Landscape and training regimes in deep learning

Mario Geiger, Leonardo Petrini, Matthieu Wyart

Institute of Physics, École Polytechnique Fédérale de Lausanne, 1015 Lausanne, Switzerland

Abstract

Deep learning algorithms are responsible for a technological revolution in a variety of tasks including image recognition or Go playing. Yet, why they work is not understood. Ultimately, they manage to classify data lying in high dimension – a feat generically impossible due to the geometry of high dimensional space and the associated curse of dimensionality. Understanding what kind of structure, symmetry or invariance makes data such as images learnable is a fundamental challenge. Other puzzles include that (i) learning corresponds to minimizing a loss in high dimension, which is in general not convex and could well get stuck bad minima. (ii) Deep learning predicting power increases with the number of fitting parameters, even in a regime where data are perfectly fitted. In this manuscript, we review recent results elucidating (i, ii) and the perspectives they offer on the (still unexplained) curse of dimensionality paradox. We base our theoretical discussion on the \((h, \alpha)\) plane where \(h\) controls the number of parameters and \(\alpha\) the scale of the output of the network at initialization, and provide new systematic measures of performance in that plane for two common image classification datasets. We argue that different learning regimes can be organized into a phase diagram. A line of critical points sharply delimits an under-parametrized phase from an over-parametrized one. In over-parametrized nets, learning can operate in two regimes separated by a smooth cross-over. At large initialization, it corresponds to a kernel method, whereas for small initializations features can be learnt, together with invariants in the data. We review the properties of these different phases, of the transition separating them and some open questions. Our treatment emphasizes analogies with physical systems, scaling arguments and the development of numerical observables to quantitatively test these results empirically. Practical implications are also discussed, including the benefit of averaging nets with distinct initial weights, or the choice of parameters \((h, \alpha)\) optimizing performance.

© 2021 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).
1. Introduction

One of the prerequisites of human or artificial intelligence is to make sense of data that often lie in large dimension. A classical case is computer vision, where one seeks to classify the content of a picture [1] whose dimension is the number of pixels. In the supervised setting considered in this review, algorithms are trained from known, labeled data. For example, one is given a training set of one million pictures of cats and dogs, and knows which is which. The goal is to build an algorithm that can learn a rule from these examples, and predict if a new picture presents a cat or a dog. After sixty years of rather moderate progress, machine learning is undergoing a revolution. Deep learning algorithms [2], which are inspired from the organization of our visual cortex, are now remarkably successful at a wide range of tasks including speech [3] and text recognition [4], self-driving cars [5] and beating the best humans at Go [6] or video games [7]. Yet, there is very limited understanding as to why these algorithms work. As explained below, there are several reasons why deep learning in particular and supervised learning in general should not work. Most prominently, the curse of dimensionality associated with the geometry of space in large dimension prohibits learning in a generic setting. If high dimensional data can be learned, then they must have a lot of structure, invariances and symmetries. Understanding what is the nature of this structure and how it can be harvested by neural nets with suitable architectures is a challenge of our times.

In part 1.1 of this introduction, we review the basic procedure of supervised learning with deep nets, together with the quantification of its success via a learning curve exponent. In part 1.2, we discuss several reasons making this success surprising. It includes the curse of dimensionality mentioned above, the putative presence of the bad minima in the loss landscape and the fact that deep learning typically works in an over-parametrized regime where the number of fitting parameters is much larger than the number of data. In part 1.3, we review two recent ideas seeking to address these paradoxes. First, in the limit where the number of network parameters diverges, deep learning converges to two distinct, well-defined algorithms (lazy training and feature learning) depending on the scale of initialization. In each regime, a global minimum of the loss is found. Second, in the context of image classification it was hypothesized that deep learning efficiently deals with the curse of dimensionality because neural nets learn to become insensitive to smooth deformations of the image.

These two bodies of work raise various questions, detailed below. In a nutshell: (i) Is there a critical number of parameters where one enters in the over-parametrized regime and bad minima in the loss disappear? What is the nature of this transition, and the geometry of the loss-landscape in its vicinity? (ii) Why does performance tend to improve asymptotically with the number of parameters even past this transition? (iii) Once in the over-parametrized regime, where does the cross-over between lazy training and feature learning take place? Which regime performs better, and how does it depend on the data structure and network architecture? (iv) How are simple invariants learnt in the feature learning regime, and how does it affect the learning curve exponent? The goal of this manuscript, laid out in the part 1.4 of this introduction, is both to review recent results addressing these questions in the context of classification in deep nets, as well as to provide new systematic empirical data unifying these results into a phase diagram.

1.1. Presentation of deep learning and quantification of its successes

Signal propagation in some architectures. Deep learning is a fitting procedure, in which the functional form used to interpolate the data depends on many parameters, and can be represented iteratively. State-of-the-art (SOTA) architectures characterizing this functional form can be extremely complex, here we restrict ourselves to essential properties. We denote by \( \tilde{f}_\theta(x) \) the output of a network corresponding to an input \( x \), parametrized by \( \theta \). We reserve the notation \( f_\theta(x) \) for the prediction model, the relation between the two will be defined in Eq. (9). For fully connected nets (FC) – which, from a theoretical point of view, are the most studied architectures – the output function can be written recursively as:

\[
\tilde{f}_\theta(x) \equiv a^{(L+1)},
\]

\[
a^{(i+1)}_\alpha = \sum_\beta \frac{1}{\sqrt{h}} W^{(i)}_{\alpha, \beta} \sigma \left( a^{(i-1)}_\beta + B^{(i)}_\beta \right),
\]

\[
a^{(1)}_\alpha = \sum_\beta \frac{1}{\sqrt{d}} W^{(1)}_{\alpha, \beta} \kappa_\alpha + B^{(1)}_\beta,
\]

where \( a^{(i)}_\alpha \) is the preactivation of neuron \( \alpha \), located at depth \( i \) and \( L \) the total number of layers. We consider networks with a fixed number of hidden layers \( L \), each of size \( h \), the network width. In the following, given that the total number of parameters follows \( N \sim Lh^2 \), we will use both \( h \) and \( N \) to refer to the network size. In our notation the set of
parameters $\theta$ includes both the weights $W_{(i)}$, and the biases $B_{(i)}$, and the non-linear activation function, e.g. the ReLU $\sigma(z) = \max(z, 0)$. As is commonly done, we use the “LeCun initialization” of the weights, for which they are scaled by a factor $1/\sqrt{h}$. It ensures that the limit of infinite width is not trivial, see e.g. discussions in [10]. We represent the network in Fig. 1.

Convolutional neural nets (CNNs), inspired from the primate brain, perform much better than FCs for a variety of tasks including image classification. Each hidden layer is composed of a number of channels, each representing the data as a feature map — itself an image. CNNs perform the same operations at distinct locations in the image, and enforce that these operations are local. CNNs are thus more constrained than FCs, and they can be obtained from the latter by imposing that some weights are identical (to enforce translational invariance) and others zero (to enforce locality).

