# 10-701: Introduction to Machine Learning Lecture 21 – Learning Theory (Infinite Case)

#### **Front Matter**

- Announcements
  - Project check-ins due on 4/8 at 11:59 PM
  - Daniel is on leave and will be for an indeterminate amount of time, please direct all course requests/questions to Henry

#### **Key Question**

• Given a hypothesis with zero/low training error, what can we say about its true error?

#### Theorem 1: Finite, Realizable Case

• For a finite hypothesis set  $\mathcal{H}$  s.t.  $c^* \in \mathcal{H}$  and arbitrary distribution  $p^*$ , if the number of labelled training data points satisfies

$$M \ge \frac{1}{\epsilon} \left( \ln(|\mathcal{H}|) + \ln\left(\frac{1}{\delta}\right) \right)$$

then with probability at least  $1-\delta$ , all  $h\in\mathcal{H}$  with  $\widehat{R}(h)=0$  have  $R(h)\leq\epsilon$ 

• Making the bound tight (setting the two sides equal to each other) and solving for  $\epsilon$  gives...

# Statistical Learning Theory Corollary: Finite, Realizable Case

• For a finite hypothesis set  $\mathcal{H}$  s.t.  $c^* \in \mathcal{H}$  and arbitrary distribution  $p^*$ , given a training data set S s.t. |S| = M, all  $h \in \mathcal{H}$  with  $\hat{R}(h) = 0$  have

$$R(h) \le \frac{1}{M} \left( \ln(|\mathcal{H}|) + \ln\left(\frac{1}{\delta}\right) \right)$$

with probability at least  $1 - \delta$ .

# Statistical Learning Theory Corollary: Finite, Agnostic Case

• For a finite hypothesis set  $\mathcal H$  and arbitrary distribution  $p^*$ , given a training data set S s.t. |S|=M, all  $h\in\mathcal H$  have

$$R(h) \le \hat{R}(h) + \sqrt{\frac{1}{2M}} \left( \ln(|\mathcal{H}|) + \ln\left(\frac{2}{\delta}\right) \right)$$

with probability at least  $1 - \delta$ .

# What happens when $|\mathcal{H}| = \infty$ ?

• For a finite hypothesis set  $\mathcal H$  and arbitrary distribution  $p^*$ , given a training data set S s.t. |S|=M, all  $h\in\mathcal H$  have

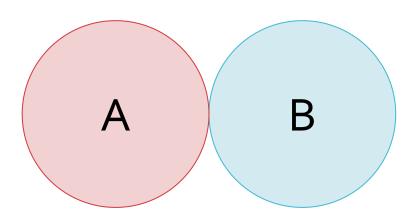
$$R(h) \le \hat{R}(h) + \sqrt{\frac{1}{2M}} \left( \ln(|\mathcal{H}|) + \ln\left(\frac{2}{\delta}\right) \right)$$

with probability at least  $1 - \delta$ .

$$P\{A \cup B\} \le P\{A\} + P\{B\}$$

$$P\{A \cup B\} = P\{A\} + P\{B\} - P\{A \cap B\}$$

### The Union Bound is Bad!

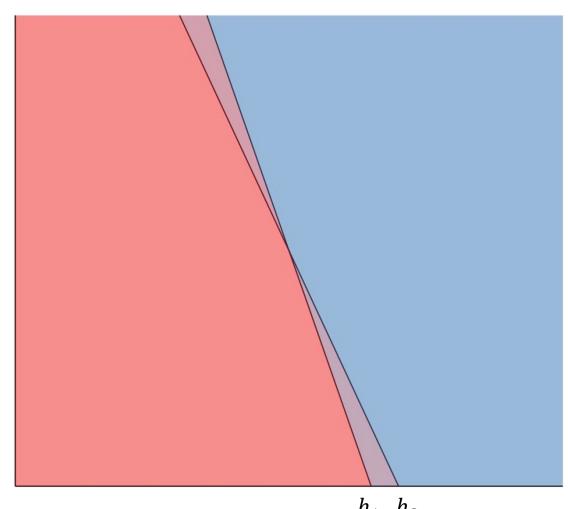


#### Intuition

If two hypotheses  $h_1, h_2 \in \mathcal{H}$  are very similar, then the events

- " $h_1$  is consistent with the first mtraining data points"
- " $h_2$  is consistent with the first mtraining data points"

will overlap a lot!



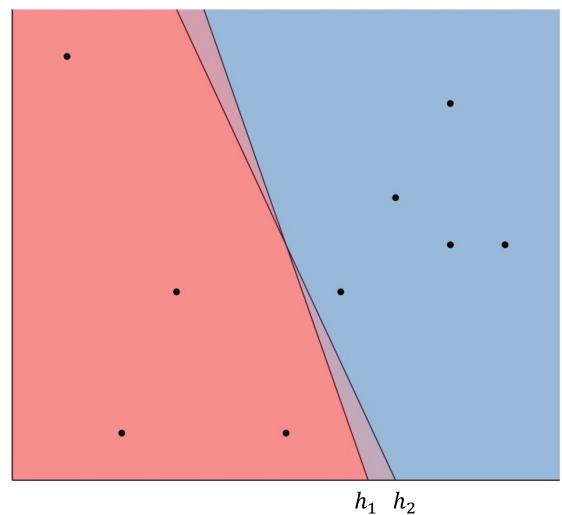
 $h_1$   $h_2$ 

#### Intuition

If two hypotheses  $h_1, h_2 \in \mathcal{H}$  are very similar, then the events

- " $h_1$  is consistent with the first mtraining data points"
- " $h_2$  is consistent with the first mtraining data points"

will overlap a lot!



