. Horizon-independent optimal prediction with log-loss in exponential families. *arXiv preprint arXiv:1305.4324*, 2013.

Bartlett, P. L. and Mendelson, S. Rademacher and gaussian complexities: Risk bounds and structural results. *Journal of Machine Learning Research*, 3(Nov):463–482, 2002.

Bartlett, P. L., Foster, D. J., and Telgarsky, M. J. Spectrally-normalized margin bounds for neural networks. In *Advances in Neural Information Processing Systems*, pp. 6241–6250, 2017a.

Bartlett, P. L., Harvey, N., Liaw, C., and Mehrabian, A. Nearly-tight vc-dimension and pseudodimension bounds for piecewise linear neural networks. *arXiv preprint arXiv:1703.02930*, 2017b.

Bartlett, P. L., Harvey, N., Liaw, C., and Mehrabian, A. Nearly-tight vc-dimension and pseudodimension bounds for piecewise linear neural networks. *Journal of Machine Learning Research*, 20(63):1–17, 2019. URL http://jmlr.org/papers/v20/17-612.html.

Blundell, C., Cornebise, J., Kavukcuoglu, K., and Wierstra, D. Weight uncertainty in neural networks. *arXiv preprint arXiv:1505.05424*, 2015.

Boucheron, S., Lugosi, G., and Massart, P. *Concentration inequalities: A nonasymptotic theory of independence*. Oxford university press, 2013.

Bousquet, O. and Elisseeff, A. Stability and generalization. *The Journal of Machine Learning Research*, 2:499–526, 2002.

Dziugaite, G. K. and Roy, D. M. Computing nonvacuous generalization bounds for deep (stochastic) neural networks with many more parameters than training data. *arXiv preprint arXiv:1703.11008*, 2017.

Gal, Y. *Uncertainty in deep learning*. PhD thesis, PhD thesis, University of Cambridge, 2016.

Gal, Y. and Ghahramani, Z. Dropout as a bayesian approximation: Representing model uncertainty in deep learning. *arXiv preprint arXiv:1506.02142*, 2, 2015.
On the generalization of bayesian deep nets

Gentil, I. Logarithmic sobolev inequality for log-concave measure from prekopa-leindler inequality. *arXiv preprint math/0503476*, 2005.

Germain, P., Bach, F., Lacoste, A., and Lacoste-Julien, S. Pac-bayesian theory meets bayesian inference. In *Advances in Neural Information Processing Systems*, pp. 1884–1892, 2016.

Golowich, N., Rakhlin, A., and Shamir, O. Size-independent sample complexity of neural networks. *arXiv preprint arXiv:1712.06541*, 2017.

Grünewald, P. D. and Mehta, N. A. A tight excess risk bound via a unified pac-bayesian-rademacher-shtarkov-mdl complexity. *arXiv preprint arXiv:1509.01240*, 2015.

Hardt, M., Recht, B., and Singer, Y. Train faster, generalize better: Stability of stochastic gradient descent. *arXiv preprint arXiv:1510.07732*, 2017.

He, K., Zhang, X., Ren, S., and Sun, J. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 770–778, 2016.

Kakade, S. M., Sridharan, K., and Tewari, A. On the complexity of linear prediction: Risk bounds, margin bounds, and regularization. In *Advances in neural information processing systems*, pp. 793–800, 2009.

Kingma, D. P., Salimans, T., and Welling, M. Variational dropout and the local reparameterization trick. In *Advances in Neural Information Processing Systems*, pp. 2575–2583, 2015.

Kuzborskij, I. and Lampert, C. H. Data-dependent stability of stochastic gradient descent. *arXiv preprint arXiv:1703.01678*, 2017.

Ledoux, M. Concentration of measure and logarithmic sobolev inequalities. In *Seminare de probabilites XXXIII*, pp. 120–216. Springer, 1999.

London, B. A pac-bayesian analysis of randomized learning with application to stochastic gradient descent. In *Advances in Neural Information Processing Systems*, pp. 2931–2940, 2017.

Louizos, C. and Welling, M. Structured and efficient variational deep learning with matrix gaussian posteriors. In *International Conference on Machine Learning*, pp. 1708–1716, 2016.

McAllester, D. A pac-bayesian tutorial with a dropout bound. *arXiv preprint arXiv:1307.2118*, 2013.

Neyshabur, B., Tomioka, R., and Srebro, N. Norm-based capacity control in neural networks. In *Conference on Learning Theory*, pp. 1376–1401, 2015.

Neyshabur, B., Bhojanapalli, S., McAllester, D., and Srebro, N. A pac-bayesian approach to spectrally-normalized margin bounds for neural networks. *arXiv preprint arXiv:1707.09564*, 2017.

Neyshabur, B., Li, Z., Bhojanapalli, S., LeCun, Y., and Srebro, N. Towards understanding the role of over-parametrization in generalization of neural networks. *arXiv preprint arXiv:1805.12076*, 2018.

Rakhlin, A., Mukherjee, S., and Poggio, T. Stability results in learning theory. *Analysis and Applications*, 3(04):397–417, 2005.

Santurkar, S., Tsipras, D., Ilyas, A., and Madry, A. How does batch normalization help optimization? In *Advances in Neural Information Processing Systems*, pp. 2483–2493, 2018.

