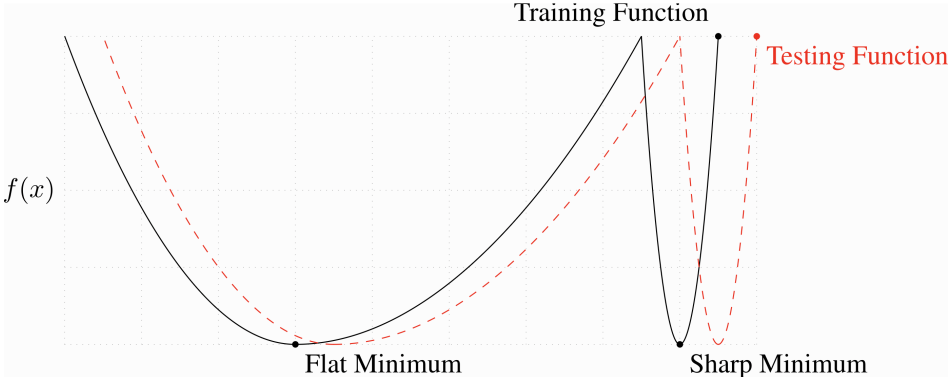
Sharpness-Aware Minimization. Mode Connectivity. Grokking. Double Descent.

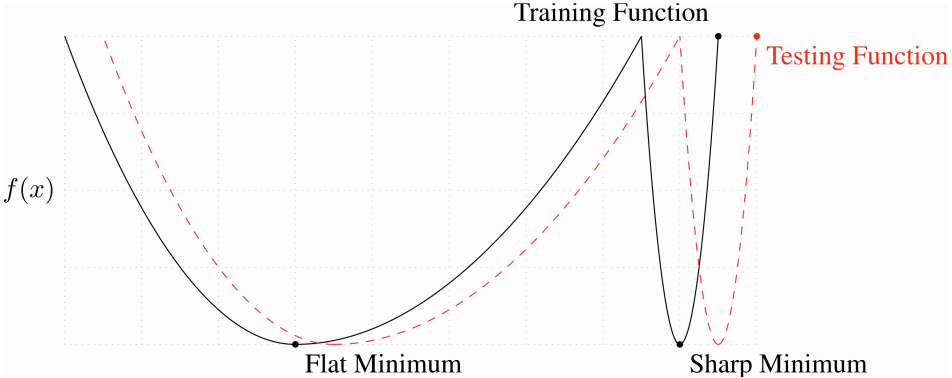
Seminar

Optimization for ML. Faculty of Computer Science. HSE University

Flat Minimum vs Sharp Minimum



Flat Minimum vs Sharp Minimum



Question

What's wrong with Sharp Minimum?

Sharpness-Aware Minimization[1]

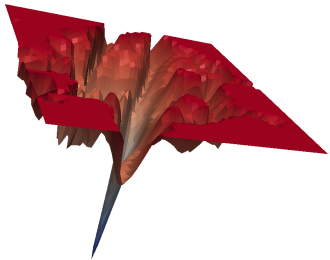


Figure 1: A sharp minimum to which a ResNet trained with SGD converged.

Sharpness-Aware Minimization[1]

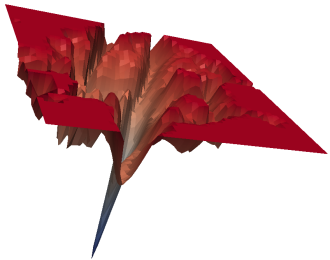


Figure 1: A sharp minimum to which a ResNet trained with SGD converged.

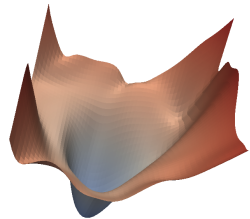


Figure 2: A wide minimum to which the same ResNet trained with SAM converged.

[1] Foret, Pierre, et al. "Sharpness-aware minimization for efficiently improving generalization." (2020).

Sharpness-Aware Minimization[1]

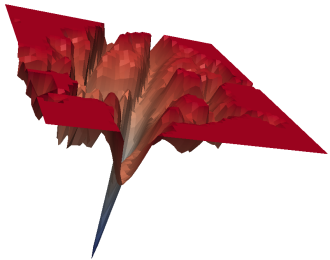


Figure 1: A sharp minimum to which a ResNet trained with SGD converged.

