Predicting trends in the quality of state-of-the-art neural networks without access to training or testing data

Charles H. Martin
Calculation Consulting
San Francisco, CA 94122, USA
charles@CalculationConsulting.com

Serena Peng
XXX
XXX, XXX
XXX

Michael W. Mahoney
ICSI and Department of Statistics,
University of California at Berkeley
Berkeley, CA 94720, USA
mmahoney@stat.berkeley.edu

ABSTRACT

In many applications, one must work with models that have been trained by someone else. For such *pretrained models*, one typically does not have access to training data or test data, and one does not know the details of how the models were built, the specifics of the data that were used to train the model, what was the loss function or hyperparameter values, how precisely the model was regularized, etc. Here, we present and evaluate quality metrics for pretrained neural network models at scale. The most promising are metrics drawn from traditional statistical learning theory (e.g., norm-based capacity control metrics) as well as metrics (e.g., fitted power law metrics used to characterize the degree of strong correlations in a system) derived from the recently-developed Theory of Heavy-Tailed Self Regularization (HT-SR). Using the publicly-available *WeightWatcher* tool, we analyze hundreds of publicly-available pretrained models, including older and current state-of-the-art models in computer vision and natural language processing. We find that norm-based metrics do a reasonably good job at predicting quality trends in well-trained models, i.e., they can be used to discriminate between "good-better-best." On the other hand, for models that may not be well-trained (which, arguably is the point of needing metrics to evaluate the quality of pretrained models), i.e., when we want to distinguish "good-bad," norm-based metrics can qualitatively fail. We also find that HT-SR metrics do much better, quantitatively better at discriminating good-better-best and qualitatively better at discriminating good-bad. HT-SR metrics can also be used to characterize fine-scale properties of models, e.g., understanding layer-wise *correlation flow*, and evaluate post-training modifications such as model distillation and model improvement.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

KEYWORDS

XXX, datasets, neural networks, gaze detection, text tagging

Woodstock '18, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122XXX

ACM Reference Format:
Charles H. Martin, Serena Peng, and Michael W. Mahoney. 2XXX. Predicting trends in the quality of state-of-the-art neural networks without access to training or testing data . In *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/1122445.1122XXX

1 INTRODUCTION

A common problem in machine learning (ML) is to evaluate the quality of a given model. A popular way to accomplish this is to train a model and then evaluate its training and/or testing error. There are many problems with this approach. Well-known problems with just examining training/testing curves include that they give very limited insight into the overall properties of the model, they do not take into account the (often extremely large human and CPU/GPU) time for hyperparameter fiddling, they typically do not correlate with other properties of interest such as robustness or fairness or interpretability, and so on. A somewhat less well-known problem, but one that is increasingly important (in particular in industrial-scale ML—where the *users* of models are not the *developers* of the models) is that one may have access to neither the training data nor the testing data. Instead, one may simply be given a model that has already been trained—a *pretrained model*—and be told to use it.

Naïvely—but in our experience commonly, among both ML practitioners and ML theorists—if one does not have access to training or testing data, then one can say absolutely nothing about the quality of a ML model. This may be true in worst-case theory, but ML models are used in practice, and there is a need for a *practical theory* to guide that practice. Moreover, if ML is to become an industrial process, then that process will become siloed: some groups will gather data, other groups will develop models, and still other groups will use those models. The users of models can not be expected to know the precise details of how the models were built, the specifics of the data that were used to train the model, what was the loss function or hyperparameter values, how precisely the model was regularized, etc. Moreover, in industry, one faces unique practical problems such as: do we have enough data for this model? Methods that are developed and evaluated on any well-defined publicly-available coprus of data, no matter how large or diverse or interesting, are clearly not going to be well-suited to address problems such as this. It is thus of great practical interest to have metrics to evaluate the quality of a ML model in the absence of training and testing data and without any detailed knowledge of the training and testing process. We seek a practical theory for pretrained models which can predict how, when, and why such models can be expected to perform well or poorly.

In this paper, we present and evaluate quality metrics for pre-trained neural network (NN) and deep neural network (DNN) models at scale. To do so, we consider a large suite of hundreds of publicly-available models, mostly from computer vision (CV) and natural language processing (NLP). By now, there are many such state-of-the-art models that are publicly-available, e.g., there are now hundreds of pretrained models in CV ($\geq$ 500) and NLP ($\approx$ 100).[1] These provide a large corpus of models that by some community standard are state-of-the-art.[2] They include [michael: XXX, XXX and XXX. MORE DETAILS.] [michael: XXX. LIST PLACES WHERE THEY ARE AVAIALBLE, HERE OR IN NEXT SECTION.] Importantly, all of these models have been trained by someone else and have been viewed to be of sufficient interest/quality to be made publicly-available, and for all of these models, we have no access to training data or testing data, and we have no knowledge of the training/testing protocols.

The *quality metrics* we consider are based on the spectral properties of the layer weight matrics. Note that unlike traditional ML approaches, however, *we do not seek a bound on the generalization* (e.g., by evaluating training/test error during training), *we do not seek a new regularizer*, and *we do not aim to evaluate a single model* (e.g., hyperparmeter optimization).[3] Instead, we want to examine different models across common architecture series, and we want to compare models between different architectures themselves, and in both cases *we aim to predict trends in the quality of pre-trained models without access to training or testing data.*

In more detail, our main contributions are the following.

- [michael: XXX TECHNICAL THING 1]
- [michael: XXX TECHNICAL THING 2]
- [michael: XXX TECHNICAL THING 3]
- [michael: XXX TECHNICAL THING 4]

MENTION: The most promising are metrics drawn from traditional statistical learning theory (e.g., norm-based capacity control metrics) as well as metrics (e.g., fitted power law metrics used to characterize the degree of strong correlations in a system) derived from the recently-developed Theory of Heavy-Tailed Self Regularization (HT-SR). AND DEFINE HT-SR ACRONYM. [michael: Sentence or two about how our metrics come from norm-based SLT and alpha-based HT-SR theory, since that is also highlighted in the abstract.]

SOMEWHERE CITE WEIGHTWATCHER: [**?**]

Organization of this paper. We start in Section 2 and Section 3 with background and an overview of our general approach. In Section 4, we study three well-known widely-available DNN CV architectures (the VGG, ResNet, and DenseNet series of models); and we provide an illustration of our basic methodology, both to evaluate the different metrics against reported test accuracies and to use quality metrics to understand model properties. Then, in Section 5, we look at several variations of a popular NLP DNN architecture (the OpenAI GPT and GPT2 models); and we show how model quality and properties vary between several variants of GPT and GPT2, including how metrics behave similarly and differently. Then, in Section 6, we present results based on an analysis of hundreds of pretraind DNN CV models, showing how well each metric is correlated with the reported test accuracies, and how the Alpha-Norm metric(s) perform remarkably well. Finally, in Section 7, we provide a brief discussion and conclusion.

