DS-GA 3001.007 Introduction to Machine Learning

Lecture 3

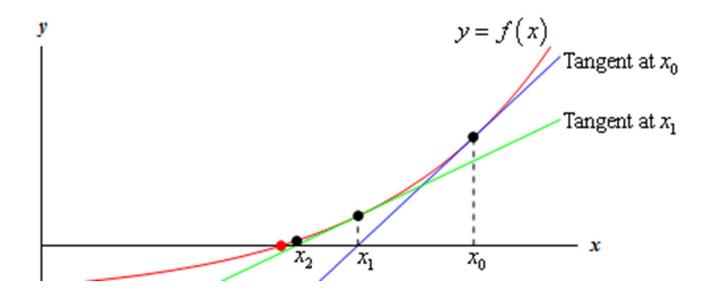
Agenda

- Review
 - Margin
- Lesson
 - ► Empirical Risk Minimization
- Demo
 - Pocket Algorithm

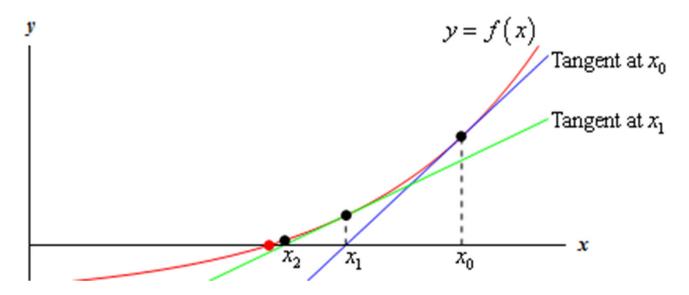


Reminders

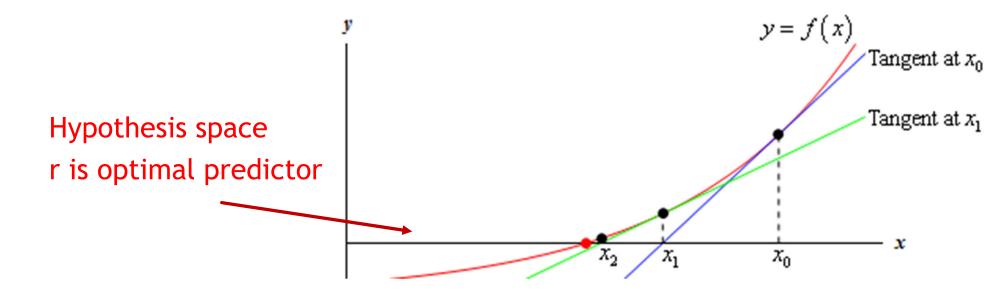
- Schedule
 - ▶ Office Hours
- Assignments
 - ► Homework Submission
- Materials
 - ▶ Links
- Surveys
 - ▶ Please complete Survey 2



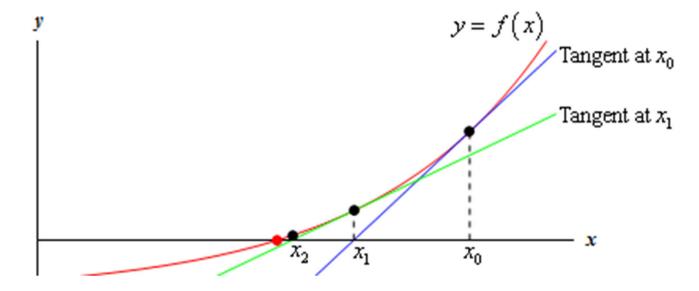
- ► Loss Function l(x)
 - ightharpoonup Set f(x) = l'(x)
 - Find r such that f(r) = 0



- ► Loss Function l(x)
 - ightharpoonup Set f(x) = l'(x)
 - Find r such that f(r) = 0

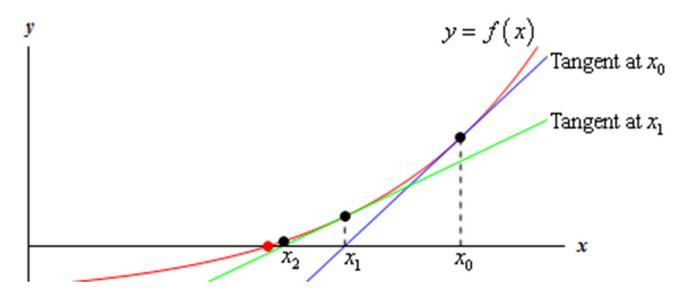


- ▶ Optimization
 - $\blacktriangleright \operatorname{Set} g(x) = x (f(x) / f'(x))$
 - ► Take $x_{t+1} = g(x_t)$



- ▶ Optimization
 - ightharpoonup Set g(x) = x m (f(x) / f'(x))
 - ► Take $x_{t+1} = g(x_t)$

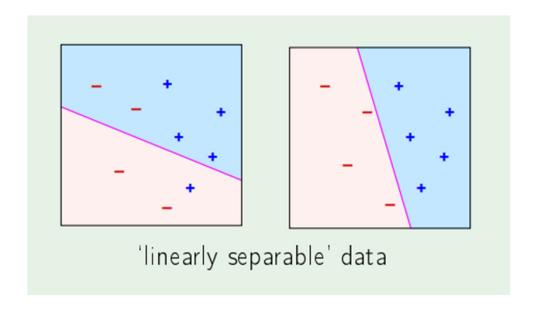
Regularization

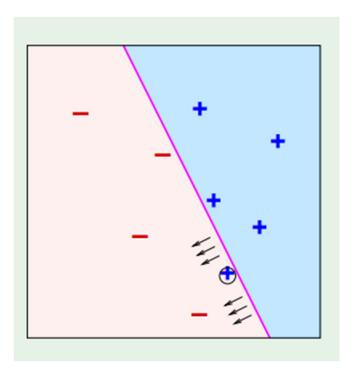


- ► Computational Complexity
 - ► Time to Run
 - ► Amount of Storage
 - ▶ Informed by Mistake Bound