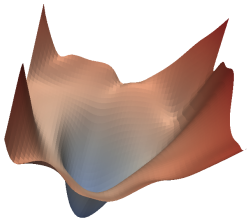


Figure 2: A wide minimum to which the same ResNet trained with SAM converged.

Sharpness-Aware Minimization (SAM) is a procedure that aims to improve model generalization by simultaneously minimizing loss value and **loss sharpness**.

[1] Foret, Pierre, et al. "Sharpness-aware minimization for efficiently improving generalization." (2020).

Learning setup

The training dataset drawn $i.i.d.$ from a distribution D:

$$S = \{(x_i, y_i)\}_{i=1}^{n},$$

where x_i – feature vector and y_i – label.

Learning setup

The training dataset drawn $i.i.d.$ from a distribution D:

$$S = \{(x_i, y_i)\}_{i=1}^{n},$$

where x_i – feature vector and y_i – label.

The training set loss:

$$L_S = \frac{1}{n} \sum_{i=1}^{n} l(\boldsymbol{w}, x_i, y_i),$$

where l – per-data-point loss function, $\boldsymbol{w}$ – parameters.

Learning setup

The training dataset drawn $i.i.d.$ from a distribution D:

$$S = \{(x_i, y_i)\}_{i=1}^{n},$$

where x_i – feature vector and y_i – label.

The training set loss:

$$L_S = \frac{1}{n} \sum_{i=1}^{n} l(\boldsymbol{w}, x_i, y_i),$$

where l – per-data-point loss function, $\boldsymbol{w}$ – parameters.

The population loss:

$$L_D = \mathbb{E}_{(x,y)}[l(\boldsymbol{w}, \boldsymbol{x}, \boldsymbol{y})]$$

What is sharpness?

Theorem

For any $\rho > 0$, with high probability over training set S generated from distribution D,

$$L_D(\boldsymbol{w}) \leq \max_{\|\boldsymbol{\epsilon}\|_2 \leq \rho} L_S(\boldsymbol{w} + \boldsymbol{\epsilon}) + h\left(\|\boldsymbol{w}\|_2^2 / \rho^2\right),$$

where $h : \mathbb{R}_+ \to \mathbb{R}_+$is a strictly increasing function (under some technical conditions on $L_D(\boldsymbol{w})$).

What is sharpness?

Theorem

For any $\rho > 0$, with high probability over training set S generated from distribution D,

$$L_D(\boldsymbol{w}) \leq \max_{\|\boldsymbol{\epsilon}\|_2 \leq \rho} L_S(\boldsymbol{w} + \boldsymbol{\epsilon}) + h\left(\|\boldsymbol{w}\|_2^2 / \rho^2\right),$$

where $h : \mathbb{R}_+ \to \mathbb{R}_+$is a strictly increasing function (under some technical conditions on $L_D(\boldsymbol{w})$).

Adding and subtracting $L_S(\boldsymbol{w})$:

$$\left[\max_{\|\in\|_2 \leq \rho} L_S(\boldsymbol{w} + \boldsymbol{\epsilon}) - L_S(\boldsymbol{w})\right] + L_{\mathcal{S}}(\boldsymbol{w}) + h\left(\|\boldsymbol{w}\|_2^2 / \rho^2\right)$$

The term in square brackets captures the **sharpness** of L_S at $\boldsymbol{w}$ by measuring how quickly the training loss can be increased by moving from $\boldsymbol{w}$ to a nearby parameter value.

Sharpness-Aware Minimization

The function h is removed in favor of a simpler constant λ. The authors propose selecting parameter values by solving the following Sharpness-Aware Minimization (SAM) problem:

$$\min_{\boldsymbol{w}} L_S^{SAM}(\boldsymbol{w}) + \lambda \|\boldsymbol{w}\|_2^2 \quad \text{where} \quad L_S^{SAM}(\boldsymbol{w}) \triangleq \max_{\|\epsilon\|_p \leq \rho} L_S(\boldsymbol{w} + \boldsymbol{\epsilon}),$$

with $\rho \geq 0$ as hyperparameter and p in $[1, \infty]$ (a little generalization, though $p = 2$ is empirically the best choice).

How to minimize L_S^{SAM}?

