Estimating Model Uncertainty of Neural Networks in Sparse Information Form

Jongseok Lee\textsuperscript{1}  Matthias Humt\textsuperscript{1}  Jianxiang Feng\textsuperscript{1,2}  Rudolph Triebel\textsuperscript{1,2}

Abstract
We present a sparse representation of model uncertainty for Deep Neural Networks (DNNs) where the parameter posterior is approximated with an inverse formulation of the Multivariate Normal Distribution (MND), also known as the information form. The key insight of our work is that the information matrix, i.e., the inverse of the covariance matrix tends to be sparse in its spectrum. Therefore, dimensionality reduction techniques such as low rank approximations (LRA) can be effectively exploited. To achieve this, we develop a novel sparsification algorithm and derive a cost-effective analytical sampler. As a result, we show that the information form can be scalably applied to represent model uncertainty in DNNs. Our exhaustive theoretical analysis and empirical evaluations on various benchmarks show the competitiveness of our approach over the current methods.

1. Introduction
Whenever machine learning methods are used for safety-critical applications such as autonomous driving, it is crucial to provide a precise estimation of the failure probability of the learned predictor. Therefore, most of the current learning approaches return distributions rather than single, most-likely predictions. However, in case of DNNs, this true failure probability tends to be severely underestimated, leading to overconfident predictions (Guo et al., 2017). The main reason for this is that DNNs are typically trained with a principle of maximum likelihood, neglecting their epistemic or model uncertainty with the point estimates of parameters.

Imposing Gaussians on model uncertainty is arguably the most popular choice as Gaussians are for approximate inference what linear maps are for algebra. For example, once the posterior distribution is inferred, the majority of computations can be performed using the well known tools of linear algebra. For DNNs however, the space complexity of using MNDs is intractable as the covariance matrix scales quadratic to the number of parameters. Consequently, approximate inference on DNNs posterior often neglects the parameter correlations (Wu et al., 2019; Kingma et al., 2015; Graves, 2011; Hernandez-Lobato & Adams, 2015) or simplifies the covariance matrix into Kronecker products of two smaller matrices (Sun et al., 2017; Louizos & Welling, 2016; Zhang et al., 2018; Park et al., 2019) regardless of the inference principles such as variational inference.

Instead, inspired by Thrun et al. (2004), we advocate to explore the dual and inverse formulation of MNDs:

\[
\tilde{x} \propto \exp \left\{ -\frac{1}{2} (\tilde{x} - \mu)^T \Sigma^{-1} (\tilde{x} - \mu) \right\}
\]

\[
= \exp \left\{ -\frac{1}{2} \tilde{x}^T \Sigma^{-1} \tilde{x} + \mu^T \Sigma^{-1} \tilde{x} \right\}
\]

\[
= \exp \left\{ -\frac{1}{2} \tilde{x}^T I \tilde{x} + \mu^T \tilde{x} \right\} \text{ or } \tilde{x} \sim \mathcal{N}(\mu, I)
\]

where the Gaussian random variable \( \tilde{x} \) is fully parameterized by the information vector \( \mu^T \) and matrix \( I \) as opposed to mean \( \mu \) and covariance matrix \( \Sigma \). Our major findings are that this so-called information form has important ramifications on developing scalable Bayesian Neural Networks. Firstly, we point out that the approximate inference for this formulation can be simplified to scalable Laplace Approximation (LA) (MacKay, 1992b; Ritter et al., 2018a), in which we improve the state-of-the-art Kronecker factored approximations of the information matrix (George et al., 2018) by correcting the diagonal variance in parameter space.

More importantly, DNNs offer a natural spectral sparsity in the information matrix (Sagun et al., 2018) as opposed to the covariance matrix. Intuitively, the information content of each parameters become weaker with increasing number of parameters and thus, sparse representations can be effectively exploited. To do so, we propose a novel low-rank representation of the given Kronecker factorization and devise a spectral sparsification algorithm that can pre-

---

\textsuperscript{1}Institute of Robotics and Mechatronics, German Aerospace Center (DLR), Wessling, Germany
\textsuperscript{2}Computer Vision Group, Technical University of Munich (TU Munich), Garching, Germany.

Correspondence to: Jongseok Lee <jongseok.lee@dlr.de>.

Proceedings of the 37\textsuperscript{th} International Conference on Machine Learning, Vienna, Austria, PMLR 119, 2020. Copyright 2020 by the author(s).
serve the Kronecker product in its eigenbasis. Based on this formulation, we further demonstrate low rank sampling computations which significantly reduces the space complexity of MND from $O(N^3)$ to $O(L^3)$ where $L$ is the chosen low-rank dimension instead of parameter space lying in high dimensional $N$ manifolds. Lastly, we also exhaustively perform both theoretical and empirical evaluations, yielding state-of-the-art results in both scalability and performance.

Our main contribution is a novel sparse representation for DNNs posterior that is backed up by scalable mathematical foot-works - more specifically: (i) an approximate inference that estimates model uncertainty in information form (section 2.2), (ii) a low-rank representation of Kronecker factored eigendecomposition (section 2.3), (iii) an algorithm to enable a LRA for the given representation of MNDs (algorithm 1) and (iv) derivation of a memory-wise tractable factored eigendecomposition (section 2.3), (iii) an algorithm 1) and (iv) derivation of a memory-wise tractable sampler (section 2.4). With our theoretical (section 2.5) and experimental results (section 4) we further showcase the state-of-the-art performance. Finally, a plug-in-and-play code is attached for enabling adoptions in practice.

