Reconciling modern machine-learning practice and the classical bias–variance trade-off

Mikhail Belkin, Daniel Hsu, Siyuan Ma, and Soumik Mandal

Department of Computer Science and Engineering, The Ohio State University, Columbus, OH 43210; Department of Statistics, The Ohio State University, Columbus, OH 43210; and Computer Science Department and Data Science Institute, Columbia University, New York, NY 10027

Edited by Peter J. Bickel, University of California, Berkeley, CA, and approved July 2, 2019 (received for review February 21, 2019)

Breakthroughs in machine learning are rapidly changing science and society, yet our fundamental understanding of this technology has lagged far behind. Indeed, one of the central tenets of the field, the bias–variance trade-off, appears to be at odds with the observed behavior of methods used in modern machine-learning practice. The bias–variance trade-off implies that a model should balance underfitting and overfitting: Rich enough to express underlying structure in data and simple enough to avoid fitting spurious patterns. However, in modern practice, very rich models such as neural networks are trained to exactly fit (i.e., interpolate) the data. Classically, such models would be considered overfitted, and yet they often obtain high accuracy on test data. This apparent contradiction has raised questions about the mathematical foundations of machine learning and their relevance to practitioners. In this paper, we reconcile the classical understanding and the modern practice within a unified performance curve. This “double-descent” curve subsumes the textbook U-shaped bias–variance trade-off curve by showing how increasing model capacity beyond the point of interpolation results in improved performance. We provide evidence for the existence and ubiquity of double descent for a wide spectrum of models and datasets, and we posit a mechanism for its emergence. This connection between the performance and the structure of machine-learning models delineates the limits of classical analyses and has implications for both the theory and the practice of machine learning.

Significance

While breakthroughs in machine learning and artificial intelligence are changing society, our fundamental understanding has lagged behind. It is traditionally believed that fitting models to the training data exactly is to be avoided as it leads to poor performance on unseen data. However, powerful modern classifiers frequently have near-perfect fit in training, a disconnect that spurred recent intensive research and controversy on whether theory provides practical insights. In this work, we show how classical theory and modern practice can be reconciled within a single unified performance curve and propose a mechanism underlying its emergence. We believe this previously unknown pattern connecting the structure and performance of learning architectures will help shape design and understanding of learning algorithms.

Author contributions: M.B., D.H., S. Ma, and S. Mandal designed research, performed research, analyzed data, and wrote the paper.

The authors declare no conflict of interest.

This article is a PNAS Direct Submission.

Published under the PNAS license.

1To whom correspondence may be addressed. Email: mbelkin@cse.ohio-state.edu.

This article contains supporting information online at www.pnas.org/lookup/suppl/doi:10.1073/pnas.1903070116/-/DCSupplemental.

Published online July 24, 2019.

www.pnas.org/cgi/doi/10.1073/pnas.1903070116

Machine learning has become key to important applications in science, technology, and commerce. The focus of machine learning is on the problem of prediction: Given a sample of training examples \((x_1, y_1), \ldots, (x_n, y_n)\) from \(\mathbb{R}^d \times \mathbb{R}\), we learn a predictor \(h_n: \mathbb{R}^d \rightarrow \mathbb{R}\) that is used to predict the label \(y\) of a new point \(x\), unseen in training.

The predictor \(h_n\) is commonly chosen from some function class \(H\), such as neural networks with a certain architecture, using empirical risk minimization (ERM) and its variants. In ERM, the predictor is taken to be a function \(h \in H\) that minimizes the empirical (or training) risk \(\frac{1}{n} \sum_{i=1}^n \ell(h(x), y_i)\), where \(\ell\) is a loss function, such as the squared loss \(\ell(y', y) = (y' - y)^2\) for regression or 0–1 loss \(\ell(y', y) = 1_{y' \neq y}\) for classification.

The goal of machine learning is to find \(h_n\) that performs well on new data (known as generalization), typically assuming the training examples are sampled randomly from a probability distribution \(P\) over \(\mathbb{R}^d \times \mathbb{R}\) and evaluate \(h_n\) on a new test example \((x, y)\) drawn independently from \(P\). The challenge stems from the mismatch between the goals of minimizing the empirical risk (the explicit goal of ERM algorithms, optimization) and minimizing the true (or test) risk \(\mathbb{E}_{(x,y) \sim P}[\ell(h(x), y)]\) (the goal of machine learning).