In order to minimize L_S^{SAM} an efficient approximation of its gradient is used. A first step is to consider the first-order Taylor expansion of $L_S(\boldsymbol{w}+\boldsymbol{\epsilon})$:

$$\boldsymbol{\epsilon}^*(\boldsymbol{w}) \triangleq \underset{\|\epsilon\|_p \leq \rho}{\arg\max} L_S(\boldsymbol{w}+\boldsymbol{\epsilon}) \approx \underset{\|\epsilon\|_p \leq \rho}{\arg\max} L_S(\boldsymbol{w}) + \boldsymbol{\epsilon}^T \nabla_{\boldsymbol{w}} L_S(\boldsymbol{w}) = \underset{\|\epsilon\|_p \leq \rho}{\arg\max} \boldsymbol{\epsilon}^T \nabla_{\boldsymbol{w}} L_S(\boldsymbol{w}).$$

How to minimize L_S^{SAM}?

In order to minimize L_S^{SAM} an efficient approximation of its gradient is used. A first step is to consider the first-order Taylor expansion of $L_S(\boldsymbol{w}+\boldsymbol{\epsilon})$:

$$\boldsymbol{\epsilon}^*(\boldsymbol{w}) \triangleq \underset{\|\epsilon\|_p \leq \rho}{\arg\max} L_S(\boldsymbol{w}+\boldsymbol{\epsilon}) \approx \underset{\|\epsilon\|_p \leq \rho}{\arg\max} L_S(\boldsymbol{w}) + \boldsymbol{\epsilon}^T \nabla_{\boldsymbol{w}} L_S(\boldsymbol{w}) = \underset{\|\epsilon\|_p \leq \rho}{\arg\max} \boldsymbol{\epsilon}^T \nabla_{\boldsymbol{w}} L_S(\boldsymbol{w}).$$

The last expression is just the argmax of the dot product of the vectors $\boldsymbol{\epsilon}$ and $\nabla_{\boldsymbol{w}} L_S(\boldsymbol{w})$, and it is well known which is the argument that maximizes it:

$$\hat{\boldsymbol{\epsilon}}(\boldsymbol{w}) = \rho \operatorname{sign}\left(\nabla_{\boldsymbol{w}} L_S(\boldsymbol{w})\right) \left|\nabla_{\boldsymbol{w}} L_S(\boldsymbol{w})\right|^{q-1} / \left(\|\nabla_{\boldsymbol{w}} L_S(\boldsymbol{w})\|_q^q\right)^{1/p},$$

where $1/p + 1/q = 1$.

How to minimize L_S^{SAM}?

In order to minimize L_S^{SAM} an efficient approximation of its gradient is used. A first step is to consider the first-order Taylor expansion of $L_S(\boldsymbol{w}+\boldsymbol{\epsilon})$:

$$\boldsymbol{\epsilon}^*(\boldsymbol{w}) \triangleq \underset{\|\epsilon\|_p \leq \rho}{\arg\max} L_S(\boldsymbol{w}+\boldsymbol{\epsilon}) \approx \underset{\|\epsilon\|_p \leq \rho}{\arg\max} L_S(\boldsymbol{w}) + \boldsymbol{\epsilon}^T \nabla_{\boldsymbol{w}} L_S(\boldsymbol{w}) = \underset{\|\epsilon\|_p \leq \rho}{\arg\max} \boldsymbol{\epsilon}^T \nabla_{\boldsymbol{w}} L_S(\boldsymbol{w}).$$

The last expression is just the argmax of the dot product of the vectors $\boldsymbol{\epsilon}$ and $\nabla_{\boldsymbol{w}} L_S(\boldsymbol{w})$, and it is well known which is the argument that maximizes it:

$$\hat{\boldsymbol{\epsilon}}(\boldsymbol{w}) = \rho \operatorname{sign}\left(\nabla_{\boldsymbol{w}} L_S(\boldsymbol{w})\right) \left|\nabla_{\boldsymbol{w}} L_S(\boldsymbol{w})\right|^{q-1} / \left(\|\nabla_{\boldsymbol{w}} L_S(\boldsymbol{w})\|_q^q\right)^{1/p},$$

where $1/p + 1/q = 1$.

