Diagnosing Convolutional Neural Networks using their Spectral Response

Victor Stamatescu  
Defence Science and Technology Group  
Edinburgh, SA 5111, Australia  
Email: victor.stamatescu@dst.defence.gov.au

Mark D. McDonnell  
Computational Learning Systems Laboratory (cls-lab.org)  
School of Information Technology and Mathematical Sciences  
University of South Australia  
Mawson Lakes, SA 5095, Australia

Abstract—Convolutional Neural Networks (CNNs) are a class of artificial neural networks whose computational blocks use convolution, together with other linear and non-linear operations, to perform classification or regression. This paper explores the spectral response of CNNs and its potential use in diagnosing problems with their training. We measure the gain of CNNs trained for image classification on ImageNet and observe that the best models are also the most sensitive to perturbations of their input. Further, we perform experiments on MNIST and CIFAR-10 to find that the gain rises as the network learns and then saturates as the network converges. Moreover, we find that strong gain fluctuations can point to overfitting and learning problems caused by a poor choice of learning rate. We argue that the gain of CNNs can act as a diagnostic tool and potential replacement for the validation loss when hold-out validation data are not available.

I. INTRODUCTION

Convolutional Neural Networks (CNNs) are computational models made of multiple processing layers whose parameters are learned from data. CNNs have been applied to a diverse range of tasks and continue to set new benchmarks in areas of computer vision, speech recognition and natural language processing [1]. Despite their widespread use, however, training on new data sets or with new models remains a complex process. This is in large part due to the wide search space of model architecture and hyper-parameters [2]. Poor choices can cause problems during training, including high bias (underfitting) or high variance (overfitting). If left undetected, such issues can severely degrade CNN performance at test time.

In this work our goal is to measure the response of CNNs trained for image classification to different input spatial frequencies. We then use this information as a way to probe and better understand the learning process. Given that some CNN layers include non-linearities, obtaining a transfer function for the entire network requires linearizing it first. We are, to our knowledge, the first to pursue this linearization approach, which is analogous to the way in which linear systems are characterized using their transfer functions.

The rest of this paper is organized as follows. Section II outlines key papers related to the spectral properties of CNNs. Section III describes the methodology, including how the spectral response was measured in a number of pre-trained CNNs. Section IV presents our experimental results, which demonstrate how spectral response can serve as a diagnostic tool during training. Finally, Section V concludes with a summary of our findings.

II. RELATED WORK

Heravi et al. [3] presented 4D visualizations of the frequency response in convolutional filter banks learned by CNNs. Based on this they proposed that the predictions output by CNNs may be sensitive to low amplitude additive noise due to the inability of the filters to suppress high spatial frequencies. Unlike their study, ours is focused on capturing the frequency response of the entire CNN, not just its linear filters.

Recent studies [4], [5], [6] have found that neural networks tend to fit low frequency components of input data first during training, while the higher frequencies are modeled more slowly at later stages. This phenomenon was investigated in terms of the regression of target functions in the Fourier domain and is used to explain how neural networks that are capable of overfitting can still generalize well on test data.

A number of other publications relating to CNN spectral properties have focused on improving processing speed and performance through new types of computational units and operators. These include spectral pooling [7], concatenated relu [8], spectral features from convolutional layer activations [9], and wavelet CNNs [10]. In particular, the pooling technique in [7] performs dimensionality reduction via truncation in the frequency domain, which preserves more information than spatial pooling.

Unlike those studies our focus is on measuring CNN spectral response to a specific test image. This is similar in some aspects to the approach taken in a number of CNN visualization methods [11], [12], [13], [14], which illustrate why a network has made its prediction for a particular input image. These methods provide 2D visualizations the input saliency or of features in higher layers. Our goal, however, is to summarize the CNN spectral response using a single metric, which can then be used in a similar way to the training and validation losses to identify problems during training.