Conventional wisdom in machine learning suggests controlling the capacity of the function class \(H\) based on the bias–variance trade-off by balancing underfitting and overfitting (cf. refs. 1 and 2): 1) If \(H\) is too small, all predictors in \(H\) may underfit the training data (i.e., have large empirical risk) and hence predict poorly on new data. 2) If \(H\) is too large, the empirical risk minimizer may overfit spurious patterns in the training data, resulting in poor accuracy on new examples (small empirical risk but large true risk).

The classical thinking is concerned with finding the “sweet spot” between underfitting and overfitting. The control of the function class capacity may be explicit, via the choice of \(H\) (e.g., picking the neural network architecture), or it may be implicit, using regularization (e.g., early stopping). When a suitable balance is achieved, the performance of \(h_n\) on the training data is said to generalize to the population \(P\). This is summarized in the classical U-shaped risk curve shown in Fig. 1A that has been widely used to guide model selection and is even thought to describe aspects of human decision making (3). The textbook corollary of this curve is that “a model with zero training error is overfit to the training data and will typically generalize poorly” (ref. 2, p. 221), a view still widely accepted.

However, practitioners routinely use modern machine-learning methods, such as large neural networks and other non-linear predictors that have very low or zero training risk. Despite the high function class capacity and near-perfect fit to training data, these predictors often give very accurate predictions on new data. Indeed, this behavior has guided a best practice in deep learning for choosing neural network architectures, specifically that the network should be large enough to permit effortless zero-loss training (called interpolation) of the training data (4). Moreover, in direct challenge to the bias–variance trade-off philosophy, recent empirical evidence indicates that neural...
networks and kernel machines trained to interpolate the training data obtain near-optimal test results even when the training data are corrupted with high levels of noise (5, 6).

The main finding of this work is a pattern in how performance on unseen data depends on model capacity and the mechanism underlying its emergence. This dependence, empirically witnessed with important model classes including neural networks and a range of datasets, is summarized in the “double-descent” risk curve shown in Fig. 1A. The curve subsumes the classical U-shaped risk curve from Fig. 1A by extending it beyond the point of interpolation.

When function class capacity is below the “interpolation threshold,” learned predictors exhibit the classical U-shaped curve from Fig. 1A. (In this paper, function class capacity is identified with the number of parameters needed to specify a function within the class.) The bottom of the U is achieved at the sweet spot which balances the fit to the training data and the susceptibility to overfitting: To the left of the sweet spot, predictors are underfitted, and immediately to the right, predictors are overfitted. When we increase the function class capacity high enough (e.g., by increasing the number of features or the size of the neural network architecture), the learned predictors achieve (near) perfect fits to the training data—i.e., interpolation. Although the learned predictors obtained at the interpolation threshold typically have high risk, we show that increasing the function class capacity beyond this point leads to decreasing risk, typically going below the risk achieved at the sweet spot in the “classical” regime.

All of the learned predictors to the right of the interpolation threshold fit the training data perfectly and have zero empirical risk. So why should some—in particular, those from richer function classes—have lower test risk than others? The answer is that the capacity of the function class does not necessarily reflect how well the predictor matches the inductive bias appropriate for the problem at hand. For the learning problems we consider (a range of real-world datasets as well as synthetic data), the inductive bias that seems appropriate is the regularity or smoothness of a function as measured by a certain function norm. This choice of norm is intended as a form of Occam’s razor: The simplest explanation compatible with the observations should be preferred (cf. refs. 7 and 8). By considering larger function classes, which contain more candidate predictors compatible with the data, we are able to find interpolating functions that have smaller norm and are thus “simpler.” Thus, increasing function class capacity improves performance of classifiers.

Related ideas have been considered in the context of margins theory (7, 9, 10), where a larger function class might permit the discovery of a classifier with a larger margin. While the margins theory can be used to study classification, it does not apply to regression and also does not predict the second descent beyond the interpolation threshold. Recently, there has been emerging recognition that certain interpolating predictors (not based on ERM) can indeed be provably statistically optimal or near optimal (11, 12), which is compatible with our empirical observations in the interpolating regime.

In the remainder of this article, we discuss empirical evidence for the double-descent curve and the mechanism for its emergence and conclude with some final observations and parting thoughts.

**Neural Networks**

In this section, we discuss the double-descent risk curve in the context of neural networks.

