CS 6316 Machine Learning

The Bias-Complexity Tradeoff

Yangfeng Ji

Department of Computer Science University of Virginia



For a real-world machine learning problem, which of the following items are usually available to us?

For a real-world machine learning problem, which of the following items are usually available to us?

- ► Training set $S = \{(x_1, y_1), ..., (x_m, y_m)\}$
- ightharpoonup Domain set $\mathfrak X$
- Label set Y

For a real-world machine learning problem, which of the following items are usually available to us?

- ► Training set $S = \{(x_1, y_1), ..., (x_m, y_m)\}$
- ightharpoonup Domain set $\mathfrak X$
- Label set Y
- ► Labeling function (the oracle) *f*
- ▶ Distribution \mathfrak{D} over $\mathfrak{X} \times \mathcal{Y}$
- ► The Bayes predictor $f_{\mathfrak{D}}(x)$

For a real-world machine learning problem, which of the following items are usually available to us?

- ► Training set $S = \{(x_1, y_1), ..., (x_m, y_m)\}$
- ightharpoonup Domain set \mathfrak{X}
- Label set Y
- ► Labeling function (the oracle) *f*
- ▶ Distribution \mathfrak{D} over $\mathfrak{X} \times \mathcal{Y}$
- ► The Bayes predictor $f_{\mathfrak{D}}(x)$
- ▶ The size of the hypothesis space \mathcal{H}
- ▶ The empirical risk of a hypothesis $h(x) \in \mathcal{H}$, $L_S(h(x))$
- ▶ The true risk of a hypothesis $h(x) \in \mathcal{H}$, $L_{\mathfrak{D}}(h(x))$

Agnostic PAC Learnability

A hypothesis class \mathcal{H} is agnostic PAC learnable if there exist a function $m_{\mathcal{H}}:(0,1)^2\to\mathbb{N}$ and a learning algorithm with the following property:

- for every distribution \mathfrak{D} over $\mathfrak{X} \times \{-1, +1\}$ and
- for every ϵ , $\delta \in (0,1)$,

when running the learning algorithm on $m \ge m_{\mathcal{H}}(\epsilon, \delta)$ i.i.d. examples generated by \mathfrak{D} , the algorithm returns a hypothesis h_{S^1} such that, with probability of at least $1 - \delta$,

$$L_{\mathfrak{D}}(h_S) \le \min_{h' \in \mathcal{H}} L_{\mathfrak{D}}(h') + \varepsilon \tag{1}$$

¹Sometimes, as $h_S(x)$ or h(x, S)

The Bayes Optimal Predictor

► The Bayes optimal predictor: given a probability distribution \mathfrak{D} over $\mathfrak{X} \times \{-1, +1\}$, the predictor is defined as

$$f_{\mathfrak{D}}(x) = \begin{cases} +1 & \text{if } \mathbb{P}[y=1|x] \ge \frac{1}{2} \\ -1 & \text{otherwise} \end{cases}$$
 (2)

▶ No other predictor can do better: for any predictor *h*

$$L_{\mathfrak{D}}(f_{\mathfrak{D}}) \le L_{\mathfrak{D}}(h) \tag{3}$$

The Bayes Optimal Predictor

► The Bayes optimal predictor: given a probability distribution \mathfrak{D} over $\mathfrak{X} \times \{-1, +1\}$, the predictor is defined as

$$f_{\mathfrak{D}}(x) = \begin{cases} +1 & \text{if } \mathbb{P}[y=1|x] \ge \frac{1}{2} \\ -1 & \text{otherwise} \end{cases}$$
 (2)

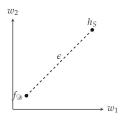
ightharpoonup No other predictor can do better: for any predictor h

$$L_{\mathfrak{D}}(f_{\mathfrak{D}}) \le L_{\mathfrak{D}}(h) \tag{3}$$

▶ Question: is $f_{\mathfrak{D}} \in \operatorname{argmin}_{h' \in \mathcal{H}} L_{\mathfrak{D}}(h')$?