III. THE CNN TRANSFER FUNCTION

A. Definition

An artificial neural network is a non-linear function $f$ with parameters $w$ that are learned during training, which maps an input tensor $x$ to an output tensor $z = f(x; w)$. This feed-forward operation is known as a forward pass or inference. In the case of CNNs, $f$ is typically composed of multiple
computational layers:
\[
z = f(x; w_1, \ldots, w_L) \\
= f_L(f_{L-1}( \ldots (f_1(x_0; w_1) \ldots; w_{L-1}); w_L),
\]
where \(x_0 = x\) is the input and each layer \(l = 1, \ldots, L\) computes an intermediate output \(x_l = f_l(x_{l-1}; w_l)\). Depending on the task, \(z\) may have the dimensions of a multidimensional tensor, a 2D matrix, a 1D vector or a scalar.

Our aim is to define a transfer function for a CNN. For a linear system, such as a low-pass filter, the transfer function is found by taking the Fourier transform of its coefficients or, alternatively, by measuring its gain and phase using sinusoidal input signals of different frequencies. CNNs, however, are highly non-linear, so the gain would depend not only on the spatial frequency of the input but also on its amplitude. We therefore need to first linearize the network about a certain operating point. Fortunately, linear approximations can be obtained by performing a backward pass through the CNN using backpropagation [11].

During training, a loss function is added as the final layer and the output becomes a scalar \(z\). Backpropagation applies the chain rule to obtain its gradient with respect to the parameters in each layer:
\[
\frac{dz}{d(w_l)} = \frac{df_L(x_{L-1}; w_L)}{d(x_{L-1})} \times \ldots \times \frac{df_{l+1}(x_l; w_{l+1})}{d(x_l)} \times \frac{df_l(x_{l-1}; w_l)}{d(w_l)},
\]
where each intermediate derivative is evaluated at an operating point set by \(x_0\) and uses the current parameter values. The resulting parameter derivatives are used by gradient descent optimization algorithms to carry out parameter updates. In Eqn. (2) we followed the convention used in [15], where data and parameter tensors are stacked into vectors.

Backpropagation in Eqn. (2) works by passing back each layer’s data derivative, which is a large Jacobian matrix, to the layer \(l\) below. A memory efficient implementation that avoids direct handling of the Jacobian involves passing back a projected derivative instead [15]:
\[
\Phi_l = \frac{d\langle \Phi_{l+1}, f_{l+1}(x_l; w_{l+1}) \rangle}{dx_l},
\]
Here the inner product \(\langle \ldots \rangle\) projects the layer along direction \(\Phi_{l+1}\), which produces a scalar whose derivative is then evaluated. When this process is repeated sequentially starting from the output layer, \(\Phi_l\) becomes the projected derivative of the network down to this layer.

Considering now the entire network, for a given projection tensor \(p\) and output \(z = f(x; w)\), a single backward pass provides the projected data derivative \(\frac{d\langle p, f(x; w) \rangle}{dx}\) of the network output with respect to its input. This was interpreted by Simonyan et al. [11] as the derivative in a first order Taylor approximation for the CNN, evaluated in the neighborhood given by the forward pass over an input \(x_0\):
\[
\frac{dz}{dx} = \frac{d\langle p, f(x; w) \rangle}{dx} \bigg|_{x=x_0}.
\]
Following this interpretation, we treat \(\frac{dz}{dx}\) as a linear system and calculate its frequency response by taking the Fourier transform \(\mathcal{F}\) and computing the amplitude spectrum (in dB):
\[
|H| = 20 \times \log_{10}(\mathcal{F} \left( \frac{dz}{dx} \right)),
\]
where \(H\) is the transfer function.

### B. Toy CNN example

![Fig. 1: Color image whose red channel is input to a toy CNN consisting of a \textit{conv} layer, which applies a Gaussian filter \(w\), followed by a \textit{relu} layer.](image)

Fig. 1: Color image whose red channel is input to a toy CNN consisting of a \textit{conv} layer, which applies a Gaussian filter \(w\), followed by a \textit{relu} layer.

We constructed a two-layer toy CNN to illustrate the above discussion, applying it to the mean-subtracted red channel of the image in Figure 1. The model consists of a linear \textit{conv} layer, which convolves the input (Figure 2a) with a 2D filter \(w\), followed by a non-linear \textit{relu} layer, which produces an output map \(z\) (Figure 2c) by applying a rectified linear unit to each pixel in the feature map produced in the previous layer (Figure 2b). The filter \(w\) is a symmetric single-channel 7 × 7 pixel Gaussian filter with \(\sigma = 1\) pixels, shown in Figure 1b.

