The success of Deep Learning: Is it all about SGD?

FCF826 Lecture 11:

- On the (lack of) Implicit Bias of SGD
- Bad Local Minima Exist
- SGD Can Reach them

Contents

• The empirical cost function that we have access to

how fast?

• The answer must depend on: 1) *n*, the sample size 2) \mathcal{H} , the hypothesis class and loss function 3) \mathcal{D} , the data distribution 4) the optimization algorithm that outputs our classifier

Last time: How fast we can approximate ERM

$\min_{h \in \mathcal{H}} \left(R_{S}[h] = \frac{1}{n} \sum_{i=1}^{n} \ell(h(x_{i}); y_{i}) \right)$

• <u>Question</u>: Can we approximate the solution to this minimization? If so



Loss landscapes and optimization in over-parameterized non-linear systems and neural networks

Chaoyue Liu^a, Libin Zhu^{b,c}, and Mikhail Belkin^c

^aDepartment of Computer Science and Engineering, The Ohio State University ^bDepartment of Computer Science and Engineering, University of California, San Diego ^cHalicioğlu Data Science Institute, University of California, San Diego

May 28, 2021

A Convergence Theory for Deep Learning via Over-Parameterization



Overparameterized Nonlinear Learning: Gradient Descent Takes the Shortest Path?

Samet Oymak^{*} and Mahdi Soltanolkotabi[†]



Simon S. Du^{*1} Jason D. Lee^{*2} Haochuan Li^{*34} Liwei Wang^{*54} Xiyu Zhai^{*6}





PL-like conditions and old elin neighborhoods around initialization/optima.



Current theoretical SOTA

Subquadratic Overparameterization for Shallow Neural Networks



Thomas Pethick¹

something odd.

CLL=convex and Lipschitz loss, SD=separable data. Depth Algorithm Setting Activ Re GD on layer 1 2 QL Re GD on layer LLCLL Re SD 2 GD SD and QL Re 2 GD LGD SD and QL Re QL GD Sm 2

Ali Ramezani-Kebrya^{1*}

Armin Eftekhari^{2†}

Volkan Cevher¹

Table 1: Scaling with the number of training data in the overparameterization regime. QL=quadratic loss,

vation	Scaling	Reference
eLU	$ ilde{\Omega}(n^2)$	Oymak and Soltanolkotabi [38]
eLU	$ ilde{\Omega}(n)$	Kawaguchi and Huang [21]
eLU	$ ilde{\Omega}(n^2)$	Song and Yang [39]
eLU	$ ilde{\Omega}(n^6)$	Du et al. [12]
eLU	$\Omega(n^8L^{12})$	Zou and Gu [44]
nooth	$ ilde{\Omega}(n^{rac{3}{2}})$	This paper

A curious observation on fitting the data

Small ReLU networks are powerful memorizers: a tight analysis of memorization capacity

Chulhee Yun MIT Cambridge, MA 02139 chulheey@mit.edu

Suvrit Sra MIT

Cambridge, MA 02139 suvrit@mit.edu

Theorem:

Any data set of size n can be memorized by a 3-layer ReLU neural network with O(n) weights.

These constructions can be made in linear time. Yet SGD on the same arch needs so much more larger overarm. Why??

Ali Jadbabaie MIT Cambridge, MA 02139 jadbabai@mit.edu

But somehow SGD does more than just that...

Rethinking Generalization [Zhang et al. ICLR 17]



Figure 1: Fitting random labels and random pixels on CIFAR10. (a) shows the training loss of various experiment settings decaying with the training steps. (b) shows the relative convergence time with different label corruption ratio. (c) shows the test error (also the generalization error since training error is 0) under different label corruptions.

• Overparameterized, SGD-trained models : Can fit even completely random labels (i.e., huge capacity) Yet, generalize well

Rethinking Generalization [Zhang et al. ICLR17]



Figure 1: Fitting random labels and random pixels on CIFAR10. (a) shows the training loss of various experiment settings decaying with the training steps. (b) shows the relative convergence time with different label corruption ratio. (c) shows the test error (also the generalization error since training error is 0) under different label corruptions.