2 BACKGROUND AND RELATED WORK

To our knowledge, there is very little work on the particular question we are addressing: namely, how to predict, in a theoretically-principled manner, the quality of large-scale state-of-the-art NNs, and to do so without access to training data or testing data or details of the training protocol, etc. Our work is, however, loosely related to several other lines of work, and we briefly discuss them here.

Statistical mechanical theory of NNs. Statistical mechanical ideas have long had influence on NN theory and practice [**? ? ?**]; and our best-performing metrics (i.e., those using fitted PL exponents and HT-SR Theory) are based on statistical mechanics ideas [**? ? ? ? ?**]. However, that the way in which we *use* statistical mechanics theory is quite different than the way it is more commonly formulated. Several very good overviews of the more common approach are available [**? ?**]. We will *use* statistical mechanics theory more as it is used in quantitative finance. Thus, much more relevant for our metholodogical approach is older work of Bouchaud, Potters, Sornette, and coworkers [**? ? ? ?**] on the statisical mechanics of heavy tailed and strongly correlated systems.

XXX. Distinguish between what we will call a *phenomenological theory* (that describes empirical relationship of phenomena to each other, in a way which is consistent with fundamental theory, but is not directly derived from that theory) and what can be called a *first principles theory* (that is applicable to tiny things but has no hope of scaling up). [charles: it is the oppposite...ab initio theory scales quite well...it is the spherical cow models of physics and ML that do not scale. What we have is a semi-empirical theory. We use real theory, but require empirical input, at least in the new stat mech work. What we have introduced is a phenomenology, which to me is different from a semi-empirical or phenomenological theory] [michael: Let's touch base to get this right.] [4]

Norm-based capacity control theory. There is also a large body of work on using norm-based metrics to bound generalization error [**? ? ?**]. In this area, theoretical work aims to prove generalization bounds, and applied work uses these norms as a regularization function to improve training. While we do find that norms provide relatively good quality metrics, at least for distinguishing good-better-best among well-trained models, we are not interested in proving generalization bounds or improving training.

Practical problems poorly addressed by theory. There are many very practical problems in ML that are poorly addressed by existing

[1] When we began this work in 2018, there were fewer than tens of such models; now in 2020, there are hundreds of such models; and we expect that in a year or two there will be an order of magnitude or more of such models.

[2] Clearly, there is a selection bias or survivorship bias here—people tend not to make publicly-available their poorly-performing models—but these models are things in the world that (like social networks or the internet) can be analyzed for their properties.

[3] We reiterate: One could use these techniques to improve training, and we have been asked about that, but we are not interested in that here. Our main goal here is to use these techniques to evaluate properties of state-of-the-art pretrained NN models.

[4] In most areas where there are complex highly-engineered systems (beyond complex AI/ML systems), one used phenomenological theory rather than first principles theory. For example, one does not try to solve the Schrödinger equation if one is interested in building a bridge or an airplane.

theory and that either motivated our work or should be addressable by our techniques. Here are several.

- **Simplicity, or lack of, accuracy metrics.** XXX.
- **Information leakage in the production pipeline.** XXX.
- **Cost of acquring labeled data.** XXX.

Importantly, there are many examples in ML where (as a practical matter) there is no reliable notion of accuracy, e.g., when generating fake text or realiztic chatbots, developing self driving cars, or just clusterting user profiles. [5]

3 METHODS

Let us write the Energy Landscape (or optimization function, parameterized by $\mathbf{W}_l$s and $\mathbf{b}_l$s) for a typical DNN with L layers, with activation functions $h_l(\cdot)$, and with $N \times M$ weight matrices $\mathbf{W}_l$ and biases $\mathbf{b}_l$, as:

$$E_{DNN} = h_L(\mathbf{W}_L \times h_{L-1}(\mathbf{W}_{L-1} \times h_{L-2}(\cdots) + \mathbf{b}_{L-1}) + \mathbf{b}_L). \quad (1)$$

We assume we are given several pretrained Deep Neural Networks (DNNs), e.g., as part of an architecture series. The models have been trained on (unspecified and unavailable) labeled data $\{d_i, y_i\} \in \mathcal{D}$, using Backprop, by minimizing some (also unspecified and unavailable) loss function $\mathcal{L}(\cdot)$. We expect that most well-trained, production-quality models will employ one or more forms of on regularization, such as Batch Normalization, Dropout, etc., and many will also contain additional structure such as Skip Connections, etc. Here, we will ignore these details, and will focus only on the layer weight matrices $\mathbf{W}_l$.

DNN Quality Metrics. Each DNN layer contains one or more layer 2D weight matrices $\mathbf{W}_l$, and/or 2D feature maps $\mathbf{W}_{i,l}$ extracted from 2D Convolutional layers. (For notational convenience, we may drop the i and/or i, l subscripts below; and we let $\mathbf{W}$ be a generic $N \times M$ weight matrix, with $N \geq M$.) We have examined a large number of possible quality metrics. The best performing metrics (recall that we can only consider metrics that do not use training/test data) depend on the norm and/or spectral properties of weight matrices, $\mathbf{W}$.[6] We consider the following metrics.

- Frobenius Norm: $\|\mathbf{W}\|_F^2 = \sum_{i,j} w_{i,j}^2 = \sum_{i=1}^M \lambda_i^2$
- Spectral Norm: $\|\mathbf{W}\|_\infty = \lambda_{max}$
- Weighted Alpha Metric: $\hat{\alpha} = \alpha \log \lambda_{max}$
- α-Norm (or α-Shatten Norm): $\|\mathbf{W}\|_\alpha^\alpha = \sum_{i=1}^M \lambda_i^\alpha$

The first two metrics are well-known in ML. The last two deserve special mention. For all these metrics, λ_i is the i^{th} eigenvalue of the *Empirical Correlation Matrix*, $\mathbf{X} = \mathbf{W}^T\mathbf{W}$, and so λ_{max} is the maximum eigenvalue of $\mathbf{X}$. (These eigenvalues are the squares of the singular values σ_i of $\mathbf{W}$, i.e., $\lambda_i = \sigma_i^2$.) For the last two metrics, the exponent α is the power law exponent that arises in the recently-developed *Theory of Heavy Tailed Self Regularization (HT-SR)* [**? ? ?**]. Operationally, α is determined by using the publicly-available *WeightWatcher* tool ([**?**]) to fit the Empirical Spectral Density (ESD) of $\mathbf{X}$, i.e., a histogram of the eigenvalues, call it $\rho(\lambda)$, to a truncated power law

$$\rho(\lambda) \sim \lambda^\alpha, \quad \lambda \leq \lambda_{max}. \quad (2)$$

[5]For example, current chatbots use perplexity as a proxy for passing a Turing test.
[6]We do not use intra-layer information from the models in our quality metrics, but as we will describe our metrics can be used to learn about that.