#### Labellings

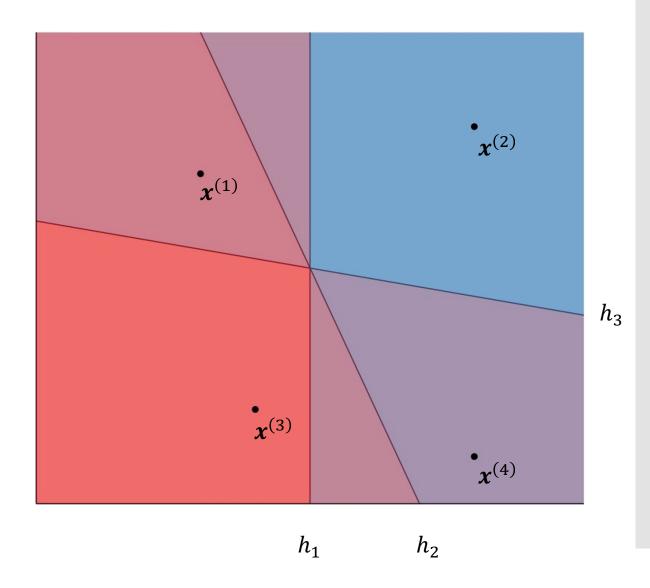
• Given some finite set of data points  $S = (x^{(1)}, ..., x^{(M)})$  and some hypothesis  $h \in \mathcal{H}$ , applying h to each point in S results in a <u>labelling</u>

• 
$$\left(h(x^{(1)}), \dots, h(x^{(M)})\right)$$
 is a vector of  $M$  +1's and -1's

- Insight: given  $S = (x^{(1)}, ..., x^{(M)})$ , each hypothesis in  $\mathcal{H}$  induces a labelling but not necessarily a unique labelling
  - The set of labellings induced by  ${\mathcal H}$  on S is

$$\mathcal{H}(S) = \left\{ \left( h(\boldsymbol{x}^{(1)}), \dots, h(\boldsymbol{x}^{(M)}) \right) \middle| h \in \mathcal{H} \right\}$$