- ► Computational Complexity
 - ► Time to Run
 - ► Amount of Storage
 - ▶ Informed by Mistake Bound
- ► Sample complexity
 - ► Amount of training data needed to learn successfully

- ► Computational Complexity
 - ► Time to Run
 - ► Amount of Storage
 - ▶ Informed by Mistake Bound
- ► Sample complexity
 - ► Amount of training data needed to learn successfully
 - ▶ Depends on the size of the hypothesis space





► Step 1 (Input)

$$e \mapsto \mathbf{f}(e) = (h_1(e), \dots, h_N(e)) = (x_1, \dots, x_N)$$

Step 1 (Input)

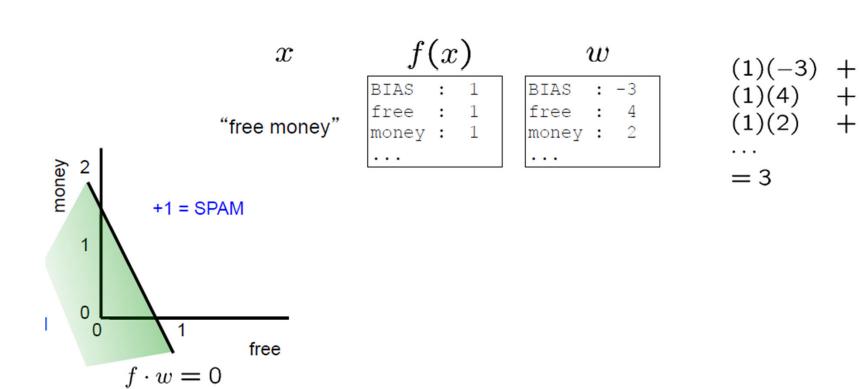
$$e \mapsto \mathbf{f}(e) = (h_1(e), \dots, h_N(e)) = (x_1, \dots, x_N)$$

Step 2 (Combine) $\langle \mathbf{w}, \mathbf{f}(e) \rangle = \sum_{i=1}^N w_i x_i$

Step 1 (Input)

$$e \mapsto \mathbf{f}(e) = (h_1(e), \dots, h_N(e)) = (x_1, \dots, x_N)$$

- ▶ Step 2 (Combine) $\langle \mathbf{w}, \mathbf{f}(e) \rangle = \sum_{i=1}^N w_i x_i$
- ▶ Step 3 (Output) $\operatorname{sign}(z) = \begin{cases} 1 & \text{if } z \ge 0 \\ -1 & \text{if } z < 0 \end{cases}$



Hypothesis

$$sign (\langle \mathbf{w}, \mathbf{f}(e) \rangle - threshold) = \begin{cases} 1 & then spam \\ -1 & then not spam \end{cases}$$
(Combine)

► Step 2 (Combine)

$$f_{N+1}(e) \equiv 1$$

$$w_{N+1} = -$$
threshold

Step 3 (Output)
$$\operatorname{sign}(\langle \mathbf{w}, \mathbf{f}(e) \rangle) = \begin{cases} 1 & \text{then spam} \\ -1 & \text{then not spam} \end{cases}$$

```
input: A training set (\mathbf{x}_1, y_1), \dots, (\mathbf{x}_m, y_m)

initialize: \mathbf{w}^{(1)} = (0, \dots, 0)

for t = 1, 2, \dots

if (\exists i \text{ s.t. } y_i \langle \mathbf{w}^{(t)}, \mathbf{x}_i \rangle \leq 0) then

\mathbf{w}^{(t+1)} = \mathbf{w}^{(t)} + y_i \mathbf{x}_i

else

output \mathbf{w}^{(t)}
```

```
1 \mathbf{w}_1 \leftarrow \mathbf{w}_0 > typically \mathbf{w}_0 = \mathbf{0}

2 \mathbf{for} \ t \leftarrow 1 \ \mathbf{to} \ T \ \mathbf{do}

3 \mathrm{RECEIVE}(\mathbf{x}_t)

4 \widehat{y}_t \leftarrow \mathrm{sgn}(\mathbf{w}_t \cdot \mathbf{x}_t)

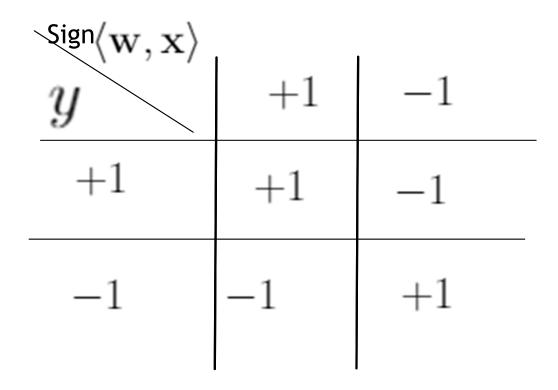
5 \mathrm{RECEIVE}(y_t)

6 \mathbf{if} \ (\widehat{y}_t \neq y_t) \ \mathbf{then}

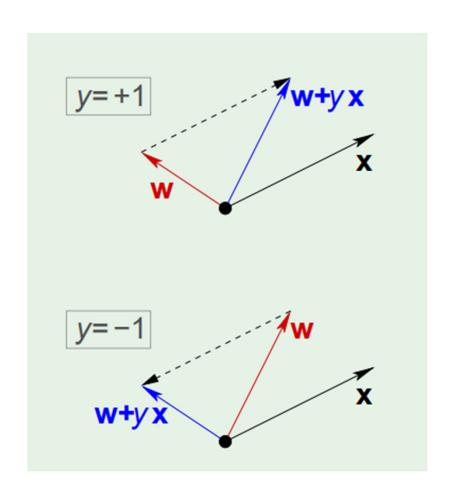
7 \mathbf{w}_{t+1} \leftarrow \mathbf{w}_t + \eta \mathbf{v}_t

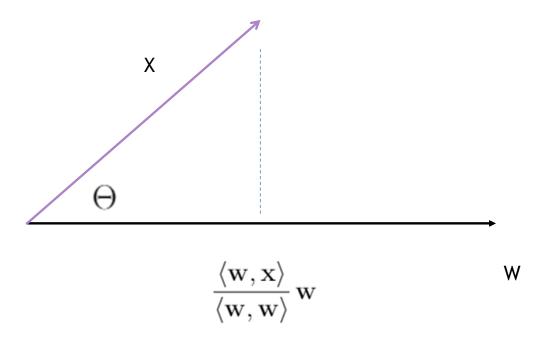
8 \mathbf{else} \ \mathbf{w}_{t+1} \leftarrow \mathbf{w}_t

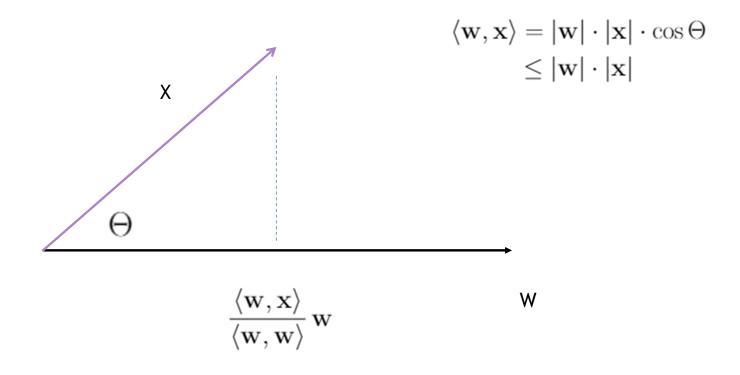
9 \mathbf{return} \ \mathbf{w}_{T+1}
```