Following the forward pass, a backward pass was used to compute the data derivative \(\frac{dz}{dx}\). As shown in Figure 3, this depends on the choice of 2D projection tensor \(p\), which has the dimensions of \(z\). In Figure 3a we used \(p\) set to 0 everywhere except \((150, 100)\), where it was 1. These coordinates correspond to a non-zero output unit in \(z\) and any such location would yield the same frequency response, which, barring edge effects, is shift-invariant. Conversely, setting \(p\) to 1 at a location where \(z\) is 0 would yield 0 everywhere in \(\frac{dz}{dx}\). As detailed in [13], this effect is due to the \textit{relu} non-linearity and is further illustrated by Figure 3b, where \(p\) was set to 1 everywhere.

The data gradient in Figure 3a is simply the flipped impulse response of the symmetric Gaussian filter at a particular location in the input image. Hence the toy CNN frequency response given input \(x\) and and our choice of \(p\) is the amplitude of the Fourier transform pair to a low-pass filter, which is the linear component of the CNN.
In order to measure the frequency response of CNNs such as AlexNet [17], which was trained to perform image classification on ImageNet [18], the tensor $p$ must match the dimension of the output vector of class probabilities $z$. This is given by the application of the $\text{softmax}$ function to the logit vector $i$ of units in the final layer:

$$z_i = \frac{\exp(i)}{\sum_{j=1}^{N} \exp(j)} \quad (6)$$

where $i = 1, \ldots, N$ is the class index and, for ImageNet, $N = 1000$ object classes. The predicted class index and its confidence score are extracted as $i = \arg\max z$ and $\text{score} = \max z$, respectively.

We consider only the frequency response for the winning class by using the projection tensor to extract a data derivative with respect to the output unit $i$ by setting all other elements in $p$ to zero. Given that scaling $p$ also scales $dz/dx$ by the same factor (see Eq. (4)), to enable comparison between different CNNs we set its non-zero element to $p_i = 1/\text{score}$. This normalizes the frequency response for the different CNN scores obtained from respective forward passes over the same input image.

Figure 5 shows the data derivative and frequency response for the red channel of a natural image and an impulse image, both obtained using AlexNet. The impulse image had the same input repeated across its red, green and blue channels. Simonyan et al. [11] refer to examples like those in Figure 5 as image-specific class saliency because they indicate which input pixels have most impact on the score. We found it difficult to characterize the shape of the resulting 2D amplitude spectra in Figure 5 with a single metric (e.g. bandwidth), however, in terms of the overall gain, taking the surface maximum provides the Maximum Gain (in dB) of the frequency response.

### D. Results: pretrained models

We used 18 CNNs trained on ImageNet from MatConvNet[4] to compare their frequency response. Figure 6 shows the data derivative and frequency response obtained for the impulse image red channel and the top-5 error rate achieved by each model on the ImageNet Large Scale Visual Recognition Challenge (ILSVRC) 2012 validation data set. We observe that the best performing models are also the most sensitive to perturbations in the input so that their frequency response tends to have higher gain. Figure 7 shows the Maximum Gain versus the error rate for each input channel in the impulse image. The best performing models tend to have maximum gains above $\sim -20$ dB whereas the worst performing models tend to have Maximum Gains below this. This trend persists if setting $p_i = \text{score}$ because all models have comparable, low scores from their forward pass over the impulse image.

### IV. Diagnose Training with Maximum Gain

Given the previous results for pre-trained CNNs, we examined the behavior the frequency response during training in an effort to answer empirically the following questions:

- Does the Maximum Gain increase as the CNN learns?
- Is Maximum Gain a useful quantity in deciding when the CNN has converged?

1http://www.vlfeat.org/matconvnet/pretrained/
To this end we trained CNNs on two public data sets using publicly available code\(^4\) that performs Stochastic Gradient Descent (SGD) using backpropagation. We then measured the Maximum Gain from the impulse image induced frequency response for snapshots of the same CNN saved after each training epoch.

We followed this approach across a set of experiments that examine the impact of learning rate on performance, as this is a known source of problems when not set appropriately. This enabled us to explore the potential for using Maximum Gain to detect such problems by comparing it to training and validation loss curves, which are normally used to probe the learning process.