Learning dynamics. Weights are learnt by fitting the training set, which is done by minimizing a loss or cost function $L$. To simplify notations, we consider a binary classification problem, with a set of $P$ distinct training data denoted $\{(x_\mu, y_\mu)\}_{\mu=1}^P$. The vector $x_\mu$ is the input, which lives in a $d$-dimensional space, and $y_\mu = \pm 1$ is its label.$^1$ $L$ is a sum on all the training set of how each datum is well-fitted:

$$L(\theta) = \frac{1}{P} \sum_{\mu=1}^P \ell(y_\mu f(x_\mu)), \tag{4}$$

where $f$ is a model and $\ell$ is a decreasing function of its argument. Popular choices include the linear ($\gamma = 1$) or quadratic ($\gamma = 2$) hinge loss $\ell(y_\mu f(x_\mu)) = \max(0, \Delta_\mu)$ with $\Delta_\mu = 1 - y_\mu f(x_\mu)$, or the cross-entropy $\ell(y_\mu f(x_\mu)) = \log(1 + \exp(-y_\mu f(x_\mu)))$. The hinge loss has the advantage that bringing the loss equation (4) to zero is equivalent to satisfying a set of constraints $\Delta_\mu < 0$, corresponding to fitting the data by a margin unity. This fact is the basis for the analogy with other satisfiability problems encountered in physics, as discussed below. This choice however does not influence significantly performance for SOTA architectures on usual benchmarks [8].

Different procedures can then be used to minimize $L$, starting from a random initialization of the weights (an important fact to keep in mind). In particular, gradient descent (GD) or stochastic gradient descent (SGD) is commonly used. At each step of GD, $\ell$ is computed and the parameters are updated following the direction of the negative gradient in the loss landscape:

$$\theta^{(t+1)} = \theta^{(t)} - \eta \nabla_{\theta} L(\theta^{(t)}), \tag{5}$$

where the learning rate $\eta$ controls the step size. For SGD, instead of computing the loss on the whole training set as defined in Eq. (4) only a random subset of the terms entering the sum is considered at each minimization time step. Various tricks can improve performance depending on the data considered, including early stopping (minimization is stopped before the loss hits bottom) or weight decay (terms are then added to the loss to prevent weights to become too large).

$^1$ It is straightforward to extend the discussion to multi-class classification problem, as well as to regression.
Fig. 2: A: Curse of dimensionality. In high dimensions, every point lies far away from its neighbors, forbidding classification based on distances alone. B: Sketch of the loss landscape. Starting from a random initialization, the dynamics could get stuck in a bad minimum of the loss. C: Usual behavior (blue line) of the test error as a function of the number of parameters, expected to be minimal when $N$ is of order of the smallest value $N^*$ where data can be fitted. Green: observations indicate that for deep learning, increasing the number of parameters generally improves behavior, even in a regime where data are perfectly fitted.

Performance. Once learning is done, generalization performance can be estimated from a test set (data not used to train, but whose distribution is identical to the training set) by computing the probability to misclassify one new datum, the so-called test error $\epsilon$. How many data are needed to learn a task is characterized by the learning curve $\epsilon(P)$. Generally, it is observed that the test error is well described by a power law decay $P^{-\beta}$ in the range of training set size $P$ available with an exponent $\beta$ that depends jointly on the data and the algorithm chosen. In [11], $\beta$ is reported for SOTA architecture for several tasks: in neural-machine translation $\beta \approx 0.3–0.36$; in language modeling $\beta \approx 0.06–0.09$; in speech recognition $\beta \approx 0.3$ and in image classification (ImageNet) $\beta \approx 0.3–0.5$.

Deep nets learn a hierarchical representation of the data. Once learning took place, it is possible to analyze to which features in the data neurons respond mostly to [9,12]. Strikingly, findings are very similar to what is found in the visual cortex of primates: neurons learn to respond to more and more abstract aspects of the data as the signal progresses through the network, as illustrated in Fig. 1. This observation is believed to be an important aspect of why deep learning works, yet understanding how abstract features are learnt dynamically, and how much it contributes to performance, remains a challenge.

1.2. Why deep learning should not work

Curse of dimensionality. General arguments suggest that $\beta$ should be extremely small – and learning thus essentially impossible – when the dimension $d$ of the data is large, which is generally the case in practice. For example in a regression task, if the only assumption on the target function is that it is Lipschitz continuous, then the test error cannot be guaranteed to decay faster than with an exponent $\beta \sim 1/d$ [13]. This curse of dimensionality [14] stems from the geometrical fact that the distance $\delta$ among nearest-neighbordatapoints decays extremely slowly in large $d$ as $\delta \sim P^{-1/d}$, as depicted in Fig. 2.A. Thus, interpolation or classification methods based on distances are expected to be very imprecise for generic data.

Bad minima in the loss landscape. Another problem, which made deep learning less popular in the 90’s, concerns learning. The loss function has no guarantees to be convex, and the parameters space is high-dimensional. What prevents then the learning dynamics to get stuck in poorly performing minima with high loss, as sketched in Fig. 2.B? In other words, under which conditions can one guarantee that training data are well fitted? Is the loss landscape similar to the energy landscape of glassy systems in physics, where the number of minima is exponential in the number of degrees of freedom [15,16]?

Over-parametrization. Finally, neural nets are often trained in the over-parametrized regime, where the number of parameters $N$ is significantly larger than the number of data points $P$. In that regime, their capacity is very large: they can fit the training set even if labels are randomized [17]. Statistical learning theory then gives no guarantees that over-fitting does not occur, and that the model learnt has any predictive power. Indeed from statistics text books one expects a bell-shape learning curve relating the test error to the number of parameters of the model, as depicted in Fig. 2.C. In this view, at small $N$ the hypothesis class of the learning algorithm is too small, leading to a bias in the learnt predictor. At large $N$, it presents a large variance due to over-fitting noise in the data. A very puzzling aspect of deep learning is that increasing $N$ passed the point where all data are perfectly fitted does not destroy predictive power, but instead improves it [18–21] as shown in Fig. 2.

---

2 A different network is trained for every $P$.

3 For data sets where a finite fraction of the training set is mislabeled, one expects the test error to eventually plateau to a finite value. However, such a saturation of the test error is not seen in practice for various benchmarks, suggesting that such a noise is small in magnitude.
1.3. Current insights on these paradoxes

No bad minima in over-parametrized networks. Recently, it was realized that the landscape of deep learning is not glassy after all, if the number of parameters is sufficient. Theoretical works that focus on nets with a huge number of parameters (and one hidden layer), and empirical work with more realistic architectures [22–25], support that the loss function is characterized by a connected level set: any two points in parameter space with identical loss are connected by a path in which the loss is constant. Moreover, empirical studies of the curvature of the loss landscape (captured by the spectrum of the Hessian) [26–28] and of SGD dynamics [29,30] reveal that the landscape displays a large number of flat directions, even at its bottom. It is not the case for under-parametrized networks [30].

These observations raise key questions. Is there a phase transition in the landscape geometry as the number of parameters grows? If so, what is its universality class? How does it affect performance?

Implicit regularization and infinite width nets. How can over-parametrized networks be predictive, if they can fit any data? It must imply that the GD or SGD dynamics lead to specific minima of the loss landscape where the function is more regular than for generic minima – a phenomenon coined implicit regularization [18,19]. As sketched in Fig. 2, performance is best as \( N \to \infty \), triggering a huge interest in that limit. To which algorithms does GD correspond to in that case?

**NTK:** The propagation of the input signal through infinite-width FC nets at initialization is now well-understood. If the weights – defined in Eqs. (3) – are initialized as i.i.d. random variables with zero mean and variance one (a set-up we consider throughout this work), the output function \( \tilde{f}(x) \) is a Gaussian random process. Its covariance can be computed recursively [31–36].