[michael: We need to be clear that this is a truncated power law fit and that λ_{max} comes from that and not the largest empirical eigenvalue.] [charles: Actually λ_{max} *is* the largest empirical eigenvalue] The Weighted Alpha Metric was introduced previously [**?**], where (on a much smaller set of data than we consider here) it was shown to correlate well with the trends in reported test accuracies of pretrained DNNs. Based on this, here we introduce and evaluate the α-Norm metric. One would expect $\hat{\alpha}$ to approximate the log α-Norm very well for $\alpha < 2$ and reasoably well for $\alpha \in [2, 5]$ [**?**].

Each of these metrics is defined for a given layer $\mathbf{W}$ matrix. For the Weighted Alpha Metric, we consider the average of $\hat{\alpha}$ over all layers, i.e., $\sum_l \hat{\alpha}_l = \sum_l \alpha_l \log \lambda_{max,l}$. [michael: Be careful to get that right.] For the norm-based metrics, we consider the *weighted* average of the log of the norm to the appropriate power. For example, for the α-Norm, we compute

$$\sum_l \log \|\mathbf{W}_l\|_{\alpha_l}^{\alpha_l} = \sum_l \alpha_l \log \|\mathbf{W}_l\|_{\alpha_l}. \quad (3)$$

Informallly, this amounts to assuming that the layer weight matrices are statistically independent, in which case we can estimate the model complexity C, or test accuracy, with a standard Product Norm (which resembles a data dependent VC complexity),

$$C \sim \|\mathbf{W}_1\| \times \|\mathbf{W}_2\| \times \cdots \times \|\mathbf{W}_L\|, \quad (4)$$

where $\|\cdot\|$ is a matrix norm. In this case, the log Complexity takes the form of an Average Log Norm,

$$\log C \sim \log \|\mathbf{W}_1\| + \log \|\mathbf{W}_2\| + \cdots + \log \|\mathbf{W}_L\|. \quad (5)$$

For the Frobenius and Spectral norms, we can use Eqn. (5) directly. For example, when taking $\log \|\mathbf{W}_l\|_F^2$, the 2 comes down and out of the sum, and thus ignoring it only changes the metric by a constant factor. For the Weighted Alpha Norm, however, α_l varies from layer to layer, and so in Eqn. (3) it cannot be taken out of the sum.

Spectral Analysis of Convolutional 2D Layers. There is some ambiguity in performing spectral analysis on Convolutional 2D (Conv2D) layers. A Conv2D layer can be represented as a 4-index tensor of dimension (w, h, in_ch, out_ch), specified by an $(w \times h)$ filter (or kernel) and in_ch / out_ch input / output channels, respectively (usually $in\_ch \leq out\_ch$). Typically, $w = h = k$, giving $(k \times k)$ tensor slices, or *pre-Activation Maps* $\mathbf{W}_{i,L}$ of dimension $(in\_ch \times out\_ch)$ each. There are at least three different approaches that have been advocated for applying the Singular Values Decomposition (SVD) to an Conv2D layer: run an SVD on each of the pre-Activation Maps $\mathbf{W}_{i,L}$, yielding $(k \times k)$ sets of M singular values; stack the feature maps into a single rectangular matrix of, say, dimension $((k \times k \times out\_ch) \times in\_ch)$, yielding in_ch singular values; compute the 2D Fourier Transform (FFT) for each of the (in_ch, out_ch) pairs, and run SVD on the resulting Fourier coeffients [**?**], leading to $\sim (k \times in\_ch \times out\_ch)$ non-zero singular values. Each method has tradeoffs. In principle, the third method is mathematically sound, but it is computationally expensive. For our analysis, because we are performing tens of thousands of calculations, we select the first method, which is numerically the fastest and is easiest to reproduce.[7]

[7]We provide a Google Colab notebook where all results can be reproduced, with the option to redo the calculations with the third option for the SVD of the Conv2D.

Normalization of Empirical Matrices. Normalization is an important, if underappreciated, practical issue. Importantly, the normalization of weight matrices does *not* affect the Power Law fits because the Heavy Tailed exponent α (as well as other metrics such as the Stable Rank and MP Soft Rank [**?** **?**]) is scale-invariant. Norm-based metrics, however, do depend strongly on the scale of the weight matrix. Typically, to apply RMT, we would usually define Correlation Matrix with $1/N$ normalization and assume that the variance of $\mathbf{X}$ is either unity or a known constant.[8] Pretrained DNNs are typically initialized with random weight matrices $\mathbf{W}_0$, with the variance already normalized to $\sqrt{1/N}$, or some variant of this, e.g., the Glorot/Xavier normalization [**?**], or a $\sqrt{2/Nk^2}$ normalization for Convolutional 2D Layers. We do not have conrol over the final empirical normalization of these models; and we do *not* normalize (or renormalize) the Empirical Correlation Matrices, i.e., we use them as-is. The only exception to this is that we do rescale the Conv2D pre-Activation Maps $\mathbf{W}_{i,L}$ by $k/\sqrt{2}$ so that they are on the same scale as the Linear layers.

The WeightWatcher Tool. We compute the metrics using the WeightWatcher tool (version 0.2.7), and we provide Jupyter notebooks in the github repo for this paper [**?**], making the results fully reproducible. [michael: XXX. FEW SENTENCES ABOUT REPRODUCIBILITY MORE GENERALLY HERE, HERE OR IN DISCUSSION/CONCLUSION.]

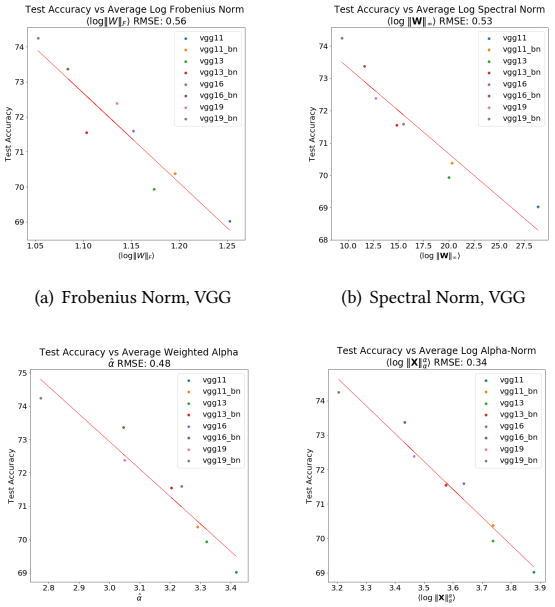
4 COMPARISON ACROSS SERIES OF CV MODELS

In this section, we examine quality metrics described in Section 3 for several Computer Vision (CV) model architecture series. This includes the VGG, ResNet, and DenseNet series of models, each of which consists of several pretrained DNN models, trained on the full ImageNet [**?**] dataset, and each of which is distributed with the current opensource pyTorch framework (version 1.4) [**?**]. This also includes a larger set of ResNet models, trained on the ImageNet-1K dataset [**?**], provided on the OSMR "Sandbox for training convolutional networks for computer vision" [**?**], which we call the ResNet-1K series.