2. Methodology

2.1. Background and Notation

A neural network is a parameterized function $f_\theta: \mathbb{R}^{N_0} \rightarrow \mathbb{R}^{N_l}$ where $\theta \in \mathbb{R}^{N_{\theta}}$ are the weights and $N_0 = N_1 + \cdots + N_l$. This function $f_\theta$ is in fact a concatenation of $l$ layers, where each layer $l \in [1, \ldots, l]$ computes $h_l = W_l a_{l-1} + a_l = \phi(h_{l-1})$. Here, $\phi$ is a nonlinear function, $a_l$ are activations, $h_l$ linear pre-activations, and $W_l$ are weight matrices. The bias terms are absorbed into $W_l$ by appending 1 to each $a_l$. Thus, $\theta = \left[ \text{vec}(W_1)^T \cdots \text{vec}(W_l)^T \right]^T$ where vec is the operator that stacks the columns of a matrix to a vector. Let $g_l = \partial h_i/\partial \theta_j$ the gradient of $h_i$ w.r.t $\theta_j$. Using LA the posterior is approximated with a Gaussian. The mean is then given by the MAP estimate $\theta_{MAP}$ and the covariance by the Hessian of the log-likelihood $(H + \tau I)^{-1}$ assuming a Gaussian prior with precision $\tau$. Using loss functions such as MSE or cross entropy and piece-wise linear activation $a_l$ (e.g RELU), a good approximation of the Hessian is the Fisher information matrix (IM) $I = \mathbb{E} \left[ \delta \theta_i \delta \theta_j^T \right]$ for the backpropagated gradients $\delta \theta_i$ and is typically scaled by the number of data points N (Martens & Grosse, 2015). IM is of size $N_0 \times N_0$ resulting in too large matrix for moderately sized DNNs.

To make the computation tractable, it is first assumed that the weights across layers are uncorrelated, which corresponds to a block-diagonal form of $I$ with blocks $I_1, \ldots, I_l$. Then, each realisation of block $I_i$ is represented as a Kronecker product $\delta \theta_i = a_i \delta \theta_i^T = a_{i-1} a_i^T \otimes g_i b_i^T$. Then, matrices $A_{i-1}$ and $G_i$ are assumed to be statistically independent:

$$I_i \approx I_{i,kfac} = \mathbb{E} \left[ a_i a_i^T \otimes g_i b_i^T \right] = A_{i-1} \otimes G_i. \quad (1)$$

We refer to Martens & Grosse (2015) for details on KFAC. Here, $A_{i-1} \in \mathbb{R}^{n_i \times n_i}$ and $G_i \in \mathbb{R}^{m_i \times m_i}$, where the number of weights is $N_i = n_i m_i$. Typically IM is scaled by the number of data points $N$ and incorporates the prior $\tau$. The herein presented parameter posterior omits the addition of prior precision and scaling term for simplicity. Here, $N$ and $\tau$ are treated as hyperparameters (Ritter et al., 2018a) similar to tempering in (Wenzel et al., 2020). KFAC scales to big data sets such as ImageNet (Krizhevsky et al., 2012) with large DNNs (Ba et al., 2017) and does not require changes in the training procedure when used for LA (Ritter et al., 2018a).

2.2. Approximate Inference in Information Form

We first employ an eigenvalue correction in the Kronecker factored eigenbasis (George et al., 2018) for LA. Layer indices $i$ are omitted and explanation applies layer-wise.

Let $I = V_{\text{true}} A_{\text{true}} V_{\text{true}}^T$ be the true eigendecomposition of IM per layer. From this it follows $A_{\text{true}} = V_{\text{true}}^T I V_{\text{true}} = \mathbb{E} \left[ (V_{\text{true}} \delta \theta_i^T V_{\text{true}})^T \right]$ and $\Lambda_{\text{true},i} = \mathbb{E} \left[ (V_{\text{true}} \delta \theta_i^T)^2 \right]$ where $i \in \{1, \ldots, N\}$ and $N$ is the number of layers of this layer. Defining the eigendecomposition of $A$ and $G$ in (1) as $A = U_S A U_A^T$ and $G = U_S G U_G^T$, it further follows $I_{i,kfac} \approx U_A \otimes G = (U_A \otimes U_G)(S_A \otimes S_G)(U_A \otimes U_G)^T$ from the properties of the Kronecker product. Now, this approximation can be improved by replacing $(S_A \otimes S_G)$ with the eigenvectors $\Lambda_{\text{true}}$, where $V_{\text{true}}$ is approximated with $(U_A \otimes U_G)$ resulting in $\Lambda_{i} = \mathbb{E} \left[ (U_A \otimes U_G)^T \delta \theta_i^T \right]$. We denote this as the eigenvalue corrected, Kronecker-factored eigenbasis (EFB):

$$I_{\text{efb}} = (U_A \otimes U_G) \Lambda (U_A \otimes U_G)^T \quad (2)$$

This technique has many desirable properties. Notably, $\|I - I_{\text{efb}}\|_F \leq \|I - I_{i,kfac}\|_F$ wrt. the Frobenius norm as the computation is more accurate by correcting the eigenvalues.