Very recently it was realized that the learning dynamics also simplifies in this limit [10,37–41]. The key insight of [10] is that the output becomes a linear function of the weights then, as sketched in Fig. 3A, B. Physically, very tiny changes of weights can interfere positively and change the output by \( \mathcal{O}(1) \) which is sufficient to learn, but is not sufficient to change the gradient \( \nabla_{\tilde{f}} \).

More formally, the gradient flow dynamics (continuous time limit of GD) at finite time can always be described by the **neural tangent kernel (NTK)** defined as:

\[
\Theta(\theta, x, y) = \nabla_{\tilde{f}} \tilde{f}_\theta(x) \cdot \nabla_{\tilde{f}} \tilde{f}_\theta(y),
\]

where \( x, y \) are two inputs and \( \nabla_{\tilde{f}} \) is the gradient with respect to the parameters \( \theta \). Specifically, \( \partial \tilde{f}(x) / \partial t \) can be expressed as a linear combination of the \( \Theta(\theta, x, x) \); i.e. \( \tilde{f} \) evolves within a space of dimension \( P \). In general, \( \Theta \) depends on \( \theta \) and thus on time and on the randomness of the initialization. Yet as \( h \to \infty \), \( \Theta(\theta, x, y) \) converges to a well-defined limit independent of initialization, and does not vary in time [10]: deep learning in that limit is thus essentially a kernel method.\(^4\)

**Feature learning (hydrodynamic) regime:** The infinite width limit can be taken differently by adding a factor \( 1/\sqrt{h} \) in the definition of the output. Then the weights must change significantly for the output to become \( \mathcal{O}(1) \) and fit the data. This recently discovered limit is called “mean field”, “rich” but also “feature learning regime” in the literature, because the neurons learn how to respond to different aspects of the input data, as in Fig. 1 – whereas, in the NTK limit, the neuron’s response evolves infinitesimally. This regime has been studied in several works focusing mostly on one-hidden layer networks [43–49], with recent development for deeper nets, see e.g. [50]. In this setting the output function for a one hidden layer reads:

\[
\tilde{f}_\theta(x) = \frac{1}{h} \sum_{i=1}^{h} W_i^{(2)} \sigma(\frac{1}{\sqrt{d}} W_i^{(1)} \cdot x + B_i),
\]

\(^4\) Kernel methods are a class of machine learning algorithms that employ a function \( K(x, x') \) – the kernel – as a similarity measure between datapoints. Typically, the predictor function can be written in the form \( f(x) = \sum_{i=1}^{p} \alpha_i K(x, x_i) \), where the parameters \( \alpha_i \) are learned and \( x_i \) are the points in the training set. Support-Vector Machines are an example of such algorithms. We suggest [42] as a reference on kernel methods.
The law of large number can then be invoked to replace Eq. (7) by an integral:

\[
\bar{f}_0(x) \rightarrow \int dW^{(2)} dW^{(1)} dB \rho(W^{(2)}, W^{(1)}, B) W^{(2)} \sigma \left( \frac{1}{\sqrt{d}} W^{(1)} \cdot x + B \right)
\] (8)

where \( \rho \) is the density of parameters. It is then straightforward to show that gradient flow leads to a dynamics on \( \rho \) of the usual type for conserved quantities: it is the divergence of a flux \( \partial \rho / \partial t = -\nabla \cdot J \). Here the divergence is computed with respect to the set of weights associated with a single neuron, and the flux follows \( J = \rho \Psi(W^{(2)}, W^{(1)}, B, \rho_t) \) where \( \Psi \) is some function that can be expressed in terms of the loss [43]. This formulation is equivalent to the hydrodynamics description of interacting particles in some external potential. Fig. 3C illustrates that when the number of particles (or neurons) is large, \( \rho \) is a more appropriate description than keeping track of all the particle positions (the weights in that case).

**Lazy training:** The fact that deep learning converges to well-defined algorithms as \( h \) diverges, explains why performance converges to a well-defined value in that limit (which will depend on the limit considered), as sketched in Fig. 2. Yet, this distinction between a regime where the NTK does not change, and one where it evolves and features are learnt can be made at finite \( h \). Chizat and Bach proposed a model of the form [51]:

\[
f_0(x) = \alpha \left[ \bar{f}_0(x) - \bar{f}_{0(t=0)}(x) \right],
\] (9)

\( \alpha = O(1) \) corresponds to the NTK initialization and \( \alpha = O(h^{-1/2}) \) to the mean-field limit. In the over-parametrized regime (our work below defines it sharply) where data are fitted, infinitesimal changes of weights are sufficient to learn when \( \alpha \to \infty \) at finite \( h \), and the NTK does not evolve in time (but has fluctuations at initialization). This regime is sometimes referred to as lazy training, in our context we will interchangeably denote it the NTK regime.

Overall, these findings are recent breakthroughs in our understanding of neural nets. Yet, they ask many questions that are central to this review. If two limits exist, which one best characterizes neural networks that are used in practice? Which limit leads to a better performance? How does it depend on the architecture and data structure? Which effect causes the improvement of performance as \( h \) increases?

**Curse and invariance toward diffeomorphisms.** Mallat and Bruna [52,53] proposed that invariance toward smooth deformations of the image, i.e. diffeomorphisms, may allow deep nets to beat the curse of dimensionality. Specifically, consider the case where the input vector \( x \) is an image. It can be thought as a function \( x(s) \) describing intensity in position \( s \), where \( s \in [0, 1]^2 \). A diffeomorphism is a bijective deformation that changes the location \( s \) of the pixels to \( s' = \tau(s) \). In our review below, it will be useful to introduce the pixel displacement field \( \xi(s) = \tau(s) - s \), analogous to the displacement field central to elasticity. We denote by \( T_s[x] \) the image deformed by \( \tau \), i.e. \( T_s[x](s) = x(\tau^{-1}(s)) \). One expects that smooth diffeomorphisms do not affect the label of an image: \( \text{Prob}(y(x) \neq y(T_s[x])) \ll 1 \) if \( \| \nabla_s \xi \| \ll 1 \).

Mallat and Bruna could handcraft CNNs, the “scattering transform”, that are insensitive to smooth diffeomorphisms and perform well:

\[
|f(x) - f(T_s[x])| \leq C_0 \| \nabla_s \xi \|.
\] (10)

They hypothesized that during training, CNNs learn to satisfy Eq. (10). In this view, by becoming insensitive to many aspects of the data irrelevant for the task, CNNs effectively reduce the data dimension and make the problem tractable.

A limitation of this framework is that it says little about how invariants are learnt dynamically. Yet, it is the center of the problem. FC nets are more expressive than CNNs, and nothing a priori prevents them from learning these invariants — yet, they presumably do not, since their performance do not compete with CNNs. Along this route, an interesting question is how to develop observables to characterize empirically the dynamical emergence of invariants. Attempts have been made using mutual information approaches [54] which display problems in such a deterministic setting [55]; or measures based on the effective dimension of the neural representation of the data [56,57] which are informative but can sometimes lead to counter-intuitive results.\(^6\) In Section 5 we discuss other observables based on kernel PCA of the NTK.

