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

Henry Chai

4/3/24

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 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 ϵ gives...

Statistical Learning **Theory** Corollary: Finite, Realizable Case • For a finite hypothesis set 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 $\widehat{R}(h) = 0$ have

> $R(h) \leq$ 1 \overline{M} $ln(|\mathcal{H}|) + ln$ 1 δ

Statistical Learning Theory Corollary: Finite, Agnostic Case • For a finite hypothesis set H and arbitrary distribution p^* , given a training data set S s.t. $|S| = M$, all $h \in \mathcal{H}$ have

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

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

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

The Union Bound is Bad!

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

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

Intuition

- If two hypotheses $h_1, h_2 \in \mathcal{H}$ are very similar, then the events
	- \cdot " h_1 is consistent with the first m training data points"
	- $\bm{\cdot}$ " h_2 is consistent with the first m training data points"
	- will overlap a lot!

Intuition

- If two hypotheses $h_1, h_2 \in \mathcal{H}$ are very similar, then the events
	- \cdot " h_1 is consistent with the first m training data points"
	- $\bm{\cdot}$ " h_2 is consistent with the first m training data points"
	- will overlap a lot!

 h_1 h_2

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 **labelling**

 \cdot $\big(h\big(\textit{\textbf{x}}^{(1)}\big),...,h\big(\textit{\textbf{x}}^{(M)}\big)\big)$ 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

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

Example: Labellings

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

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

 $h_1\bigl(\pmb{x}^{(1)}\bigr)$, $h_1\bigl(\pmb{x}^{(2)}\bigr)$, $h_1\bigl(\pmb{x}^{(3)}\bigr)$, $h_1\bigl(\pmb{x}^{(4)}\bigr)$ $= (-1, +1, -1, +1)$

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

 $\left(h_2(x^{(1)}), h_2(x^{(2)}), h_2(x^{(3)}), h_2(x^{(4)})\right)$ $= (-1, +1, -1, +1)$

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

 $\left(h_3(x^{(1)}), h_3(x^{(2)}), h_3(x^{(3)}), h_3(x^{(4)})\right)$ $= (+1, +1, -1, -1)$

Example: Labellings

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

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

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

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

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

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

 h_1 h_{2}

Growth Function

 The **growth function** of ℋ is the maximum number of distinct labellings H can induce on **any** set of M data points: $g_{\mathcal{H}}(M) = \max_{\mathcal{S} \cup \mathcal{S} \cup \mathcal{S}}$ $S : |S| = M$ $\mathcal{H}(\mathcal{S}%)=\left\{ \mathcal{M}_{\alpha}^{\dag}\right\} ,$

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

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

• What is $g_{\mathcal{H}}(3)$?

Function: Example

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

 $Growth$ What is $g_{\mathcal{H}}(3)$?

Function: Example

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

 $Growth$ What is $g_{\mathcal{H}}(3)$?

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

• What is $g_{\mathcal{H}}(3)$?

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

$$
\cdot g_{\mathcal{H}}(3)=8=2^3
$$

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

• What is $g_{\mathcal{H}}(4)$?

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

• What is $g_{\mathcal{H}}(4)$?

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

• What is $g_{\mathcal{H}}(4)$?

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

• What is $g_{\mathcal{H}}(4)$?

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

• What is $g_{\mathcal{H}}(4)$?

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

• What is $g_{\mathcal{H}}(4)$?

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

$$
\cdot g_{\mathcal{H}}(4)=14<2^4
$$

 $|\mathcal{H}(S_1)| = 14$ $|\mathcal{H}(S_2)| = 14$

Theorem 3: Vapnik-Chervonenkis (VC)-Bound

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

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

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

 \cdot *M* appears on both sides of the inequality...

Theorem 3: Vapnik-**Chervonenkis** (VC)-Dimension $\cdot d_{VC}(\mathcal{H})$ = 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 H \cdot 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 H can shatter and
	- 2. \vec{A} a set of $C + 1$ data points that H can shatter

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

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

Henry Chai - 4/3/24

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

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

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

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

 $\cdot x^{(m)} \in \mathbb{R}$ and $\mathcal{H} =$ all 1-dimensional positive rays, i.e., all hypotheses of the form $h(x; a) = sign(x - a)$ $x^{(1)} | x^{(2)}$ \boldsymbol{a}

 $\cdot x^{(m)} \in \mathbb{R}$ and $\mathcal{H} =$ all 1-dimensional positive rays, i.e., all hypotheses of the form $h(x; a) = sign(x - a)$ $\cdot d_{VC}(\mathcal{H}) = 1$ $x^{(1)} | x^{(2)}$ \boldsymbol{a}

Henry Chai - 4/3/24

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

• What is $g_{\mathcal{H}}(m)$?

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

• What is $g_{\mathcal{H}}(m)$?

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

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

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

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

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

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

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

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

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

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

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

- $\cdot x^{(m)} \in \mathbb{R}^2$ and $\mathcal{H} =$ all 2-dimensional positive convex sets
- What are $d_{VC}(\mathcal{H})$ and $g_{\mathcal{H}}(M)$?

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

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

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

Theorem 3: Vapnik-Chervonenkis (VC)-Bound

 \cdot Infinite, realizable case: for any hypothesis set $\mathcal H$ 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 $R(h) \leq \epsilon$

Statistical Learning **Theory Corollary**

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

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

Theorem 4: Vapnik-Chervonenkis (VC)-Bound

• Infinite, agnostic case: for any hypothesis set 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 $|R(h) - \hat{R}(h)| \leq \epsilon$

Statistical Learning Theory Corollary

 \cdot 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

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

Approximation **Generalization Tradeoff**

How well does *generalize?* $R(h) \leq \widehat{R}(h) + 0$ 1 $\frac{1}{M}\left(d_{VC}(\mathcal{H}) + \log \right)$ 1 δ How well does h

approximate c^* ?