**Random Fourier Features.** We first consider a popular class of nonlinear parametric models called random Fourier features (RFF) (13), which can be viewed as a class of 2-layer neural networks with fixed weights in the first layer. The RFF model family \( \mathcal{H}_N \) with \( N \) (complex-valued) parameters consists of functions

\[
h(x) = \sum_{k=1}^{N} a_k \phi(x; v_k)
\]

where \( \phi(x; v) := e^{\sqrt{-1} \langle v, x \rangle} \),

and the vectors \( v_1, \ldots, v_N \) are sampled independently from the standard normal distribution in \( \mathbb{R}^d \). (We consider \( \mathcal{H}_N \) as a class of real-valued functions with \( 2N \) real-valued parameters by taking real and imaginary parts separately.) Note that \( \mathcal{H}_N \) is a randomized function class, but as \( N \to \infty \), the function class becomes a closer and closer approximation to the reproducing kernel Hilbert space (RKHS) corresponding to the Gaussian kernel, denoted by \( \mathcal{H}_\infty \). While it is possible to directly use \( \mathcal{H}_\infty \) [e.g., as is done with kernel machines (14)], the random classes \( \mathcal{H}_N \) are computationally attractive to use when the sample size \( n \) is large but the number of parameters \( N \) is small compared with \( n \).

Our learning procedure using \( \mathcal{H}_N \) is as follows. Given data \( (x_1, y_1), \ldots, (x_n, y_n) \) from \( \mathbb{R}^d \times \mathbb{R} \), we find the predictor \( h_{kn} \in \mathcal{H}_N \) via ERM with squared loss. That is, we minimize the empirical risk objective

\[
\frac{1}{n} \sum_{i=1}^{n} (h(x_i) - y_i)^2
\]

over all functions \( h \in \mathcal{H}_N \). When the minimizer is not unique (as is always the case when \( N > n \)), we choose the minimizer whose coefficients \( (a_1, \ldots, a_N) \) have the minimum \( \ell_2 \) norm. This choice of norm is intended as an approximation to the RKHS norm \( ||h||_{\mathcal{H}_\infty} \), which is generally difficult to compute for arbitrary functions in \( \mathcal{H}_N \). For problems with multiple outputs (e.g., multiclass classification), we use functions with vector-valued outputs and the sum of the squared losses for each output.
In Fig. 2, we show the test risk of the predictors learned using $H_N$ on a subset of the popular dataset of handwritten digits called MNIST. Fig. 2 also shows the $\ell_2$ norm of the function coefficients, as well as the training risk. We see that for small values of $N$, the test risk shows the classical U-shaped curve consistent with the bias-variance trade-off, with a peak occurring at the interpolation threshold $N = n$. Some statistical analyses of RFF suggest choosing $N \sim \sqrt{n \log n}$ to obtain good test risk guarantees (15).

The interpolation regime connected with modern practice is shown to the right of the interpolation threshold, with $N > n$. The model class that achieves interpolation with fewest parameters ($N = n$ random features) yields the least accurate predictor. (In fact, it has no predictive ability for classification.) But as the number of features increases beyond $n$, the accuracy improves dramatically, exceeding that of the predictor corresponding to the bottom of the U-shaped curve. The plot also shows that the predictor $h_{n,\infty}$ obtained from $H_\infty$ (the kernel machine) outperforms the predictors from $H_N$ for any finite $N$.

What structural mechanisms account for the double-descent shape? When the number of features is much smaller than the sample size, $N < n$, classical statistical arguments imply that the training risk is close to the test risk. Thus, for small $N$, adding more features yields improvements in both the training and the test risks. However, as the number of features approaches $n$, the accuracy improves dramatically, exceeding that of the predictor corresponding to the bottom of the U-shaped curve. This results in classical overfitting as predicted by the bias-variance trade-off and prominently manifested at the peak of the curve, where the fit becomes exact.