### 1.4. Organization of the manuscript

To think about the results above and the questions they raise in a unified manner, it is useful to consider Fig. 4. It shows novel empirical data for the performance of neural nets in the plane \((h, \tilde{h})\) where \( h \) is the width and \( \tilde{h} \) the rescaled initialization amplitude \( \tilde{a} = \sqrt{h} a \). Specifically, the ensemble test error of fully-connected nets trained with GD on MNIST (a data set of handwritten digits [59]) and CIFAR10 (images of planes, dogs, etc. [60]) is shown — samples from these datasets are reported in Fig. 5. This ensemble test error is computed by preparing, for each point in the phase diagram, \( M = 15 \) nets with different initialization. The test error of the mean predictor \( f \) over the 15 trained nets is then shown. The black region corresponds to the under-parametrized regime where the loss of individual nets does not converge to

---

\(^5\) This space is in fact discrete due to the finite number of pixels, but this does not alter the discussion.

\(^6\) The effective dimension is defined from how the distance \( \delta \) among neighboring points varies with their number \( P \), i.e. \( \delta \sim P^{-1/\delta H} \). Its interpretation can be delicate, as it is observed to sometimes increase as the information propagates in the network, which cannot be the case for the true dimension of the manifold representing the data.
Fig. 4. Phase diagram for the performance of deep learning in the width $h$ v.s. rescaled initialization magnitude $\hat{\alpha} = \sqrt{h}\alpha$ plane, where $\alpha$ is defined in Eq. (9). The architecture corresponds to a fully-connected neural network with two hidden layers trained with gradient flow [58]. Binary classification was performed for Left MNIST binary (odd/even) and Right CIFAR10 binary (classes have been regrouped in two sets). The training sets have been reduced to 5000 samples. These data sets were first projected on 10 and 30 PCAs, respectively. This dimensionality reduction of the problem is useful to study the jamming transition but not necessary to investigate the over-parametrized regime [58]. This choice does not affect qualitatively the geometry of the diagram however. The colormap shows the generalization of the ensemble average over 15 samples. The full black line indicates the cross-over from feature to lazy training. It is defined as the location for which the change of the NTK after training $\Delta \theta = \theta(t = \infty) - \theta(0)$ is equal in norm to its magnitude at initialization, i.e. $\|\Delta \theta\|/\|\theta(0)\| = 1$. Choosing other values for this ratio (see dashed lines) does not affect qualitatively the geometry of the cross-over line. The vertical color lines indicate the jamming transition where the training loss hits zero (in the black region the training loss does not reach zero). Its precise position depends on the time the simulation is allowed to run [8], as indicated in legend (using a GPU V100 and the gradient flow algorithm of [58] — gradient descent with adaptive learning rate). It is expected and corresponds to the usual critical slowing down occurring near phase transitions. Horizontal dashed lines correspond to the measures done in Fig. 6. The code used to generate these data is available at https://doi.org/10.5281/zenodo.4322828.

Fig. 5. Sample images for the datasets MNIST and CIFAR10. MNIST contains $28 \times 28$ grayscale images of handwritten digits 0 to 9. CIFAR10 contains $32 \times 32$ color images of 10 categories: airplane, automobile, bird, cat, deer, dog, frog, horse, ship, truck.

zero after learning. As discussed below, its boundary corresponds to a line of critical points corresponding to a “jamming transition” where the system stops displaying a rough landscape. In the colored over-parametrized regime, the black line indicates a cross-over separating the lazy training regime (where the total change of the NTK of individual nets during learning is small in relative terms) from a feature learning regime (where the NTK evolves significantly).

Fig. 6 shows the curves for the test error and the ensemble test error for three values of $\alpha$, as $h$ varies. At the jamming transition, the test error displays a peak as observed in [61]. A similar peak occurs in regression problems [21], where it has a simpler origin and occurs when the number of parameters matches the number of data. This shape for the test error has since then been coined double-descent [62]. Interestingly, as shown in Fig. 6 this phenomenon occurs independently
of the value of $\tilde{\alpha}$ (and thus of the over-parametrized regime one enters into passed jamming) and vanishes when the ensemble average is taken, as observed in [63] and recently confirmed in [64].

Our goal is to review, in non-technical terms, concepts and arguments justifying such a phase diagram and discuss the learning of invariants in this context. In Section 2, we will argue that the boundary of the black region in Fig. 4 is a line of critical point, analogous to the jamming transition occurring in repulsive particles with finite-range interactions. For wider nets, the landscape is not glassy and displays many flat directions. We will provide a simple geometric argument justifying why this transition in deep nets fall into the universality classes of ellipsoid (rather than spherical) particles, which fixes the properties of the landscape (such as the spectrum of the Hessian) near the transition. We will mention an argument à la Landau justifying the cusp in the test error at that point. In Section 3, we will provide a quantitative explanation as to why the test error keeps improving as the width increases passed this transition. Increasing width turns out to eliminate the noise due to the random initialization of the weights, eventually leading to the well-defined algorithms introduced above. Ensemble averaging at finite width efficiently eliminates this source of noise as well as the double descent, as shown in Fig. 6. In Section 4, we will explain why the cross-over between the lazy and feature learning regimes corresponds asymptotically to a flat line in Fig. 4. We will review observations that lazy training outperforms feature learning for standard data sets of images for fully connected architectures, but not for CNNs architectures, corresponding to a larger learning curve exponent $\beta$. In Section 5, we review arguably the simplest model in which a neural net learns invariants in the data structure, by considering that labels do not depend on some directions in input space. As observed in real data, two distinct training exponents $\beta$ in the lazy and feature learning can then be computed. We conclude by discussing open questions.

2. Loss landscape and jamming transition

Minimizing a loss is very similar to minimizing an energy. Describing the energy landscape of physical systems is a much studied problem, especially in the context of glasses. Progress was made on this topic in the last fifteen years by considering finite range interactions, for which bringing the energy to zero is equivalent to satisfying a set of constraints. In that case, the landscape is controlled by a critical point [65–67], the so-called jamming transition. It occurs as the particle density $\phi$ increases. For $\phi > \phi_c$, a gradient descent from a random initial position of the particles gets stuck in one – out of many – meta-stable states, corresponding to a glassy solid as depicted in Fig. 7B, D. For lower densities, the gradient descent reaches zero energy, as sketched in Fig. 7E: particles can freely move without restoring forces, and the landscape has many flat directions. It corresponds to the situations depicted in Fig. 7A, C.

There are two universality classes for jamming, leading to distinct properties for the curvature of the landscape (i.e. the spectrum of the Hessian) [68–73], for the structure of the packing obtained [74–77] and for the dynamical response to a perturbation [78,79]. Spheres and ellipses fall in distinct classes as illustrated in Fig. 7. More generally, the jamming transition occurs generically in satisfiability problems with continuous degrees of freedom (it can be defined with discrete degrees of freedom [80], but then differs qualitatively; in particular, the present discussion does not apply to the discrete case). It occurs in the perceptron [81–83] but also for deep nets [8,81].
Fig. 7. Sketch of the jamming transition for repulsive spheres and ellipses. (a, b, c, d) Both systems transition from a fluid to a solid as the density passes some threshold, noted \( \phi_S \) for spheres and \( \phi_E \) for ellipses. (e) For denser packings, the potential energy \( U \) becomes finite. (f) The ratio \( N_{\Delta}/N \) between the number of particles in contact \( N_{\Delta} \) (corresponding to unsatisfied constraints) and the number of degrees of freedom \( N \) jumps discontinuously to a finite value, which is unity for spheres but smaller for ellipses. (g, h) This difference has dramatic consequence on the energy landscape, in particular on the spectrum of the Hessian. In both cases, the spectrum becomes non-zero at jamming, but it displays a delta function with finite weight for ellipses (indicating strictly flat directions), followed by a gap with no eigenvalues, followed by a continuous spectrum (h, full line). For spheres, there is no delta function nor gap (g, full line). As one enters the jammed phase, in both cases a characteristic scale \( \lambda \sim \sqrt{U} \) appears in the spectrum (g and h, dotted lines).