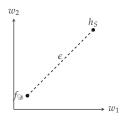
The Gap between h_S and $f_{\mathfrak{D}}$

For illustration purpose, let us assume the gap between h_S and $f_{\mathfrak{D}}$ can be visualized in the following plot



The Gap between h_S and $f_{\mathfrak{D}}$

For illustration purpose, let us assume the gap between h_S and $f_{\mathfrak{D}}$ can be visualized in the following plot



- ▶ h_S = argmin_{$h' \in \mathcal{H}$} $L_S(h')$: learned by minimizing the empirical risk
- $f_{\mathfrak{D}}$: the optimal predictor if we know the data distribution \mathfrak{D}

Question

Q: For a given hypothesis space \mathcal{H} , does

$$f_{\mathfrak{D}} \in \underset{h'}{\operatorname{argmin}} L_{\mathfrak{D}}(h')$$
 (4)

hold?

Question

Q: For a given hypothesis space \mathcal{H} , does

$$f_{\mathfrak{D}} \in \operatorname*{argmin}_{h'} L_{\mathfrak{D}}(h') \tag{4}$$

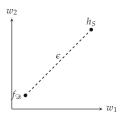
hold?

A: it depends the selection of the hypothesis space \mathcal{H} , usually not.

Example: if $f_{\mathfrak{D}}$ is a nonlinear classifier, while we choose to use logistic regression.

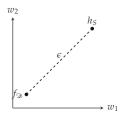
Outline

The previous example implies the error gap between h_S and $f_{\mathfrak{D}}$ can be decomposed into two components



Outline

The previous example implies the error gap between h_S and $f_{\mathfrak{D}}$ can be decomposed into two components



Two different perspectives of the decomposition

- ► The bias-complexity tradeoff: from the perspective of learning theory
- ► The bias-variance tradeoff: from the perspective of statistical learning/estimation

The Bias-Complexity Tradeoff

Basic Learning Procedure

The basic component of formulating a learning process

- ▶ Input/output space $\mathfrak{X} \times \mathcal{Y}$
- ► Hypothesis space ℋ
- Learning via empirical risk minimization

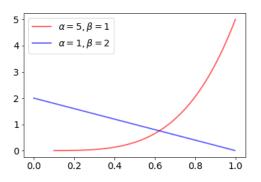
$$h_S \in \underset{h' \in \mathcal{H}}{\operatorname{argmin}} L_S(h')$$
 (5)

► Goal: analyzing the true error of h_S , $L_{\mathfrak{D}}(h_S)$

Example

Consider the binary classification problem with the data sampled from the following distribution

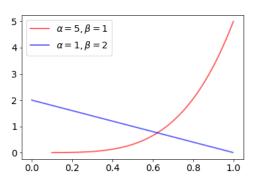
$$\mathcal{D} = \frac{1}{2} \Re(x; 5, 1) + \frac{1}{2} \Re(x; 1, 2) \tag{6}$$



Given the distribution, we can compute the true risk/error of the Bayes predictor $f_{\mathfrak{D}}$ as

$$L_{\mathfrak{D}}(f_{\mathfrak{D}}) = \frac{1}{2} \mathfrak{B}(x > b_{\text{Bayes}}; 5, 1) + \frac{1}{2} (1 - \mathfrak{B}(x > b_{\text{Bayes}}; 1, 2))$$

= 0.11799 (7)



The hypothesis space $\mathcal H$ is defined as

$$h_i(x) = \begin{cases} +1 & x > \frac{i}{N} \\ -1 & x < \frac{i}{N} \end{cases}$$
 (8)

where $N \in \mathbb{N}$ is a predefined integer

The hypothesis space $\mathcal H$ is defined as

$$h_i(x) = \begin{cases} +1 & x > \frac{i}{N} \\ -1 & x < \frac{i}{N} \end{cases}$$
 (8)

where $N \in \mathbb{N}$ is a predefined integer

- This is an unrealizable case
- ► The value of *N* is the size of the hypothesis space

The hypothesis space $\mathcal H$ is defined as

$$h_i(x) = \begin{cases} +1 & x > \frac{i}{N} \\ -1 & x < \frac{i}{N} \end{cases}$$
 (8)

where $N \in \mathbb{N}$ is a predefined integer

- This is an unrealizable case
- ► The value of *N* is the size of the hypothesis space
- ightharpoonup The best hypothesis in ${\mathcal H}$

