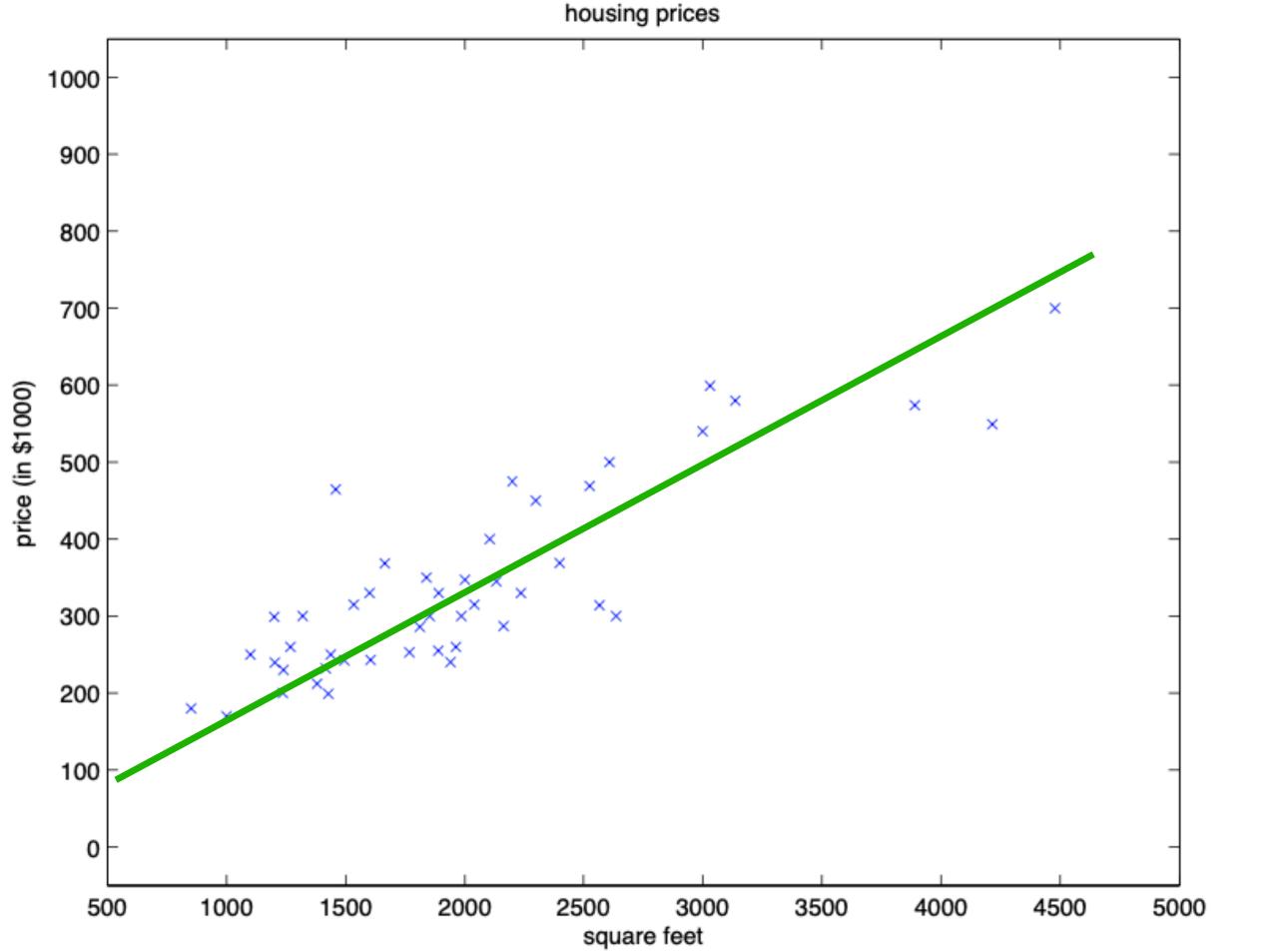
Empirical Risk Minimization

Announcements

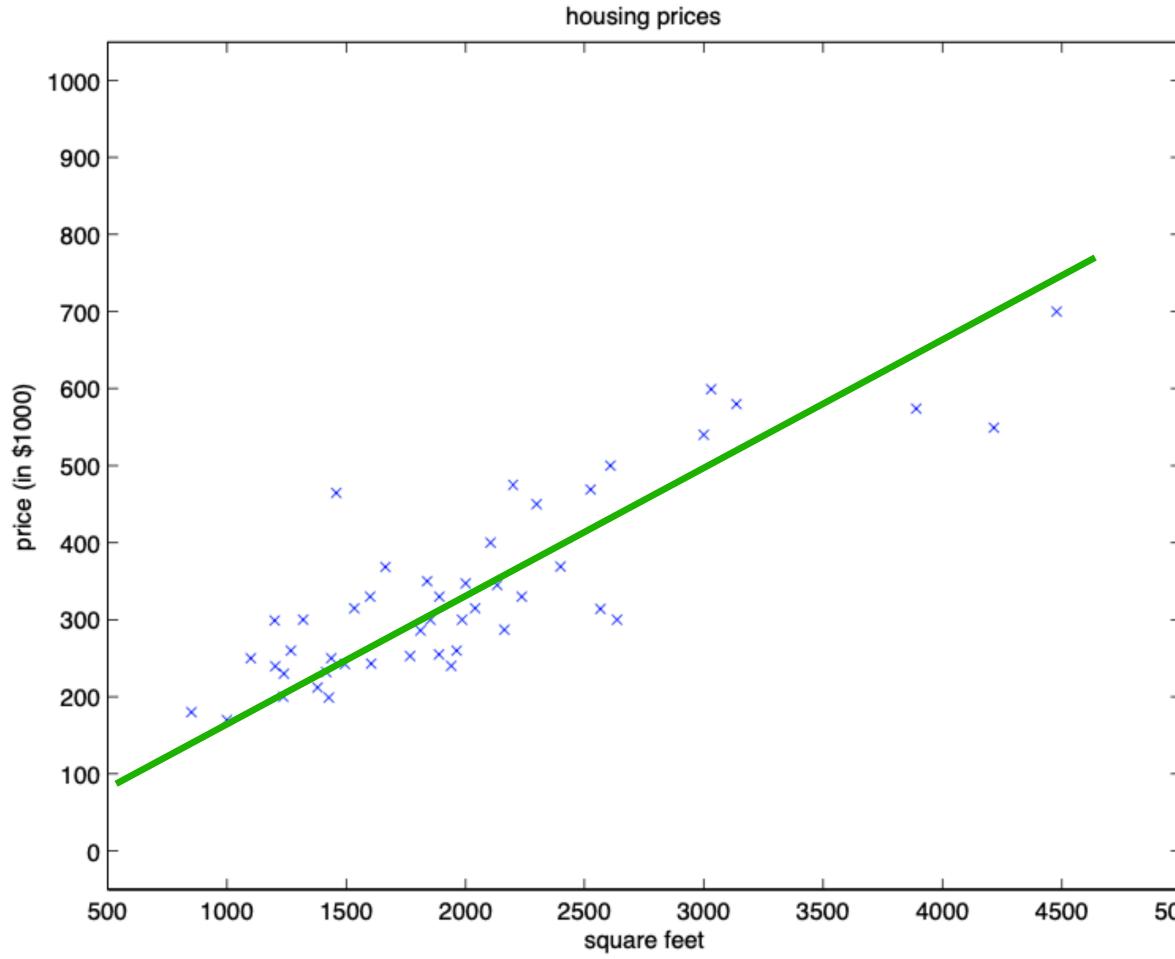
Recap on Linear Regression

Given dataset $\mathcal{D} = \{x_i, y_i\}, x_i \in \mathbb{R}^d, y_i \in \mathbb{R}$



Recap on Linear Regression