Source: From [8].

Fig. 8. A Phase diagram indicating where the hinge loss hits zero (in blue) or not (in white) at the end of training, as the number of parameters \( N \) and training points \( P \) vary, for the MNIST data set discussed above (binary classification, 10 PCAs) trained with a FC nets with 3 hidden layers. B Number of unsatisfied patterns \( N_{\Delta}/N \) as a function of the loss at the end of training, following the arrow indicated in panel A. Here \( N \) is fixed, and \( P = 1, \ldots, 70k \). C The spectrum of the dominant term in the Hessian near jamming \( H_0 \) (averaged over the run at jamming, in the rectangle of B) presents a delta function in zero and a gaped continuous spectrum at high frequencies, a generic feature of hypostatic jamming. D Fluctuations of the output function along the arrow shown in A, averaged over 20 initial conditions. It decays asymptotically as a power-law \( N^{-1/4} \) for the MNIST data set. At jamming, these fluctuations explode, consistent with a quadratic singularity.

Source: From [8,63].

We will recall below a geometric argument introduced in [8] determining the universality class of the jamming transition. For deep nets, jamming belongs to the universality class of ellipses [8,61]. The spectrum of the loss near the jamming transition displays zero modes, a gap and a continuous part, as measured in Fig. 8.C. Another implication of this analogy is the number \( N_{\Delta} \) of data whose margin is smaller than unity after learning, which contributes to the loss. These data are conceptually similar to the support vectors central to SVM algorithms. For particles, \( N_{\Delta} \) corresponds the number of pairs of particles still overlapping after energy minimization. As illustrated in Fig. 8.B, \( N_{\Delta}/N \) jumps from zero to a value strictly smaller than one at jamming where the loss becomes positive, precisely as ellipses do.

Geometric argument fixing the universality class. Here we seek to give a simple intuition of the result of [8] (a more rigorous argument can be found there). We consider continuous satisfiability problems where one seeks to minimize an energy or
loss function of the type:

\[ \mathcal{U} = \sum_{\mu \in m} \frac{1}{2} \Delta_{\mu}^2, \]  

(11)

where the sum is made on all constraints that are not satisfied, corresponding to \( \Delta_\mu > 0 \). The quantities \( \Delta_\mu \) can depend in general on the \( N \) degrees of freedom of the system. For systems of particles, \( \mathcal{U} \) is an energy and \( \Delta_\mu \) is the overlap between a pair \( \mu = (i,j) \) of particles \( i \) and \( j \). For spheres it reads \( \Delta_{ij} = 2R - r_{ij} \) where \( R \) is the particle radius and \( r_{ij} = \|r_i - r_j\| \) the distance between particles \( i \) and \( j \). In that case, \( N \) is the number of particles times the spatial dimension.

For the perceptron or deep nets, \( \mathcal{U} \) corresponds to a quadratic hinge loss generally denoted \( \mathcal{L} \) defined in Eq. (4) (it is straightforward to extend these arguments to other hinge losses with \( \gamma > 1 \) [8,65], the case \( \gamma = 1 \) of the linear hinge shares many similarities with those but also display interesting differences [84]). As defined in the introduction, in that case \( \Delta_\mu = 1 - f'(x_\mu)y_\mu \).

As the jamming transition is a singular point, it is useful — but not strictly necessary — to think of approaching from the glassy (large density \( \phi \) or under-parametrized) phase. It corresponds to \( \mathcal{U} \to 0 \) as sketched in Fig. 7E, F, implying that \( \Delta_\mu \to 0 \forall \mu \in m \). As argued in [85], for each \( \mu \in m \) the constraint \( \Delta_\mu = 0 \) defines a manifold of dimension \( N - 1 \). Satisfying \( N_A \) such equations thus generically leads to a manifold of solutions of dimension \( N - N_A \). Imposing that solutions exist thus implies that, at jamming, one has:

\[ N_A \leq N. \]  

(12)

Note that this argument implicitly assumes that the \( N_A \) constraints are independent, see [8] for more discussions.

An opposite bound can be obtained by considerations of stability, by imposing that in a stable minimum the Hessian must be positive definite [68]. The Hessian is an \( N \times N \) matrix which can be written as:

\[ \mathcal{H}_\mathcal{U} = \sum_{\mu \in m} \nabla \Delta_\mu \otimes \nabla \Delta_\mu + \sum_{\mu \in m} \Delta_\mu \mathcal{H}_{\Delta_\mu} = \mathcal{H}_0 + \mathcal{H}_p, \]  

(13)

where \( \mathcal{H}_{\Delta_\mu} \), the Hessian of \( \Delta_\mu \), and \( \mathcal{H}_0 \) and \( \mathcal{H}_p \) correspond to the first and the second sum, respectively. \( \mathcal{H}_0 \) is positive semi-definite, since it is the sum of \( N_A \) positive semi-definite matrices of rank unity; thus \( \text{rk}(\mathcal{H}_0) \leq N_A \), implying that the null-space of \( \mathcal{H}_0 \) is at least of dimension \( N - N_A \). \( \mathcal{H}_p \) becomes very small approaching jamming, since the \( \Delta_\mu \)’s vanish. Let us denote by \( N^- \) the number of negative eigenvalues of \( \mathcal{H}_p \). Requiring that \( \mathcal{H}_\mathcal{U} \) has no negative eigenvalues thus implies:

\[ N_A \geq N^- . \]  

(14)

For spheres [66] (as well as for the perceptron if a negative margin is used while constraining the norm of the weight vector), \( \mathcal{H}_p \) is negative definite and \( N^- = N \). This results stems from the fact that \( \mathcal{H}_{\Delta_\mu} \) is negative semi-definite. Indeed \( \mathcal{H}_{\Delta_\mu} \) characterizes the second order change of overlap between particles, and is negative because the distance between spheres moving transversely to their relative direction always increase following Pythagoras theorem. In that case we thus have \( N_A \geq N \). Together with Eq. (12) that leads to \( N_A = N \): as spheres jam the number of degrees of freedom and the number of constraints (stemming from contacts) are equal, as empirically observed [65]. This property is often called isostaticity.

However, in other problems such as ellipses and deep nets, \( \mathcal{H}_{\Delta_\mu} \) and thus \( \mathcal{H}_p \) have positive eigenvalues. Indeed the overlap between two ellipses can increase if one of them rotates. Likewise, for a fully-connected ReLU net and random data at initialization, \( \mathcal{H}_p \) has a symmetric spectrum and \( N^- \approx N/2 \). Generically one expects then jamming to occur with \( N_A < N \) as sketched for ellipses in Fig. 7 and shown empirically for neural nets learning MNIST in Fig. 8. Jamming is then referred to as “hypostatic”. The associated consequences on the spectrum of the hessian shown on the same figures are derived in specific cases in [70,71,86]; it always presents a delta function in zero and a gap at jamming.