$$y \langle \mathbf{w_t}, \mathbf{x} \rangle$$
$$y \langle \mathbf{w_{t+1}}, \mathbf{x} \rangle = y \langle \mathbf{w_t}, \mathbf{x} \rangle + |\mathbf{x}|^2$$





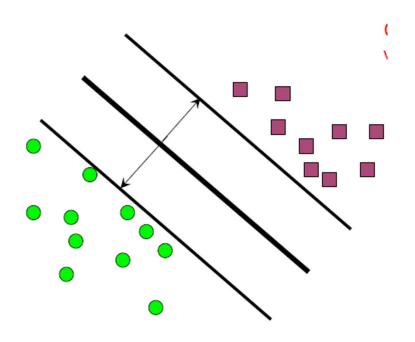


► Assume that the data is linearly separable. Set

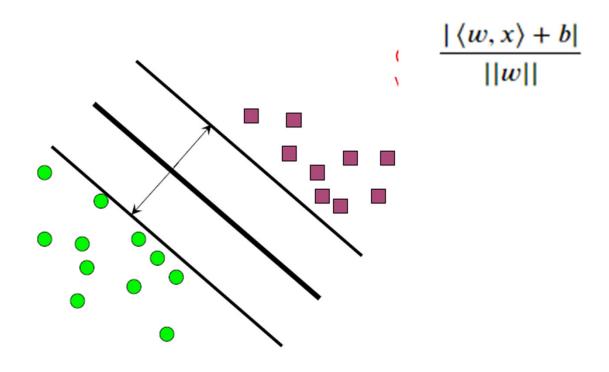
$$\rho = \min_{1 \le t \le T} \frac{y_i \langle \mathbf{w}, \mathbf{x}_t \rangle}{|\mathbf{v}|}$$
$$r = \max_{1 \le i \le T} |\mathbf{x}_i|$$

► The maximum number of mistakes made by the perceptron algorithm is

$$\frac{r^2}{\rho^2}$$



The distance between x and the plane defined by (w,b) is



Assume that the data is linearly separable. Set

$$\rho = \min_{1 \le t \le T} \frac{y_i \langle \mathbf{w}, \mathbf{x}_t \rangle}{|\mathbf{v}|}$$
$$r = \max_{1 \le i \le T} |\mathbf{x}_i|$$

► The maximum number of mistakes made by the perceptron algorithm is

$$\frac{r^2}{\rho^2}$$

Set

$$I \subset T$$
 with $\#I = M$

$$M\rho \leq \frac{\mathbf{v} \cdot \sum_{t \in I} y_t \mathbf{x}_t}{\|\mathbf{v}\|} \leq \left\| \sum_{t \in I} y_t \mathbf{x}_t \right\|$$
 (Cauchy-Schwarz inequality)

$$M\rho \leq \frac{\mathbf{v} \cdot \sum_{t \in I} y_t \mathbf{x}_t}{\|\mathbf{v}\|} \leq \left\| \sum_{t \in I} y_t \mathbf{x}_t \right\|$$
 (Cauchy-Schwarz inequality)
$$= \left\| \sum_{t \in I} (\mathbf{w}_{t+1} - \mathbf{w}_t) \right\|$$
 (definition of updates)