Given dataset $\mathcal{D} = \{x_i, y_i\}, x_i \in \mathbb{R}^d, y_i \in \mathbb{R}$

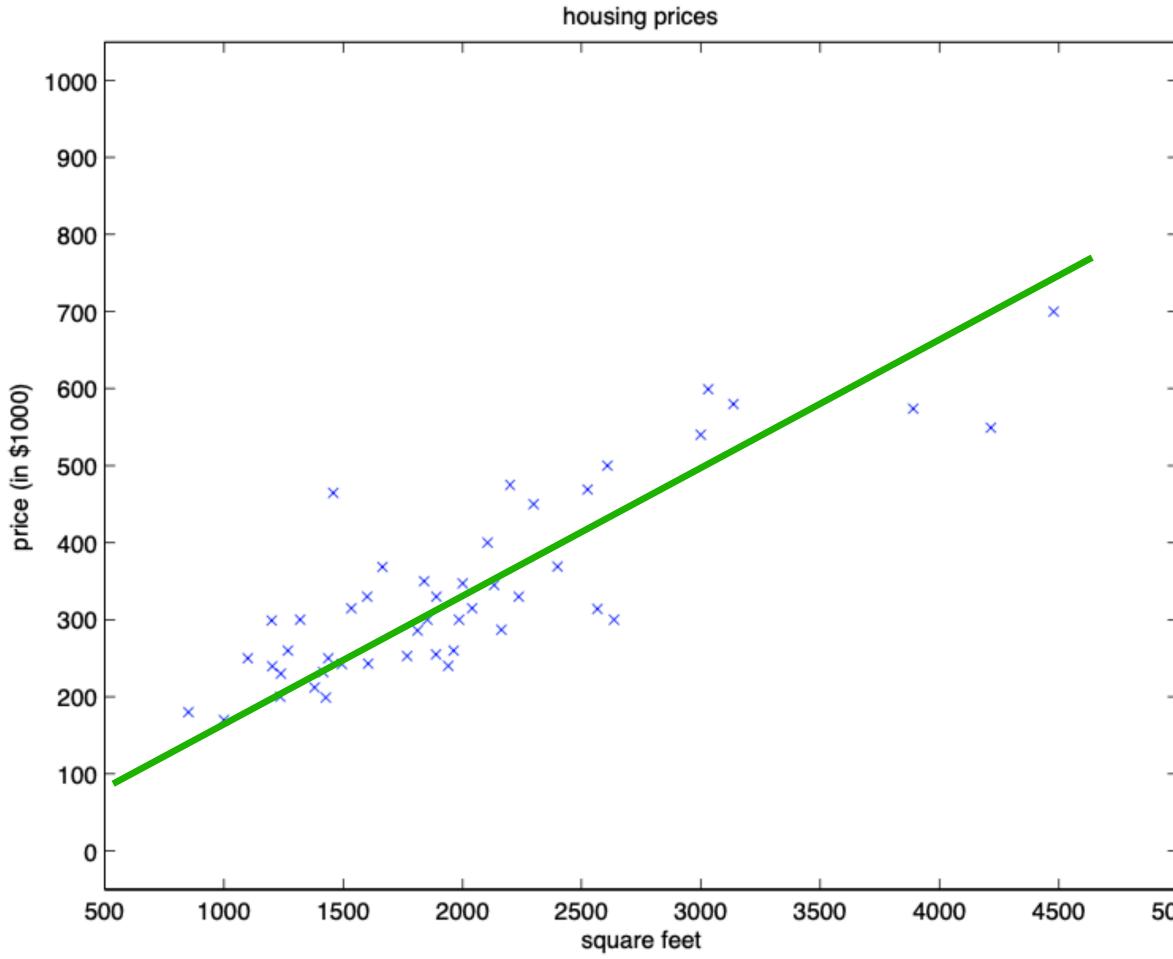


Least Regression with squared loss:

$$\underset{w}{\operatorname{arg\,min}} \sum_{i=1}^{n} (w^{\mathsf{T}} x_i - y_i)^2$$