A. Training on MNIST

We examined the behavior of Maximum Gain for an impulse image while training on the MNIST handwritten digit image data set\(^{23}\), which contains 10 classes and consists of 60,000/10,000 training/validation grayscale images that are 28 × 28 pixels in size. For these experiments we chose to use the simple and well understood LeNet architecture\(^{24}\), which does not require a complex learning rate schedule to train properly. The CNN was made of three \textit{conv} layers and one \textit{fully-connected} layer, interspersed with non-linearities in the form of two \textit{max pool} layers and a \textit{relu} layer.

We began by training the CNN using a default learning rate of 0.001 over 20 epochs, the results of which are the red curves in Figures\(^5\) and\(^6\). Here the Maximum Gain rises initially, then remains flat after \(\sim 10\) epochs. The corresponding training loss decreases over all epochs as the fit to the training data improves, while the validation loss decreases slowly up to epoch \(\sim 12\) after which it too becomes flat. The corresponding error rates have similar behavior. Here the Maximum Gain provides a similar diagnostic information as the validation loss.

In Figure\(^5\) the learning rate was increased by \(\times 2, \times 3\) and \(\times 4\), which progressively increased the variability of the Maximum Gain curves. In the case of the largest learning rate, training and validation losses begin to rise beyond epoch 7, which indicates that the CNN is not learning, and the Maximum Gain curve no longer exhibits smoothly increasing or constant behavior, as was the case for a learning rate of 0.001.

The learning rate was next reduced by factors 1/3 and 1/10 in Figure\(^9\). Maximum Gain is not as sensitive to these changes, however, for the lowest learning rate, it slowly rises over 20 epochs. This indicates that the network would continue to learn if trained for longer. Given the fixed number of epochs, these Maximum Gain curves indicate that the two higher learning rates are more appropriate. This is confirmed by the validation errors, which provide the additional insight that after 20 epochs the learning rate of 0.001 performs better than the learning rate of 0.001/3.

B. Training on CIFAR-10

We next measured the Maximum Gain during training on the CIFAR-10 image data set\(^{25}\), which contains 10 classes and consists of 50,000/10,000 training/validation color images that are 32 × 32 pixels in size. The Maximum Gain obtained for each input color channel was averaged in order to only have one value per model. As this is a more difficult data set than MNIST, a larger LeNet architecture was deployed, with four \textit{conv} layers, two \textit{average pool} layers and one \textit{fully-connected} layer together with two \textit{max pool} layers and four \textit{relu} layers. Results from a second architecture\(^{26}\) are compared in the discussion below (IV-C2).

The CNN was initially trained with a learning rate of 0.05 over 45 epochs and this corresponds to the red curves in Figures\(^10\) and\(^11\). The Maximum Gain drops at first, then remains steady up to epoch \(\approx 27\), where it becomes more variable. This corresponds to a rise in validation loss coupled with decreasing training loss and shows that the Maximum Gain curve is able to detect the problem of strong overfitting.

Figure\(^10\) shows that increasing the learning rate leads to additional variability in the Maximum Gain curve at all epochs.

---

\(^{4}\)http://www.vlfeat.org/matconvnet/training/

---

To this end we trained CNNs on two public data sets using publicly available code\(^4\) that performs Stochastic Gradient Descent (SGD) using backpropagation. We then measured the Maximum Gain from the impulse image induced frequency response for snapshots of the same CNN saved after each training epoch.

We followed this approach across a set of experiments that examine the impact of learning rate on performance, as this is a known source of problems when not set appropriately. This enabled us to explore the potential for using Maximum Gain to detect such problems by comparing it to training and validation loss curves, which are normally used to probe the learning process.

A. Training on MNIST

We examined the behavior of Maximum Gain for an impulse image while training on the MNIST handwritten digit image data set\(^{23}\), which contains 10 classes and consists of 60,000/10,000 training/validation grayscale images that are 28 × 28 pixels in size. For these experiments we chose to use the simple and well understood LeNet architecture\(^{24}\), which does not require a complex learning rate schedule to train properly. The CNN was made of three \textit{conv} layers and one \textit{fully-connected} layer, interspersed with non-linearities in the form of two \textit{max pool} layers and a \textit{relu} layer.