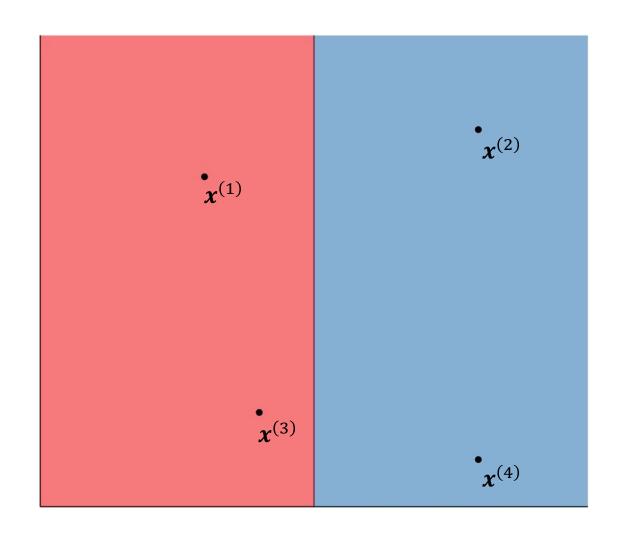
$$\mathcal{H} = \{h_1, h_2, h_3\}$$



$$\mathcal{H} = \{h_1, h_2, h_3\}$$

$$(h_1(x^{(1)}), h_1(x^{(2)}), h_1(x^{(3)}), h_1(x^{(4)}))$$

$$= (-1, +1, -1, +1)$$

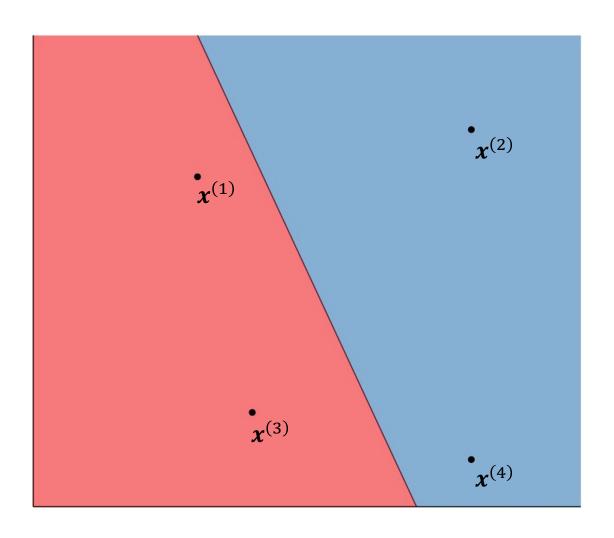


 $h_1$ 

$$\mathcal{H} = \{h_1, h_2, h_3\}$$

$$(h_2(x^{(1)}), h_2(x^{(2)}), h_2(x^{(3)}), h_2(x^{(4)}))$$

$$= (-1, +1, -1, +1)$$

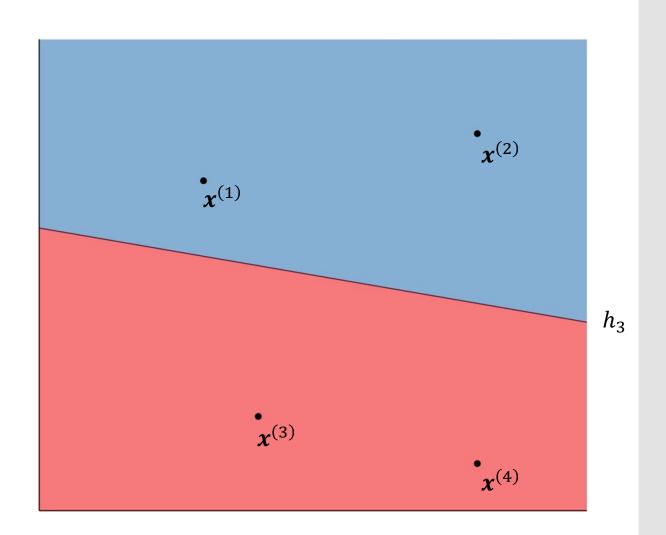


 $h_2$ 

$$\mathcal{H} = \{h_1, h_2, h_3\}$$

$$(h_3(x^{(1)}), h_3(x^{(2)}), h_3(x^{(3)}), h_3(x^{(4)}))$$

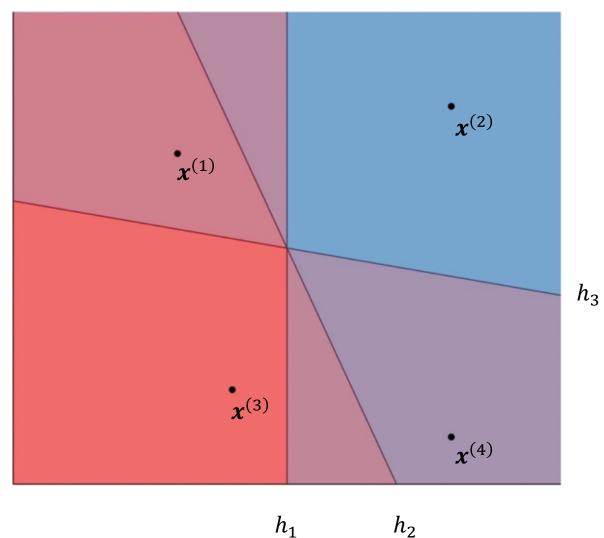
$$= (+1, +1, -1, -1)$$



$$\mathcal{H} = \{h_1, h_2, h_3\}$$

$$\mathcal{H}(S)$$
  
= {(+1, +1, -1, -1), (-1, +1, -1, +1)}

$$|\mathcal{H}(S)| = 2$$

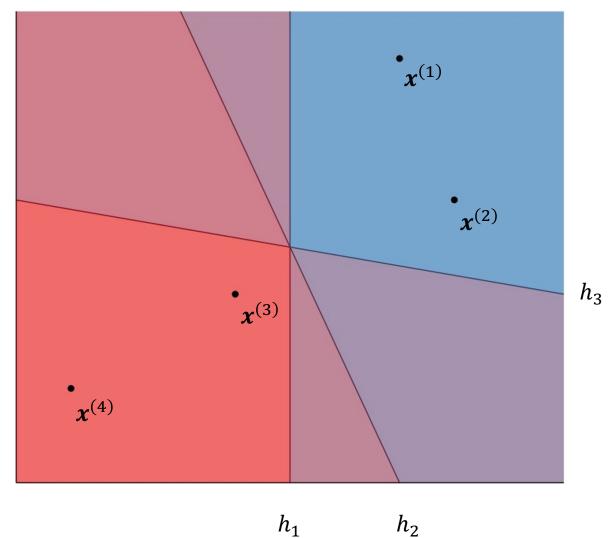


 $h_1$ 

$$\mathcal{H} = \{h_1, h_2, h_3\}$$

$$\mathcal{H}(S) = \{(+1, +1, -1, -1)\}$$

$$|\mathcal{H}(S)| = 1$$



### Growth Function

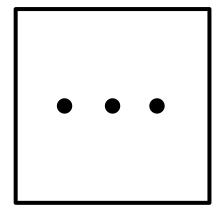
• The <u>growth function</u> of  $\mathcal H$  is the maximum number of distinct labellings  $\mathcal H$  can induce on *any* set of M data points:

$$g_{\mathcal{H}}(M) = \max_{S:|S|=M} |\mathcal{H}(S)|$$

- $g_{\mathcal{H}}(M) \leq 2^M \ \forall \ \mathcal{H} \ \text{and} \ M$
- $\mathcal{H}$  shatters S if  $|\mathcal{H}(S)| = 2^M$
- If  $\exists S$  s.t. |S| = M and  $\mathcal{H}$  shatters S, then  $g_{\mathcal{H}}(M) = 2^M$

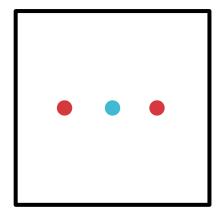
•  $\mathbf{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional linear separators

• What is  $g_{\mathcal{H}}(3)$ ?

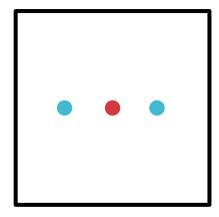


•  $\mathbf{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional linear separators

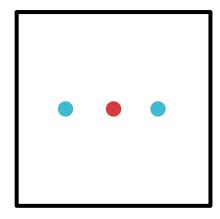
• What is  $g_{\mathcal{H}}(3)$ ?



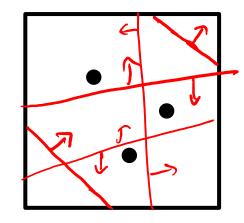
•  $\mathbf{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional linear separators



•  $\mathbf{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional linear separators



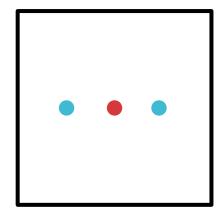
$$|\mathcal{H}(S_1)| = 6$$



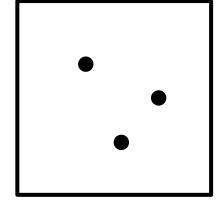
$$|\mathcal{H}(S_2)| = 8$$

•  $\pmb{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H}=$  all 2-dimensional linear separators

• 
$$g_{\mathcal{H}}(3) = 8 = 2^3$$



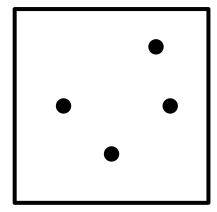
$$|\mathcal{H}(S_1)| = 6$$



$$|\mathcal{H}(S_2)| = 8$$

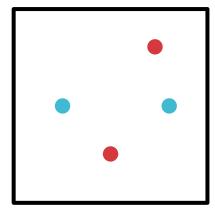
•  $\mathbf{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional linear separators

• What is  $g_{\mathcal{H}}(4)$ ?

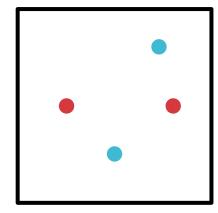


•  $\mathbf{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional linear separators

• What is  $g_{\mathcal{H}}(4)$ ?

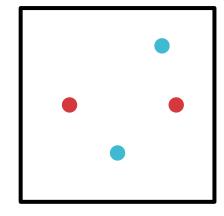


•  $\mathbf{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional linear separators

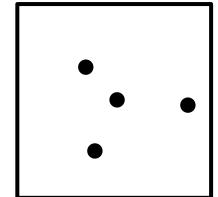


$$|\mathcal{H}(S_1)| = 14$$

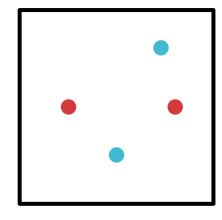
•  $\mathbf{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional linear separators



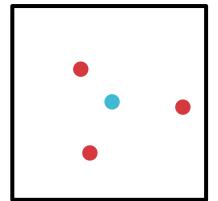
$$|\mathcal{H}(S_1)| = 14$$



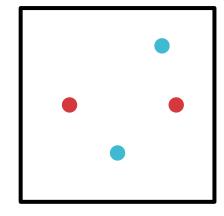
•  $\mathbf{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional linear separators



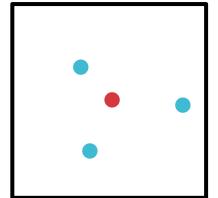
$$|\mathcal{H}(S_1)| = 14$$



•  $\mathbf{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional linear separators