$$M\rho \leq \frac{\mathbf{v} \cdot \sum_{t \in I} y_t \mathbf{x}_t}{\|\mathbf{v}\|} \leq \left\| \sum_{t \in I} y_t \mathbf{x}_t \right\|$$
 (Cauchy-Schwarz inequality)
$$= \left\| \sum_{t \in I} (\mathbf{w}_{t+1} - \mathbf{w}_t) \right\|$$
 (definition of updates)
$$= \|\mathbf{w}_{T+1}\|$$
 (telescoping sum, $\mathbf{w}_0 = 0$)

$$M\rho \leq \frac{\mathbf{v} \cdot \sum_{t \in I} y_t \mathbf{x}_t}{\|\mathbf{v}\|} \leq \left\| \sum_{t \in I} y_t \mathbf{x}_t \right\|$$
 (Cauchy-Schwarz inequality)
$$= \left\| \sum_{t \in I} (\mathbf{w}_{t+1} - \mathbf{w}_t) \right\|$$
 (definition of updates)
$$= \|\mathbf{w}_{T+1}\|$$
 (telescoping sum, $\mathbf{w}_0 = 0$)
$$= \sqrt{\sum_{t \in I} \|\mathbf{w}_{t+1}\|^2 - \|\mathbf{w}_t\|^2}$$
 (telescoping sum, $\mathbf{w}_0 = 0$)

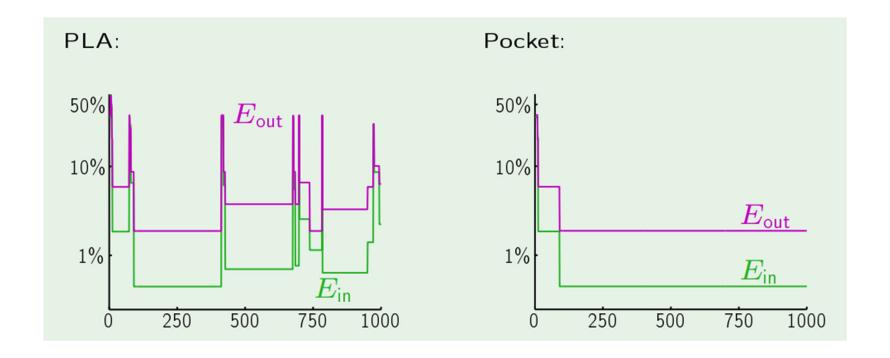
$$M\rho \leq \frac{\mathbf{v} \cdot \sum_{t \in I} y_t \mathbf{x}_t}{\|\mathbf{v}\|} \leq \left\| \sum_{t \in I} y_t \mathbf{x}_t \right\|$$
 (Cauchy-Schwarz inequality)
$$= \left\| \sum_{t \in I} (\mathbf{w}_{t+1} - \mathbf{w}_t) \right\|$$
 (definition of updates)
$$= \|\mathbf{w}_{T+1}\|$$
 (telescoping sum, $\mathbf{w}_0 = 0$)
$$= \sqrt{\sum_{t \in I} \|\mathbf{w}_{t+1}\|^2 - \|\mathbf{w}_t\|^2}$$
 (telescoping sum, $\mathbf{w}_0 = 0$)
$$= \sqrt{\sum_{t \in I} \|\mathbf{w}_t + y_t \mathbf{x}_t\|^2 - \|\mathbf{w}_t\|^2}$$
 (definition of updates)

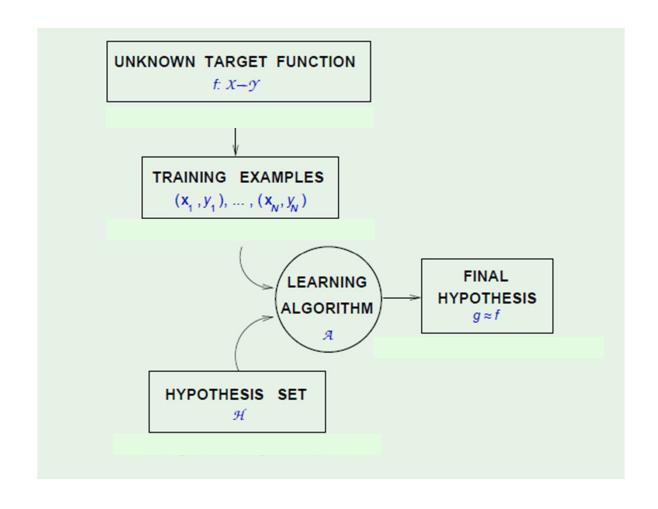
$$M\rho \leq \frac{\mathbf{v} \cdot \sum_{t \in I} y_t \mathbf{x}_t}{\|\mathbf{v}\|} \leq \left\| \sum_{t \in I} y_t \mathbf{x}_t \right\|$$
 (Cauchy-Schwarz inequality)
$$= \left\| \sum_{t \in I} (\mathbf{w}_{t+1} - \mathbf{w}_t) \right\|$$
 (definition of updates)
$$= \|\mathbf{w}_{T+1}\|$$
 (telescoping sum, $\mathbf{w}_0 = 0$)
$$= \sqrt{\sum_{t \in I} \|\mathbf{w}_{t+1}\|^2 - \|\mathbf{w}_t\|^2}$$
 (telescoping sum, $\mathbf{w}_0 = 0$)
$$= \sqrt{\sum_{t \in I} \|\mathbf{w}_t + y_t \mathbf{x}_t\|^2 - \|\mathbf{w}_t\|^2}$$
 (definition of updates)
$$= \sqrt{\sum_{t \in I} 2 y_t \mathbf{w}_t \cdot \mathbf{x}_t + \|\mathbf{x}_t\|^2}$$