We use our quality metrics to perform *coarse model analysis*, comparing and contrasting the three model series (or four, if ResNet-1K is included), permitting us to predict trends in model quality. We also use perform a more *fine layer analysis* as a function of depth for these models, providing novel insights among the VGG, ResNet, and DenseNet architectures.

Coarse Analysis: Quality Metrics versus Reported Test Accuracies. We have examined the performance of the four quality metrics (Frobenius norm, Spectral norm, Weighted Alpha, and α-Norm) applied to each of the VGG, ResNet, ResNet-1K, and DenseNet series. To start, Figure 1 considers the VGG series (in particular, the pretrained models VGG11, VGG13, VGG16, and VGG19, with and without BatchNormalization), and it plots the four quality metrics versus the reported Test accuracies [**?**], as well as a basic linear regression line. All four metrics correlate quite well with the reported Top1 Accuracies, with smaller norms and smaller values

[8]For formal proofs of Heavy Tailed results, one typically needs a different normalization such as $1/N^{1-\alpha}$.



(a) Frobenius Norm, VGG (b) Spectral Norm, VGG

(c) Weighted Alpha, VGG (d) α-Norm, VGG

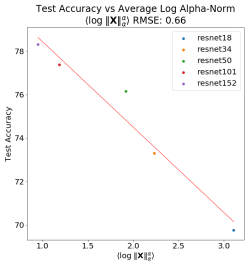
Figure 1: Comparison of quality metrics versus reported test accuracy for pretrained VGG models, trained on ImageNet, available in pyTorch. XXX Plots will be updated and replaced. [michael: Figures are unreadable, can we make fonts bigger, etc.]

Series	Num. Models	$\|\mathbf{W}\|_F$ Metric	$\|\mathbf{W}\|_\infty$ Metric	$\hat{\alpha}$ Metric	$\|\mathbf{X}\|_\alpha^\alpha$ Metric
VGG	6	0.56	0.53	0.48	**0.42**
ResNet	5	0.9	1.4	**0.61**	0.66
ResNet-1K	19	2.4	3.6	**1.8**	1.9
DenseNet	4	0.3	0.26	**0.16**	0.21

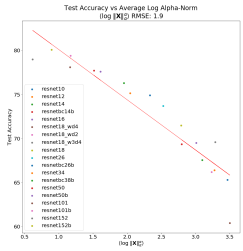
Table 1: RMSE (smaller is better) for linear fits of quality metrics to Reported Top1 Test Error for pretrained models in each architecture series. VGG, ResNet, and DenseNet were pretrained on ImageNet, and ResNet-1K was pretrained on ImageNet-1K. [michael: Are the numbers in this table stale; if they get updated, then we need to modify the test at at least two places, on actual numbers and on what is best.]

of $\hat{\alpha}$ implying better generalziation (i.e., greater accuracy, lower error). While all four metrics perform well, notice that the Log α-Norm metric ($\log \|\mathbf{W}\|_\alpha^\alpha$) performs best (with an RMSE of 0.42, see Table 1); and the Weighted Alpha metric ($\hat{\alpha} = \alpha \log \lambda_{max}$), which is an approximation to the Log α-Norm metric [**?**], performs second best (with an RMSE of 0.48, see Table 1).

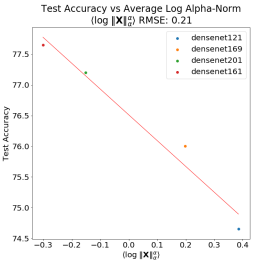
Figure 2 plots the Log α-Norm metric for the full ResNet, ResNet-1K, and DenseNet series. (A much more detailed set of plots, including the behavior of all four methods on each of the series, is available at [**?**].) Here, the Log α-Norm is much better that the Log Frobenius/Spectral norm metrics (although, as Table 1 shows, it is



(a) ResNet, α-Norm

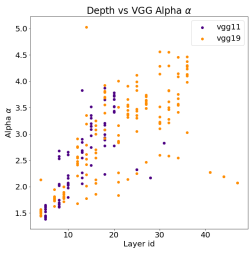


(b) ResNet-1K, α-Norm

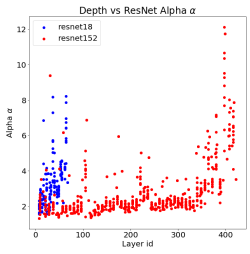


(c) DenseNet, α-Norm

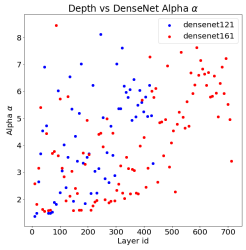
Figure 2: α-Norm versus reported Top1 Error for ResNet, ResNet-1K, and DenseNet models. The corresponding results for VGG are shown in Figure 1(d).



(a) VGG



(b) ResNet-1K



(c) DenseNet

Figure 3: Layer Analysis. PL exponent α versus layer id, for VGG, ResNet-1K, and DenseNet models. (Y axes on each plot are different.) ResNet-1K exhibits different and much more stable behavior across layers. This contrasts with how VGG gets gradually worse in deeper layers and how DenseNet is worse and much more erratic. We interpret this in the text as quantifying a *correlation flow* across the layers.

actually slightly worse than the Weighted Alpha metric). Notice also that ResNet series, which has been trained on the full ImageNet dataset, has an RMSE of 0.66, whereas the ResNet-1K series, which has been trained on the much smaller ImageNet-1K dataset, also correlated wells, but has a much larger RMSE of 1.9.

See Table 1 for a summary of results for Top1 Accuracies for all four metrics on all four model series. Similar results (not shown) are obtained for the Top5 Accuracies. Overall, for the the ResNet, ResNet-1K, and DenseNet series, all metrics perform relatively well, the Log α-Norm metric performs second best, and the Weighted Alpha metric performs best. These model series are all well-trodden, and our results indicate that norm-based metrics and PL-based metrics can both distinguish among "good-better-best" models, with PL-based metrics performing somewhat better.

Layer Analysis: Correlation Flow in CV Models. We can learn much more about a pretrained model by going beyond average values to examining quality metrics for each layer weight matrix, $\mathbf{W}$, as a function of depth (or layer id). For example, we can plot [just] the PL exponent, α,[9] as a function of depth. See Figure 3, which plots α for each layer (the first layer corresponds to data, the last layer to labels) for the least accurate (shallowest) and most accurate (deepest) model in each of the VGG (without BatchNormalization), ResNet-1K, and DenseNet series. (Again, much more detailed set of plots is available at [**?**]; but note that the corresponding layer-wise plots for Frobenius and Spectral norms are much less interesting than the results we present here.)

[9]That is, here we consider just α for each layer, not $\hat{\alpha}$ or $\|\mathbf{W}\|_{\alpha}^{\alpha}$.