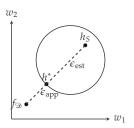
$$h^* \in \operatorname*{argmin}_{h' \in \mathscr{H}} L_{\mathfrak{D}}(h') \tag{9}$$

▶ Very likely the best predictor in \mathcal{H} is not the Bayes predictor, unless $b_{\text{Bayes}} \in \{\frac{i}{N} : i \in [N]\}$

Error Decomposition

The error gap between h_S and $f_{\mathfrak{D}}$ can be decomposed as two parts

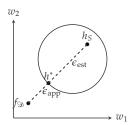
$$L_{\mathfrak{D}}(h_S) - L_{\mathfrak{D}}(f_{\mathfrak{D}}) = \epsilon_{\mathsf{app}} + \epsilon_{\mathsf{est}}$$
 (10)



Error Decomposition

The error gap between h_S and $f_{\mathfrak{D}}$ can be decomposed as two parts

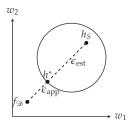
$$L_{\mathfrak{D}}(h_S) - L_{\mathfrak{D}}(f_{\mathfrak{D}}) = \epsilon_{\mathsf{app}} + \epsilon_{\mathsf{est}}$$
 (10)



- ▶ Approximation error ϵ_{app} caused by selecting a specific hypothesis space \mathcal{H} (model bias)
- ► Estimation error ϵ_{est} caused by selecting h_S with a specific training set

Approximation Error ϵ_{app}

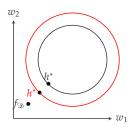
To reduce the approximation error $\epsilon_{\rm app}$, we could increase the size of the hypothesis space



The cost is that we also increase the size of training set, in order to maintain the overall error in the same level (recall the sample complexity of finite hypothesis spaces).

Approximation Error ϵ_{app}

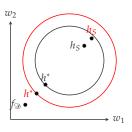
To reduce the approximation error $\epsilon_{\rm app}$, we could increase the size of the hypothesis space



The cost is that we also increase the size of training set, in order to maintain the overall error in the same level (recall the sample complexity of finite hypothesis spaces).

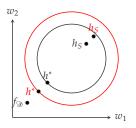
Estimation Error ϵ_{est}

On the other hand, if we use the same training set S, then we may have a larger estimation error



Estimation Error ϵ_{est}

On the other hand, if we use the same training set S, then we may have a larger estimation error

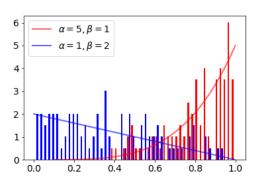


The bias-complexity tradeoff: find the right balance to reduce both approximation error and estimation error.

Example: 200 training examples

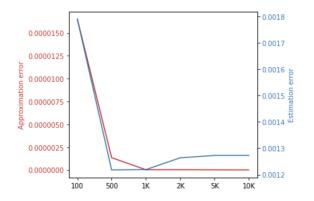
We randomly sampled 100 examples from each class

$$\mathfrak{D} = \frac{1}{2} \mathfrak{B}(x; 5, 1) + \frac{1}{2} \mathfrak{B}(x; 1, 2) \tag{11}$$



Example: 200 training examples

Given 200 training examples, the errors with respect to different hypothesis space is the following (x axis is the size of \mathcal{H})

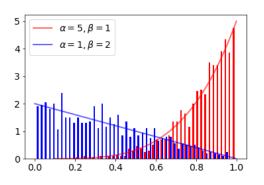


There is a tradeoff with respect to the size of \mathcal{H}

Example: 2000 training examples

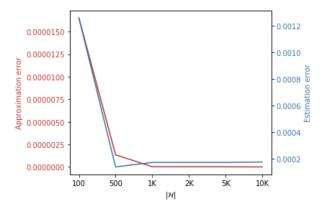
We randomly sampled 1000 examples from each class

$$\mathfrak{D} = \frac{1}{2} \mathfrak{B}(x; 5, 1) + \frac{1}{2} \mathfrak{B}(x; 1, 2) \tag{12}$$



Example: 2000 training examples

With these 2000 training examples, the errors with respect to different hypothesis space is the following