Thus

$$\nabla_{\boldsymbol{w}} L_S^{SAM}(\boldsymbol{w}) \approx \nabla_{\boldsymbol{w}} L_S(\boldsymbol{w}+\hat{\boldsymbol{\epsilon}}(\boldsymbol{w})) = \left.\frac{d(\boldsymbol{w}+\hat{\boldsymbol{\epsilon}}(\boldsymbol{w}))}{d\boldsymbol{w}} \nabla_{\boldsymbol{w}} L_S(\boldsymbol{w})\right|_{\boldsymbol{w}+\hat{\boldsymbol{\epsilon}}(w)}$$

$$= \nabla_w L_S(\boldsymbol{w})|_{\boldsymbol{w}+\hat{\boldsymbol{\epsilon}}(\boldsymbol{w})} + \left.\frac{d\hat{\boldsymbol{\epsilon}}(\boldsymbol{w})}{d\boldsymbol{w}} \nabla_{\boldsymbol{w}} L_S(\boldsymbol{w})\right|_{\boldsymbol{w}+\hat{\boldsymbol{\epsilon}}(\boldsymbol{w})}$$

Sharpness-Aware Minimization

Modern frameworks can easily compute the preceding approximation. However, to speed up the computation, second-order terms can be dropped obtaining:

$$\nabla_{\boldsymbol{w}} L_S^{SAM}(\boldsymbol{w}) \approx \nabla_{\boldsymbol{w}} L_S(w)\Big|_{\boldsymbol{w}+\hat{\boldsymbol{\epsilon}}(\boldsymbol{w})}$$

Sharpness-Aware Minimization

Modern frameworks can easily compute the preceding approximation. However, to speed up the computation, second-order terms can be dropped obtaining:

$$\nabla_{\boldsymbol{w}} L_S^{SAM}(\boldsymbol{w}) \approx \nabla_{\boldsymbol{w}} L_S(w)\big|_{\boldsymbol{w}+\hat{\boldsymbol{\epsilon}}(\boldsymbol{w})}$$

Input: Training set $\mathcal{S} \triangleq \cup_{i=1}^{n}\{(\boldsymbol{x}_i, \boldsymbol{y}_i)\}$, Loss function $l : \mathcal{W} \times \mathcal{X} \times \mathcal{Y} \to \mathbb{R}_+$, Batch size b, Step size $\eta > 0$, Neighborhood size $\rho > 0$.
Output: Model trained with SAM
Initialize weights $\boldsymbol{w}_0$, $t = 0$;
while *not converged* **do**
  Sample batch $\mathcal{B} = \{(\boldsymbol{x}_1, \boldsymbol{y}_1), ...(\boldsymbol{x}_b, \boldsymbol{y}_b)\}$;
  Compute gradient $\nabla_{\boldsymbol{w}} L_{\mathcal{B}}(\boldsymbol{w})$ of the batch's training loss;
  Compute $\hat{\boldsymbol{\epsilon}}(\boldsymbol{w})$ per equation 2;
  Compute gradient approximation for the SAM objective (equation 3): $\boldsymbol{g} = \nabla_w L_{\mathcal{B}}(\boldsymbol{w})|_{\boldsymbol{w}+\hat{\boldsymbol{\epsilon}}(\boldsymbol{w})}$;
  Update weights: $\boldsymbol{w}_{t+1} = \boldsymbol{w}_t - \eta \boldsymbol{g}$;
  $t = t + 1$;
end
return $\boldsymbol{w}_t$

Algorithm 1: SAM algorithm

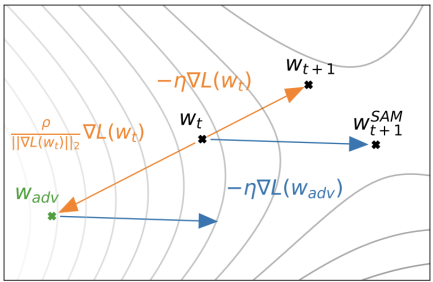


Figure 2: Schematic of the SAM parameter update.

SAM results

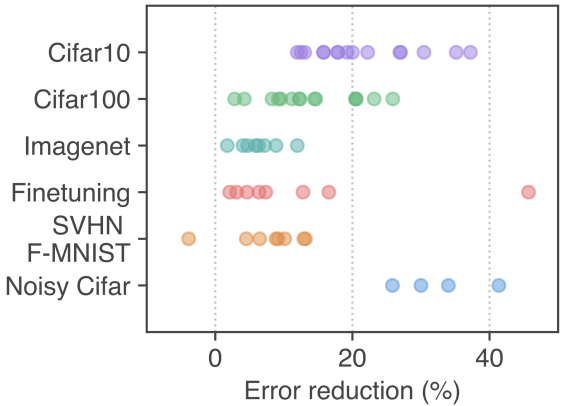


Figure 4: Error rate reduction obtained by switching to SAM. Each point is a different dataset / model / data augmentation.