To the right of the interpolation threshold, all function classes are rich enough to achieve zero training risk. For the classes $H_N$ that we consider, there is no guarantee that the most regular, smallest norm predictor consistent with training data (namely $h_{n,\infty}$, which is in $H_\infty$) is contained in the class $H_N$ for any finite $N$. But increasing $N$ allows us to construct progressively better approximations to that smallest norm function. Thus, we expect to have learned predictors with largest norm at the interpolation threshold and for the norm of $h_{n,N}$ to decrease monotonically as $N$ increases, thus explaining the second descent segment of the curve. This is what we observe in Fig. 2, and indeed $h_{n,\infty}$ has better accuracy than all $h_{n,N}$ for any finite $N$. Favoring small norm interpolating predictors turns out to be a powerful inductive bias on MNIST and other real and synthetic datasets (6). For noiseless data, we make this claim mathematically precise in SI Appendix.

Additional empirical evidence for the same double-descent behavior using other datasets is presented in SI Appendix. For instance, we demonstrate double descent for rectified linear unit (ReLU) random feature models, a class of ReLU neural networks with a setting similar to that of RFF. We also describe a simple synthetic model, which can be regarded as a 1D version of the RFF model, where we observe the same double-descent behavior.

**Neural Networks and Backpropagation.** In general multilayer neural networks (beyond RFF or ReLU random feature models), a learning algorithm will tune all of the weights to fit the training data, typically using versions of stochastic gradient descent (SGD), with backpropagation to compute partial derivatives. This flexibility increases the representational power of neural networks, but also makes ERM generally more difficult to implement. Nevertheless, as shown in Fig. 3, we observe that increasing the number of parameters in fully connected 2-layer neural networks leads to a risk curve qualitatively similar to that observed with RFF models. That the test risk improves beyond the interpolation threshold is compatible with the conjectured “small norm” inductive biases of the common training algorithms for neural networks (16, 17).

We note that this transition from under- to overparameterized regimes for neural networks was also previously observed by refs. 18–21. In particular, ref. 21 draws a connection to the physical phenomenon of “jamming” in particle systems.
The computational complexity of ERM with neural networks makes the double-descent risk curve difficult to observe. Indeed, in the classical underparameterized regime ($N \ll n$), the non-convexity of the ERM optimization problem causes the behavior of local search-based heuristics, like SGD, to be highly sensitive to their initialization. Thus, if only suboptimal solutions are found for the ERM optimization problems, increasing the size of a neural network architecture may not always lead to a corresponding decrease in the training risk. This suboptimal behavior can lead to high variability in both the training and test risks that masks the double-descent curve.

It is common to use neural networks with an extremely large number of parameters (22). But to achieve interpolation for a single output (regression or 2-class classification) one expects to need at least as many parameters as there are data points. Moreover, if the prediction problem has more than one output (as in multiclass classification), then the number of parameters needed should be multiplied by the number of outputs. This is indeed the case empirically for neural networks shown in Fig. 3. Thus, for instance, datasets as large as ImageNet (23), which has $\approx 10^6$ examples and $\approx 10^5$ classes, may require networks with $\approx 10^5$ parameters to achieve interpolation; this is larger than many neural network models for ImageNet (22). In such cases, the classical regime of the U-shaped risk curve is more appropriate to understand generalization. For smaller datasets, these large neural networks would be firmly in the overparameterized regime, and simply training to obtain zero training risk often results in good test performance (5).

Additional results with neural networks are given in SI Appendix.

**Decision Trees and Ensemble Methods**

Does the double-descent risk curve manifest with other prediction methods besides neural networks? We give empirical evidence that, when AdaBoost and random forests are used with maximally large (interpolating) decision trees, the flexibility of the fitting methods yields interpolating predictors that are more robust to noise in the training data than the predictors produced by rigid, noninterpolating methods (e.g., AdaBoost or random forests with shallow trees). This in turn is said to yield better generalization. The averaging of the (near) interpolating trees ensures that the resulting function is substantially smoother than any individual tree, which aligns with an inductive bias that is compatible with many real-world problems.

We can understand these flexible fitting methods in the context of the double-descent risk curve. Observe that the size of a decision tree (controlled by the number of leaves) is a natural way to parameterize the function class capacity: Trees with only 2 leaves correspond to 2-piecewise constant functions with an axis-aligned boundary, while trees with $n$ leaves can interpolate $n$ training examples. It is a classical observation that the U-shaped bias–variance trade-off curve manifests in many problems when the class capacity is considered this way (2). (The interpolation threshold may be reached with fewer than $n$ leaves in many cases, but $n$ is clearly an upper bound.) To further enlarge the function class, we consider ensembles (averages) of several interpolating trees. So, beyond the interpolation threshold, we use the number of such trees to index the class capacity. When we view the risk curve as a function of class capacity defined in this hybrid fashion, we see the double-descent curve appear just as with neural networks (Fig. 4 and SI Appendix). We observe a similar phenomenon using $L_2$ boosting (26, 27), another popular ensemble method; the results are reported in SI Appendix.