Both errors are smaller, but the tradeoff still exists

Summary

Three components in this decomposition

- ▶ $h_S \in \operatorname{argmin}_{h' \in \mathcal{H}} L_S(h')$: the ERM predictor given the training set S
- ▶ $h^* \in \operatorname{argmin}_{h' \in \mathcal{H}} L_{\mathfrak{D}}(h')$: the optimal predictor from \mathcal{H}
- $f_{\mathfrak{D}}$: the Bayes predictor given \mathfrak{D}

Summary

Three components in this decomposition

- ▶ $h_S \in \operatorname{argmin}_{h' \in \mathcal{H}} L_S(h')$: the ERM predictor given the training set S
- ▶ $h^* \in \operatorname{argmin}_{h' \in \mathcal{H}} L_{\mathfrak{D}}(h')$: the optimal predictor from \mathcal{H}
- $f_{\mathfrak{D}}$: the Bayes predictor given \mathfrak{D}

Balancing strategy:

- we can incrase the complexity of hypothesis space to reduce the bias, e.g.,
 - enlarge the hypothesis space (as in the running example)
 - replacing linear predictors with nonlinear predictors

Summary

Three components in this decomposition

- ▶ $h_S \in \operatorname{argmin}_{h' \in \mathcal{H}} L_S(h')$: the ERM predictor given the training set S
- ▶ $h^* \in \operatorname{argmin}_{h' \in \mathcal{H}} L_{\mathfrak{D}}(h')$: the optimal predictor from \mathcal{H}
- $f_{\mathfrak{D}}$: the Bayes predictor given \mathfrak{D}

Balancing strategy:

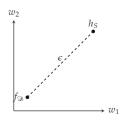
- we can incrase the complexity of hypothesis space to reduce the bias, e.g.,
 - enlarge the hypothesis space (as in the running example)
 - replacing linear predictors with nonlinear predictors
- ▶ in the meantime, we have to increase the training size to reduce the approximation error.

The Bias-Variance Tradeoff

A New Perspective

Let us analyze the error ϵ without the assumption of

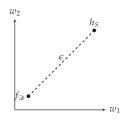
- ▶ knowing the best predictor from \mathcal{H} , $h^* \in \operatorname{argmin}_{h' \in \mathcal{H}} L_{\mathfrak{D}}(h')$
- changing the size of S



A New Perspective

Let us analyze the error ϵ without the assumption of

- ▶ knowing the best predictor from \mathcal{H} , $h^* \in \operatorname{argmin}_{h' \in \mathcal{H}} L_{\mathfrak{D}}(h')$
- changing the size of S



We still need (1) the ERM predictor h_S and (2) the Bayes predictor $f_{\mathfrak{D}}$

A New Way of Decomposition

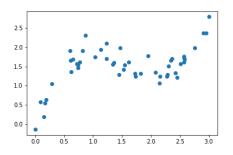
- ... by considering
 - ightharpoonup the randomness in *S* with *m* training examples
 - ▶ the average prediction given by E[h(x, S)] where $S \sim \mathfrak{D}^m$

Data Generation Model

Consider the following data generation model

- \blacktriangleright $X \sim U[0,1]$ uniform distribution
- $Y = \mathcal{N}(X + \sin(2X), \sigma^2)$ with $\sigma^2 = 0.1$

An example of *S* is

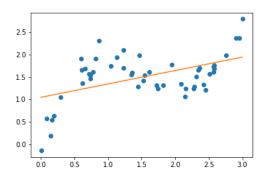


Hypothesis Spaces

Given *S* and the following hypothesis space \mathcal{H}_1

$$\mathcal{H}_1 = \{ w_0 + w_1 x : w_0, w_1 \in \mathbb{R} \} \tag{13}$$

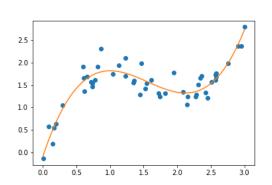
the regression result



Hypothesis Spaces (Cont.)

Given S and the following hypothesis space \mathcal{H}_3

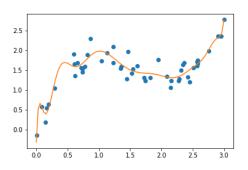
$$\mathcal{H}_3 = \{w_0 + w_1 x + w_2 x^2 + w_3 x^3 : w_0, w_1, w_2, w_3 \in \mathbb{R}\}$$
 (14) the regression result



Hypothesis Spaces (Cont.)