However, there is an approximation in EFB since $(U_A \otimes U_G)$ is still an approximation of the true eigenbasis $V_{\text{true}}$. Intuitively, EFB only performs a correction of the diagonal elements in the eigenbasis, but when mapping back to the parameter space this correction is again harmed by the inexact estimate of the eigenvectors. Although an exact estimation of the eigenvectors is infeasible, it is important to note that the diagonals of the exact IM $\Lambda_{i} = \mathbb{E} \left[ \delta \theta_i^2 \right]$ can be computed efficiently using back-propagation. This motivates the idea
Estimating Model Uncertainty of Neural Networks in Sparse Information Form

to correct the approximation further as follows:

\[
I_{\text{inf}} = (U_A \otimes U_G)d(A(U_A \otimes U_G)) + D \text{ where}
\]

\[
D_{\text{inf}} = \mathbb{E}[\delta \theta^2] = \sum_{j=1}^{nm} (v_{i,j} \sqrt{\Lambda_j})^2.
\]

In (3), we have represented \((U_A \otimes U_G)d(A(U_A \otimes U_G))\) as 
\[\sum_{j=1}^{nm} (v_{i,j} \sqrt{\Lambda_j})^2\] where \(V = (U_A \otimes U_G) \in \mathbb{R}^{m \times nm}\) is a
Kronecker product with row elements \(v_{i,j}\) (see definition 1 below).
It follows from the properties of the Kronecker product that \(i = m(\alpha - 1) + \gamma\). The derivation is shown in supplemental
materials. Note that the Kronecker products are never directly evaluated but the diagonal matrix \(D\) can be
computed recursively, making it computationally feasible.

**Definition 1:** For \(U_A \in \mathbb{R}^{m \times a}\) and \(U_G \in \mathbb{R}^{m \times mn}\). the Kronecker product of \(V = U_A \otimes U_G \in \mathbb{R}^{nm \times nm}\) is given by
\(V_{i,j} = U_{A_{m}} U_{G_{i,n}}\), with \(i = m(\alpha - 1) + \gamma\) and \(j = m(\beta - 1) + \zeta\), \(\alpha \in \{1, \ldots, n\}\) and \(\beta \in \{1, \ldots, n\}\) are row and column indices
of \(U_A\). So as \(\gamma \in \{1, \ldots, m\}\) and \(\zeta \in \{1, \ldots, m\}\) for \(U_G\).

Now, the parameter posterior distribution can be represented in an information form \(N^{-1}\) of MND as shown below:

\[
p(\theta | x) \sim N(\theta_{MAP}, I_{\text{inf}}^{-1})
\]

\[
= N^{-1}(\theta_{MAP}^V, (U_A \otimes U_G)d(A(U_A \otimes U_G)) + D).
\]

This shows how an information form of MND can be computed using LA, and from its graphical interpretation, keeping
the diagonals of IM exact has also a consequence of obtaining information content of the parameters accurate
(Paskin, 2003). We note that, similar insights have been studied for Bayesian tracking problems (Thrun et al., 2004)
without adoptions in practice (Bailey & Durrant-Whyte, 2006; Thrun & Liu, 2005; Eustice et al., 2006).

For a full Bayesian analysis with DNNs, however, the samples of the resulting posterior are to be drawn from the
information matrix instead of the covariance matrix. For this, an efficient sampling computation is proposed next.

2.3. Model Uncertainty in Sparse Information Form

Sampling from the posterior is crucial. For example, an important use-case of the parameter posterior is estimat-
ing the predictive uncertainty for test data \((x^*, y^*)\) by a full
Bayesian analysis with \(K_{MC}\) samples. This step is typically approximated with Monte-carlo integration (Gal, 2016):

\[
p(y^* | x, y) \approx \frac{1}{K_{MC}} \sum_{k=1}^{K_{MC}} y^*(x, \theta^k) \quad \text{for } \theta^k \sim N^{-1}(\theta_{MAP}^V, I_{\text{inf}}^{-1}).
\]

However, this operation is non-trivial as the sampling computation requires \(O(N^3)\) complexity (the cost of inversion
and finding a symmetrical factor) and for matrices that lie in a high dimensional space, it is computationally infeasible.
While previous works (Martens & Grosse, 2015) showed that Kronecker products of two matrices can be exploited
along a fidelity-cost trade-off, our main aim is to introduce an alternative form of the Gaussian posterior family.

Observing that the eigenvalues of IM tends to be close to zero for the overparameterized DNNs (Sagun et al., 2018),
information form can naturally leverage dimensionality reduction in IM (in oppose to the covariance matrix). Intu-
ritively speaking, as more and more parameters are used to explain the same set of data, information of these parameters
tends to be smaller, and we can make use of this tendency.

To this end, we propose the low rank form in (4) as a first step, in which we preserve the Kronecker product in
eigenvectors. Here, we highlight that the proposed form differs from conventional LRA which do not preserve the
Kronecker product in eigenvectors (i.e \((U_A \otimes U_G)_{1:1}\) for top
L eigenvalues). Two main advantages of this representation are that it avoids the memory-wise expensive computation
of evaluating the matrix \((U_A \otimes U_G)\), where \(U_A\) and \(U_G\) are sub-matrices of \(U_A\) and \(U_G\). respectively. This formulation
also results in sampling computation that is \(O(L^2)\) in cost instead of \(O(N^3)\), which we demonstrate later in section 2.4.

\[
I_{\text{inf}} \approx I_{\text{inf}} = (U_A \otimes U_G)_{1:1}(U_A \otimes U_G)_{1:1} + D
\]

Here, \(A_{1:1} \in \mathbb{R}^{L \times L}, U_A \in \mathbb{R}^{m \times a}\) and \(U_G \in \mathbb{R}^{n \times g}\) denote low
rank form of corresponding eigenvalues and vectors (depicted in figure 1). Naturally, it follows that \(L = aG, N = mn\)
and furthermore, the persevered rank \(L\) corresponds to preserving top \(K\) and additional \(J\) eigenvalues (resulting in \(L \geq K, L =AG = K+J\)) as explained with an example.