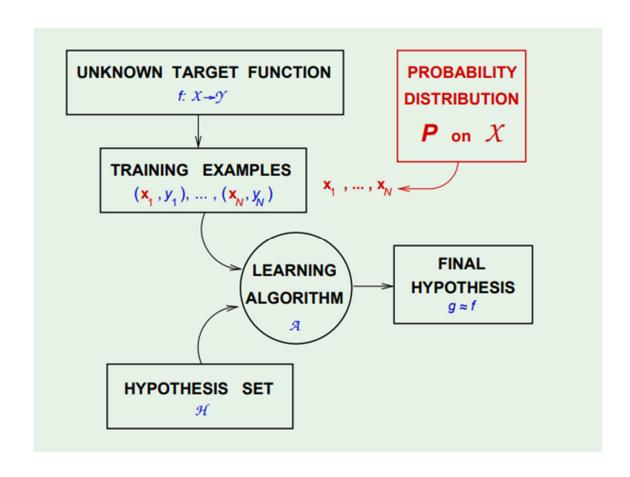
$$\begin{split} M\rho &\leq \frac{\mathbf{v} \cdot \sum_{t \in I} y_t \mathbf{x}_t}{\|\mathbf{v}\|} \leq \left\| \sum_{t \in I} y_t \mathbf{x}_t \right\| & \text{(Cauchy-Schwarz inequality)} \\ &= \left\| \sum_{t \in I} (\mathbf{w}_{t+1} - \mathbf{w}_t) \right\| & \text{(definition of updates)} \\ &= \|\mathbf{w}_{T+1}\| & \text{(telescoping sum, } \mathbf{w}_0 = 0) \\ &= \sqrt{\sum_{t \in I} \|\mathbf{w}_{t+1}\|^2 - \|\mathbf{w}_t\|^2} & \text{(telescoping sum, } \mathbf{w}_0 = 0) \\ &= \sqrt{\sum_{t \in I} \|\mathbf{w}_t + y_t \mathbf{x}_t\|^2 - \|\mathbf{w}_t\|^2} & \text{(definition of updates)} \\ &= \sqrt{\sum_{t \in I} 2 \underbrace{y_t \mathbf{w}_t \cdot \mathbf{x}_t}_{\leq 0} + \|\mathbf{x}_t\|^2} \\ &\leq \sqrt{\sum_{t \in I} \|\mathbf{x}_t\|^2} \leq \sqrt{Mr^2}. \end{split}$$

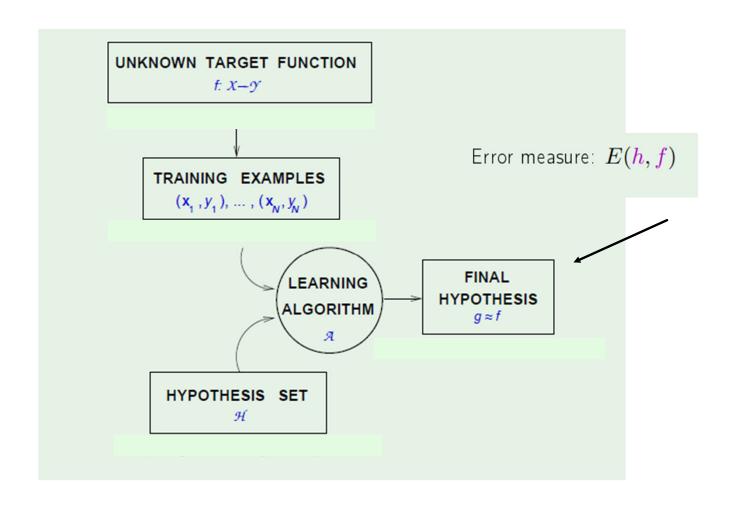
- ► Pocket Algorithm
 - 1. Set the weight w to w_0 of PLA
 - 2. For t = 0,...,T-1 do
 - 1. Run PLA for one update to obtain w_{t+1}
 - 2. Count number of misclassfications
 - 3. If w_{t+1} is better than w_{t} then set w to w_{t+1}