Recap on Linear Regression

Given dataset $\mathcal{D} = \{x_i, y_i\}, x_i \in \mathbb{R}^d, y_i \in \mathbb{R}$



Derivation of Normal equation: $L(w) := \sum_{i=1}^{n} (w^{\mathsf{T}} x_i - y_i)^2$

 $\nabla_w L(w) =$

Hard margin SVM:

$\min_{w,b} \|w\|_2^2$

$\forall i: y_i(w^{\mathsf{T}}x_i + b) \ge 1$

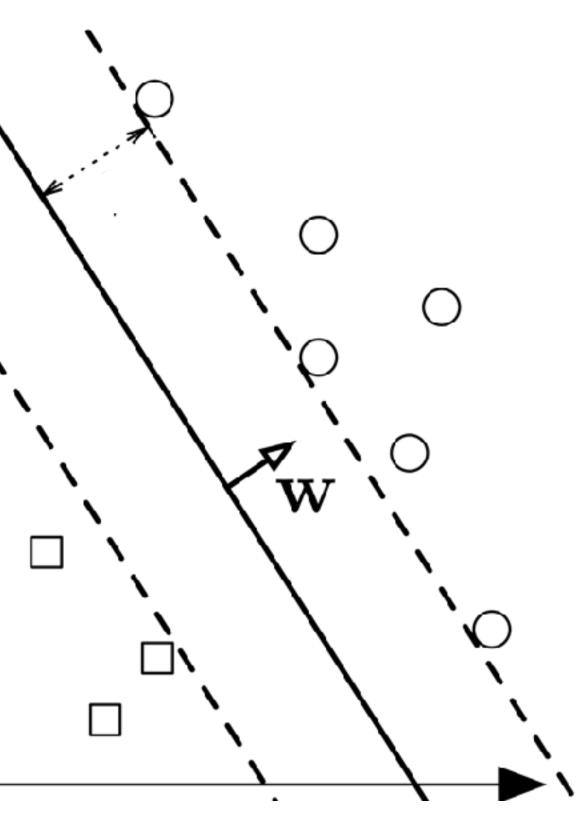
Given dataset $\mathcal{D} = \{x_i, y_i\}, x_i \in \mathbb{R}^d, y_i \in \{+1, -1\}$

Given dataset $\mathcal{D} = \{x_i, y_i\}, x_i \in \mathbb{R}^d, y_i \in \{+1, -1\}$

Hard margin SVM:

 $\min_{w,b} \|w\|_2^2$

 $\forall i: y_i(w^{\mathsf{T}}x_i + b) \ge 1$



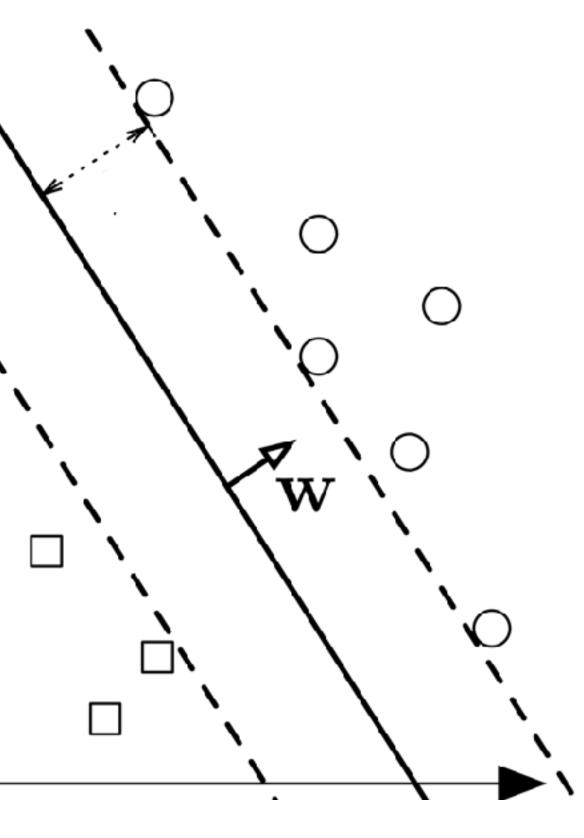
Width of the "street":

Given dataset $\mathcal{D} = \{x_i, y_i\}, x_i \in \mathbb{R}^d, y_i \in \{+1, -1\}$

Hard margin SVM:

 $\min_{w,b} \|w\|_2^2$

 $\forall i: y_i(w^{\mathsf{T}}x_i + b) \ge 1$



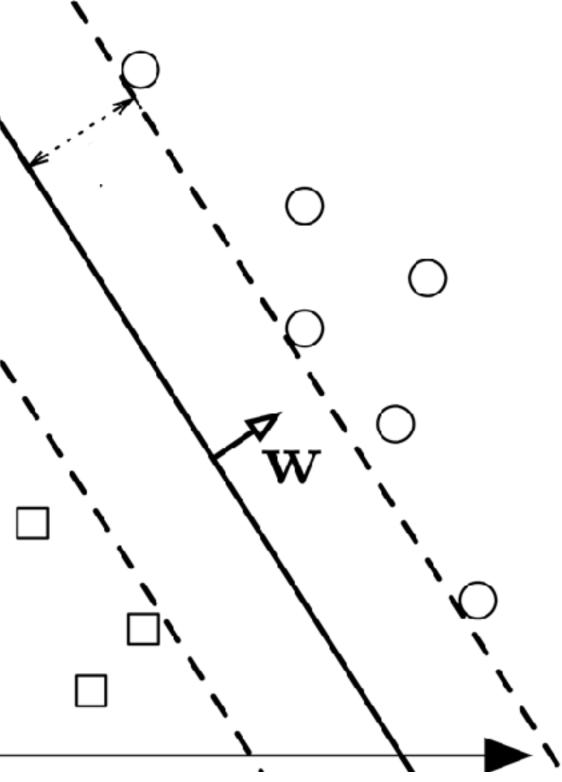
Width of the "street": $2/||w||_2$

Hard margin SVM:

 $\min \|w\|_2^2$ w,b

 $\forall i: y_i(w^{\mathsf{T}}x_i + b) \ge 1$

Given dataset $\mathcal{D} = \{x_i, y_i\}, x_i \in \mathbb{R}^d, y_i \in \{+1, -1\}$



Width of the "street": $2/\|w\|_{2}$

Find a "street" that has largest width, while keep all the points outside of the street



Outline for Today

1. Empirical Risk Minimization

2. Examples on loss & hypothesis classes

3. Regularization



We have some distribution *P*, dataset $\mathcal{D} = \{x_i, y_i\}_{i=1}^n$



Recall the general supervised learning setting:

ERM

We have some distribution *P*, dataset $\mathcal{D} = \{x_i, y_i\}_{i=1}^n$

Each data point is i.i.d sampled from P, i.e., $x_i, y_i \sim P$

Hypothesis $h: \mathcal{X} \to \mathbb{R}$, & hypothesis class $\mathcal{H} := \{h\} \subset \mathcal{X} \mapsto \mathbb{R}$

ERM

We have some distribution P, dataset $\mathcal{D} = \{x_i, y_i\}_{i=1}^n$

Each data point is i.i.d sampled from P, i.e., $x_i, y_i \sim P$

ERM

We have some distribution P, dataset $\mathcal{D} = \{x_i, y_i\}_{i=1}^n$

Each data point is i.i.d sampled from P, i.e., $x_i, y_i \sim P$

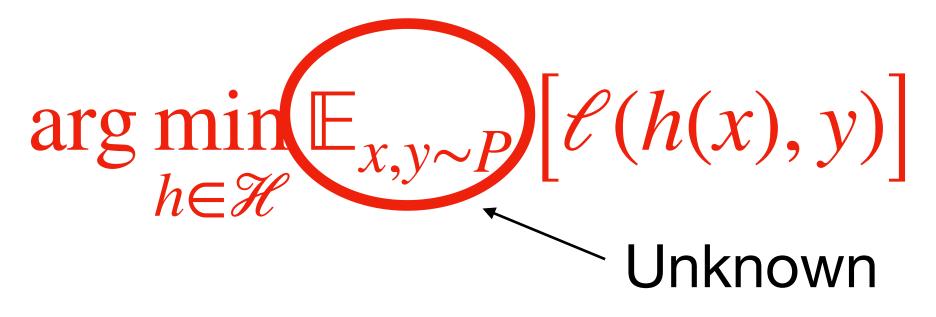
Hypothesis $h: \mathcal{X} \to \mathbb{R}$, & hypothesis class $\mathcal{H} := \{h\} \subset \mathcal{X} \mapsto \mathbb{R}$

Loss function: $\ell(h(x), y)$

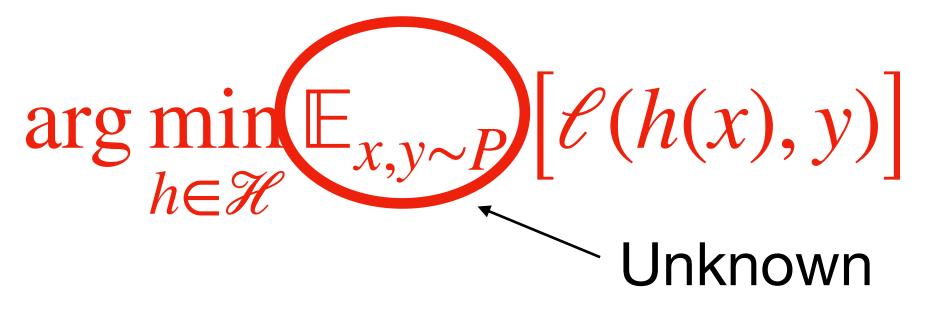




 $\underset{h \in \mathcal{H}}{\operatorname{arg\,min}} \mathbb{E}_{x, y \sim P} \left[\ell(h(x), y) \right]$