**Why can’t LRA directly be used?:** Let a matrix \(E = U_{1:6}A_{1:6}U_{1:6}^T \in \mathbb{R}^{6 \times 6}\) with \(U_{1:6} = [u_1 \cdots u_6] \in \mathbb{R}^{6 \times 6}\) with
\(u_i\) the eigenvectors and \(A_{1:6} = \text{diag}(\lambda_1, \ldots, \lambda_6) \in \mathbb{R}^{6 \times 6}\) in a descending order. In this toy example, LRA with
3 top 3 eigenvalues results: \(E_{LRA} = U_{1:3}A_{1:3}U_{1:3}^T \in \mathbb{R}^{6 \times 6}\). Instead, if the eigenvector matrices are expressed in
Kronecker product structure, \(E_{kron} = (U_{A_{1:6}} \otimes U_{G_{1:6}})A_{1:6}(U_{A_{1:6}} \otimes U_{G_{1:6}})^T \in \mathbb{R}^{6 \times 6}\). For LRA, it’s not trivial to directly preserve
the top 3 eigenvalues \(A_{1:3}\) and corresponding eigenvectors \((U_{A_{1:6}} \otimes U_{G_{1:6}})_{1:3}\). Because as \((U_{A_{1:6}} \otimes U_{G_{1:6}})_{1:3} = [u_{A_1} u_{G_1} u_{A_2} u_{G_2} u_{A_3} u_{G_3}]\), preserving the eigenvectors with Kronecker structure results in having to store
more eigenvectors: \(U_{A_{1:6}} = [u_{A_1} u_{A_2}]\) and \(U_{G_{1:6}} = [u_{G_1} u_{G_2}]\). Consequently, additional eigenvalue \(A_4\) needs to be saved
so that \(E_{kron} = (U_{A_{1:6}} \otimes U_{G_{1:6}})A_{1:4}(U_{A_{1:6}} \otimes U_{G_{1:6}})^T \in \mathbb{R}^{6 \times 6}\).
then, how to achieve a LRA that preserves Kronecker structures in eigenvectors? For this, we propose algorithm 1 (also illustrated in figure 1). To select the additional eigenvectors and -values correctly, we need to introduce a definition on indexing rules of Kronecker factored diagonal matrices.

**Definition 2:** For diagonal matrices $S_A \in \mathbb{R}^{mn \times n}$ and $S_G \in \mathbb{R}^{mn \times m}$, the Kronecker product of $\Lambda = S_A \otimes S_G \in \mathbb{R}^{mn \times mn}$ is given by $\Lambda_i = s_{\alpha \beta} s_{\gamma \zeta}$, where the indices $i = m(\alpha - 1) + \zeta$ with $\beta \in [1, \ldots, m]$ and $\zeta \in [1, \ldots, n]$. Then, given $i$ and $m$, $\beta = \text{floor}(\frac{i}{m}) + 1$ and given $\beta$, $m$, and $\zeta$, $\alpha = i - m(\beta - 1)$.

Notations in algorithm 1 are also depicted in figure 1. Now we explain this computation with a toy example below.

**Algorithm 1 for a toy example:** To explain, the same toy example can be revisited. Firstly, we aim to preserve the top 3 eigenvalues, $i \in \{1, 2, 3\}$, which are indices of eigenvalues $\Lambda_{1:3}$ (step 1). Then, $\beta \in \{1, 2\}$ and $\zeta \in \{1, 2\}$ can be computed using definition 2 (step 2). This relation holds as $\Lambda$ is computed from $S_A \otimes S_G$, and thus, $U_A$ and $U_G$ are their corresponding eigenvectors, respectively. Then we produce $U_{A_{i,2}}$ and $U_{G_{i,2}}$ according to $\beta$ and $\zeta$ (step 3). Again, in order to fulfill the Kronecker product operation, we need to find the eigenvalues $j \in \{1, 2, 3, 4\}$, and preserve $\Lambda_{1:a}$ (step 4&5). This results in saving top 3 and additional 1 eigenvalues. Algorithm 1 provides the generalization of these steps and even if eigendecomposition does not come with a descending order, the same logic trivially applies.

Next, we describe the last step of the sampling derivation.

### 2.4. Low Rank Sampling Computations

Consider drawing samples $\theta^i_s \in \mathbb{R}^{mn}$ from the representation:

$$\theta^i_s \sim \mathcal{N}^{-1}(\theta_{\text{MAP}}^i, (U_A \otimes U_G)\Lambda_{1:L}(U_A \otimes U_G)^T + D).$$

Typically, drawing such samples $\theta^i_s$ requires finding a symmetrical factor of the covariance matrix (e.g., Cholesky decomposition) which is cubic in cost $O(N^3)$ (here $N = mn$). Furthermore, in our representation, it requires first an inversion of IM and then the computation of a symmetrical factor which overall constitutes two operations of cost $O(N^3)$. Clearly, if $N$ lies in a high dimension sampling becomes infeasible. Therefore, we need a sampling computation that performs these operations in the dimensions of low rank L.