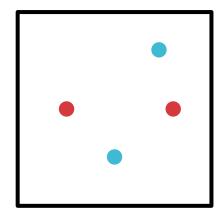


$$|\mathcal{H}(S_1)| = 14$$

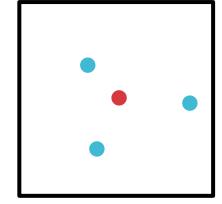


•  $\mathbf{x}^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional linear separators

• 
$$g_{\mathcal{H}}(4) = 14 < 2^4$$



$$|\mathcal{H}(S_1)| = 14$$



$$|\mathcal{H}(S_2)| = 14$$

#### Theorem 3: Vapnik-Chervonenkis (VC)-Bound

• Infinite, realizable case: for any hypothesis set  ${\cal H}$  and distribution  $p^*$ , if the number of labelled training data points satisfies

$$M \ge \frac{2}{\epsilon} \left( \log_2(2g_{\mathcal{H}}(2M)) + \log_2\left(\frac{1}{\delta}\right) \right)$$

then with probability at least  $1 - \delta$ , all  $h \in \mathcal{H}$  with  $R(h) \ge \epsilon$  have  $\hat{R}(h) > 0$ 

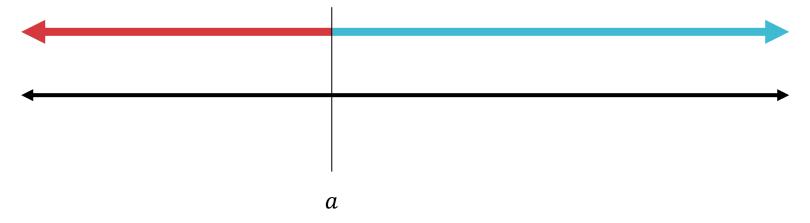
• *M* appears on both sides of the inequality...

### Theorem 3: Vapnik-Chervonenkis (VC)-Dimension

- $d_{VC}(\mathcal{H})=$  the largest value of M s.t.  $g_{\mathcal{H}}(M)=2^{M}$ , i.e., the greatest number of data points that can be shattered by  $\mathcal{H}$ 
  - If  ${\mathcal H}$  can shatter arbitrarily large finite sets, then  $d_{VC}({\mathcal H})=\infty$
  - $g_{\mathcal{H}}(M) = O(M^{d_{VC}(\mathcal{H})})$  (Sauer-Shelah lemma)

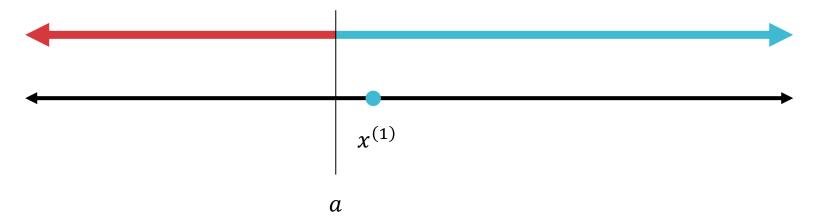
- To prove that  $d_{VC}(\mathcal{H}) = C$ , you need to show
  - 1.  $\exists$  some set of C data points that  $\mathcal{H}$  can shatter and
  - 2.  $\not\exists$  a set of C+1 data points that  $\mathcal{H}$  can shatter

•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive rays, i.e., all hypotheses of the form  $h(x; a) = \operatorname{sign}(x - a)$ 



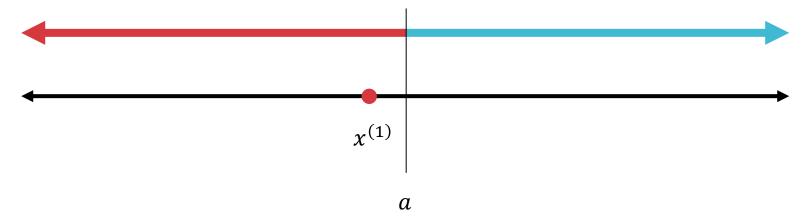
• What is  $d_{VC}(\mathcal{H})$ ?

•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive rays, i.e., all hypotheses of the form  $h(x; a) = \operatorname{sign}(x - a)$ 



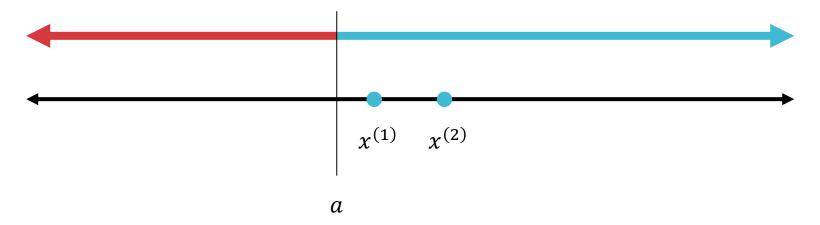
• What is  $d_{VC}(\mathcal{H})$ ?

•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive rays, i.e., all hypotheses of the form  $h(x; a) = \operatorname{sign}(x - a)$ 



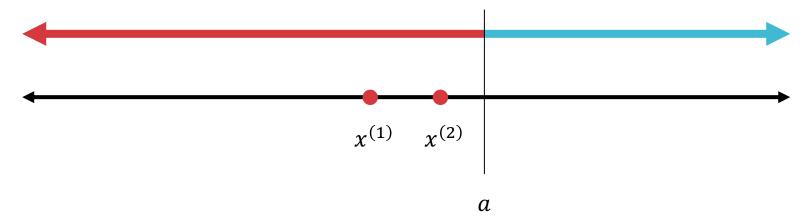
• What is  $d_{VC}(\mathcal{H})$ ?

•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive rays, i.e., all hypotheses of the form  $h(x; a) = \operatorname{sign}(x - a)$ 



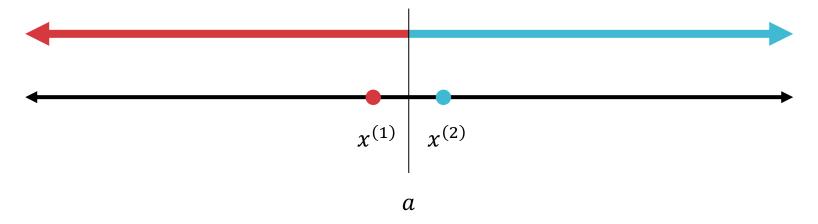
• What is  $d_{VC}(\mathcal{H})$ ?