We began by training the CNN using a default learning rate of 0.001 over 20 epochs, the results of which are the red curves in Figures\(^5\) and\(^6\). Here the Maximum Gain rises initially, then remains flat after \(\sim 10\) epochs. The corresponding training loss decreases over all epochs as the fit to the training data improves, while the validation loss decreases slowly up to epoch \(\sim 12\) after which it too becomes flat. The corresponding error rates have similar behavior. Here the Maximum Gain provides a similar diagnostic information as the validation loss.

In Figure\(^5\) the learning rate was increased by \(\times 2, \times 3\) and \(\times 4\), which progressively increased the variability of the Maximum Gain curves. In the case of the largest learning rate, training and validation losses begin to rise beyond epoch 7, which indicates that the CNN is not learning, and the Maximum Gain curve no longer exhibits smoothly increasing or constant behavior, as was the case for a learning rate of 0.001.

The learning rate was next reduced by factors 1/3 and 1/10 in Figure\(^9\). Maximum Gain is not as sensitive to these changes, however, for the lowest learning rate, it slowly rises over 20 epochs. This indicates that the network would continue to learn if trained for longer. Given the fixed number of epochs, these Maximum Gain curves indicate that the two higher learning rates are more appropriate. This is confirmed by the validation errors, which provide the additional insight that after 20 epochs the learning rate of 0.001 performs better than the learning rate of 0.001/3.

B. Training on CIFAR-10

We next measured the Maximum Gain during training on the CIFAR-10 image data set\(^{25}\), which contains 10 classes and consists of 50,000/10,000 training/validation color images that are 32 × 32 pixels in size. The Maximum Gain obtained for each input color channel was averaged in order to only have one value per model. As this is a more difficult data set than MNIST, a larger LeNet architecture was deployed, with four \textit{conv} layers, two \textit{average pool} layers and one \textit{fully-connected} layer together with two \textit{max pool} layers and four \textit{relu} layers. Results from a second architecture\(^{26}\) are compared in the discussion below (IV-C2).

The CNN was initially trained with a learning rate of 0.05 over 45 epochs and this corresponds to the red curves in Figures\(^10\) and\(^11\). The Maximum Gain drops at first, then remains steady up to epoch \(\approx 27\), where it becomes more variable. This corresponds to a rise in validation loss coupled with decreasing training loss and shows that the Maximum Gain curve is able to detect the problem of strong overfitting.

Figure\(^10\) shows that increasing the learning rate leads to additional variability in the Maximum Gain curve at all epochs.


This corresponds to higher training and validation losses and error rates due to a degradation of the learning process. The effect of reducing rate by factors 1/3 and 1/10 is shown in Figure 11. The Maximum Gain curves become smooth and increase between epochs $\sim 7$ and 45. In particular, the black curve for the lowest learning rate of 0.0055 suggests that the CNN has not yet converged. The blue curve, on the other hand, which corresponds to a learning rate of 0.05/3, also has higher variability at later epochs where the model overfits.

C. Discussion

1) Using Maximum Gain to select the learning rate and detect overfitting: Based on the preceding experiments, we summarize the key aspects of the learning process that Maximum Gain curves can diagnose:

- High variability across all epochs indicates that the learning rate is set too high.
- Smooth gradual rise across all epochs indicates that the learning rate is too low or that training for longer would noticeably improve performance.
- A rise followed by a smooth flattening suggests that the model has begun to converge.
- Smooth, flat behavior followed by high variability indicates when strong overfitting occurs and that it is time to stop training.

A caveat of this is that one must determine empirically what constitutes ‘high variability’ for a particular CNN architecture and data set by trialing a few learning rates. In terms of detecting model overfitting, however, what is ‘high’ or ‘low’ variability can be determined from the same curve.

2) Impact of model architecture: We trained a Network in Network (NIN) on CIFAR-10 using a learning rate of 0.005 for 100 epochs. Figure 12 shows that this achieves lower validation error than LeNet, which experiences strong overfitting beyond epoch 70. The LeNet Maximum Gain curve is flat up to this point, after which it becomes more variable and comparable to that of NIN, which is flat. This demonstrates that absolute value of Maximum Gain is not a reliable indicator of performance.