In the VGG models, Figure 3 shows that the PL exponent α systematically increases as we move down the network, from data to labels, in the Conv2D layers, starting with $\alpha \lesssim 2.0$ and reaching all the way to $\alpha \sim 5.0$; and then, in the last three, large, fully-connected (FC) layers, α stabilizes back down to $\alpha \in [2, 2.5]$. This is seen for all the VGG models (again, only the shallowest and deepest are shown in this figure), indicating that the main effect of increasing depth is to increase the range over which α increases, thus leading to larger α values in later Conv2D layers of the VGG models. This is quite different than the behavior of either the ResNet-1K models or the DenseNet models.

For the ResNet-1K models, α also increases in the last few layers (more dramatically, in fact, observe the differing scales on the Y axes). However, as the ResNet-1K models get deeper, there is a wide range over which α values tend to remain small. [michael: Can we say something about exceptions which are larger than for VGG or DenseNet.] [charles: You have the same plots I do..what do you want to say >] [michael: Are they small or different types of layers or something?] [charles: Not that I am aware of. Ill think on it] This is seen for other models in the ResNet-1K series, but it is most pronounced for the larger ResNet-1K (152) model, where α remains relatively stable at $\alpha \sim 2.0$, from the earliest layers all the way until we reach close to the final layers.

For the DenseNet models, α tends to increase as the layer id increases, in particular for layers toward the end. While this is similar to what is seen in the VGG models, with the DenseNet models, α values increase almost immediately after the first few layers, and the variance is much larger (in particular for the earlier and middle layers, where it can range all the way to $\alpha \lesssim 8.0$) and much less systematic throughout the network.

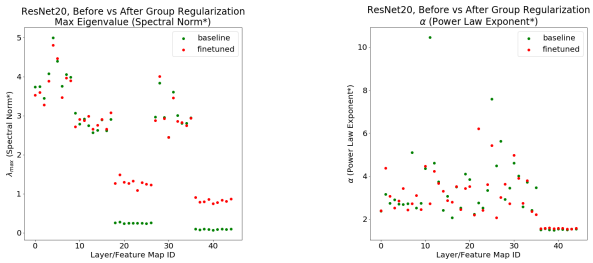
Recall the differences—in particular, the number of residual connections—between the VGG, ResNet, and DenseNet architectures. VGG, while a fine model in many ways, was limited by needing massive FC layers at the end of the model, requiring significant memory and computational resources, and it's poor conditioning led to problems with vanishing gradients. The empirical manifestations of this (on weight matrices) are that fitted α values get much worse for deeper layers. ResNet greatly improved on VGG by introducing residual connections, allowing for greater accurary with far fewer parameters. (Indeed, ResNet models of up to 1000 layers have been trained.) We conjuecture that the effeciency and effectivness of ResNet is reflected in the smaller and more stable $\alpha \sim 2.0$, across nearly all layers, indicating that the inner layers are very well correlated and strongly optimized. This should also be contrasted with the DenseNet model, which contains many connections between every layer. Our results (large α, meaning they even a HT model is probably a poor fit) suggest that DenseNet has too many connections, diluting high quality interactions across layers, and leaving many layers very poorly optimized.

More generally, we can understand Figure 3 in terms of the *flow of correlation*, as follows. Recall that the Log α-Norm metric and the Weighted Alpha metric are based on HT-SR Theory [**? ? ?**], which is in turn based on ideas from the statisical mechanics of heavy tailed and strongly correlated systems [**? ? ? ?**]. There, one expects well-trained systems which exhibit correlations over many size scales to have ESDs that can be well-fit by PLs, with PL exponents $\alpha \approx 2$. Much larger values of α indicate very poor fits, but the presence of many adjacent layers with relatively good PL fits *suggests* that those adjacent layers "impedance match" well and that the correlations that are captured by one layer propagate well to subsequent layers. Informally, one would expect a DNN model to perform well when it fascilitates the propagation of information/features across layers. In the absence of training/test data, we can to try to quantify this by measuring the PL properties of empirical weight matrices. Smaller α values correspond to layers in which correlations across multiple scales are better captured [**? ?**], and thus we expect that small values of α that are stable across multiple layers enable better *correlation flow* through the network.

Layer Analysis: Differences Between PL Metrics and Norm Metrics. The similarity between norm-based metrics and α-based metrics suggests a question: is the Weighted Alpha metric just a variation of the more familiar norm-based metrics, or does it capture something different? More generally, do fitted α values contain information not captured by norms? To show that it is not just a variation and that α does capture something different, consider the following example, which looks at a compressed / distilled DNN model [**?**].

We consider ResNet20, trained on CIFAR10, before and after applying the Group Regularization technique, as implemented in the `distiller` package.[10] We analyze the available pre-trained 4D_regularized_5Lremoved baseline and fine-tuned models. The reported baseline test accuracies ($Top1 = 91.45$ and $Top5 = 99.75$) are better than the reported fine-tuned test accuracies ($Top1 = 91.02$ and $Top5 = 99.67$) [**?**]. The previous results on ResNet (Table 1 and Figure 2 might suggest that the baseline Spectral Norm should be *smaller* than those of the layers in the fine-tuned model. [michael: Do we have something backwards here: where we observed that the average norm to increase with decreasing test error (as it "should" not), whereas the average PL exponent α decreases (as "expected" from HT-SR Theory).] In both cases (Frobenius norm results not shown), we observe the opposite. Figure 4 presents the Spectral Norm (λ_{max}) and PL exponent (α) for each individual layer weight matrix $\mathbf{W}_l$.[11] On the other hand, the α values do not differ systematically between the baseline and fine-tuned models. [michael: Some comment about big jump in norm; but fix previous backwards question first.] Also (not shown), the average (unweighted) baseline α is *smaller* than the fine-tuned average (as would be predicted by HT-SR Theory, on which $\hat{\alpha}$ is based).

[michael: XXX. WORK ON THIS PAR AFTER DO NLP EXAMPLES.] Our interpretation of this is the following. The pre-trained models in the `distiller` package have passed some quality metric, but they are much less well trodden than any of the VGG/ResNet/DenseNet models we condisered previously. Norms are often used as regularizers, and thys they are a natural metric to consider, e.g., during training or distillation. The PL α captures more subtle correlations. The reason for this is that the `distiller` Group Regularization technique has the unusual effect of increasing the norms of the $\mathbf{W}$ feature maps for at least two of the Conv2D layers. [michael: This impedance shuffling or whatever it is called messes up norms, but the strong correlations are still preserved, as seen in the $\hat{\alpha}$ metric,



(a) λ_{max} for ResNet20 layers (b) α for ResNet20 layers

Figure 4: Layer Analysis. ResNet20, distilled with Group Regularization, as implemented in the `distiller` (4D_regularized_5Lremoved) pre-trained models. Spectral Norm, λ_{max}, and, PL exponent, α, for individual layer, versus layer id, for both between baseline (before distillation, shown in green) and fine-tuned (after distillation, shown in red) pre-trained models.