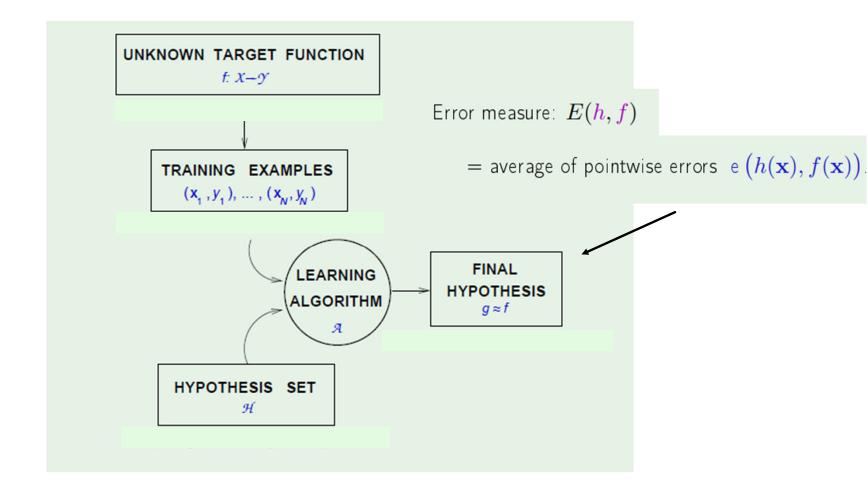
Demo









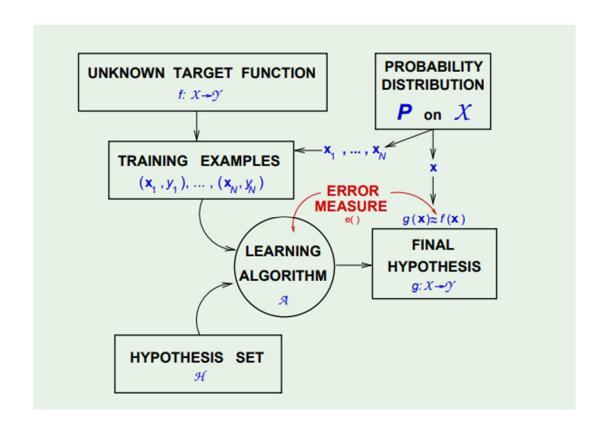


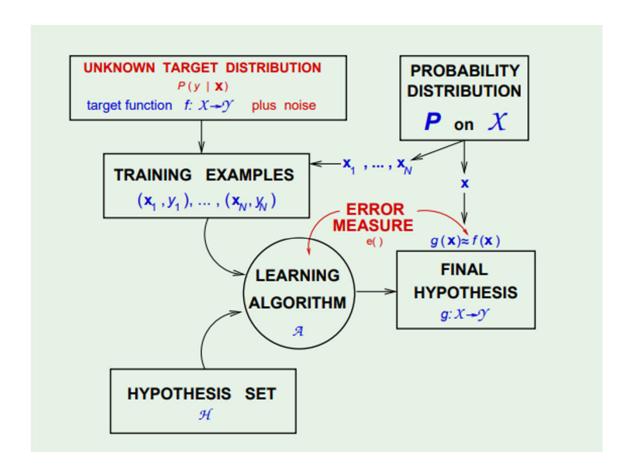
In-sample error:

$$E_{\mathrm{in}}(h) = \frac{1}{N} \sum_{n=1}^{N} e\left(h(\mathbf{x}_n), f(\mathbf{x}_n)\right)$$

Out-of-sample error:

$$E_{\mathrm{out}}(h) = \mathbb{E}_{\mathbf{x}} [e(h(\mathbf{x}), f(\mathbf{x}))]$$

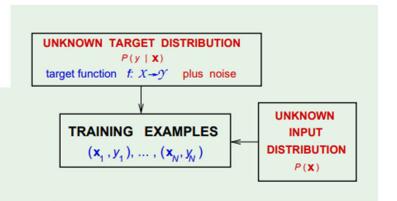




The target distribution $P(y \mid \mathbf{x})$ is what we are trying to learn

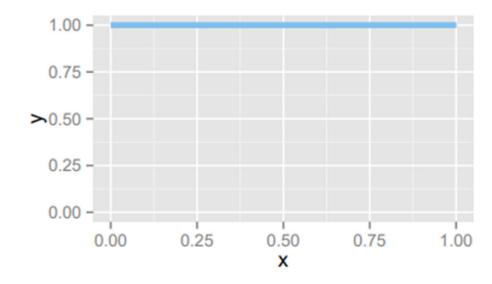
The input distribution $P(\mathbf{x})$ quantifies relative importance of \mathbf{x}

Merging $P(\mathbf{x})P(y|\mathbf{x})$ as $P(\mathbf{x},y)$ mixes the two concepts



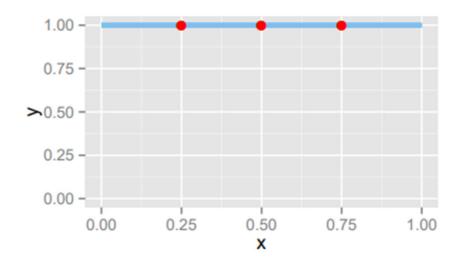
- 1. Can we make sure that $E_{
 m out}(g)$ is close enough to $E_{
 m in}(g)$?
- 2. Can we make $E_{
 m in}(g)$ small enough?

 $P_{\mathfrak{X}} = \mathsf{Uniform}[0,1], \ Y \equiv 1 \ (\mathsf{i.e.} \ Y \ \mathsf{is always} \ 1).$



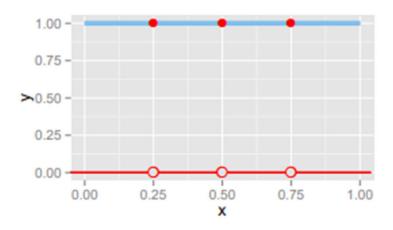
 $\mathfrak{P}_{\mathfrak{X}\times\mathfrak{Y}}.$

 $P_{\mathfrak{X}}=\mathsf{Uniform}[\mathsf{0,1}],\ Y\equiv 1$ (i.e. Y is always 1).



A sample of size 3 from $\mathfrak{P}_{\mathfrak{X}\times\mathfrak{Y}}.$

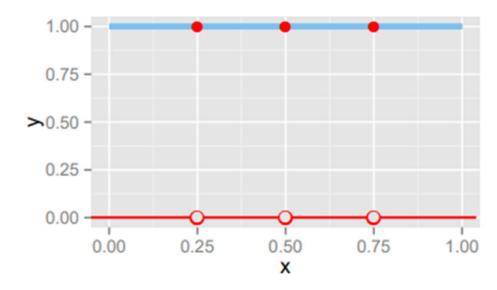
 $P_{\mathfrak{X}} = \mathsf{Uniform}[0,1], \ Y \equiv 1 \ (\mathsf{i.e.} \ Y \ \mathsf{is always} \ 1).$



A proposed prediction function:

$$\hat{f}(x) = 1(x \in \{0.25, 0.5, 0.75\}) = \begin{cases} 1 & \text{if } x \in \{0.25, .5, .75\} \\ 0 & \text{otherwise} \end{cases}$$

 $P_{\mathfrak{X}} = \mathsf{Uniform}[0,1], \ Y \equiv 1 \ (\mathsf{i.e.} \ Y \ \mathsf{is always} \ 1).$



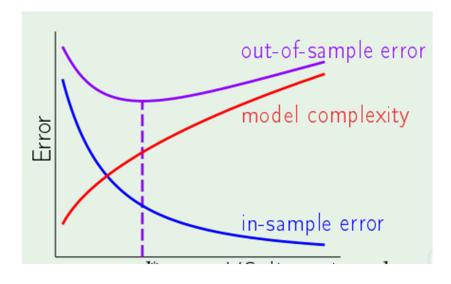
Under square loss or 0/1 loss: \hat{f} has Empirical Risk = 0 and Risk = 1.