Let us define $X^i \in \mathbb{R}^{mn}$ as the samples from a standard MND. Then, the samples $\theta^i_s$ can be computed analytically as,

$$\theta^i_s = \theta_{\text{MAP}} + F^s X^i$$

where

$$F^s = D^{-\frac{1}{2}}(I_{nm} - D^{-\frac{1}{2}}(U_A \otimes U_G)\Lambda_{1:L}^{\frac{1}{2}}(U_A \otimes U_G)^T D^{-\frac{1}{2}})(C^{-1} + V^T V)^{-1}\Lambda_{1:L}^{\frac{1}{2}}(U_A \otimes U_G)^T D^{-\frac{1}{2}}).$$

$$\text{cost: } O(L^3) \ll O(N^3)$$

![Figure 1. Illustration of algorithm 1](image-url)
We outline theoretical guarantees of our approach below.

\[ V_i = D^{-\frac{1}{2}} (U_i \otimes U_i) A_{i:L}^{-1} \]  

and \( C = A_c^{-T} (B_c - I_L) A_c^{-1} \)

with \( A_c \) and \( B_c \) being the Cholesky decomposed matrices of \( V_s^T V_s \in \mathbb{R}^{L \times L} \) and \( V_s^T V_s + I_L \in \mathbb{R}^{L \times L} \) such that:

\[ A_c A_c^T = V_s^T V_s \quad \text{and} \quad B_c B_c^T = V_s^T V_s + I_L. \]

Consequently, the matrices in (6) are defined as \( C \in \mathbb{R}^{L \times L} \), \((C^{-1} + V_s^T V_s) \in \mathbb{R}^{L \times L} \) and identity matrix \( I_L \in \mathbb{R}^{L \times L} \). In this way, the two operations namely Cholesky decomposition and inversion that are cubic in cost \( O(N^3) \) are reduced to the low rank dimension \( L \) with complexity \( O(L^3) \). The complete derivation is in supplementary materials where we further show how the Kronecker structure in eigendecomposition can be exploited to compute \( F^T X^T \) using the vec trick.

2.5. Theoretical Guarantees

We outline theoretical guarantees of our approach below. Note that these properties hold regardless of data and model.

**Lemma 1:** Let \( I \) be the real information matrix, and let \( I_{inf} \) and \( I_{efb} \) be the INF and EFB estimates of it respectively. It is guaranteed to have \( \|I - I_{efb}\|_F \geq \|I - I_{inf}\|_F \).

**Corollary 1:** Let \( I_{kfac} \) and \( I_{inf} \) be KFAC and our estimates of real information matrix \( I \) respectively. Then, it is guaranteed to have \( \|I - I_{kfac}\|_F \geq \|I - I_{inf}\|_F \).

**Lemma 2:** Let \( I \) be the real information matrix, and let \( \hat{I}_{inf}, \hat{I}_{efb}, \) and \( I_{kfac} \) be the low rank INF, EFB and KFAC estimates of it respectively. Then, it is guaranteed to have \( \|\text{diag}(I) - \text{diag}(I_{efb})\|_F \geq \|\text{diag}(I) - \text{diag}(I_{kfac})\|_F \geq 0 \) and \( \|\text{diag}(I) - \text{diag}(I_{inf})\|_F = 0. \) Furthermore, if the eigenvalues of \( \hat{I}_{inf} \) contains all non-zero eigenvalues of \( I_{inf} \), it follows: \( \|I - I_{efb}\|_F \geq \|I - \hat{I}_{inf}\|_F \).

Proofs along with a further remarks and theoretical analysis on (i) error bounds of the proposed LRA and (ii) validity of the posterior can be found in supplementary materials.

3. Related Works

**Sparse Information Filters:** Thrun et al. (2004) proposed the extended sparse information filter (SEIF), which is a dual form of the extended Kalman filter. A key property of SEIF is that all update equations can be executed in constant time, which is achieved by relying on the information form and its sparsity. Our work brings the key ideas of SEIF in the context of approximate Bayesian inference for DNNs.

![Illustration of the main idea and the pipeline sketch.](image)

**Figure 2. Illustration of the main idea and the pipeline sketch.** We demonstrate that approximate Bayesian inference can work with the inverse covariance matrix - the information matrix. From its graphical interpretation (Paskin, 2003), the diagonal elements represent the information content of the node while its off-diagonal elements represent the link between the nodes. Our approach is designed with this insight where we sparsify the weak links while keeping the information content of the node accurate.

**Approximation of the Hessian:** The Hessian of DNNs is prohibitively too large as its size is quadratic to the number of parameters. For this problem, an efficient approximation is a layer-wise Kronecker factorization (Martens & Grosse, 2015; Botev et al., 2017) with demonstrably impressive scalability (Ba et al., 2017). In a recent extension by George et al. (2018) the eigenvalues of the Kronecker factored matrices are re-scaled so that the diagonal variance in its eigenbasis is exact. The work demonstrates a provable method of achieving improved performance. We heavily build upon these for Bayesian DNNs, as well-built software infrastructures such as (Dangel et al., 2020) already exists.

**Laplace Approximation:** Instead of methods rooted in variational inference (Hinton & van Camp, 1993) and sampling (Neal, 1996), we utilize LA (MacKay, 1992b) for the inference principle. Recently, diagonal (Becker & Lecun, 1989) and Kronecker-factorized approximations (Botev et al., 2017) to the Hessian have been applied to LA by Ritter et al. (2018a). The authors have further proposed to use LA in continual learning (Ritter et al., 2018b), and demonstrate competitive results by significantly outperforming its benchmarks (Kirkpatrick et al., 2017; Zenke et al., 2017). Building upon Ritter et al. (2018a) for approximate inference, we propose to use more expressive posterior distribution than matrix normal distribution. Concurrently, Kristiadi et al. (2019)
(2020) provides a formal statement on how approximate inference such as LA can mitigate overconfident behavior of DNNs with ReLU for a binary classification case.