•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive rays, i.e., all hypotheses of the form  $h(x; a) = \operatorname{sign}(x - a)$ 

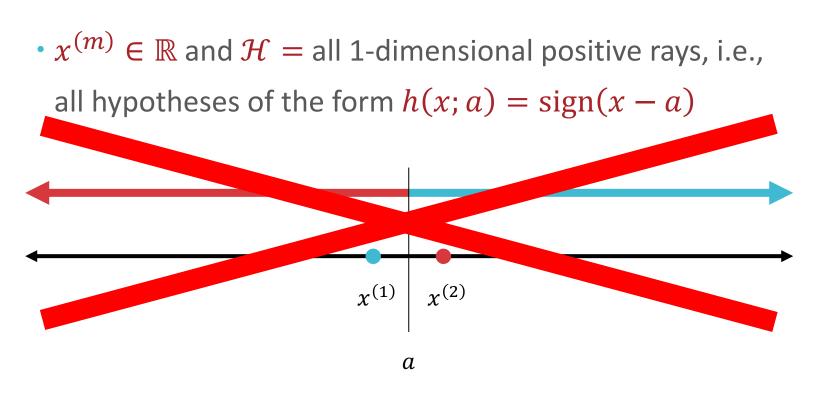


• What is  $d_{VC}(\mathcal{H})$ ?

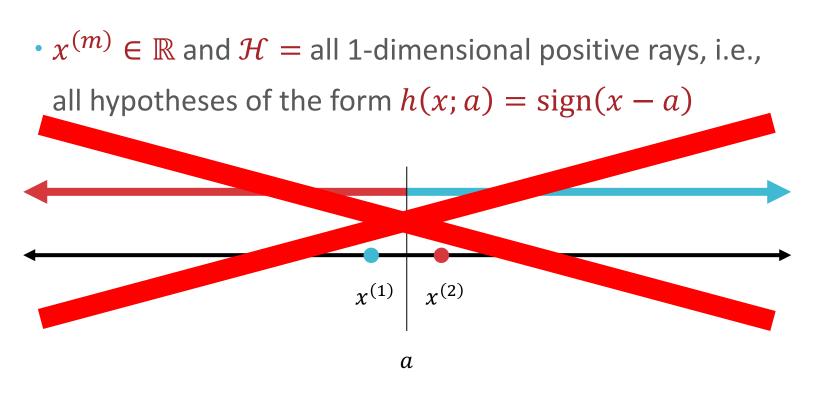
•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive rays, i.e., all hypotheses of the form  $h(x; a) = \operatorname{sign}(x - a)$ 



• What is  $d_{VC}(\mathcal{H})$ ?

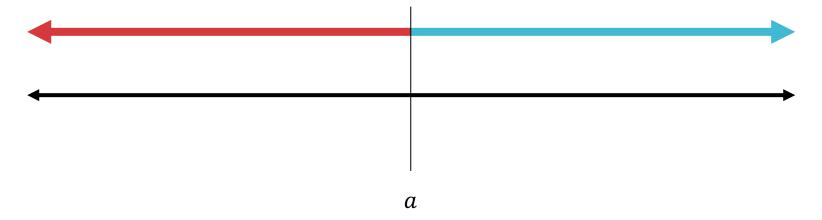


• What is  $d_{VC}(\mathcal{H})$ ?



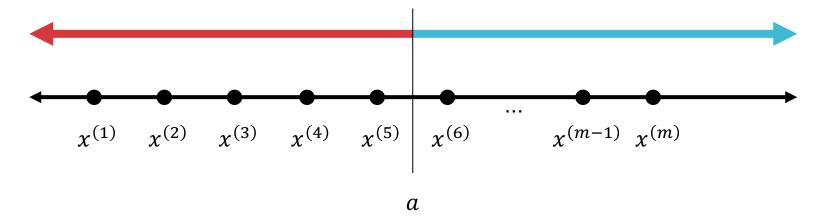
•  $d_{VC}(\mathcal{H}) = 1$ 

•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive rays, i.e., all hypotheses of the form  $h(x; a) = \operatorname{sign}(x - a)$ 



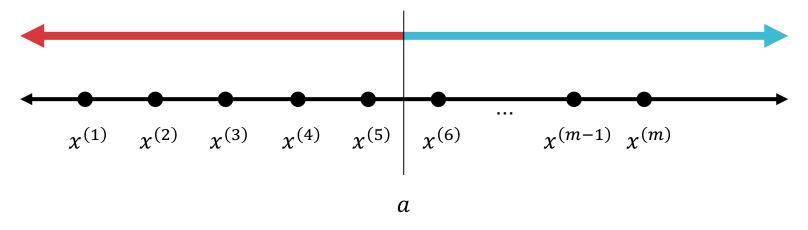
• What is  $g_{\mathcal{H}}(m)$ ?

•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive rays, i.e., all hypotheses of the form  $h(x; a) = \operatorname{sign}(x - a)$ 



• What is  $g_{\mathcal{H}}(m)$ ?

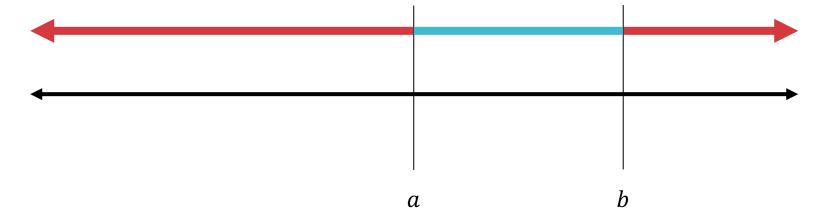
•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive rays, i.e., all hypotheses of the form  $h(x; a) = \operatorname{sign}(x - a)$ 



•  $g_{\mathcal{H}}(m) = m + 1 = O(m^1)$ 

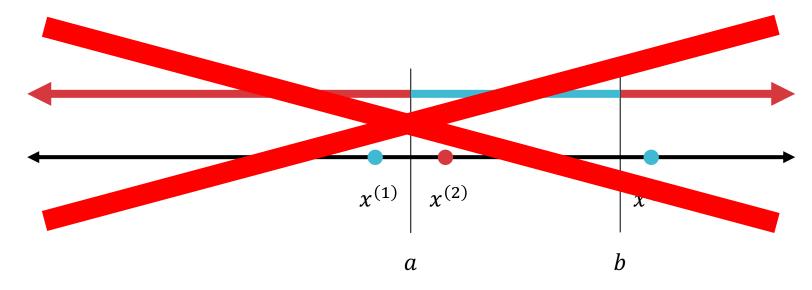
•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive intervals

## VC-Dimension: Example



• What are  $d_{VC}(\mathcal{H})$  and  $g_{\mathcal{H}}(m)$ ?