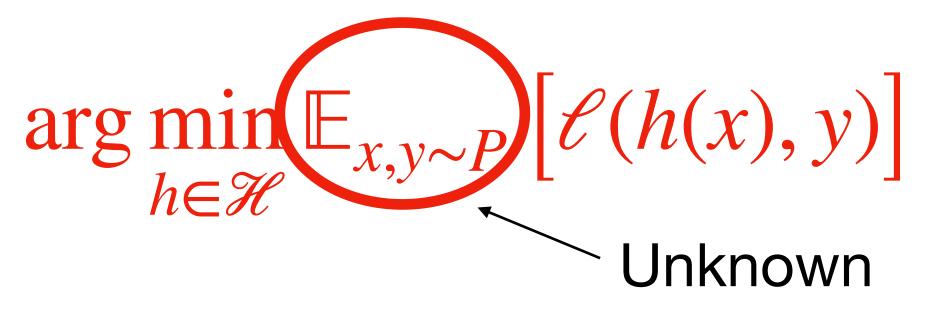






Instead we have its **empirical** version



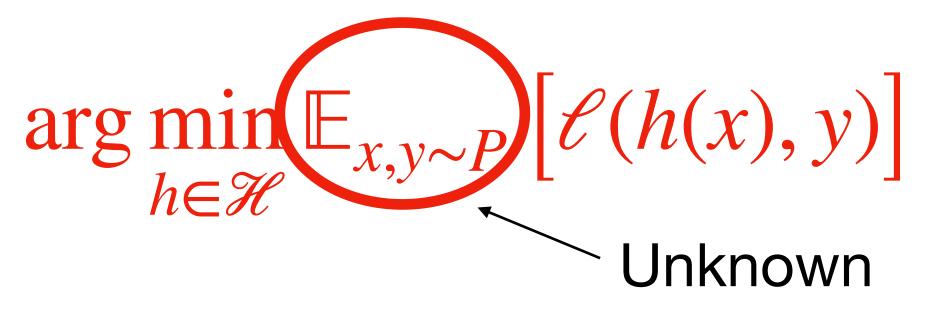


Instead we have its **empirical** version





 $\arg\min_{h\in\mathscr{H}}\frac{1}{n}\sum_{i=1}^{n}\left[\ell(h(x_i), y_i)\right]$ l = I



Instead we have its **empirical** version





$$\sum_{i=1}^{n} \left[\ell(h(x_i), y_i) \right]$$

Empirical risk / Empirical error

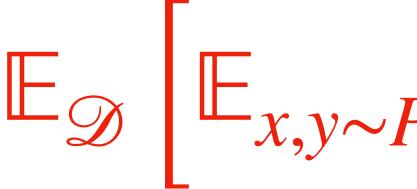
 $\hat{h}_{ERM} := \arg\min_{h \in \mathcal{H}} \frac{1}{n} \sum_{i=1}^{n} \left[\ell(h(x_i), y_i) \right]$

 $\hat{h}_{ERM} := \arg\min_{h \in \mathcal{H}} \frac{1}{n} \sum_{i=1}^{n} \left[\ell(h(x_i), y_i) \right]$

We often are interested in the true performance of \hat{h}_{ERM} :

 $\hat{h}_{ERM} := \arg\min_{h \in \mathcal{H}} \frac{1}{n} \sum_{i=1}^{n} \left[\ell(h(x_i), y_i) \right]$

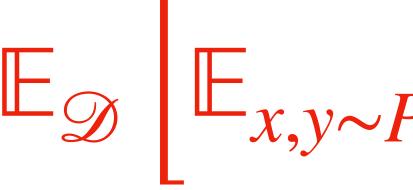
We often are interested in the true performance of \hat{h}_{ERM} :



 $\mathbb{E}_{\mathcal{D}} \mid \mathbb{E}_{x, y \sim P} \ell(\hat{h}_{ERM}(x), y)$

 $\hat{h}_{ERM} := \arg\min_{h \in \mathcal{H}} \frac{1}{n} \sum_{i=1}^{n} \left[\ell(h(x_i), y_i) \right]$

We often are interested in the true performance of \hat{h}_{ERM} :



Note \hat{h}_{ERM} is a random quantity as it depends on data ${\mathscr D}$

 $\mathbb{E}_{\mathcal{D}} \mid \mathbb{E}_{x,y\sim P} \ell(\hat{h}_{ERM}(x), y)$

 $\hat{h}_{ERM} := \arg\min_{h \in \mathcal{H}} \frac{1}{n} \sum_{i=1}^{n} \left[\ell(h(x_i), y_i) \right]$

We often are interested in the true performance of \hat{h}_{ERM} :

$$\mathbb{E}_{\mathscr{D}} \mid \mathbb{E}_{x,y \sim F}$$

Note \hat{h}_{ERM} is a random quantity as it depends on data \mathscr{D} e.g., In LR: $\hat{w} = (XX^{T})^{-1}XY$.

 $P\ell(\hat{h}_{ERM}(x), y)$

Ideally, we want the true loss of ERM to be small:

 $\mathbb{E}_{\mathscr{D}} \left| \mathbb{E}_{x, y \sim P} \ell(\hat{h}_{ERM}(x), y) \right| \approx \min_{h \in \mathscr{H}} \mathbb{E}_{x, y \sim P} \ell(h(x), y)$

Ideally, we want the true loss of ERM to be small:

 $\mathbb{E}_{\mathscr{D}}\left[\mathbb{E}_{x,y\sim P}\ell(\hat{h}_{ERM}(x),y)\right] \approx \min_{h\in\mathscr{H}}\mathbb{E}_{x,y\sim P}\ell(h(x),y)$