In the context of variational inference, SLANG (Mishkin et al., 2018) share similar spirit to ours in using a low-rank plus diagonal form of covariance where the authors show the benefits of low-rank approximation in detail. Yet, SLANG is different to ours as it does not explore Kronecker structures. SWA (Maddox et al., 2018), SWAG (Maddox et al., 2019) and subspace inference (Izmailov et al., 2019) have also demonstrated strong results by exploring the insights on loss landscape of DNNs. We also acknowledge there exists alternatives paradigms. Some examples are the post-hoc calibrations (Guo et al., 2017; Wenger et al., 2020), ensembles (Lakshminarayanan et al., 2017) and combining Bayesian Neural Networks with probabilistic graphical models such as Conditional Random Fields (Feng et al., 2019).

**Dimensionality Reduction:** A vast literature is available for dimensionality reduction beyond principal component analysis (Wold et al., 1987) and singular value decomposition (Golub & Reinsch, 1971; Van Der Maaten et al., 2009). To our knowledge though, dimensionality reduction in Kronecker factored eigendecomposition has not been studied.

### 4. Experimental Results

We perform an empirical study with regression, classification and active learning tasks. The chosen datasets are toy regression, UCI (Dua & Graff, 2017), MNIST (Lecun et al., 1998), CIFAR10 (Krizhevsky, 2009) and ImageNet (Krizhevsky et al., 2012) datasets. In total, 10 baseline with default 3 LA-based approaches (Diag, KFAC and EFB) are compared, and we also study the effects of varying LRA.

Our main aim is to introduce the sparse information form of MND in the context of Bayesian Deep Learning, and thus, the experiments are designed to show the insight that spectral sparsification does not induce significant approximation errors while reducing the space complexity of using an expressive and structured posterior distribution. More importantly, we demonstrate that our method scales to datasets of ImageNet size and large architectures, and push the method further to compete with existing approaches. Implementation details can be found in supplementary materials.

#### 4.1. Small Scale Experiments

Firstly, evaluations on toy regression and UCI datasets are presented. Due to the small scale of the set-up, these experiments have advantages that we can not only evaluate the quality of uncertainty estimation, but also directly compare various approximations to the Hessian with LRA. The later empirically validates our theoretic claims and further connects the qualities of uncertainty estimates and the approximates of the Hessian. For the toy regression problem, we consider a single-layered network with 7 units. We have used 100 uniformly distributed points $x \sim U(-4, 4)$ and samples $y \sim N(x^2, 3^2)$. On UCI datasets we follow Hernandez-Lobato & Adams (2015) in which each dataset is split into 20 sets. A single layered network with 50 units are used with an exception of protein, where we have used 100 units.

We initially perform a direct evaluation of computed IM with a measure on normalized Frobenius norm of error $err_{NF}$ w.r.t the block-wise exact IM. Note that this is only possible for the small network architectures. The results are shown in figure 3 and table 1 for toy regression and UCI datasets respectively. Across all the experiments, we find that INF is exact on diagonal elements regardless of the ranks while KFAC and EFB induces significant errors. On off-diagonals, INF with full rank performs similar to EFB while decreasing the ranks of INF tend to increase the errors. Interestingly, INF with only 5% of the ranks, often outperforms KFAC

![Figure 3. Effects of Low Rank Approximation in Frobenius norm of error.](image)

**Figure 3. Predictive uncertainty.** The black dots and the black lines are data points $(x, y)$. The red and blue lines show predictions of the deterministic network and the mean output respectively. Upto three standard deviations are shown with blue shades.

![Figure 4.](image)

**Figure 4.**
We next show that our method can also perform a downstream task such as active learning. In this scenario, we further study the effects of LRA. For this purpose, we choose 3 UCI datasets (Boston Housing, Wine, and Energy) closely following Hernández-Lobato & Adams (2015). In detail, the model is a neural network with a single layer of 10 hidden units. We employ the same criterion as MacKay (1992a) which linearizes the propagation of variance of weights to the output. Besides comparing with a baseline: random selection strategy, we also compare 3 different number of ranks (20%, 50%, 100%) to verify the influence of LRA.

As shown in figure 5, uncertainty estimates of INF enable the model to learn more quickly and lead to statistically significant improvements when compared to the random selection strategy. Further, even after cutting the ranks significantly, the performance can be maintained. This can be clearly seen on both Boston Housing and Energy datasets: the mean RMSE of lower percentage version decreased, while their standard deviation mostly overlap. On Wine, there is nearly no decrease in performance with lower ranks. To summarize, our experiments show that INF can perform active learning, and LRA does not jeopardize the task.

4.2. Classification Tasks

Next, we evaluate predictive uncertainty on classification tasks where the proposed LRA is strictly necessary. To this end, we choose the classification tasks with known and unknown classes, e.g. a network is not only trained and evaluated on MNIST but also tested on notMNIST. Note that under such tests, any probabilistic methods should report their evaluations on both known and unknown classes with the same hyperparameter settings. This is because Bayesian

Visualization of predictive uncertainty is shown in figure 4 for the toy regression. Here, HMC (Neal, 1996) acts as ground truth while we compare our approach to KFAC and Bayes-by-backprop or BBB (Blundell et al., 2015). The hyperparameter sets for KFAC is chosen similar to (Ritter et al., 2018a) while INF did not require the tuning of hyperparameters (after ensuring that IM is non-degenerate similar to MacKay (1992b)). All the methods show higher uncertainty in the regimes far away from training data where BBB showing the most difference to HMC. Furthermore, KFAC predicts rather high uncertainty even within the regions that are covered by the training data. INF produces the most comparable fit to HMC with accurate uncertainty estimates. In supplementary materials, further comparison studies can be found. Furthermore, we also report the results of UCI experiments where we compare the reliability of uncertainty estimates using the test log-likelihood as a measure, and demonstrate competitive results as well as limitations.