**Effect of the number of training data \( P \).** The location of the jamming transition \( N^*(P) \) depends on \( P \). This dependence is linear for random data but sub-linear for structured data [8], as exemplified in Fig. 8A. Denoting \( N^- = C_0 N \), and using Eq. (14) together with \( N_A \leq P \), we obtain \( N^*(P) \leq P/C_0 \), guaranteeing convergence to a zero loss for a number of parameters linear in \( P \) if \( C_0 > 0 \). We conjecture \( C_0 \) to remain bounded by a strictly positive value for large \( N \) for generic data and architectures used in practice.\(^9\) \( C_0 \) can be measured a posteriori, leading to the bound corresponds to the dotted line in Fig. 8A. \( C_0 \) a priori depends on the choice of architecture, dynamics and data set. Controlling its value a priori is yet out of reach,\(^10\) and would lead to a rather tight guarantee of convergence toward a global minimum of the loss.

---

\(^8\) Particles can always sit right at jamming if an infinitesimal pressure is applied to the system. In the context of neural nets, it can also be achieved by introducing an additional term in the loss of the type \( \lambda |\theta(t) - \theta(t = 0)|^2 \) penalizing the square evolution of the weights (called “weight decay”) of vanishing magnitude \( \lambda \to 0^- \).

\(^9\) This fact does not hold for linear or polynomial activation function, see discussion in [8].

\(^10\) Controlling \( \mathcal{H}_0 \) and \( \mathcal{H}_p \) during learning was done only in the limit \( N \to \infty \) which does not apply near jamming [87].
Effect of the scale of initialization $\tilde{\alpha}$. It is apparent in Fig. 4 that the location of the jamming transition depends on the scale of initialization $\tilde{\alpha}$. From this figure, we observe the following general trend: the jamming transition occurs with less parameters when the test error of the ensemble-averaged predictor is small. It follows the intuition that an easier rule to learn should correspond to less parameters to fit the data.

Effect of the jamming transition on performance. As the jamming transition is approached, the norm $\|f_N\|$ of the predictor diverges [8], which is responsible in the cusp in the double descent displayed by the test error in Fig. 6. This divergence was first pointed out for regression [21]. Yet for classification, the divergence defers quantitatively and is compatible with an inverse power-law, as illustrated in Fig. 8.D. It can be understood using an argument à la Landau, inspired by results on the perceptron [81,83]. The intuitive idea is that, by increasing the norm of the predictor, one reduces effectively the unit margin required by the hinge loss to fit the data. For $N < N^*$, data cannot be fitted even with a vanishing margin.

Specifically, consider that the norm of the predictor $\|f_N\|$ is fixed during training and denote by $N^*(\epsilon)$ the jamming transition as a function of the margin $\epsilon$. Assume (as occurs for the perceptron) that $N^*(\epsilon)$ is a smooth function of $\epsilon$, such that $N^*(\epsilon) \approx N^*(0) + N^*(0)\epsilon$. For $N$ just above $N^*(0)$, margins of magnitude unity cannot be fitted for a fixed norm of the predictor, but they can if that norm is allowed to increase by a factor $N^*(0)/(N-N^*(0))$. Indeed it effectively reduces the margin by that amount to some effective value $\tilde{\epsilon} \equiv \epsilon(N-N^*(0))/N^*(0)$. By construction, $\tilde{\epsilon}$ satisfies $N^*(\tilde{\epsilon}) = N$. This argument justifies the observed inverse power-law.

Note that any perturbation to gradient flow (such as early stopping, using stochastic gradient descent or weight decay) will destroy this divergence.\(^{11}\) Such regularizations are thus most efficient near jamming [61].

3. Double descent and the benefits of overparametrization

To avoid bad minima in the loss landscape, it is thus sufficient to crank up $N$ passed that point, and how fast the test error reaches its asymptotic behavior [63]. Essentially, at infinite width learning corresponds to well-defined algorithms as discussed in introduction, but these algorithms become noisier when the width is finite. Indeed as $N \sim h^2$ increases, the fluctuations on the learnt output function induced by the random initialization of the weights decrease [88]. It follows $\|f_N(\tilde{\alpha}) - f_N(\tilde{\alpha})\| \sim N^{-1/4}$ as shown in Fig. 8.D, where $\{f_N\}$ is obtained by ensemble-averaging outputs trained with different initial randomizations. This result is true both for the lazy training [63] and the feature learning [58] regime, as justified below. The associated increase in test error is quadratic in the fluctuations (it is obvious for a mean square error loss, but is also true for classification under reasonable assumptions [63]), leading to $\epsilon(\tilde{f}_N) - \epsilon(f_N) \sim N^{-1/2}$ as observed [63]. This effect is responsible for the double descent, as can be directly checked by considering the training curve $\epsilon(\{f_N\})$ of the ensemble average function $\{f_N\}$ in Fig. 6 which does not display a second descent. More generally as apparent in Fig. 4, at fixed $\tilde{\alpha} = \sqrt{h}a$, the ensemble average test error weakly varies with $h$ once in the over-parametrized regime.

In the lazy training regime, the fluctuations $\langle\|f_N(\tilde{\alpha}) - f_N(\tilde{\alpha})\|\rangle \sim N^{-1/4}$ simply mirror the fluctuations of the NTK induced by initialization, argued to follow $\|\Theta_N(\tilde{\alpha}) - \Theta_N(\tilde{\alpha})\| \sim N^{-1/4} \sim h^{-1/2}$ in [63], as analytically confirmed since then [89,90]. For simple losses and gradient descent, the predictor $f_N$ must acquire the same fluctuations [63], as observed.

Similar fluctuations induced by initial conditions $\langle\|f_N(\tilde{\alpha}) - f_N(\tilde{\alpha})\|\rangle \sim N^{-1/4}$ with identical consequences occur in the feature learning regimes in neural nets [58]. Such fluctuations are certainly expected at initialization for a one-hidden layer, since the density of neurons parameters $\rho$ introduced in Eq. (8) must have finite sampling fluctuations of order $\delta \rho \sim 1/\sqrt{\rho} \sim N^{-1/4}$ as expected from the central limit theorem. Because in the asymptotic regime $N \rightarrow \infty$ the value of $\rho$ at initialization affects the learnt function, the magnitude of fluctuations $\delta \rho$ (and thus of the learnt function $f_N$) induced by the random initialization will still scale as $N^{-1/4}$ after learning, as rigorously proven for a one-hidden layer in [91].

Overall, this scaling theory supports that for generic data sets and deep architectures, the second descent results from the noise induced by finite $N$ effects and initialization on the limiting algorithms reached as $N \rightarrow \infty$. In other words, the variance of the learnt predictor is reduced in this limit, as its dependence on initialization vanishes. One interesting practical implication of this result, apparent in Figs. 4 and 6, is that optimal performance is found by ensemble averaging nets of limited width passed their jamming transition.

Since these arguments were proposed, the double descent curve has been analytically computed in the simple case of linear data in the limit of infinite dimension and random features machines [47,92], where it was also shown [93,94] to result from the fluctuations of the kernel that vanish with increasing number of neurons, confirming the present explanation.

\(^{11}\) They are relevant perturbations in the sense of critical phenomena.
4. Disentangling the NTK and feature learning regimes

As discussed in the previous section, wider nets are more predictive. A comparable gain of performance can however be obtained already at intermediate width, by ensemble averaging outputs over multiple initialization of the weights. As apparent in Fig. 4, the rescaled magnitude of initialization \( \tilde{a} = \alpha \sqrt{h} \) which allows to cross-over between the lazy training and feature learning regimes does affect performance. Which regime best characterizes deep nets used in practice? Which one performs better? Some predictions of the NTK regime appear to hold in realistic architectures [39], and training nets in NTK limit can achieve good performance on real datasets [40,95,96]. Yet, in several cases the feature learning regime beats the NTK [51,97], in line with the common idea that building an abstract representation of the data such as sketched in Fig. 1 is useful. Several theoretical works show that NTK under-performs for specific, simple models of data [14,98–101].