Mode Connectivity[2]

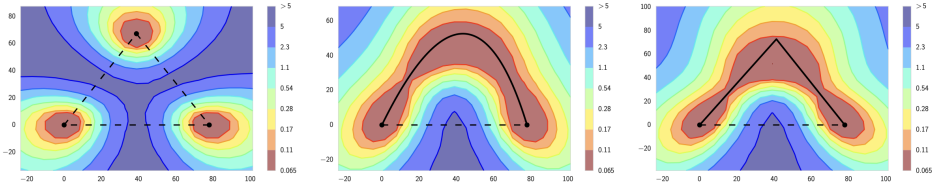


Figure 5: The l_2-regularized cross-entropy train loss surface of a ResNet-164 on CIFAR-100, as a function of network weights in a two-dimensional subspace. In each panel, the horizontal axis is fixed and is attached to the optima of two independently trained networks. The vertical axis changes between panels as we change planes (defined in the main text). Left: Three optima for independently trained networks. Middle and Right: A quadratic Bezier curve, and a polygonal chain with one bend, connecting the lower two optima on the left panel along a path of near-constant loss. Notice that in each panel a direct linear path between each mode would incur high loss.

[2] Garipov, Timur, et al. "Loss surfaces, mode connectivity, and fast ensembling of dnns." Advances in neural information processing systems 31 (2018).

Curve-Finding Procedure

- Weights of pretrained networks:

$$\widehat{w}_1, \widehat{w}_2 \in \mathbb{R}^{|\text{net}|}$$

- Define parametric curve: $\phi_\theta(\cdot) : [0,1] \to \mathbb{R}^{|\text{net}|}$

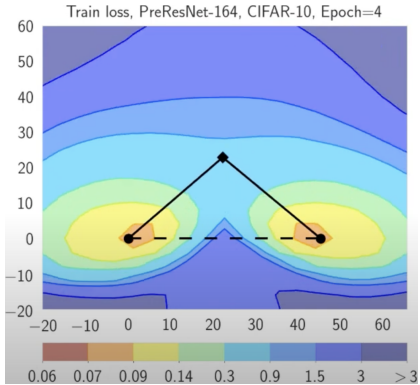
$$\phi_\theta(0) = \widehat{w}_1, \quad \phi_\theta(1) = \widehat{w}_2$$

- DNN loss function:

$$\mathcal{L}(w)$$

- Minimize averaged loss w.r.t. θ:

$$\underset{\theta}{\text{minimize}} \;\; \ell(\theta) = \int_0^1 \mathcal{L}\left(\phi_\theta(t)\right) dt = \mathbb{E}_{t\sim U(0,1)} \mathcal{L}\left(\phi_\theta(t)\right)$$



Curve-Finding Procedure

- Weights of pretrained networks:

$$\widehat{w}_1, \widehat{w}_2 \in \mathbb{R}^{|\text{net}|}$$

- Define parametric curve: $\phi_\theta(\cdot) : [0,1] \to \mathbb{R}^{|\text{net}|}$

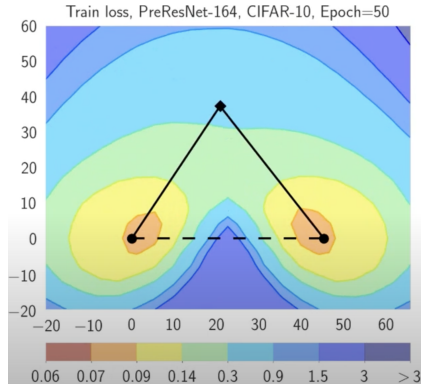
$$\phi_\theta(0) = \widehat{w}_1, \quad \phi_\theta(1) = \widehat{w}_2$$