4.2. Active Learning

We next show that our method can also perform a downstream task such as active learning. In this scenario, we further study the effects of LRA. For this purpose, we choose 3 UCI datasets (boston housing, wine, and energy) closely following Hernández-Lobato & Adams (2015). In details the model is a neural network with a single layer of 10 hidden units. We employ the same criterion as MacKay (1992a) which linearizes the propagation of variance of weights to the output. Besides comparing with a baseline: random

by a significant margin (e.g. Naval, Power, Protein). These observations are expected by the design of our approach and highlights the benefits of the information form. As the exact diagonals of IM are known and simple to compute (as oppose to the covariance matrix), we can design methods with theoretical guarantees on approximation quality of IM. Moreover, as the spectrum of IM tends to be sparse, LRA can be effectively exploited without inducing significant errors. For UCI experiments, we further study the varying effects of LRA in supplementary materials.
Table 2. Results of classification experiments. Accuracy and ECE are evaluated on in-domain distribution (MNIST and CIFAR10) whereas entropy is evaluated on out-of-distribution (notMNIST and SHVN). Lower the better for ECE. Higher the better for entropy.

<table>
<thead>
<tr>
<th>Experiment</th>
<th>Measure</th>
<th>NN</th>
<th>Diag</th>
<th>KFAC</th>
<th>MC-dropout</th>
<th>Ensemble</th>
<th>EFB</th>
<th>INF</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST vs notMNIST</td>
<td>Accuracy</td>
<td>0.993</td>
<td>0.9935</td>
<td>0.9929</td>
<td>0.9929</td>
<td>0.9937</td>
<td>0.9929</td>
<td>0.9927</td>
</tr>
<tr>
<td></td>
<td>ECE</td>
<td>0.395</td>
<td>0.0075</td>
<td>0.0078</td>
<td>0.0105</td>
<td>0.0635</td>
<td>0.012</td>
<td>0.0069</td>
</tr>
<tr>
<td></td>
<td>Entropy</td>
<td>0.055±0.133</td>
<td>0.555±0.199</td>
<td>0.599±0.199</td>
<td>0.562±0.199</td>
<td>0.596±0.133</td>
<td>0.618±0.185</td>
<td>0.635±0.19</td>
</tr>
<tr>
<td>CIFAR10 vs SHVN</td>
<td>Accuracy</td>
<td>0.8606</td>
<td>0.8659</td>
<td>0.8572</td>
<td>N/A</td>
<td>0.8651</td>
<td>0.8638</td>
<td>0.8646</td>
</tr>
<tr>
<td></td>
<td>ECE</td>
<td>0.0819</td>
<td>0.0358</td>
<td>0.0351</td>
<td>N/A</td>
<td>0.0809</td>
<td>0.0343</td>
<td>0.0084</td>
</tr>
<tr>
<td></td>
<td>Entropy</td>
<td>0.245±0.215</td>
<td>0.4129±0.197</td>
<td>0.408±0.197</td>
<td>N/A</td>
<td>0.370±0.192</td>
<td>0.417±0.196</td>
<td>0.4338±0.18</td>
</tr>
</tbody>
</table>

Neural Networks can be always highly uncertain, which may seem to work well for out-of-distribution (OOD) detection tasks but overestimates the uncertainty, even for the correctly classified samples within the training data distribution. For evaluating predictive uncertainty on known classes, Expectation Calibration Error (ECE Guo et al. (2017)) has been used. Normalized entropy is reported for evaluating predictive uncertainty on unknown classes. LeNet with ReLU and a L2 coefficient of 1e-8 has been chosen for MNIST dataset, which constitutes of 2 convolution layers followed by 2 fully connected layers. The networks are intentionally trained to over-fit or over-confident, so that we can observe the effects of capturing model uncertainty. For CIFAR10, we choose VGG like architecture with 2 convolution layers followed by 3 fully connected layers. We used batch normalization instead of dropout layers.

The results are reported in table 2 where we also compared to MC-dropout (Gal, 2016) and deep ensemble (Lakshminarayanan et al., 2017), which are widely used baselines in practice. For CIFAR10, we omitted MC-dropout as additionally inserting dropout layers would result in a different network and thus, the direct comparisons would not be difficult. For LA-based methods, we have reported the best results after searching 300 hyperparameters each. We find this evaluation protocol to be crucial, as LA-based methods are sensitive to these regularizing hyperparameters. Importantly, these results demonstrate that when projected to different success criteria, no inference methods largely win uniformly. Yet these experiments also show empirical evidence that our method works in principle and compares well to the current state-of-the-art. Estimating the layer-wise parameter posterior distribution in a sparse information form of MND, and demonstrating a low rank sampling computations, we show an alternative approach of designing scalable, high performance and practical inference framework.