The Minimum expected loss we could get if we knew P

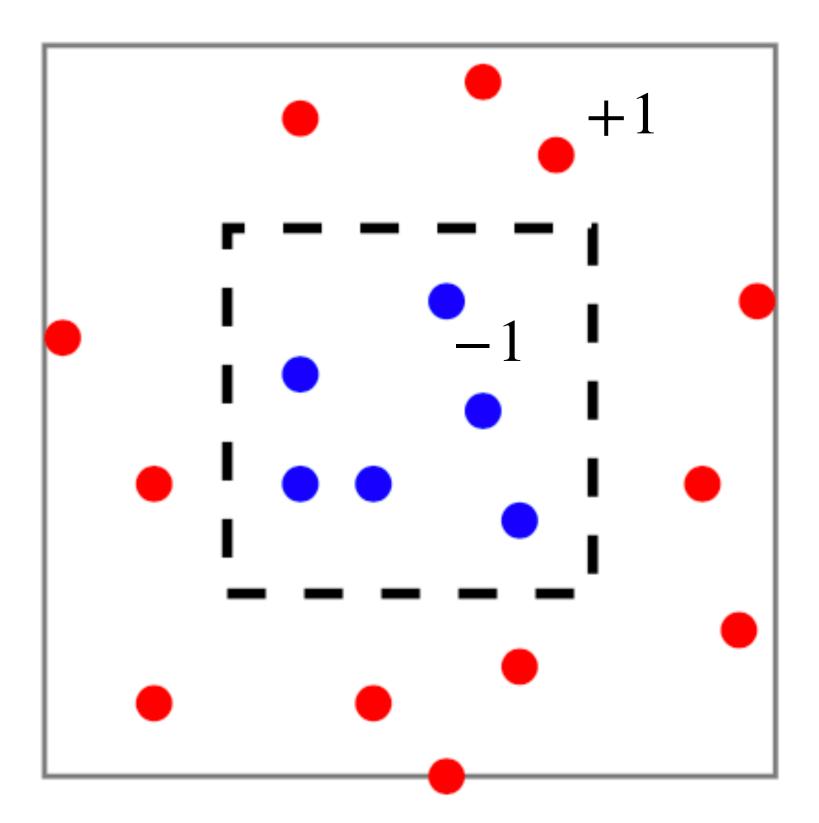
Ideally, we want the true loss of ERM to be small:

$$\mathbb{E}_{\mathscr{D}}\left[\mathbb{E}_{x,y\sim P}\ell(\hat{h}_{ERM}(x),y)\right] \approx \min_{h\in\mathscr{H}}\mathbb{E}_{x,y\sim P}\ell(h(x),y)$$

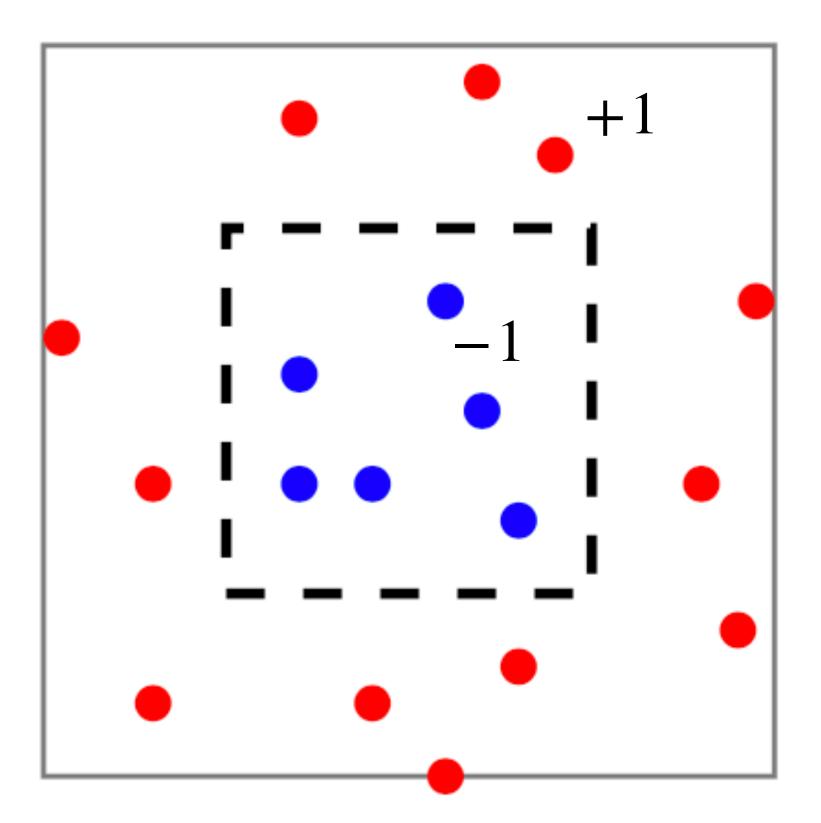
The Minimum expected loss we could get if we knew P