Overparameterized, SGD-trained models :
I. Can fit even completely random labels (
2. Yet, generalize well

Open Question: How can this be?

Possible Explanations of Generalization

• Maybe every model that fits the training data generalizes (no bad global minima)

• Maybe SGD is special "can avoid" bad global minima (implicit regularization)?

• Maybe the data distribution is what allows everything to fall into place?

Maybe all interpolating points generalize!

What is a bad global minimum?



Bad Minima = zero margin/complex boundary => 100% train error + poor test



Bad Global Minima Exist





Bad Global Minima Exist CIFAR10







Bad Global Minima Exist CIFAR10

CIFAR10





not all interpolating solutions are good



Possible Explanations of Generalization

• Maybe every model that fits the training data generalizes (no bad global minima)

• Maybe SGD is special "can avoid" bad global minima (implicit regularization)?

• Maybe the data distribution is what allows everything to fall into place?

nope



Maybe (S)GD is special?

ullet

GD + LS = a red herring

- The iterates of GD look like

$$w_{k+1} = w_k - \frac{\gamma}{2} \nabla L(x_k)$$
$$= w_k - \gamma X(X^T)$$

 (w_k)

 $(w_k - y)$

- The iterates of GD look like

$$w_{k+1} = w_k - \frac{\gamma}{2} \nabla L(w_k)$$
$$= w_k - \gamma X(X^T w_k - \gamma X(X^T w_k - \gamma XX^T) w_k - \gamma XX^T) w_k - \gamma XX^T - \gamma XX^$$

Let's say we want to solve a least squares problem $\min ||X^Tw - y||^2$ with GD ${\mathcal W}$

-y)

 $+ \gamma X y$

 $Y_{d-1} + (I_d - \gamma X X^T) \gamma X y + \gamma X y$

- The iterates of GD look like

$$\begin{split} w_{k+1} &= w_k - \frac{\gamma}{2} \nabla L(w_k) \\ &= w_k - \gamma X(X^T w_k - y) \\ &= (I_d - \gamma X X^T) w_k + \gamma X y \\ &= (I_d - \gamma X X^T)^2 w_{k-1} + (I_d - \gamma X X^T) \gamma X y + \gamma X y \\ &= (I_d - \gamma X X^T)^2 w_{k-1} + \gamma \left(\sum_{i=0}^1 (I_d - \gamma X X^T)^i\right) X y \end{split}$$

$$= w_k - \gamma X(X^T w_k - y)$$

= $(I_d - \gamma X X^T) w_k + \gamma X y$
= $(I_d - \gamma X X^T)^2 w_{k-1} + (I_d - \gamma X X^T) \gamma X y + \gamma X y$
= $(I_d - \gamma X X^T)^2 w_{k-1} + \gamma \left(\sum_{i=0}^1 (I_d - \gamma X X^T)^i\right) X y$

- The iterates of GD look like

$$\begin{split} w_{k+1} &= w_k - \frac{\gamma}{2} \nabla L(w_k) \\ &= w_k - \gamma X(X^T w_k - y) \\ &= (I_d - \gamma X X^T) w_k + \gamma X y \\ &= (I_d - \gamma X X^T)^2 w_{k-1} + (I_d - \gamma X X^T) \gamma X y + \gamma X y \\ &= (I_d - \gamma X X^T)^2 w_{k-1} + \gamma \left(\sum_{i=0}^1 (I_d - \gamma X X^T)^i\right) X y \\ &= (I_d - \gamma X X^T)^k w_0 + \gamma \left(\sum_{i=0}^{k-1} (I_d - \gamma X X^T)^i\right) X y \end{split}$$

Let's say we want to solve a least squares problem $\min ||X^Tw - y||^2$ with GD

GD + LS = a red herring

The iterates look like $w_{k+1}(I_d - \gamma XX^T)^k w_0 + \gamma \left(\sum_{i=0}^{k-1} (I_d - \gamma XX^T)^i\right) Xy$

- Assuming we start at zero, the iterates of GD look like

The iterates look like $w_{k+1}(I_d - \gamma XX^T)^k w_0 + \gamma \left(\sum_{i=0}^{k-1} (I_d - \gamma XX^T)^i\right) Xy$