4.4. Large Scale Experiments

To show the scalability of our method, we conduct an extensive experimental evaluation on the ImageNet dataset, using 5 DNNs. This result alone is a key benefit of estimating model uncertainty of DNNs in sparse information form since approximate Bayesian inference only involves the computations of the information matrix in a training-free manner and the method boosts relaxed assumptions about the model when compared to MC-dropout (e.g. no specific regularizer is required). We also emphasize that the proposed diagonal correction requires only back-propagated gradients. EFB also uses the same gradients in their update step, and the whole chain takes around 8 hours on ImageNet with 1 NVIDIA Volta GPU. This means that one can store the exact diagonals of the Fisher during EFB computations and simply add a correction term without involving any data. Thus, the added computational overhead due to the diagonal correction is negligible in practice. Similar to section 4.3, we evaluate the both calibration and OOD detection performances. SWAG and SWA are the chosen baselines, as Maddox et al. (2019) demonstrated that these methods scale to the ImageNet dataset. Moreover, to achieve comparability for large-scale settings, we scaled the other LA-based methods up so that they are applicable to ImageNet. This was not available in the original papers, and it constitutes an advance in evaluating LA-based methods for realistic scenarios. More importantly, we perform an extensive hyperparameter search over 100 randomly selected configurations for each LA-based methods. We believe that such protocols are required for fair evaluations of LA-based methods.

To directly compare the calibration across different methods, a variant of the reliability diagram (Maddox et al., 2019) is used (figure 6 for ResNet 18). We present results for all other
architectures in supplementary materials. Here, we observe that all LA variants significantly outperform SGD, SWA and SWAG. Results of OOD detection tasks are reported in figure 7 where we also show the predictive uncertainty of the in-domain data for checking the under-confident behavior (Grimmett et al., 2015; Mund et al., 2015; Grimmett et al., 2013). We use artistic impressions and paintings of landscapes and objects as OOD data. Again, SGD, SWAG, and SWA are in turn significantly outperformed by INF, which clearly separates in-distribution and OOD data. These results show the competitiveness of our approach for the real-world applications. However, we also find that all the LA-based methods almost identically yield strong results, clearly separating the in-distribution and OOD data.

While our method scales to ImageNet, we do not find that improvements in terms of Frobenius norm of error translates to performance in uncertainty estimation. This is the effects of regularizing hyperparameters ($\tau$ and N) which is a limitation of LA based approaches. We find a counter-intuitive result that Diag LA performs similar to ours and KFAC. It is therefore a strong alternative in practice where its complexity is superior than others (see table 3). Yet, ours, as we use rank 100 in the experiments, are significantly superior in space complexity when compared to EFB and KFAC, while modeling the weight correlations. Therefore, we find the main use-case of INF: the applications such as aerial systems (Lee et al., 2018; 2020) and medical devices (Petrou et al., 2018a;b) which cannot afford much more memory due to the limited on-board computations, and requires structured form of model uncertainty, unlike Diag. Last but not least, the mathematical tools we develop and the idea of working on the inverse space of MND can also be useful in the context of variational inference as an example.

5. Conclusion

This work introduces the sparse information form as an alternative Gaussian posterior family for which, we presented novel mathematical tools such as a sparsification algorithm for the Kronecker factored eigendecomposition, and demonstrated how to efficiently sample from the resulting distribution. Our experiments show that our approach yields accurate estimates of the information matrix with theoretical guarantees, compares well to the current methods for the task of uncertainty estimation, scales to large scale data-sets while reducing space complexity, and can also be utilized for downstream tasks such as active learning.

Acknowledgements

We thank the anonymous reviewers and area chairs for their time and thoughtful comments. The authors also acknowledge the support of Helmholtz Association, the project ARCHES (contract number ZT-0033) and the EU-project AUTOPILOT (contract number 731993). Jianxiang Feng is supported by the Munich School for Data Science (MUDS) and Rudolph Triebel is a member of MUDS.

Table 3. Network Space Complexity Comparison: The total number of information matrix parameters and its size in MB are reported for ResNet and DenseNet variants. Lower the better. Here, we also check if the methods take into account the weight correlations (corr).

<table>
<thead>
<tr>
<th>Model</th>
<th>Parameters</th>
<th>Size</th>
<th>Corr</th>
<th>Parameters</th>
<th>Size</th>
<th>Corr</th>
<th>Parameters</th>
<th>Size</th>
<th>Corr</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResNet18</td>
<td>11,679,912</td>
<td>44.6</td>
<td>X</td>
<td>95,013,546</td>
<td>362.4</td>
<td>✓</td>
<td>108,695,458</td>
<td>407.0</td>
<td>✓</td>
</tr>
<tr>
<td>ResNet50</td>
<td>25,503,912</td>
<td>97.3</td>
<td>X</td>
<td>153,851,562</td>
<td>586.9</td>
<td>✓</td>
<td>179,355,474</td>
<td>684.2</td>
<td>✓</td>
</tr>
<tr>
<td>ResNet152</td>
<td>60,041,384</td>
<td>229.0</td>
<td>X</td>
<td>389,519,018</td>
<td>1485.9</td>
<td>✓</td>
<td>449,560,402</td>
<td>1714.9</td>
<td>✓</td>
</tr>
<tr>
<td>DenseNet121</td>
<td>7,895,208</td>
<td>30.1</td>
<td>✓</td>
<td>103,094,954</td>
<td>393.3</td>
<td>✓</td>
<td>110,990,162</td>
<td>423.4</td>
<td>✓</td>
</tr>
<tr>
<td>DenseNet161</td>
<td>28,461,064</td>
<td>108.6</td>
<td>✓</td>
<td>379,105,514</td>
<td>1446.2</td>
<td>✓</td>
<td>407,566,578</td>
<td>1554.7</td>
<td>✓</td>
</tr>
</tbody>
</table>

Figure 7. Entropy histograms ResNet50: From left to right: SGD, SWA, SWAG and INF. While SGD, SWA and SWAG fail to separate in- and out-of-domain data, INF is able to almost completely differentiate between known and unknown data.
References