In [58], this question was investigated systematically for deep nets in the \((\alpha, h)\) plane, where \(\alpha\) is the scale of initialization introduced in [51] as defined in Eq. (9). This study developed numerical methods of adaptive learning rates to follow gradient flow while changing \(\alpha\) by ten decades. The main results are as follows:

(i) The cross-over between the two regimes occur when \(\alpha \sqrt{h} = O(1)\) as apparent in Fig. 4, extending the result of [51] limited to one hidden layer nets. For \(\alpha \sqrt{h} \ll 1\), \(\|\Delta \theta \| / \| \theta \| \gg 1\) while the opposite holds true when \(\alpha \sqrt{h} \gg 1\). Here \(\Delta \theta = \theta(t) - \theta(t = 0)\) characterizes the evolution of the tangent kernel and \(t\) is the learning time. It is convenient to divide the loss by \(\alpha^2\) and consider \(\tilde{L} \equiv L/\alpha^2\), which can be shown to ensure that the dynamics occurs on a time scale independent of \(\alpha\) in the large \(\alpha\) limit [51,58]. This result holds true for the usual choices of loss (cross-entropy, hinge, etc.) at any finite time. It also holds true for \(t \rightarrow \infty\) if the hinge loss is used, since in that case convergence to a zero loss occurs in finite time independently of \(h\) and \(\alpha\).

Here we provide a schematic argument justifying this result, see [58] for a more detailed analysis. The variation of the output \(f\) with respect to the pre-activation \(a\) (which are of order one at initialization) of a given neuron is of order \(\partial f / \partial a \sim \alpha / \sqrt{h}\). This result is obvious for the last hidden layer (using that the last weights are of order \(1/\sqrt{h}\)), but can be justified recursively at all layers, as discussed in [58] and derived implicitly in the NTK study [10]. For gradient flow, the variation \(\Delta a\) of pre-activation due to the evolution of the bias (considering the previous weights leads to a similar scaling) must be of order \(\Delta a \sim t(\partial \tilde{L} / \partial f)(\partial f / \partial a) \sim t / \alpha \sqrt{h}\) using that \(\partial \tilde{L} / \partial f \sim 1 / \alpha^2\). Thus \(\Delta a\) is of order \(1 / \alpha \sqrt{h}\) at the end of training (since a zero hinge loss is reached on a time scale \(t = O(1)\)). The NTK regime must thus break down when \(\Delta a \sim 1\) when the relation between weights and output must become non-linear, corresponding to a cross-over for \(\alpha^* \sim 1 / \sqrt{h}\) for large \(h\).

A similar line of thought can be used at intermediate width. When reducing \(h\) so as to approach the jamming transition from the over-parametrized phase, the norm of the output – and therefore weights and pre-activations – explode as reviewed in Section 2. One is never then in the lazy training regime, and the relationship between the variation of weights and the output must become non-linear. Thus, in the vicinity of the jamming transition, the networks always lie in the feature learning regime. Consequently, the cross-over lines separating lazy and feature learning must bend up and never cross the jamming line in Fig. 4. We do observe curves qualitatively bending up as expected (yet it is hard to make precise measurements very close to jamming).

(ii) For fully-connected nets and gradient descent, the NTK tends to outperform the feature learning regime, as exemplified in the Left panel of Fig. 9. This result was found for a variety of data sets (MNIST, Fashion-MNIST, CIFAR10, etc.), except for MNIST 10 PCA. It is apparent in Fig. 4, where the best performance for MNIST 10 PCA appears to occur the cross-over region \(\tilde{a} \sim 1\).

(iii) For CNN architectures, feature learning outperforms the NTK regime as shown in the central panel of Fig. 9. It corresponds to a larger training curve exponent \(\beta\), as appears in the right panel of Fig. 9. (ii, iii) were recently confirmed by the Google team [64].
These observations raise various questions. What are the advantages and drawbacks of feature learning, and why are the latter more apparent in FC rather than CNN architectures? For modern CNN architectures, is the improvement of the learning curve exponent $\beta$ in the feature learning regime key to understand how the curse of dimensionality is beaten? Is it associated with learning invariants in the data? In our opinion, the answers to these questions are yet unknown. To start tackling these questions, in the next section we study a simple model of invariant data for which the improvement of the learning curve exponent $\beta$ in the feature learning regime can be computed.

5. Learning simple invariants by compressing irrelevant input dimensions

How can the curse of dimensionality be beaten? A favorable aspect of various data sets such as images is that the data distribution $P(\mathbf{x})$ is very anisotropic, consistent with the notion that the data lie in a manifold of lower dimension. In that case, the distance between neighboring data reduces faster with growing $P$, improving kernel methods [102]. The positive effect of a moderate anisotropy can also be shown for kernel classification [103] and regression [101,104]. Yet, even in simple data sets like MNIST of CIFAR10, the intrinsic dimensions remain significant ($d_{\text{int}} \approx 14$ and $d_{\text{int}} \approx 30$ respectively [102]). This effect helps but cannot resolve the curse of dimensionality for complex data sets: indeed using Laplace or Gaussian kernels (which are very similar to the NTK of fully connected nets) lead to $\beta \approx 0.4$ for MNIST (which is decent) but $\beta \approx 0.1$ for CIFAR10, which implies very slow learning as the number of data increases.

As discussed in the introduction, another popular idea is that data sets as images are learnable because they display many invariant transformations that leave the labels unchanged. By becoming insensitive to those, the network essentially reduces the dimension of the data. This view is consistent with the notion that deep learning leads to an abstract neural representation of the data sketched in Fig. 1. This effect may be responsible for our observation in the right panel of Fig. 9 that the training curve exponent $\beta$ is more favorable in the feature learning regime. However, understanding how invariants are built dynamically and how it affects performance and $\beta$ remains a challenge.

Specific models of data can be built [44,92,101,105] in which lazy training does not learn at all, whereas neural nets trained in the feature learning regime succeed. However, these models that consider the limit $d \to \infty$, $P \to \infty$ with $P/d$ fixed do not capture the two finite and distinct learning curve exponents $\beta$ observed in the two regimes.

The stripe model. In [98,103,106], a simple model of invariant is considered. The labels do not depend on $d_\perp = d - d_\parallel$ directions of input space, so that $y(\mathbf{x}) = y(\mathbf{x}_\parallel)$ where $\mathbf{x} = (\mathbf{x}_\perp, \mathbf{x}_\parallel)$. $\mathbf{x}_\perp$ could correspond for example to uninformative pixels near the boundaries of pictures. Clearly kernel methods whose kernel are designed to only depends on $\mathbf{x}_\parallel$ would perform better on these data than isotropic kernels, since they would operate in $d_\parallel$ (instead of $d$) dimensions, see e.g. [101]. How do neural nets discover such an invariance on their own?

For gradient descent, with the logistic loss, a one-hidden layer can be shown to correspond to a max-margin classifier in a certain non-Hilbertian space of functions [98]. Dimension-independent guarantees on performance can then be obtained if the data can be separated after projection in a low dimensional space. The analysis is rigorous and general, but requires to go to extremely long times not used in practice and does not predict values for $\beta$.