- DNN loss function:

$$\mathcal{L}(w)$$

- Minimize averaged loss w.r.t. θ:

$$\underset{\theta}{\text{minimize}} \;\; \ell(\theta) = \int_0^1 \mathcal{L}\left(\phi_\theta(t)\right) dt = \mathbb{E}_{t\sim U(0,1)} \mathcal{L}\left(\phi_\theta(t)\right)$$



Curve-Finding Procedure

- Weights of pretrained networks:

$$\widehat{w}_1, \widehat{w}_2 \in \mathbb{R}^{|\text{net}|}$$

- Define parametric curve: $\phi_\theta(\cdot) : [0,1] \to \mathbb{R}^{|\text{net}|}$

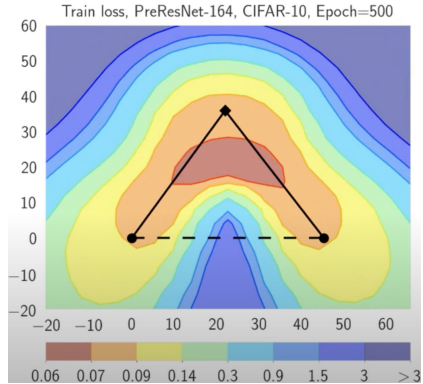
$$\phi_\theta(0) = \widehat{w}_1, \quad \phi_\theta(1) = \widehat{w}_2$$

- DNN loss function:

$$\mathcal{L}(w)$$

- Minimize averaged loss w.r.t. θ:

$$\underset{\theta}{\text{minimize}} \;\; \ell(\theta) = \int_0^1 \mathcal{L}\left(\phi_\theta(t)\right) dt = \mathbb{E}_{t\sim U(0,1)} \mathcal{L}\left(\phi_\theta(t)\right)$$



Grokking[3]

- After achieving zero train loss the weights continue evolving in a kind of random walk manner
- It is possible that they slowly drift to a wider minima
- Recently discovered grokking effect confirms this hypo

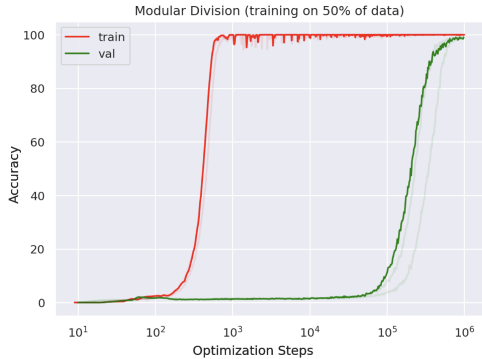


Figure 6: Grokking: A dramatic example of generalization far after overfitting on an algorithmic dataset.

[3]Power, Alethea, et al. "Grokking: Generalization beyond overfitting on small algorithmic datasets." (2022).

Double Descent[4]

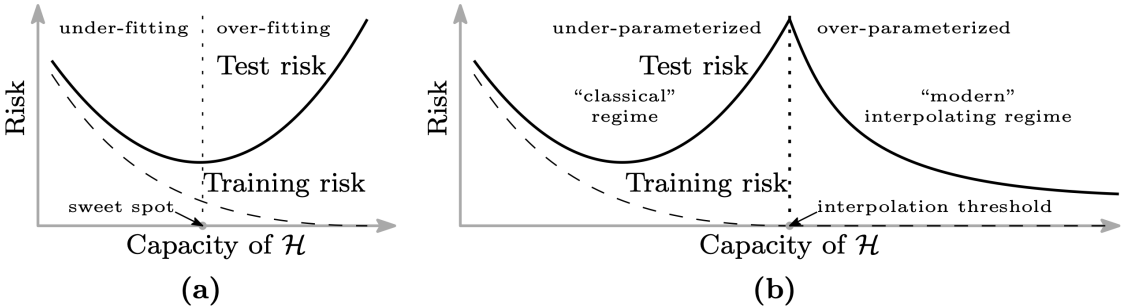


Figure 7: Curves for training risk (dashed line) and test risk (solid line). (a) The classical U-shaped risk curve arising from the bias-variance trade-off. (b) The double descent risk curve, which incorporates the U-shaped risk curve (i.e., the "classical" regime) together with the observed behavior from using high capacity function classes (i.e., the "modern" interpolating regime), separated by the interpolation threshold. The predictors to the right of the interpolation threshold have zero training risk.

[4]Belkin, Mikhail, et al. "Reconciling modern machine-learning practice and the classical bias–variance trade-off." (2019)