- Assuming we start at zero, the iterates of GD look like

$$w_{k+1} = \gamma \left(\sum_{i=0}^{k-1} \left(x_{i}\right)\right)$$

The iterates look like $w_{k+1}(I_d - \gamma XX^T)^k w_0 + \gamma \left(\sum_{i=0}^{k-1} (I_d - \gamma XX^T)^i\right) Xy$

 $(I_d - \gamma X X^T)^i \bigg) X y$

- Assuming we start at zero, the iterates of GD look like

$$w_{k+1} = \gamma \left(\sum_{i=0}^{k-1} \left(\sum_{i=0}^{k-1}$$

What does that imply? Let's take GD to infinity

GD + LS = a red herring

The iterates look like $w_{k+1}(I_d - \gamma XX^T)^k w_0 + \gamma \left(\sum_{i=0}^{k-1} (I_d - \gamma XX^T)^i\right) Xy$

 $(I_d - \gamma X X^T)^i \right) X y$

- Assuming we start at zero, the iterates of GD look like

$$w_{k+1} = \gamma \left(\sum_{i=0}^{k-1} \left(\sum_{i=0}^{k-1}$$

What does that imply? Let's take GD to infinity $w_{\infty} = \gamma \left(\sum_{i=0}^{\infty} (I_d - \gamma X X^T)^i \right) X y$

GD + LS = a red herring

The iterates look like $w_{k+1}(I_d - \gamma XX^T)^k w_0 + \gamma \left(\sum_{k=0}^{k-1} (I_d - \gamma XX^T)^i\right) Xy$

 $(I_d - \gamma X X^T)^i \right) X y$

- The iterates look like $w_{k+1}(I_d \gamma XX^T)^k w_0 +$
- Assuming we start at zero, the iterates of GD look like

$$w_{k+1} = \gamma \left(\sum_{i=0}^{k-1} (I_d - \gamma X X^T)^i \right) X y$$

What does that imply? Let's take GD to infinity $w_{\infty} = \gamma \left(\sum_{i=0}^{\infty} (I_d) \right)$

Do you remember what this infinite sum converges to?

GD + LS = a red herring

$$\gamma \left(\sum_{i=0}^{k-1} (I_d - \gamma X X^T)^i \right) X y$$

$$-\gamma X X^T)^i \right) X y$$

- Assuming we start at zero, the iterates of GD look like

$$w_{k+1} = \gamma \left(\sum_{i=0}^{k-1} \left(\sum_{i=0$$

What does that imply? Let's take GD to infinity $w_{\infty} = \gamma \left(\sum_{i=0}^{\infty} (I_d - \gamma X X^T)^i \right) X y$

i=0

GD + LS = a red herring

The iterates look like $w_{k+1}(I_d - \gamma XX^T)^k w_0 + \gamma \left(\sum_{i=0}^{k-1} (I_d - \gamma XX^T)^i\right) Xy$

 $(I_d - \gamma X X^T)^i \left(X y \right)$



- Let's take GD to infinity

 $w_{\infty} = (X^T X)^{-1} X y$

GD + LS = a red herring

- Let's take GD to infinity

Do you remember what this is called? \bullet

GD + LS = a red herring

Let's say we want to solve a least squares problem $\min ||X^Tw - y||^2$ with GD W

 $w_{\infty} = (X^T X)^{-1} X y$

- Let's take GD to infinity

Do you remember what this is called? The minimum Euclidean norm solution of squares solution to $X^T w = y$

 ${\mathcal W}$

GD + LS = a red herring

Let's say we want to solve a least squares problem $\min \|X^Tw - y\|^2$ with GD W

 $w_{\infty} = (X^T X)^{-1} X y$

 $\arg\min\|w\|_2, \text{ s.t. } W^T x = y$

IMPLICIT BIAS/Regularization??!!!