Given *S* and the following hypothesis space \mathcal{H}_{15}

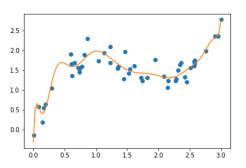
$$\mathcal{H}_{15} = \{ w_0 + w_1 x + \dots + w_{15} x^{15} : w_0, w_1, \dots, w_{15} \in \mathbb{R} \}$$
 (15)



Hypothesis Spaces (Cont.)

Given *S* and the following hypothesis space \mathcal{H}_{15}

$$\mathcal{H}_{15} = \{ w_0 + w_1 x + \dots + w_{15} x^{15} : w_0, w_1, \dots, w_{15} \in \mathbb{R} \}$$
 (15)



- ► Intuitively, the degree of the polynomials indicates the potential/complexity of the hypothesis space
- Refer to the VC dimension section for more discussion

Error Decomposition

The difference between the best hypothesis h(x, S) and the Bayes predictor $f_{\mathfrak{D}}(x)$ is measured as

$$\epsilon^2 = \{h(x, S) - f_{\mathfrak{D}}(x)\}^2 \tag{16}$$

Introduce E[h(x, S)] into the calculation, we have

$$\epsilon^2 = \{h(x,S) - E[h(x,S)] + E[h(x,S)] - f_{\mathfrak{D}}(x)\}^2$$

Error Decomposition

The difference between the best hypothesis h(x, S) and the Bayes predictor $f_{\mathfrak{D}}(x)$ is measured as

$$\epsilon^2 = \{h(x, S) - f_{\mathfrak{D}}(x)\}^2 \tag{16}$$

Introduce E[h(x, S)] into the calculation, we have

$$\epsilon^{2} = \{h(x,S) - E[h(x,S)] + E[h(x,S)] - f_{\mathfrak{D}}(x)\}^{2}$$

$$= \{h(x,S) - E[h(x,S)]\}^{2} + \{E[h(x,S)] - f_{\mathfrak{D}}(x)\}^{2}$$

$$+2\{h(x,S) - E[h(x,S)]\} \cdot \{E[h(x,S)] - f_{\mathfrak{D}}(x)\}$$

Review: Mean

Given a random variable X and its probability density function p(x)

- Mean: $E[X] = \int xp(x)dx$
- Approximation to the mean with samples $\{x_1, \ldots, x_m\}$

$$E[X] \approx \frac{1}{m} \sum_{i=1}^{m} x_i \tag{17}$$

- ▶ Property: $E[\alpha X] = \alpha E[X]$ for α is determinstic
- Example: the mean of a Gaussian distribution $\mathcal{N}(x; \mu, \sigma^2)$

$$E[X] = \mu \tag{18}$$

Review: Variance

Given a random variable X, its probability density function p(x), and its mean E[X]

- ► Variance: $Var(X) = E[(X E[X])^2]$
- Example: the variance of a Gaussian distribution $\mathcal{N}(x; \mu, \sigma^2)$

$$Var(X) = \sigma^2 \tag{19}$$

Review: Variance

Given a random variable X, its probability density function p(x), and its mean E[X]

- ► Variance: $Var(X) = E[(X E[X])^2]$
- Example: the variance of a Gaussian distribution $\mathcal{N}(x; \mu, \sigma^2)$

$$Var(X) = \sigma^2 \tag{19}$$

$$Var(X) = E[(X - E[X])^{2}]$$

$$= E[X^{2} - 2XE[X] + E[X]^{2}]$$

$$= E[X^{2}] - 2E[X]E[X] + E[X]^{2}$$

$$= E[X^{2}] - E[X]^{2}$$

Error Decomposition (Cont.)

Taking the expectation of ϵ^2

$$E\left[\epsilon^{2}\right] = E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}^{2}\right] + \left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}^{2} + 2E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}\right] \cdot \left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}$$

Error Decomposition (Cont.)

Taking the expectation of ϵ^2

$$E\left[\epsilon^{2}\right] = E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}^{2}\right] + \left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}^{2}$$

$$+2E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}\right] \cdot \left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}$$

$$= E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}^{2}\right] + \left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}^{2}$$

$$+2\left\{E\left[h(x,S)\right] - E\left[h(x,S)\right]\right\} \cdot \left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}$$

Error Decomposition (Cont.)