Shalev-Shwartz, S., Shamir, O., Srebro, N., and Sridharan, K. Stochastic convex optimization. In *COLT*, 2009.

Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., and Salakhutdinov, R. Dropout: A simple way to prevent neural networks from overfitting. *The Journal of Machine Learning Research*, 15(1):1929–1958, 2014.

Takimoto, E. and Warmuth, M. K. The last-step minimax algorithm. In *International Conference on Algorithmic Learning Theory*, pp. 279–290. Springer, 2000.

Wei, C. and Ma, T. Data-dependent sample complexity of deep neural networks via lipschitz augmentation. In *Advances in Neural Information Processing Systems*, pp. 9722–9733, 2019.

Xiao, H., Rasul, K., and Vollgraf, R. Fashion-mnist: a novel image dataset for benchmarking machine learning algorithms, 2017.

Yang, J., Sun, S., and Roy, D. M. Fast-rate pac-bayes generalization bounds via shifted rademacher processes. In *Advances in Neural Information Processing Systems*, pp. 10802–10812, 2019.

Zhang, C., Bengio, S., Hardt, M., Recht, B., and Vinyals, O. Understanding deep learning requires rethinking generalization. *arXiv preprint arXiv:1611.03530*, 2016.

Zhang, H., Dauphin, Y. N., and Ma, T. Fixup initialization: Residual learning without normalization. *arXiv preprint arXiv:1901.09321*, 2019.
A. Appendix

A.1. Extended results

We provide an additional results for the optimization experiments. We optimized MLP models at different depth levels using Fashion-MNIST dataset.

Table 2. We optimize models of different depth levels, where one corresponds to the linear model, two corresponds to two layers and so on. We report the avg. test loss, avg. train loss, bound on $C(\lambda, p)$, and the KL value.

| Prior Variance | One |   |   |   |   |   |   | Two |   |   |   |   | Three |   |   |   | Four |   |   |   | Five |   |   |   |
|----------------|-----|---|---|---|---|---|---|-----|---|---|---|---|------|---|---|---|-----|---|---|---|-----|---|---|---|
|                |     | 0.0004 | 0.01 | 0.05 | 0.1 | 0.3 | 0.5 | 0.7 |
| Test Loss      | 0.79 | 0.57 | 0.45 | 0.46 | 1.04 | 1.59 | 10.43 |
| Train Loss     | 0.77 | 0.55 | 0.41 | 0.39 | 0.86 | 1.31 | 9.97 |
| MGF bound ($\lambda = m$) | 10.57 | 67.31 | inf | inf | inf | inf | inf |
| MGF bound ($\lambda = \sqrt{m}$) | 0.0001 | 0.0011 | 0.0296 | 0.143 | 1.812 | 6.386 | 14.74 |
| KL             | 14255 | 7829 | 2430 | 1648 | 5379 | 8440 | 35299 |
| Test Loss      | 1.46 | 0.71 | 0.35 | 0.31 | 0.42 | 0.6 | 10.43 |
| Train Loss     | 1.46 | 0.69 | 0.29 | 0.2 | 0.3 | 0.49 | 9.97 |
| MGF bound ($\lambda = m$) | 0.014 | 0.53 | inf | inf | inf | inf | inf |
| MGF bound ($\lambda = \sqrt{m}$) | 0.0 | 0.0 | 0.005 | 0.12 | 16.86 | inf | inf |
| KL             | 28222 | 22053 | 6983 | 9180 | 98648 | 168266 | 209935 |
| Test Loss      | 2.3 | 0.92 | 0.34 | 0.31 | 0.42 | 0.83 | 2.39 |
| Train Loss     | 2.3 | 0.91 | 0.28 | 0.19 | 0.35 | 0.79 | 1.76 |
| MGF bound ($\lambda = m$) | 0.0 | 0.0 | 0.002 | 32.16 | inf | inf | inf |
| MGF bound ($\lambda = \sqrt{m}$) | 0.0 | 0.0 | 0.0 | 0.04 | 64.48 | inf | inf |
| KL             | 0 | 29826 | 9219 | 1648 | 547636 | 198760 | 374718 |
| Test Loss      | 2.3 | 2.3 | 0.34 | 0.31 | 0.44 | inf | inf |
| Train Loss     | 2.3 | 2.3 | 0.26 | 0.18 | 0.38 | inf | inf |
| MGF bound ($\lambda = m$) | 0.0 | 0.0 | 0.0 | 2.81 | inf | inf | inf |
| MGF bound ($\lambda = \sqrt{m}$) | 0.0 | 0.0 | 0.0 | 0.01 | inf | inf | inf |
| KL             | 0 | 0 | 10859 | 10165 | 388842 | nan | nan |
| Test Loss      | 2.3 | 2.3 | 0.34 | 0.31 | 1.3 | inf | inf |
| Train Loss     | 2.3 | 2.3 | 0.25 | 0.18 | 1.28 | inf | inf |
| MGF bound ($\lambda = m$) | 0.0 | 0.0 | 0.0 | 0.19 | inf | inf | inf |
| MGF bound ($\lambda = \sqrt{m}$) | 0.0 | 0.0 | 0.0 | 0.003 | inf | inf | inf |
| KL             | 0 | 0 | 11918 | 10986 | 353632 | nan | nan |