**Concluding Thoughts**

The double-descent risk curve introduced in this paper reconciles the U-shaped curve predicted by the bias–variance trade-off and the observed behavior of rich models used in modern machine-learning practice. The positied mechanism that underlies its emergence is based on common inductive biases and hence can explain its appearance (and, we argue, ubiquity) in machine-learning applications.

We conclude with some final remarks.

**Historical Absence.** The double-descent behavior may have been historically overlooked on account of several cultural and practical barriers. Observing the double-descent curve requires a parametric family of spaces with functions of arbitrary complexity. The linear settings studied extensively in classical statistics usually assume a small, fixed set of features and hence fixed fitting capacity. Richer families of function classes are typically used in the context of nonparametric statistics, where smoothing and regularization are almost always used (28). Regularization, of all forms, can both prevent interpolation and change the effective capacity of the function class, thus attenuating or masking the interpolation peak.

The RFF model is a popular and flexible parametric family. However, these models were originally proposed as a computationally favorable alternative to kernel machines. This computational advantage over traditional kernel methods holds only for $N \ll n$, and hence models at or beyond the interpolation threshold are typically not considered.

The situation with general multilayer neural networks is slightly different and more involved. Due to the nonconvexity of the ERM optimization problem, solutions in the classical underparameterized regime are highly sensitive to initialization.

*These trees are trained in the way proposed in random forest except without bootstrap resampling. This is similar to the PERT method of ref. 25.
tive bias owes to the specific training procedure used, which
the interpolation constraints. For neural networks, the induc-
mental norm solution in the reproducing kernel Hilbert space,
of features tends to infinity they approach the minimum func-
mum norm linear regression in the feature space. As the number
Inductive Bias.
In this paper, we have dealt with several types
peak. Effect that, as discussed above, makes it difficult to observe the
Interpolation peak.

Moreover, as we have seen, the peak at the interpolation thresh-
old is observed within a narrow range of parameters. Sampling of
parameter space that misses that range may lead to the mis-
leading impression that increasing the size of the network simply
improves performance. Finally, in practice, training of neural
networks is typically stopped as soon as (an estimate of the) test
risk fails to improve. This early stopping has a strong regularizing
effect that, as discussed above, makes it difficult to observe the
interpolation peak.

Inductive Bias. In this paper, we have dealt with several types of
methods for choosing interpolating solutions. For random
Fourier features, solutions are constructed explicitly by mini-
mum norm linear regression in the feature space. As the number
of features tends to infinity they approach the minimum func-
tion with respect to the reproducing kernel Hilbert space, a
solution which maximizes functional smoothness subject to
the interpolation constraints. For neural networks, the inductive
bias owes to the specific training procedure used, which
was supported by NSF Grant RI-1815697. D-H. was supported by NSF Grant CCF-1740833 and a Sloan Research Fellowship.

Optimization and Practical Considerations. In our experiments,
appropriately chosen “modern” models usually outperform the
optimal classical model on the test set. But another important
practical advantage of overparameterized models is in optimiza-
tion. There is a growing understanding that larger models are
c “easy” to optimize as local methods, such as SGD, converge to
global minima of the training risk in overparameterized regimes
(e.g., ref. 30). Thus, large interpolating models can have low
test risk and be easy to optimize at the same time, in particu-
lar with SGD (31). It is likely that the models to the left of the
interpolation peak have optimization properties qualitatively dif-
ferent from those to the right, a distinction of significant practical
import.

Outlook. The classical U-shaped bias–variance trade-off curve has
shaped our view of model selection and directed applica-
tions of learning algorithms in practice. The understanding of
model performance developed in this work delineates the lim-
its of classical analyses and opens additional lines of inquiry
to study and compare computational, statistical, and math-
ematical properties of the classical and modern regimes in
machine learning. We hope that this perspective, in turn, will
help practitioners choose models and algorithms for optimal
performance.

ACKNOWLEDGMENTS. M.B. was supported by NSF Grant RI-1815697. D-H. was supported by NSF Grant CCF-1740833 and a Sloan Research Fellowship.