Taking the expectation of ϵ^2

$$E\left[\epsilon^{2}\right] = E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}^{2}\right] + \left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}^{2}$$

$$+2E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}\right] \cdot \left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}$$

$$= E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}^{2}\right] + \left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}^{2}$$

$$+2\left\{E\left[h(x,S)\right] - E\left[h(x,S)\right]\right\} \cdot \left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}$$

$$= E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}^{2}\right] + \left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}^{2}$$

The Bias-Variance Decomposition

The expected error is decomposed as

$$E\left[\epsilon^{2}\right] = \underbrace{E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}^{2}\right]}_{\text{variance}} + \underbrace{\left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}^{2}}_{\text{bias}^{2}}$$

The Bias-Variance Decomposition

The expected error is decomposed as

$$E\left[\epsilon^{2}\right] = \underbrace{E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}^{2}\right]}_{\text{variance}} + \underbrace{\left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}^{2}}_{\text{bias}^{2}}$$

▶ **bias**: how far the expected prediction E[h(x, S)] diverges from the optimal predictor $f_{\mathfrak{D}}(x)$

The Bias-Variance Decomposition

The expected error is decomposed as

$$E\left[\epsilon^{2}\right] = \underbrace{E\left[\left\{h(x,S) - E\left[h(x,S)\right]\right\}^{2}\right]}_{\text{variance}} + \underbrace{\left\{E\left[h(x,S)\right] - f_{\mathfrak{D}}(x)\right\}^{2}}_{\text{bias}^{2}}$$

- **bias**: how far the expected prediction E[h(x, S)] diverges from the optimal predictor $f_{\mathfrak{D}}(x)$
- ▶ **variance**: how a hypothesis learned from a specific S diverges from the average prediction E[h(x, S)]

Computing E[h(x, S)]

The key of computing E[h(x, S)] is to eliminate the randomness introduced by S

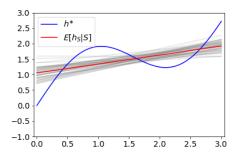
- 1: **for** $k = 1, \dots, K$ **do**
- Sample a traing set S_k with size m from the data generation model
- 3: Find the best hypothesis via $h(x, S_k) \in \operatorname{argmin}_{h'} L(h', S_k)$
- 4: end for
- 5: Output:

$$E[h(x,S)] \approx \frac{1}{K} \sum_{k=1}^{K} h(x,S_k)$$

The larger *K*, the better approximation

Example: Bias and Variance

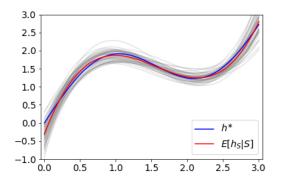
With K = 50, m = 100, and \mathcal{H}_1 , we can visualize the bias and variance of a linear regression example as following



High bias and low variance (Underfitting)

Example: Bias and Variance (Cont.)

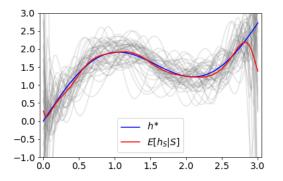
Same training set with \mathcal{H}_3



Both bias and variance are fine

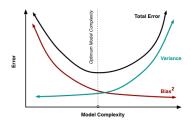
Example: Bias and Variance (Cont.)

Same training set with \mathcal{H}_{15}



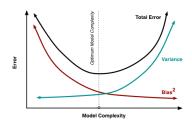
Low bias and high variance (Overfitting)

The Bias-Variance Tradeoff



- **bias**: how far the expected prediction E[h(x, S)] diverges from the optimal predictor $f_{\mathfrak{D}}(x)$
 - Error of this part is caused by the selection of a hypothesis space

The Bias-Variance Tradeoff



- **▶ bias**: how far the expected prediction E[h(x, S)] diverges from the optimal predictor $f_{\mathfrak{D}}(x)$
 - ► Error of this part is caused by *the selection of a hypothesis space*
- ▶ **variance**: how a hypothesis learned from a specific S diverges from the average prediction E[h(x, S)]
 - Error of this part is caused by using a particular data set S

The VC Dimension

Definition

Reference