[10] For details, see https://nervanasystems.github.io/distiller/#distiller-documentation and also https://github.com/NervanaSystems/distiller.

[11] Here, we only include layer matrices or feature maps with $M \geq 50$.

and the model quality is good. CLARIFY.] [michael: XXX. INTERPRET IN TERMS OF XXX GOOD VERSUS BAD, AS OPPOSED TO GOOD BETTER BEST.]

5 COMPARISON OF NLP TRANSFORMER MODELS

[michael: Need to say that such large α values don't mean much.]
[michael: Need to highlight difference between α and $\hat{\alpha}$.]

In this section, we examine the quality metrics described in Section 3 for several NLP model architectures.

apply more generally, where they differ, e.g., how the layer Spectral Norm behaves unexpectedly, while the α-based metrics can give insight into how well trained a model is.

[michael: We show that this not only works for CV, so we look at NLP. We now look in detail at the alpha metric, the spectral norm, and the new norm. We compare good and bad models, and a series of increasingly big models trained on big data sets. We show why alpha works but spectral norm is not enough
]

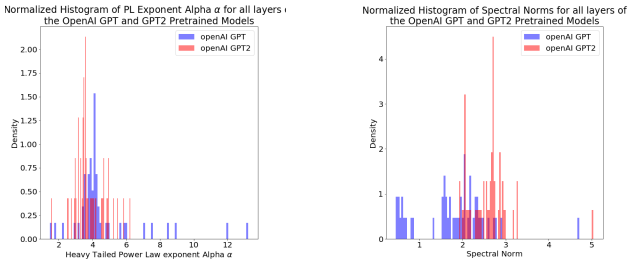
Within the past two years, nearly 100 open source, pre-trained DNNs for NLP have emerged, based on the revolutionary Transformer architecture. This includes variants of BERT, Transformer-XML, GPT, etc. The Transformer architectures consist of blocks of Attention layers, containing two large, Feed Forward (Linear) weight matrics [**?**]. In contrast to the smaller pre-Activation maps arising in Cond2D layers, Attention matrices are significantly larger, and frequently under-correlated, with generally larger Heavy Tailed Power Law exponents α (when fitting the ESD). Here, we breifly look at a few popular pretrained NLP DNNs to demonstrate that the Theory of Heavy Tailed Self-Regularization also applies to NLP models and not just CV models, and to highlight how to use the theory to identify poorly trained models where the empirical norm metrics will perform poorly.

OpenAI GPT Models. We use the *WeightWatcher* tool to analyze the OpenAI GPT and GPT2 models, which gives us the opportunity to analyze the effect of both training the same model with different size data sets, and increasing sizes of both the data set and architectures. These models have generated significant media attention because of their remarkable ability to generate fake text that appears to be real and the potential misuse of this. For this reason, the original GPT model was trained on on a deficient data set, rendering the model interesting but not fully functional. Later, OpenAI released a much improved model– GPT2 (small)–which has the same architecture and number of layers as GPT, but has been trained on a larger and better data set (and with other changes), making it remarkably good at generating (near) human-quality fake text. By comparing the poorly trained GPT to the well trained GPT2, we indentify empirical indidcators for when model has in fact been poorly trained and may perform poorly when deployed.

[charles: more here ?] We analyze GPT models deployed with the popular HuggingFace PyTorch library. GPT has 12 layers, with 4 Multi-head Attention Blocks, giving 48 Layer Weight Matrices $\mathbf{W}$. Each Block has 2 components, the Self Attention (attn) and the Projection (proj) matrics. The self-attention matrices are larger, of dimension (2304×768) or (3072×768). The projection layer concatenates the self-attention results into a vector (of dimension 768). This gives 50 large matrices.

Series	Num. Layers	$\|\mathbf{W}\|_F$ Metric	$\|\mathbf{W}\|_\infty$ Metric	$\hat{\alpha}$ Metric	$\|\mathbf{X}\|_\alpha^\alpha$ Metric
GPT	49	1.64	1.72	7.01	7.28
GPT (small)	49	2.04	2.54	9.62	9.87
GPT2 medium	98	2.08	2.58	9.74	10.01
GPT2 large	146	1.85	1.99	7.67	7.94
GPT2 xl	194	1.86	1.92	7.17	7.51

Table 2: Average value for each of the four metrics for pretrainnd OpenAI GPT and GPT2 models.



(a) Power Law Exponent (α) (b) log Spectral Norm ($\log \|\mathbf{W}\|_\infty$)

Figure 5: Comparison of Heavy Tailed Power Law exponents α, and log Spectral Norms $\log \|\mathbf{W}\|_\infty$ for the OpenAI GPT and GPT2 (small) pretrained models.

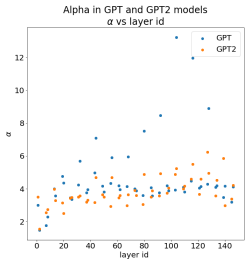
Because GPT and GPT are trained on different data sets, the initial Embedding matrices differ in shape. GPT has an initial Token and Positional Embedding layers, of dimension (40478×768) and (512×768), resp, whereas GPT2 has input Embeddings of shape (50257×768) and (1024×768), resp. Interstingly, they also have very spectral properties, also shown below.

The OpenAI GPT2 (English) models are: [gpt-small, gpt-medium, gpt-large, and gpt-xl], having include 12, 24, 36, and 48 layers, resp., with increasingly larger weight matrices. The model card for GPT2 is published on github.[12]. Table 2 reports results for the average log norm metrics, using *weightwatcher (0.2.7)*, and with fully reproducible Jupyter notebooks.[13]

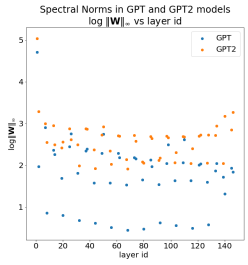
Empirical Quality Metrics for GPT and GPT2. We first compare the distribution of Heavy Tailed Power Law exponents α in GPT and GPT2. They are very differenmt, with GPT2 having both a notably smaller mean α, and far fewer, unusually large outliers. Figure **??** shows the empirical density (histogram) of α for all layers in GPT (blue) and GPT2 (red). [charles: discuss more]

Indeed, the α metric makes a good quality metric for comparing these models. Figure 5(a) compares the PL exponent α for the GPT and GPT2 models for all layers, As expected, the improved GPT2 model has, on average, smaller α than the older GPT, with all $\alpha \leq 6$. Indeed, the deficient GPT model has numerous weight matrices with unsually large fitted exponents, indicating that they are not

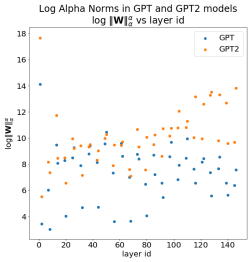
[12] https://github.com/openai/gpt-2/blob/master/model_card.md
[13] https://github.com/CalculatedContent/kdd2020