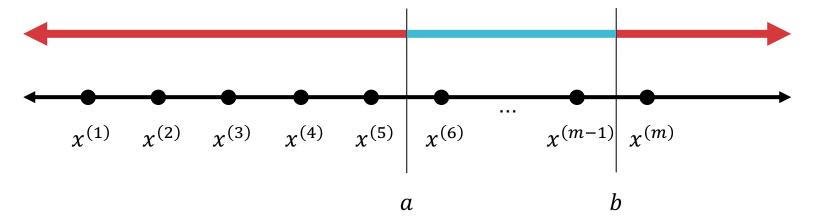
•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive intervals



• What are  $d_{VC}(\mathcal{H})$  and  $g_{\mathcal{H}}(m)$ ?

•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive intervals

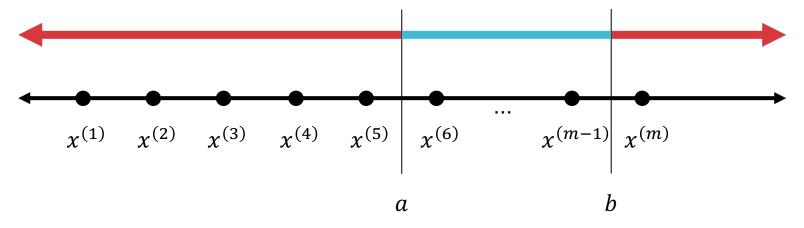
## VC-Dimension: Example



• What are  $d_{VC}(\mathcal{H})$  and  $g_{\mathcal{H}}(m)$ ?

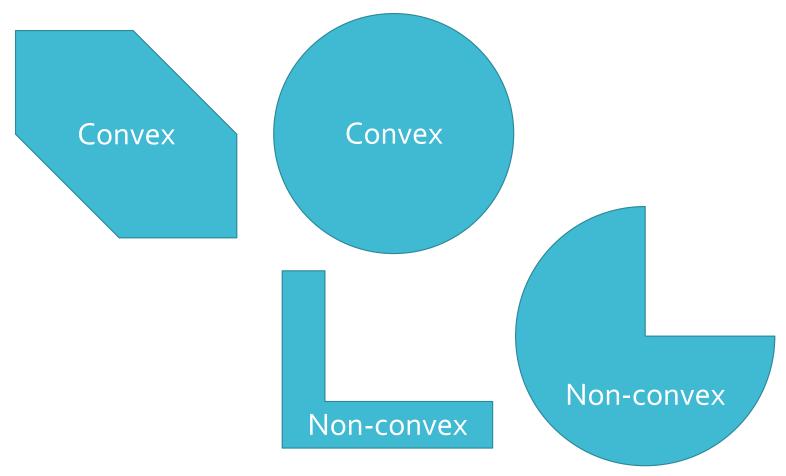
•  $x^{(m)} \in \mathbb{R}$  and  $\mathcal{H} =$  all 1-dimensional positive intervals

## VC-Dimension: Example



•  $d_{VC}(\mathcal{H})=2$  and  $g_{\mathcal{H}}(m)={m+1 \choose 2}+1=O(m^2)$ 

•  $x^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional positive convex sets

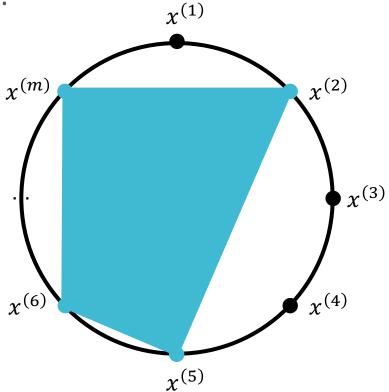


•  $x^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional positive convex sets

• What are  $d_{VC}(\mathcal{H})$  and  $g_{\mathcal{H}}(M)$ ?

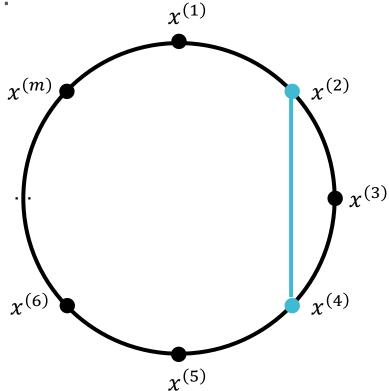
•  $x^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional positive convex sets

• What are  $d_{VC}(\mathcal{H})$  and  $g_{\mathcal{H}}(M)$ ?



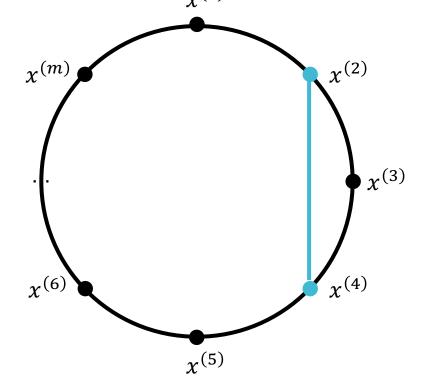
•  $x^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional positive convex sets

• What are  $d_{VC}(\mathcal{H})$  and  $g_{\mathcal{H}}(M)$ ?



•  $x^{(m)} \in \mathbb{R}^2$  and  $\mathcal{H} =$  all 2-dimensional positive convex sets

•  $d_{VC}(\mathcal{H}) = \infty$  and  $g_{\mathcal{H}}(M) = 2^M = O(M^{\infty})_{\chi^{(1)}}$ 



#### Theorem 3: Vapnik-Chervonenkis (VC)-Bound

• Infinite, realizable case: for any hypothesis set  ${\cal H}$  and distribution  $p^*$ , if the number of labelled training data points satisfies

$$M = O\left(\frac{1}{\epsilon}\left(d_{VC}(\mathcal{H})\log\left(\frac{1}{\epsilon}\right) + \log\left(\frac{1}{\delta}\right)\right)\right)$$

then with probability at least  $1-\delta$ , all  $h\in\mathcal{H}$  with

$$\widehat{R}(h) = 0$$
 have  $R(h) \le \epsilon$ 

#### Statistical Learning Theory Corollary

• Infinite, realizable case: for any hypothesis set  $\mathcal{H}$  and distribution  $p^*$ , given a training data set S s.t. |S| = M, all  $h \in \mathcal{H}$  with  $\hat{R}(h) = 0$  have

$$R(h) \le O\left(\frac{1}{M}\left(d_{VC}(\mathcal{H})\log\left(\frac{M}{d_{VC}(\mathcal{H})}\right) + \log\left(\frac{1}{\delta}\right)\right)\right)$$

with probability at least  $1 - \delta$ .