- Let's say we want to solve a least squares problem $\min \|X^Tw y\|^2$ with GD W
- Let's take GD to infinity

 $W_{\infty} = (X)$

Do you remember what this is called? The minimum Euclidean norm solution of squares solution to $X^T w = y$

 ${\mathcal W}$

out of all the linear functions that interpolate the training data, (S)GD selects the minimal Euclidean norm one. Wow.

$$TX)^{-1}Xy$$

 $\arg\min\|w\|_2, \text{ s.t. } W^T x = y$

Theorem

For linear least squares GD converges to the minimum norm solution of $X^T w = y$

GD is IMPLICITLY regularizing against large norm solutions? It's Implicitly biased towards GENERALIZABLE solutions?

GD + LS = a red herring

Theorem

solution to the LS problem.



Well, linear LS is what's special

ANY algorithm that converges to 0-error and whose iterates converge to $w_{\infty} = \sum a_i x_i$ returns a min norm



All interpolating solutions in the data span are min norm

Theorem

solution to the LS problem.



OK so maybe GD is ... not that special???



All interpolating solutions



ANY algorithm that c

solution to the LS pro











The Implicit Bias of Gradient Descent on Separable Data

Daniel Soudry Elad Hoffer Mor Shpigel Nacson Department of Electrical Engineering, Technion Haifa, 320003, Israel

Suriya Gunasekar Nathan Srebro

Toyota Technological Institute at Chicago Chicago, Illinois 60637, USA

Theorem 3 For any dataset which is linearly separable (Assumption 1), any β -smooth decreasing loss function (Assumption 2) with an exponential tail (Assumption 3), any stepsize $\eta < 1$ $2\beta^{-1}\sigma_{\max}^{-2}(\mathbf{X})$ and any starting point $\mathbf{w}(0)$, the gradient descent iterates (as in eq. 2) will behave as:

> $\mathbf{w}(t) = \hat{\mathbf{w}} \log t + \boldsymbol{\rho}(t) ,$ (3)

where $\hat{\mathbf{w}}$ is the L_2 max margin vector (the solution to the hard margin SVM):

 $\hat{\mathbf{w}} = \operatorname{argmin} \|\mathbf{w}\|^2 \text{ s.t. } \mathbf{w}^\top \mathbf{x}_n \ge 1,$ (4) $\mathbf{w} {\in} \mathbb{R}^d$

and the residual grows at most as $\|\boldsymbol{\rho}(t)\| = O(\log \log(t))$, and so

 $\lim_{t\to\infty}$

Furthermore, for almost all data sets (all except measure zero), the residual $\rho(t)$ is bounded.

DANIEL.SOUDRY@GMAIL.COM ELAD.HOFFER@GMAIL.COM MOR.SHPIGEL@GMAIL.COM

> SURIYA@TTIC.EDU NATI@TTIC.EDU

$$\frac{\mathbf{w}(t)}{\left\|\mathbf{w}(t)\right\|} = \frac{\hat{\mathbf{w}}}{\left\|\hat{\mathbf{w}}\right\|}.$$



Does SGD really regularize??

Implicit Regularization in ReLU Networks with the Square Loss

Gal Vardi GAL.VARDI@WEIZMANN.AC.IL and **Ohad Shamir** OHAD.SHAMIR@WEIZMANN.AC.IL Weizmann Institute of Science

Editors: Mikhail Belkin and Samory Kpotufe

Abstract

Understanding the implicit regularization (or implicit bias) of gradient descent has recently been a very active research area. However, the implicit regularization in nonlinear neural networks is still poorly understood, especially for regression losses such as the square loss. Perhaps surprisingly, we prove that even for a single ReLU neuron, it is impossible to characterize the implicit regularization with the square loss by any explicit function of the model parameters (although on the positive side, we show it can be characterized approximately). For one hidden-layer networks, we prove a similar result, where in general it is impossible to characterize implicit regularization properties in this manner, except for the "balancedness" property identified in Du et al. (2018). Our results suggest that a more general framework than the one considered so far may be needed to understand implicit regularization for nonlinear predictors, and provides some clues on what this framework should be.

Implicit Regularization in ReLU Networks with the Square Loss

Gal Vardi Weizmann Ins Editors: Mik Understa very acti poorly u prove the with the side, we a simila in this n suggest implicit should b



IANN.AC.IL

been a s is still gly, we rization oositive operties results erstand nework

But maybe some form of hard to describe regularization is happening???