(a) Power Law Exponent (α)

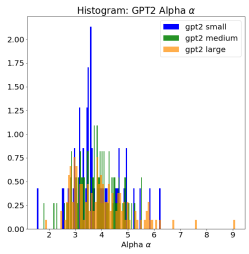


(b) log Spectral Norm (log $\|\mathbf{W}\|_\infty$)

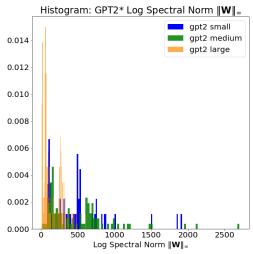


(c) log Alpha-Norm (log $\|\mathbf{X}\|_\alpha^\alpha$)

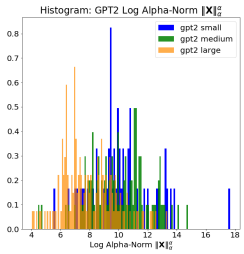
Figure 6: Comparison of Correlation Flow and Spectral Norm for OpenAI GPT and GPT2



(a) Power Law Exponent (α)



(b) log Spectral Norm (log $\|\mathbf{W}\|_\infty$)



(c) log Alpha-Norm (log $\|\mathbf{X}\|_\alpha^\alpha$)

Figure 7: Comparison of Power Law Exponnents, Spectral Norm, and Alpha-Norm for different size models in the GPT2 architecture series. *Note: the log spectral norms (b) histogram omits the first 2 layers, corresponding to the embedding layer, which are normalized differently and have anamolously large values.

Heavy Tailed at all. Indeed, we may expect that a poorly trained model will not exhibit consistent Heavy Tailed behavior in all layers.

However, as seen in Figure 5(b), the poorly trained GPT model has many smaller (log) Spectral Norms log $\|\mathbf{W}\|_\infty$ than the GPT2, which would be inconsistent with a belief that smaller Spectral Norm is always better. Indeed, because there are so many anamously small $\|\mathbf{W}\|_\infty$, it appears that the GPT model may be exhibiting a kind of rank collapse. This is an extremely important observation because it demonstrates that while the Spectral Norm may correlate well with predicted test error, it is not a good indicator of the overall quality of a model, and using it as an empirical metric may give spurious results when applied to poorly trained or otherwise deficient models.

Note that Figure 5(b) also shows a couple anomalously large Spectral Norms. From Figure 6(b) (below), we see that these correspond to the first embedding layer(s). These layers appear to have a normalization, and therefore a differenc scale. For example, in GPT, most layers, the maximum eigenvalue $\lambda_{max} \sim O(10-100)$, but in the first embedding layer, the maximum is of order N (the number of words in the embedding), or $\lambda_{max} \sim O(10^5)$. For GPT and GPT2, we layer all layers as-is (although one may to normalize the first 2 layers by $\mathbf{X}$ by $\frac{1}{N}$, or to treat them as an outlier). Here, we do not include them in our computed average metrics in Table 2, and do not include them in the histogram plot in Figure 5(b).

Correlation Flow in GPT and GPT2. also differs significantly between GPT and GPT2. Figure 6(a) plots α vs the depth (i.e. a layer id) for each model.

[charles: Discuss Spectral Norm, alpha-Norm]

GPT2: small, medium, large, xl. We now look across the series of increasingly improving GPT2 models, examining both our PL exponent α, as well as the various Norm metrics. As we move from small to xl, both the PL exponents α, and the peak of distribtion of log Norm metrics shifts from larger to smaller values. Figure 7 shows the histograms over the layer weight matrics for fitted α, and the log Spectral Norm log $\|\mathbf{W}\|_\infty$ and log Alpha-Norm log $\|\mathbf{W}\|_\alpha^\alpha$ metrics.

We see that the average α decreases with increasing model size, althogh, the differences are less noticible between GTP2 mkodels than between the GPT and GPT2 models. Unlike GPT, however, the Layer (log) Spectral Norms log $|\mathbf{W}\|_\infty$ and (log) Alpha-Norms log $|\mathbf{W}\|_\alpha^\alpha$ behave more as expected for GPT2 layers, with the larger models consistently having smaller norms. Likewise, Figure 7(b) shows decreasing average log Spectral Norms with the larger models. As we have seen in the trends of other well trained models.

We do notice, however, that while the peaks of the α is getting smaller, towards 2.0, the tails of the distribution shifts right, with larger GPT2 models having more usually large α. We suspect this indicates that these larger GPT2 models are overparameterized and/or not yet fully optimized and require datasets even larger than the recent XL 1.5B release [**?**].

6 COMPARISON OF ALL PRETRAINED CV MODELS

[michael: Now we go back to the CV models and look at over 100 of them, and draw' more broad conclusions about why alpha and the new norm is better, by looking at the MSE]

Here, we use the Weightwatcher tool to analyze 466 pretrained computer vision models Pytorch. These image classification and segmentation models are pretrained on nine datasets, ImageNet-1K, and CIFAR-10, CIFAR-100, Street View House Numbers (SVHN), Caltech-UCSD Birds-200-2011 (CUB-200-2011), Pascal VOC2012, ADE20K, Cityscapes, and Common Objects in Context (COCO). The pretrained models and their accuracy metrics are summarized in the osmr github

[charles: We actually don't run regressions on all these datasetsm, BUT we could present them in the Figure below to show that alpha is a good metric for these kinds of models, in contrast to the NLP, where alpha is frequently too large to run a regression]

[charles: This section needs a lot of work]

[charles: insert link in the footnote]

and a full summary of all the models analyzed is included in the Appendix. For our analysis, we then group models by architecture and datasets for further analysis.

In this paper, we propose that the Weightwatcher tool could be used to predict the trends in the generalization accuracy of deep neutral network without a test set. To test our proposition, we choose simple linear regression to analyze the relationship between the Weightwatcher metrics and the traditional accuracy metric obtained with a test set (we avoid polynomial regressions as they are more prone to overfitting and does not make economic sense). On the left-hand-side of regression, we have the Top1 errors, Top5 errors as reported for ImageNet-1K models, Error

To further refine our analysis, we run three batches of linear regressions. First at the global level, we divide models by datasets and run regression separately on all models of a certain dataset, regardless of the architecture. At this level, the plots are quite noisy and clustered as each architecture has its own accuracy trend but, you could still see that most plots show positive relationship with positive coefficients

[charles: see examples in Figure X]

(Here we omit the results for CUB-200-2011, Pascal-VOC2012, ADE20K, and COCO datasets as there are less than 15 models for those datasets and thus the regression is less statistically significant)

[charles: insert plots for Figure X]

For the second batch, we plot the regression for models of each architecture-datasets combination, which shows the relationship between the progression of the model accuracy and Weightwatcher metrics more clearly and precisely. For example, as you could see in the Figure X2,

[charles: Add an example, UPDATE when we have the results from the new codes]

Insert plots for Figure X2

While running each regression, we record the R-squared and mean squared errors (MSE) for each regression. We then filter out regressions with less than five datapoints and models with structural outliers.