In [103,106], the hinge loss is considered. In that case, the dynamics stops after a reasonable time. If the density of data points does not vanish at the interface between labels, and if the latter is sufficiently smooth (e.g. planar or cylindrical), it is found that the test error decays as a power law in both regimes. For the lazy training regime, scaling arguments inspired by electrostatics lead to $\beta_{\text{lazy}} = d/(3d-2)$. Feature learning performs better, as one find $\beta_{\text{graph}} = (d + d_\parallel/2)/(3d-2)$. The key effect leading to an improvement of the feature learning regime is illustrated in Fig. 10 for $d_\parallel = 1$, called the stripe model: due to the absence of gradient in the orthogonal direction, the weights only grow along the $d_\parallel$ dimensions. Thus, for an infinitesimal initialization of the weights ($\alpha \to 0$), the neurons align along the informative coordinate in the data. Accordingly, in relative terms, they become less sensitive to $\mathbf{x}_\perp$, which merely acts as a source of noise. This denoising is limited by the finite size of the training set. Specifically, it is found that $\Lambda \equiv W_\parallel/W_\perp \sim \sqrt{P}$ where $W_\parallel$ and $W_\perp$ are the characteristic scales of the first layer of weights in the informative and uninformative directions respectively. This effect is equivalent to a geometrical compression of magnitude $\Lambda$ of the input in the uninformative direction. Indeed performing this compression by considering the transformed data $(\mathbf{x}_\parallel, \mathbf{x}_\perp/\Lambda)$, and learning these in the NTK regime gives very similar performance as learning the original data in the feature regime, see the right panel of Fig. 10.

Kernel PCA of the NTK reveals a geometric compression of invariants. The stripe models illustrates that neural nets in the feature learning regime can learn to become insensitive to transformations in the data that do not affect the labels. This insensitivity is limited by the sampling noise associated with a finite data set. Is this phenomenon also occurring for more modern architectures and more subtle invariants characterizing images? Measurements of the intrinsic dimension of the neural representation of data [56,57] or mutual information estimates [54] suggest that it may be so, but as mentioned in introduction these observables have some limitations.

In the feature learning regime, the NTK evolves in time. This evolution leads to a better kernel for the task considered. Indeed, using a kernel method based on the NTK obtained at the end of training leads to essentially identical performance than the neural net itself [106]. This observation is consistent with previous ones showing that the NTK “improves” in

\footnote{A Laplace kernel has the functional form $K(\mathbf{x}, \mathbf{x}') = K(||\mathbf{x} - \mathbf{x}'||) \propto e^{-\|\mathbf{x} - \mathbf{x}'\|/\sigma}$. A Gaussian kernel $K(\mathbf{x}, \mathbf{x}') = K(||\mathbf{x} - \mathbf{x}'||) \propto e^{-\|\mathbf{x} - \mathbf{x}'\|^2/(2\sigma^2)}$. The bandwidth $\sigma$ controls the decay speed of $K$ as its argument increases.}
Fig. 10. Left: Distribution of the weights vectors $\vec{W}^{(1)}$ pondered by the neuron second weight $W^{(2)}$, shown at different time points during the learning process (as characterized by the value of the loss in legend) for the stripe model. It reveals an alignment of the first layer of weight vectors in the informative direction. Training data points are also shown, and colored depending on their labels. Right: Training curve $\epsilon(P)$ of a one hidden layer in the feature learning regime (blue), the NTK regime (red) and the NTK regime after compressing the data in the perpendicular direction by the factor $\Lambda$ (dashed red). Note the similarity between this curve and the blue one, supporting that the main effect of learning feature for these data is the geometric compression of uninformative directions in input space.

Source: From [106].

Fig. 11. Relationship between the kernel PCA of the NTK (obtained both at initialization and after learning) and the labels. The mutual information (characterizing the amount of correlation) between the top eigenvectors of the Gram matrix and the labels (A, B) and their projection $\omega$, (C, D) get large after learning for both the stripe model (learnt with a FC with one hidden-layer) and MNIST (learnt with a CNN).

Source: From [106].

time [107,108], in the following sense. For kernels we can always write $\Theta(x, y) = \psi(x) \cdot \psi(y)$, where $\psi(x)$ is a vector of features. In the case of the NTK, $\psi(x)$ can be chosen as the gradient of the output $f$ with respect to the weights — see Eq. (6). Kernels tend to perform better [109] if the vector of labels $\{y(x_i)\}_{i=1...P}$ has large coefficients along the first PCAs of the features vectors $\{\psi(x_i)\}_{i=1...P}$ (an operation called kernel PCA [110]). Such an alignment between the first PCAs of the features vectors of the NTK and the vector of labels is observed during learning [107,108].

Although there is no general theory as to why such an alignment occurs, the stripe model provides a plausible explanation for this effect. In that case, this improvement must occur because one evolves from an isotropic kernel to an anisotropic one with diminished sensitivity to uninformative directions $x_\perp$. As a result, the top kernel PCA becomes more informative on the label (Fig. 11.A) on which they project more (Fig. 11.C). The same result is observed for a CNN trained on MNIST as shown in Fig. 11.B, D. Overall, this view supports that the improvement of the NTK reveals the geometric compression of uninformative directions in the data.

6. Conclusion

Do not be afraid of bad minima! Just crank-up the number of parameters until you pass a jamming transition. Beyond that point, bad minima are not encountered, and you can bring the loss to zero. Depending on the network width and on how you scale the value of your function at initialization, deep learning can then behave as a kernel method, or can alternatively learn features. Simple scaling arguments delimit the corresponding phase diagram, and appear to hold for benchmark data sets. Remarkably, these arguments depend very little on the specific data considered. Their practical implication is that ensemble averaging nets with different initialization past the jamming transition can be an effective procedure, as found by different groups [58,63,64].

Taking into account where you are in this phase diagram is arguably key to understand outstanding questions on deep learning. It is true for example for the role of stochasticity in the dynamics, which appears to improve performance. It is natural that using stochastic gradient descent instead of gradient flow will help near jamming, because the noise will regularize the divergence of the predictor norm — an effect that can already be obtained with early stopping [61]. Likewise, for repulsive particles temperature regularizes singularity near the jamming transition [111]. Yet, it would be useful to study its effect on performance for the distinct regions of the phase diagram. It would be particularly interesting to know if one of the main effects of stochasticity in the over-parametrized limit is to push upward the cross-over between the lazy and feature learning regime in Fig. 4, thus improving performance in CNNs where feature learning outperforms lazy training.
Ultimately, the central question left to understand is performance, and how the curse of dimensionality is beaten in deep nets. Even at an empirical level, the idea that invariance toward diffeomorphisms is the central phenomenon behind this success is not established. At the theoretical level, this view has not been combined with the recent improvement of our understanding of learning, which is mostly focused on fully connected nets. In comparison, the effort to model how CNNs learn features is more modest, despite that only those architectures tend to work well in practice. Such studies would arguably require to design simple canonical models of data presenting complex invariants, which are currently scarce.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We acknowledge G. Birolì, S. d’Ascoli, F. Cagnetta, A. Favero, F. Gabriel, C. Hongler, A. Jacot, J. Paccolat, L. Pillaud-Vivien, S. Spigler, L. Sagun, U. Tomasini, K. Tyloo and all members of the PCSL group for discussions. This work was partially supported by the grant from the Simons Foundation (#454953 Matthieu Wyart). M.W. thanks the Swiss National Science Foundation for support under Grant No. 200021-165509.

References