The impact of model capacity in shown in Figure 13, where we reduced and increased the number of filters in each LeNet conv layer by $\times 1/4$ and $\times 4$, respectively. The smaller model underfits, but its Maximum Gain curve is similar to the original, albeit with some additional variability. Hence, Maximum Gain does not detect underfitting, however, this is already highlighted by the high training error. The larger model overfits from epoch 15 and this is reflected in its Maximum Gain curve, which becomes increasingly variable.

V. CONCLUSION

In this work we have defined the transfer function of a CNN by using its input data derivative, which is obtained for a given input image via backpropagation. We characterized the resulting frequency response in terms of its peak value, which we called the Maximum Gain. Comparing CNNs with different architectures that were trained for image classification...
Fig. 7: Maximum Gain for channel of an impulse image input to the ImageNet models of Figure 6 versus their top-5 error rate on the ILSVRC 2012 validation set.

Fig. 8: Training LeNet on MNIST: separate training runs illustrate the effects of increasing a learning rate of 0.001 (red) by \( \times 2 \) (green), \( \times 3 \) (blue) or \( \times 4 \) (black) on the maximum gain as well as on the training/validation (solid/dashed lines) losses and error rates.

Fig. 9: Training LeNet on MNIST: separate training runs illustrate the effects of reducing a learning rate of 0.001 (red) by \( \times \frac{1}{3} \) (blue) or \( \times \frac{1}{10} \) (black) on the maximum gain as well as on the training/validation (solid/dashed lines) losses and error rates.
on ImageNet, we found that better performing models tend to have higher Maximum Gain for an impulse image. Intrigued by this observation, we examined the behavior Maximum Gain during training and found that, when the learning process works well, it rises with training epoch and then saturates.

Experiments on MNIST and CIFAR-10 showed that Maximum Gain can provide similar information about the learning process as the validation loss. We propose that Maximum Gain can provide similar information about the learning process. When the learning process works well, it rises with training epoch and then saturates.

Acknowledgments

Discussions with Dr. Sebastien Wong of University of South Australia and Dr. Hugh Kennedy of DST Group are gratefully acknowledged.

References

[1] Y. LeCun, Y. Bengio, and G. Hinton, “Deep Learning,” nature, vol. 521, no. 7553, p. 436, 2015.
[2] B. Zoph, V. Vasudevan, J. Shlens, and Q. V. Le, “Learning Transferable Architectures for Scalable Image Recognition,” arXiv:1707.07012, 2017.
[3] E. J. Heravi, H. H. Aghdam, and D. Puig, “Analyzing Stability of Convolutional Neural Networks in the Frequency Domain,” arXiv:1511.03042, 2015.
[4] N. Rahaman, D. Arpit, A. Baratin, F. Draxler, M. Lin, F. A. Hamprecht, Y. Bengio, and A. Courville, “On the Spectral Bias of Deep Neural Networks,” arXiv:1806.08734, 2018.
[5] Z.-Q. J. Xu, Y. Zhang, and Y. Xiao, “Training behavior of deep neural network in frequency domain,” arXiv:1807.01251, 2018.
[6] Z. J. Xu, “Understanding training and generalization in deep learning by Fourier analysis,” arXiv:1808.04295, 2018.
[7] O. Rippel, J. Snoek, and R. P. Adams, “Spectral Representations for Convolutional Neural Networks,” in Advances in Neural Information Processing Systems (NIPS), 2018, pp. 2449–2457.
[8] W. Shang, K. Sohn, D. Almeida, and H. Lee, “Understanding and Improving Convolutional Neural Networks via Concatenated Rectified Linear Units,” in International Conference on Machine Learning (ICML), 2016, pp. 2217–2225.
Fig. 12: Training on CIFAR-10 with learning rate of 0.005: comparison of the maximum gain as well as the training (solid lines) and validation (dashed lines) losses and error rates for the LeNet (red) or NIN (black) architectures.

Fig. 13: Training LeNet on CIFAR-10 with learning rate of 0.005: scaling the original number of filters (red) in conv layers by \( \times 4 \) (black) and by \( \times 1/4 \) (blue). Training/validation losses and error rates are shown as solid/dashed lines.