Can SGD reach bad global minima?



• Of course ... if you initialize at a bad global min.

But, SGD still converges to them, if adversarially initialized even without loss-landscape knowledge

We can construct initializers using only <u>unlabeled data</u> From which SGD is attracted to bad global minima



Adversarial Initialization



for every image $x \in S$ repeat R times zero-out a random subset of N % pixels in x give it a random label Add it to set C

SGD

Input: Training dataset S; Replication factor R; Noise factor N

Train to 100% accuracy on C, from a random init using vanilla

How Vanilla SGD gets in bad global minima

Random Initialization

True labels

Random labels



True labels





SGD "repairs" the boundary just enough to fit the data

Can't "forget" the bad initialization



Regularization saves the day

Vanilla SGD



Data augmentation L2 regularization







A recap of the setups





True labels Random Init

Random labels Random Init

Vanilla SGD





True labels, Adversarial Init

True labels labels, Adversarial init



- Data Sets:
- Hyperparameters tuned for faster convergence on train

Random Initializer

Random labels + VSGD

Adversarial Initializer



Experiments

Cifar 10/100, CINIC 10, Restricted Imagenet • Architectures: VGG16, Resnet18/50, DenseNet40



Main Findings

- The model found is close to the adversarial initialization.
- SGD escaping adversarial initialization.
- Any two of {DA, M, L2} are enough.

Adversarial initialization causes VSGD up to 40% drop in test accuracy

• Data augmentation, momentum, and L2 regularization all contribute to





TL;DR: Everything converges to 100% train accuracy



Test Accuracy





TL;DR: Test error deteriorates for Vanilla SGD and Adv initialization



Model Complexity



ResNet 50 trained on CIFARIO.

TL;DR: SGD on adv init has higher complexity measures compared to all other models

Effect of Replication Factor



TL;DR: The more you augment the randomly labeled set, the worse test error becomes

What is the point of all this

Implicit bias is likely weak in comparison to explicit regularization

Regularization affects the entire search dynamics, not just around global minima

The importance of regularization even very far away from the minima of the loss landscape.

Possible Explanations of Generalization

• Maybe every model that fits the training data generalizes (no bad global minima)

Current implicit bias studies can't capture such a strong effect
Maybe SGD is special "can avoid" bad global minima (implicit regularization)?

• Maybe the data distribution is what allows everything to fall into place?

nope



Possible Explanations of Generalization

• Maybe every model that fits the training data generalizes (no bad global minima)

Current implicit bias studies can't capture such a strong effect
Maybe SGD is special "can avoid" bad global minima (implicit regularization)?

• Maybe the data distribution is what allows everything to fall into place?

Nobody knows

nope



reading list

Soudry, D., Hoffer, E., Nacson, M.S., Gunasekar, S. and Srebro, N., 2018. The implicit bias of gradient descent on separable data. The Journal of Machine Learning Research, 19(1), pp.2822-2878. Vancouver https://www.jmlr.org/papers/volume19/18-188/18-188.pdf

Gunasekar, S., Lee, J., Soudry, D. and Srebro, N., 2018, July. Characterizing implicit bias in terms of optimization geometry. In International Conference on Machine Learning (pp. 1832-1841). PMLR. Vancouver http://proceedings.mlr.press/v80/gunasekar18a/gunasekar18a.pdf

Neyshabur, B., Tomioka, R. and Srebro, N., 2014. In search of the real inductive bias: On the role of implicit regularization in deep learning. arXiv preprint arXiv:1412.6614. Vancouver https://arxiv.org/pdf/1412.6614.pdf

Vardi, G. and Shamir, O., 2021, July. Implicit regularization in relu networks with the square loss. In Conference on Learning Theory (pp. 4224-4258). PMLR. http://proceedings.mlr.press/v134/vardi21b/vardi21b.pdf

Liu, S., Papailiopoulos, D. and Achlioptas, D., 2020. Bad global minima exist and sgd can reach them. Advances in Neural Information Processing Systems, 33, pp.8543-8552. Vancouver https://arxiv.org/abs/1906.02613