[charles: Define and give an example of the structural outliers]

Dataset	# of Models
imagenet-1k	78
svhn	30
cifar-100	30
cifar-10	18
cub-200-2011	12

Table 3: Datasets used

Architecture	# of Models
ResNet	30
SENet/SE-ResNet/SE-PreResNet/SE-ResNeXt	24
DIA-ResNet/DIA-PreResNet	18
ResNeXt	12
WRN	12
DLA	6
PreResNet	6
ProxylessNAS	6
VGG/BN-VGG	6
IGCV3	6
EfficientNet	6
SqueezeNext/SqNxt	6
ShuffleNet	6
DRN-C/DRN-D	6
ESPNetv2	6
HRNet	6
SqueezeNet/SqueezeResNet	6

Table 4: Architectures used

	Frobenius Norm $\langle \log \|\mathbf{W}\|_F \rangle$	Spectral Norm $\langle \log \|\mathbf{W}\|_\infty \rangle$	Weighted Alpha $\langle \hat{\alpha} = \alpha \log \lambda_{max} \rangle$	Alph $\langle \log$
R^2 (mean)	0.63	0.55	0.64	
R^2 (std)	0.34	0.36	0.29	
MSE (mean)	4.54	9.62	3.14	
MSE (std)	8.69	23.06	5.14	

Table 5: Comparison of linear regression fits for different average log norm metrics across 5 computer vision datasets, 17 Architectures, covering 168 (out of 309) different pretrained DNNs. We only conclude regressions for architecturs with 4 or more data points [charles: and which are postively correlated with the test error?]**. These results can be readily reproduced using the Google Colab notebooks accompanying thie paper [?]**

[charles: What are the structrual outliers we chose ?]

Insert a plot for outliers, OPTIONAL

[charles: These tables could go to appendix. We need references]

[charles: Still preliminary, only 309 data points here]

Results.

7 CONCLUSION

[michael: Where, if anywhere to put the following:

- MOVE TO LATER: COMMENT ON HOW LOG NORM first and last layers behave, maybe somewhere else.

- MOVE TO LATER: COMMENT ON HOW LOG PORM for GPT includes unusually high alpha, not meaningful other than to show the trend.

]

XXX. PUT CONCLUSION HERE AND WEAVE IN COMMENTS FROM BELOW.

Some other comments that we need to weave into a narrative eventually after later sections are written:

- GPT versus GPT2. What happens when we don't have enough data? This is the main question, and we can use out metrics to evaluate that, but we also get very different results for GPT versus GPT2.
- The spectral norm is a regularizer, used to distinguish good-better-best, not a quality metric. For example, it can "collapse," and for bad models we can have small spectral norm. So, it isn't really a quality metric.
- One question that isn't obvious is whether regularization metrics can be used as quality metrics. One might think so, but the answer isn't obviously yes. We show that the answer is No. A regularizer is designed to select a unique solution from a non-unique good-better-best. Quality metrics can also distinguish good versus bad.
- (We should at least mention this is like the statistical thing where we evaluate which model is better, as oposed to asking if a given model is good, I forget the name of that.)
- There are cases where the model is bad but regularization metric doesn't tell you that. Quality should be correlated in an empirical way. Correlated with good-better-best; but also tell good-bad.
- Question: why not use regularier for quality? Answer: A regularizer selects from a given set of degenerate models one which is nice or unique. It doesn't tell good versus bad, i.e., whether that model class is any good.
- Thus, it isn't obvious that norm-based metrics should do well, and they don't in general.
- We give examples of all of these: bad data; defective data; and distill models in a bad way. (Of course, bad data means bad model, at least indirectly, since the quality of the data affects the properties of the model.)
- We can select a model and change it, i.e., we don't just do hyperparameter fiddling.

ACKNOWLEDGMENTS

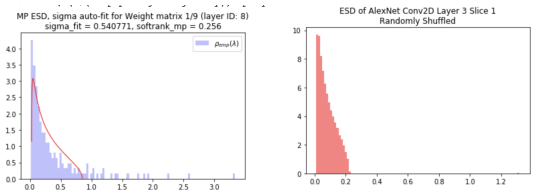
MWM would like to acknowledge ARO, DARPA, NSF, and ONR for providing partial support of this work.

A APPENDIX

XXX. APPENDIX.

[michael: I put this here for now as a placeholder. Where to put it. Maybe in a discussion/conclusion if there is space.]

XXX.. XXX. THIS VERIFICATION IS NOT ABOUT CONV LAYERS, IT IS ABOUT PL MORE GENERALLY, CORRECT? WE SHOULD CLARIFY AND SQUISH. To verify that our approach is meaningful, we need to confirm that the ESD is neither due to a random matrix, nor due to unsually large matrix elements, but, in fact, captures correlations learned from the data. We examine typical layer for the pretained AlexNet model (distributed with pyTorch). Figure 9(a) displays the ESD for the first slice (or matrix **W**) of the third Conv2D layer, extracted from a 4-index Tensor of shape (384, 192, 3, 3). The red line displays the best fit to a random matrix, using the Marchenko pastur theory [**?**]. We can see the random matrix model does not describe the ESD very well. For comparison, Figure 9(b) shows the ESD of the same matrix, randomly shuffled; here looks similar to the red line plot of the orginal ESD. In fact, the empircal ESD is better modeled with a truncated power law distribtion. [michael: We may want to give a one-sentence summary of this par and fig at the end of the previous par.] [charles: Here, on the RMT MP stuff, I think it makes sense to point back]



(a) Actual ESD (b) ESD of randomly shuffled matrix

Figure 9: ESD of AlexNet Conv2D pre-Activation map for Layer 3 Slice 1, actual and randomized. [michael: Need better figs here.]

Although the ESD is *Heavy Tailed*, this does not imply that the orginal matrix **W** is itself heavy tailed–only the correlation matrix **X** is. If **W** was, then it would contain 1 or more unusually large matrix elements, and they would dominate the ESD. Of course the randomized **W** would also be heavy tailed, but its ESD neither resembles the original nor is it heavy tailed. So we can rule out **W** being heavy tailed. [michael: These comments seem out of place, since they hold more generally than for the Conv2D layers.] [charles: Agreed. We could move this up. We have never really talked about this, but it is essential to explain the difference between assuming W is heavy tailed , which confuses everyone]

These plots tell us that the pre-activation maps of the Conv2D contains significant correlations learned from the data. By modeling the ESD with a power law distribution λ^{α}, we can characterize the amount of correlation learned; the smaller the exponent α, the more correlation in the weight matrix. [michael: These comments seem out of place, since they hold more generally than for the Conv2D layers.]