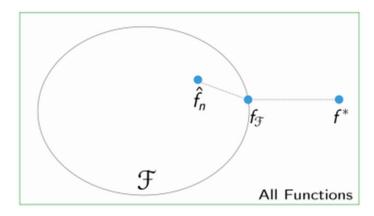
- 1. Can we make sure that $E_{
 m out}(g)$ is close enough to $E_{
 m in}(g)$?
- 2. Can we make $E_{
 m in}(g)$ small enough?

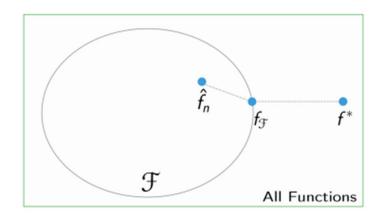
Model complexity
$$\uparrow$$
 $E_{
m in}$ \downarrow Model complexity \uparrow $E_{
m out}-E_{
m in}$ \uparrow

- 1. Can we make sure that $E_{
 m out}(g)$ is close enough to $E_{
 m in}(g)$?
- 2. Can we make $E_{
 m in}(g)$ small enough?

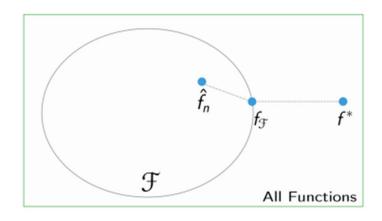
Model complexity	\uparrow	$E_{ m in}$	\downarrow
Model complexity	\uparrow	$E_{ m out}-E_{ m in}$	\uparrow



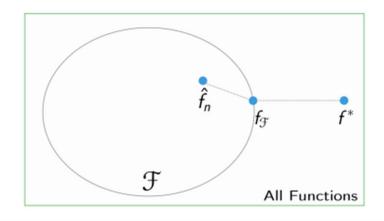




$$f^* = \underset{f}{\operatorname{arg\,min}} \mathbb{E}\ell(f(x), y)$$



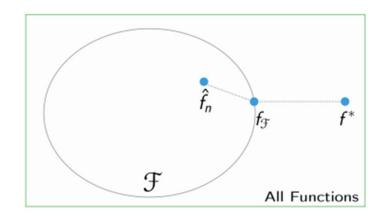
$$f^* = \underset{f}{\operatorname{arg\,min}} \mathbb{E}\ell(f(x), y)$$
$$f_{\mathcal{F}} = \underset{f \in \mathcal{F}}{\operatorname{arg\,min}} \mathbb{E}\ell(f(x), y))$$



$$f^* = \underset{f}{\operatorname{arg\,min}} \mathbb{E}\ell(f(x), y)$$

$$f_{\mathcal{F}} = \underset{f \in \mathcal{F}}{\operatorname{arg\,min}} \mathbb{E}\ell(f(x), y))$$

$$\hat{f_n} = \underset{f \in \mathcal{F}}{\operatorname{arg\,min}} \frac{1}{n} \sum_{i=1}^n \ell(f(x_i), y_i)$$

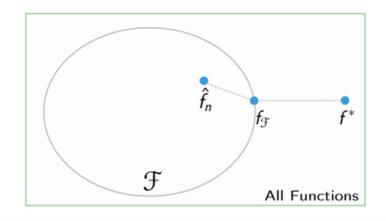


$$f^* = \underset{f}{\operatorname{arg\,min}} \mathbb{E}\ell(f(x), y)$$

$$f_{\mathcal{F}} = \underset{f \in \mathcal{F}}{\operatorname{arg\,min}} \mathbb{E}\ell(f(x), y))$$

$$\hat{f}_n = \underset{f \in \mathcal{F}}{\operatorname{arg\,min}} \frac{1}{n} \sum_{i=1}^n \ell(f(x_i), y_i)$$

• Approximation Error (of \mathcal{F}) = $R(f_{\mathcal{F}}) - R(f^*)$

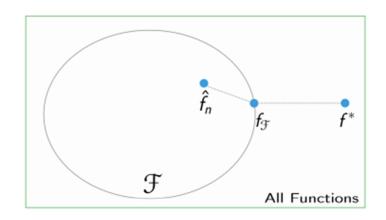


$$f^* = \underset{f}{\operatorname{arg \, min}} \mathbb{E}\ell(f(x), y)$$

$$f_{\mathcal{F}} = \underset{f \in \mathcal{F}}{\operatorname{arg \, min}} \mathbb{E}\ell(f(x), y))$$

$$\hat{f_n} = \underset{f \in \mathcal{F}}{\operatorname{arg \, min}} \frac{1}{n} \sum_{i=1}^n \ell(f(x_i), y_i)$$

- Approximation Error (of \mathcal{F}) = $R(f_{\mathcal{F}}) R(f^*)$
- Estimation error (of \hat{f}_n in \mathcal{F}) = $R(\hat{f}_n) R(f_{\mathcal{F}})$



$$f^* = \underset{f}{\operatorname{arg\,min}} \mathbb{E}\ell(f(x), y)$$

$$f_{\mathcal{F}} = \underset{f \in \mathcal{F}}{\operatorname{arg\,min}} \mathbb{E}\ell(f(x), y))$$

$$\hat{f}_n = \underset{f \in \mathcal{F}}{\operatorname{arg\,min}} \frac{1}{n} \sum_{i=1}^n \ell(f(x_i), y_i)$$