Approximation Generalization **Tradeoff**

Agnostic cases as for any hypothesis cases as $d_{VC}(\mathcal{H})$ increases $R(h) \leq \widehat{R}(h) + 0$ 1 $\frac{1}{M}\left(d_{VC}(\mathcal{H}) + \log \right)$ 1 δ

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 $d_{VC}(\mathcal{H})$

Bias-Variance **Tradeoff**

$$
h_S \in \mathcal{H} = \text{the hypothesis trained on training data } S
$$
\n
$$
\cdot \operatorname{err}_D(h_S) = \mathbb{E}_{x \sim D} \left[\left(h_S(x) - c^*(x) \right)^2 \right]
$$
\n
$$
\cdot \mathbb{E}_S[\operatorname{err}_D(h_S)] = \mathbb{E}_S \left[\mathbb{E}_{x \sim D} \left[\left(h_S(x) - c^*(x) \right)^2 \right] \right]
$$
\n
$$
= \mathbb{E}_{x \sim D} \left[\mathbb{E}_S \left[\left(h_S(x) - c^*(x) \right)^2 \right] \right]
$$
\n
$$
= \mathbb{E}_{x \sim D} \left[\mathbb{E}_S[h_S(x)^2 - 2h_S(x)c^*(x) + c^*(x)^2] \right]
$$
\n
$$
= \mathbb{E}_{x \sim D} \left[\mathbb{E}_S[h_S(x)^2] - 2\overline{h}(x)c^*(x) + c^*(x)^2 \right]
$$
\n
$$
\cdot \text{where } \overline{h}(\vec{x}) = \mathbb{E}_S[h_S(x)] \approx \frac{1}{k} \sum_{i=1}^k h_{S_i}(x)
$$

Assume a regression task with squared error and let

Bias-Variance Tradeoff¹

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

•
$$
err_D(h_S) = \mathbb{E}_{x \sim D} \left[\left(h_S(x) - c^*(x) \right)^2 \right]
$$

$$
\begin{aligned}\n\mathbf{E}_{\mathcal{S}}[err_D(h_{\mathcal{S}})] &= \mathbb{E}_{\mathbf{x} \sim D}[\mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\mathbf{x})^2] - 2\bar{h}(\mathbf{x})c^*(\mathbf{x}) + c^*(\mathbf{x})^2] \\
&= \mathbb{E}_{\mathbf{x} \sim D}[\mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\mathbf{x})^2] - \bar{h}(\mathbf{x})^2 \\
&\quad + \bar{h}(\mathbf{x})^2 - 2\bar{h}(\mathbf{x})c^*(\mathbf{x}) + c^*(\mathbf{x})^2] \\
&= \mathbb{E}_{\mathbf{x} \sim D}\left[\mathbb{E}_{\mathcal{S}}[h_{\mathcal{S}}(\mathbf{x})^2 - \bar{h}(\mathbf{x})^2] + (\bar{h}(\mathbf{x}) - c^*(\mathbf{x}))^2\right] \\
&= \mathbb{E}_{\mathbf{x} \sim D}[\text{Variance of } h_{\mathcal{S}}(\mathbf{x}) + \text{Bias of } \bar{h}(\mathbf{x})]\n\end{aligned}
$$

Bias-Variance Tradeoff

How much does *h*
\nchange if the training
\ndata set changes?
\n
$$
\mathbb{E}_{S}[err_{D}(h_{S})] = \mathbb{E}_{x \sim D} \left[\mathbb{E}_{S}[h_{S}(x)^{2} - \bar{h}(x)^{2}] + (\bar{h}(x) - c^{*}(x))^{2} \right]
$$
\n
$$
\begin{array}{c}\n\text{How well on} \\
\text{average does } h\n\end{array}
$$

approximate c^* ?

Bias-Variance Tradeoff

How well could *h*
approximate
anything?

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

How well on
average does *h*

Henry Chai - 4/3/24

approximate c^* ?

Bias-Variance Tradeoff

Increasing as
$$
\mathcal{H}
$$

\nbecomes more complex

\n
$$
\mathbb{E}_{S}[err_{D}(h_{S})] = \mathbb{E}_{x \sim D} \left[\mathbb{E}_{S}[h_{S}(x)^{2} - \bar{h}(x)^{2}] + \left(\bar{h}(x) - c^{*}(x) \right)^{2} \right]
$$
\nDeccreases as \mathcal{H}

\nbecomes more

complex

Bias-Variance Tradeoff: Example

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

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

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

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

Bias-Variance Tradeoff: Example

Bias-Variance Tradeoff: Example

 \mathcal{H}_0

 \mathcal{H}_1

Bias-Variance Tradeoff: Example

Bias-Variance Tradeoff: Example

Variance of $h_S(x) \approx 0.25$

Bias of $\bar{h}(x) \approx 0.50$ Bias of $\bar{h}(x) \approx 0.21$ Variance of $h_S(x) \approx 1.74$ $\mathbb{E}_{S}[err_{D}(h_{S})] \approx 0.75$ $\mathbb{E}_{S}[err_{D}(h_{S})] \approx 1.95$

Tradeoff: Example $(N = 5)$

Variance of $h_S(x) \approx 0.10$

Bias of $\bar{h}(x) \approx 0.50$ Bias of $\bar{h}(x) \approx 0.21$ Variance of $h_S(x) \approx 0.21$ $\mathbb{E}_{S}[err_{D}(h_{S})] \approx 0.60$ $\mathbb{E}_{S}[err_{D}(h_{S})] \approx 0.42$