#### Theorem 4: Vapnik-Chervonenkis (VC)-Bound

• Infinite, agnostic case: for any hypothesis set  ${\cal H}$  and distribution  $p^*$ , if the number of labelled training data points satisfies

$$M = O\left(\frac{1}{\epsilon^2} \left( d_{VC}(\mathcal{H}) + \log\left(\frac{1}{\delta}\right) \right) \right)$$

then with probability at least  $1 - \delta$ , all  $h \in \mathcal{H}$  have

$$|R(h) - \hat{R}(h)| \le \epsilon$$

#### Statistical Learning Theory Corollary

• Infinite, agnostic case: for any hypothesis set  $\mathcal H$  and distribution  $p^*$ , given a training data set S s.t. |S|=M, all  $h\in\mathcal H$  have

$$R(h) \le \hat{R}(h) + O\left(\sqrt{\frac{1}{M}}\left(d_{VC}(\mathcal{H}) + \log\left(\frac{1}{\delta}\right)\right)\right)$$

with probability at least  $1 - \delta$ .

#### Approximation Generalization Tradeoff

How well does *h* generalize?

$$R(h) \le \hat{R}(h) + O\left(\sqrt{\frac{1}{M}\left(d_{VC}(\mathcal{H}) + \log\left(\frac{1}{\delta}\right)\right)}\right)$$

How well does *h* approximate *c*\*?

#### Approximation Generalization Tradeoff

$$Increases\ as$$
 
$$d_{VC}(\mathcal{H})\ increases$$
 
$$R(h) \leq \widehat{R}(h) + O\left(\sqrt{\frac{1}{M}}\Big(d_{VC}(\mathcal{H}) + \log\Big(\frac{1}{\delta}\Big)\Big)\right)$$
 Decreases as 
$$d_{VC}(\mathcal{H})\ increases$$

#### Key Takeaways

- For infinite hypothesis sets, use the VC-dimension (or the growth function) as a measure of complexity
  - Computing  $d_{VC}(\mathcal{H})$  and  $g_{\mathcal{H}}(M)$
  - Connection between VC-dimension and the growth function (Sauer-Shelah lemma)
  - Sample complexity and statistical learning theory style bounds using  $d_{VC}(\mathcal{H})$

• Assume a regression task with squared error and let  $h_S \in \mathcal{H} =$  the hypothesis trained on training data S

• 
$$err_p(h_S) = \mathbb{E}_{x \sim p^*}[(h_S(x) - c^*(x))^2]$$
 $E_S[err_D(h_S)] = E_S[E_{x \sim p^*}[(h_S(x) - c^*(x))^2]]$ 
 $f = E_{x \sim p^*}[E_S[h_S(x)^2 - 2h_S(x)c^*(x) + c^*(x)^2]]$ 
 $f = E_{x \sim p^*}[E_S[h_S(x)^2] - 2h_S(x)c^*(x) + c^*(x)^2]$ 

where  $h(x) = average hypothesis = E[h_S(x)]_{60}$ 

 Assume a regression task with squared error and let  $h_S \in \mathcal{H}$  = the hypothesis trained on training data S

• 
$$err_{D}(h_{S}) = \mathbb{E}_{x \sim D} [(h_{S}(x) - c^{*}(x))^{2}]$$

•  $E_{x \sim p^{*}} [E_{S} [h_{S}(x)^{2}] - Zh(x) c^{*}(x) + C^{*}(x)^{2}]$ 

=  $E_{x \sim p^{*}} [E_{S} [h_{S}(x)^{2}] - h(x)^{2} + h(x)^{2}$ 

-  $Zh(x) c^{*}(x) + C^{*}(x)^{2}]$ 

=  $E_{x \sim p^{*}} [E_{S} [h_{S}(x)^{2} - h(x)^{2}]$ 

+  $(h_{S}(x)^{2}) - h(x)^{2}$ 

+  $(h_{S}(x)^{2}) - h(x)^{2}$ 

=  $E_{x \sim p^{*}} [E_{S} [h_{S}(x)^{2} - h(x)^{2}]$ 

=  $E_{x \sim p^{*}} [Variance of h_{S}(x) + b_{RS} of R]^{61}$ 

How much does *h* change if the training data set changes?

$$\mathbb{E}_{S}[err_{D}(h_{S})] = \mathbb{E}_{\boldsymbol{x} \sim D} \left[ \mathbb{E}_{S} \left[ h_{S}(\boldsymbol{x})^{2} - \overline{h}(\boldsymbol{x})^{2} \right] + \left( \overline{h}(\boldsymbol{x}) - c^{*}(\boldsymbol{x}) \right)^{2} \right]$$

How well on average does h approximate  $c^*$ ?

How well could *h* approximate anything?

$$\mathbb{E}_{S}[err_{D}(h_{S})] = \mathbb{E}_{\boldsymbol{x} \sim D} \left[ \mathbb{E}_{S} \left[ h_{S}(\boldsymbol{x})^{2} - \overline{h}(\boldsymbol{x})^{2} \right] + \left( \overline{h}(\boldsymbol{x}) - c^{*}(\boldsymbol{x}) \right)^{2} \right]$$

How well on average does h approximate  $c^*$ ?

becomes more complex  $\mathbb{E}_{S}[err_{D}(h_{S})] = \mathbb{E}_{x \sim D} \left[ \mathbb{E}_{S} \left[ h_{S}(x)^{2} - \bar{h}(x)^{2} \right] + \left( \bar{h}(x) - c^{*}(x) \right)^{2} \right]$ 