- Approximation Error (of \mathcal{F}) = $R(f_{\mathcal{F}}) R(f^*)$
- Estimation error (of \hat{f}_n in \mathcal{F}) = $R(\hat{f}_n) R(f_{\mathcal{F}})$

Excess Risk
$$(\hat{f}_n)$$
 = $R(\hat{f}_n) - R(f^*)$
 = $R(\hat{f}_n) - R(f_{\mathcal{F}}) + R(f_{\mathcal{F}}) - R(f^*)$.

estimation error approximation error

$$f^* = \operatorname*{arg\,min}_f R(f)$$

$$f^* = \operatorname*{arg\,min}_f R(f) = \operatorname*{arg\,min}_f \mathbb{E}[\mathbf{1}(f(X) \neq Y)]$$

$$f^* = \mathop{\arg\min}_{f} R(f) = \mathop{\arg\min}_{f} \mathbb{E}[\mathbf{1}(f(X) \neq Y)] = \mathop{\arg\min}_{f} P(f(X) \neq Y),$$

$$f^* = \mathop{\arg\min}_{f} R(f) = \mathop{\arg\min}_{f} \mathbb{E}[\mathbf{1}(f(X) \neq Y)] = \mathop{\arg\min}_{f} P(f(X) \neq Y),$$

where $(X, Y) \sim P_{\mathcal{X} \times \mathcal{Y}}$.

$$f^* = \operatorname*{arg\,min}_f R(f) = \operatorname*{arg\,min}_f \mathbb{E}[\mathbf{1}(f(X) \neq Y)] = \operatorname*{arg\,min}_f P(f(X) \neq Y),$$

where $(X, Y) \sim P_{\mathcal{X} \times \mathcal{Y}}$. Let

$$f_1(x) = \operatorname*{arg\,max}_y P(Y = y \mid X = x),$$

$$f^* = \mathop{\arg\min}_{f} R(f) = \mathop{\arg\min}_{f} \mathbb{E}[\mathbf{1}(f(X) \neq Y)] = \mathop{\arg\min}_{f} P(f(X) \neq Y),$$

where $(X, Y) \sim P_{\mathcal{X} \times \mathcal{Y}}$. Let

$$f_1(x) = \operatorname*{arg\,max}_y P(Y = y \mid X = x),$$

$$\begin{array}{rcl}
P(f_1(X) \neq Y) & = & \sum_x P(f_1(x) \neq Y | X = x) P(X = x) \\
& = & \sum_x (1 - P(f_1(x) = Y | X = x)) P(X = x)
\end{array}$$

$$f^* = \mathop{\arg\min}_{f} R(f) = \mathop{\arg\min}_{f} \mathbb{E}[\mathbf{1}(f(X) \neq Y)] = \mathop{\arg\min}_{f} P(f(X) \neq Y),$$

where $(X, Y) \sim P_{\mathcal{X} \times \mathcal{Y}}$. Let

$$f_1(x) = \operatorname*{arg\,max}_y P(Y = y \mid X = x),$$

$$P(f_{1}(X) \neq Y) = \sum_{x} P(f_{1}(x) \neq Y | X = x) P(X = x)$$

$$= \sum_{x} (1 - P(f_{1}(x) = Y | X = x)) P(X = x)$$

$$\leq \sum_{x} (1 - P(f_{2}(x) = Y | X = x)) P(X = x) \text{ (Defn of } f_{1})$$

$$f^* = \arg\min_f R(f) = \arg\min_f \mathbb{E}[\mathbf{1}(f(X) \neq Y)] = \arg\min_f P(f(X) \neq Y),$$
 where $(X,Y) \sim P_{\mathcal{X} \times \mathcal{Y}}$. Let
$$f_1(x) = \arg\max_f P(Y=y \mid X=x),$$

$$\begin{array}{lcl} P(f_{1}(X) \neq Y) & = & \sum_{x} P(f_{1}(x) \neq Y | X = x) P(X = x) \\ & = & \sum_{x} (1 - P(f_{1}(x) = Y | X = x)) P(X = x) \\ & \leq & \sum_{x} (1 - P(f_{2}(x) = Y | X = x)) P(X = x) & \text{(Defn of } f_{1}) \\ & = & \sum_{x} P(f_{2}(x) \neq Y | X = x) P(X = x) \\ & = & P(f_{2}(X) \neq Y). \end{array}$$

$$f^* = \mathop{\arg\min}_{f} R(f) = \mathop{\arg\min}_{f} \mathbb{E}[\mathbf{1}(f(X) \neq Y)] = \mathop{\arg\min}_{f} P(f(X) \neq Y),$$

where $(X, Y) \sim P_{\mathcal{X} \times \mathcal{Y}}$. Let

$$f_1(x) = \operatorname*{arg\,max}_{y} P(Y = y \mid X = x),$$

$$P(f_{1}(X) \neq Y) = \sum_{x} P(f_{1}(x) \neq Y | X = x) P(X = x)$$

$$= \sum_{x} (1 - P(f_{1}(x) = Y | X = x)) P(X = x)$$

$$\leq \sum_{x} (1 - P(f_{2}(x) = Y | X = x)) P(X = x) \text{ (Defn of } f_{1})$$

$$= \sum_{x} P(f_{2}(x) \neq Y | X = x) P(X = x)$$

$$= P(f_{2}(X) \neq Y).$$

Thus $f^* = f_1$.