Increases as  ${\cal H}$ 

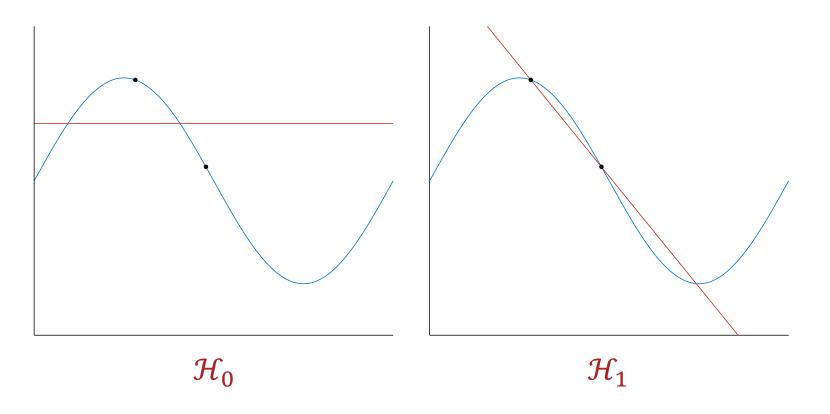
Decreases as  $\mathcal{H}$  becomes more complex

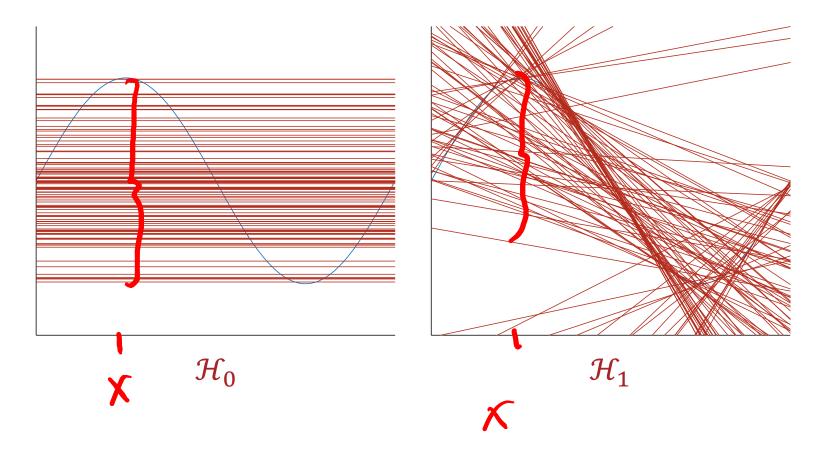
•  $x^{(i)} \in \mathbb{R}$  and  $D = \text{Uniform}(0, 2\pi)$ 

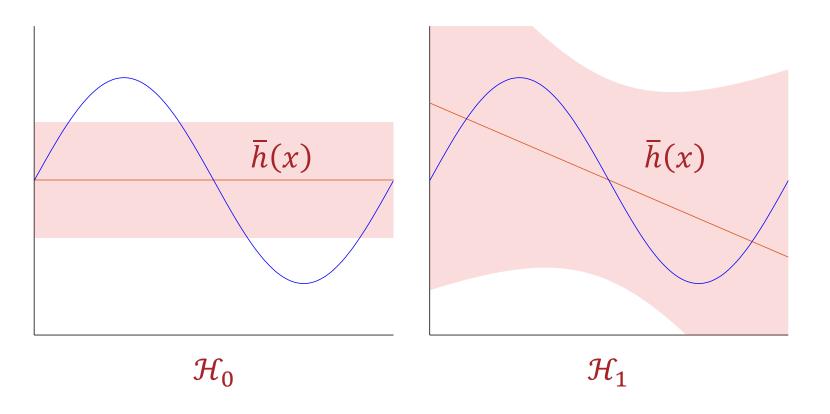
•  $c^* = \sin(\cdot)$ , i.e.,  $y = \sin(x)$ 

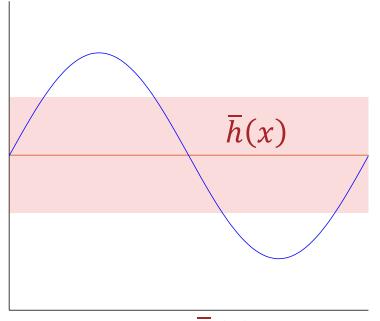
•  $N = 2 \to \mathcal{D} = \{ (x^{(1)}, \sin(x^{(1)})), (x^{(2)}, \sin(x^{(2)})) \}$ 

•  $\mathcal{H}_0 = \{h : h(x) = b\}$  and  $\mathcal{H}_1 = \{h : h(x) = ax + b\}$ 

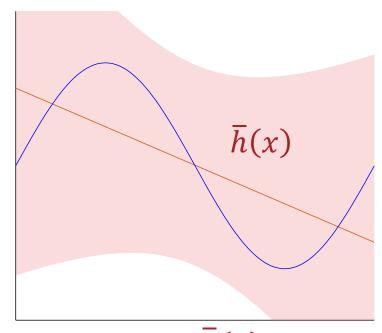






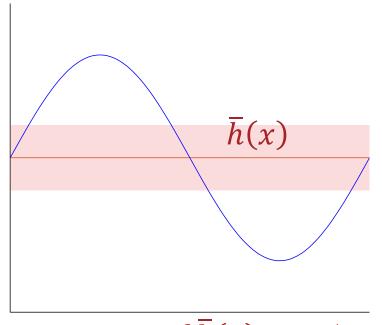


Bias of  $\bar{h}(x) \approx 0.50$ Variance of  $h_S(x) \approx 0.25$  $\mathbb{E}_S[err_D(h_S)] \approx 0.75$ 

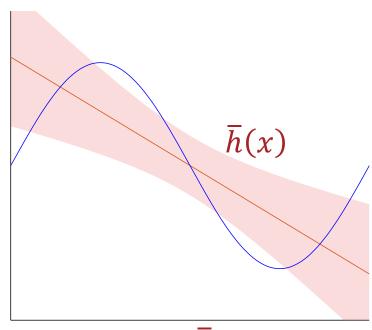


Bias of  $\bar{h}(x) \approx 0.21$ Variance of  $h_S(x) \approx 1.74$  $\mathbb{E}_S[err_D(h_S)] \approx 1.95$ 

#### Bias-Variance Tradeoff: Example (N = 5)



Bias of  $\bar{h}(x) \approx 0.50$ Variance of  $h_S(x) \approx 0.10$  $\mathbb{E}_S[err_D(h_S)] \approx 0.60$ 



Bias of  $\bar{h}(x) \approx 0.21$ Variance of  $h_S(x) \approx 0.21$  $\mathbb{E}_S[err_D(h_S)] \approx 0.42$