However, this may not hold if we are not careful about designing \mathscr{H}



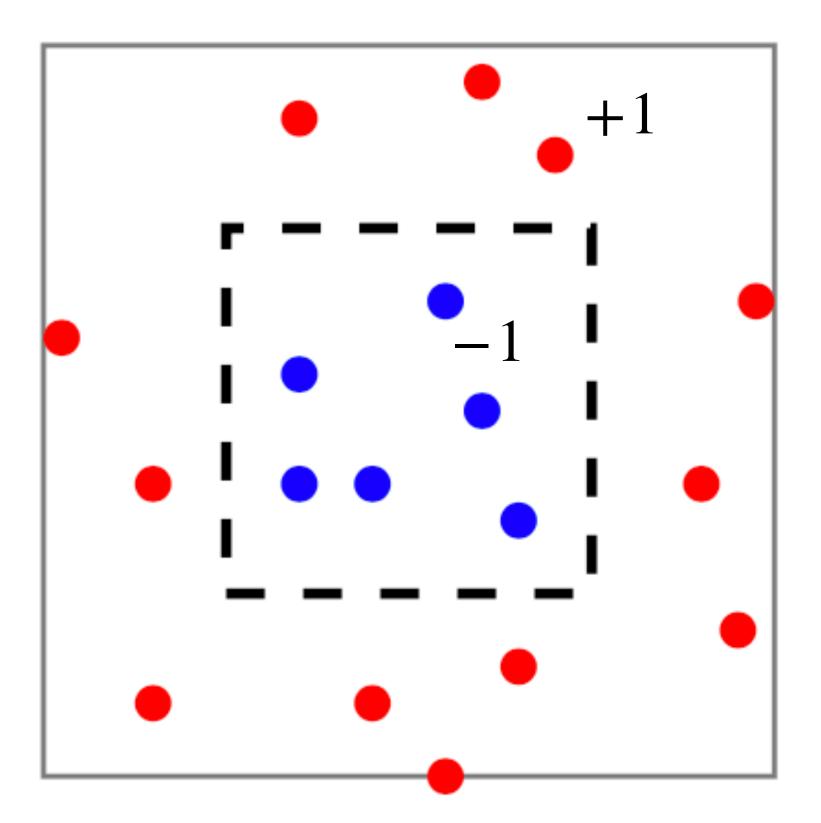


Example:



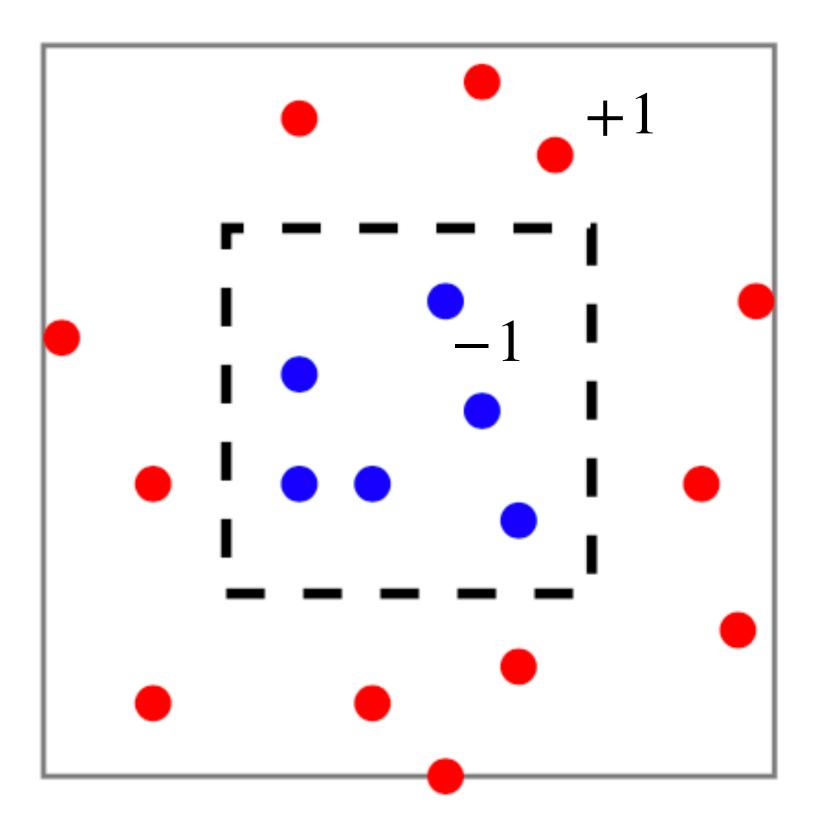
Example:

Consider a hypothesis class *H* contains ALL mappings from $x \rightarrow y$



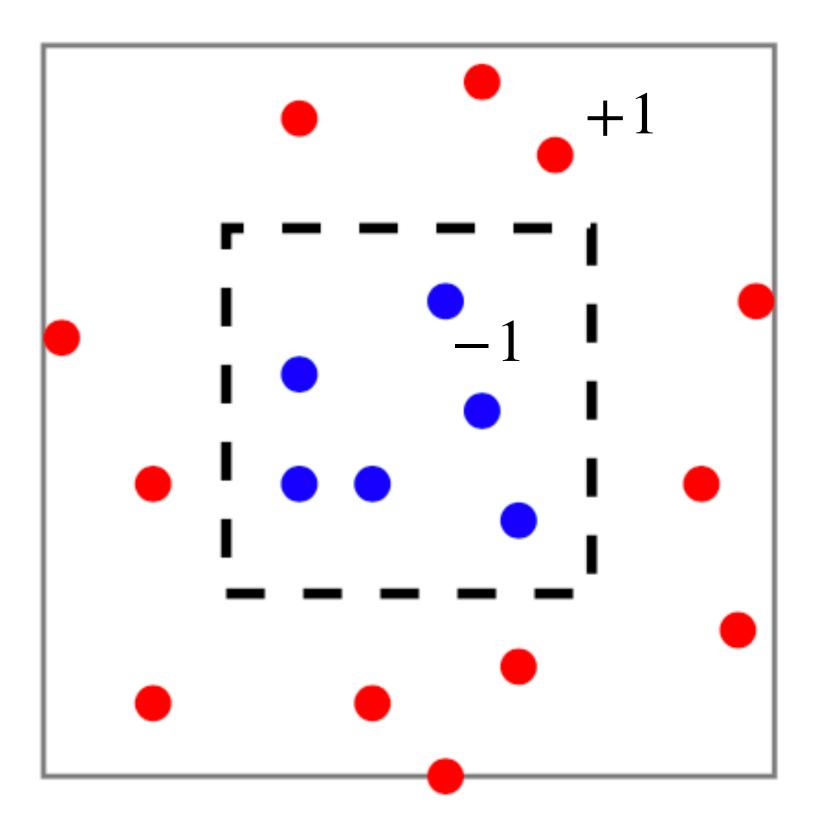
Example:

- Consider a hypothesis class *H* contains ALL mappings from $x \rightarrow y$
 - Zero one loss $\ell(h(x), y) = \mathbf{1}(h(x) \neq y)$



Example:

- Consider a hypothesis class *H* contains ALL mappings from $x \rightarrow y$
 - Zero one loss $\ell(h(x), y) = \mathbf{1}(h(x) \neq y)$
- Let us consider this solution that memorizes data:



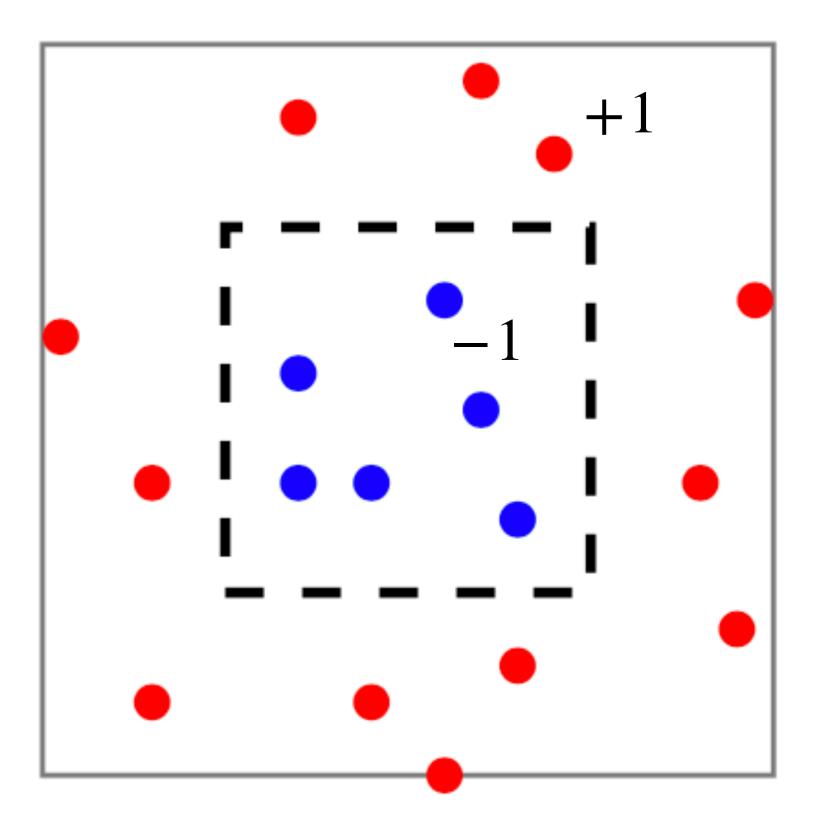
Example:

Consider a hypothesis class *H* contains ALL mappings from $x \rightarrow y$

Zero one loss $\ell(h(x), y) = \mathbf{1}(h(x) \neq y)$

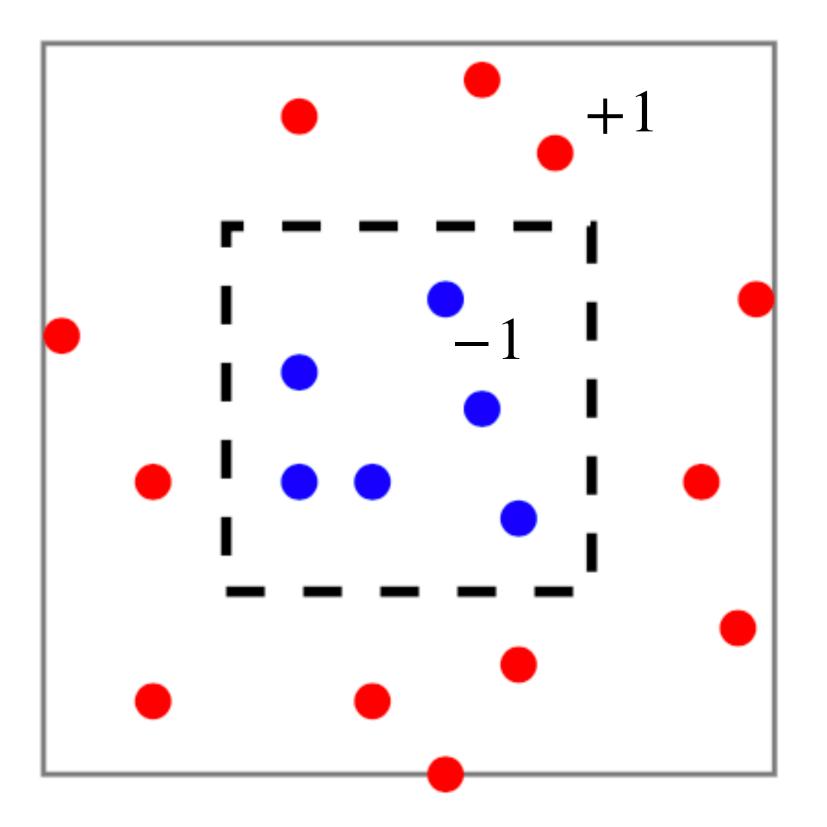
Let us consider this solution that memorizes data:

$$\hat{h}(x) = \begin{cases} y_i & \text{if } \exists i, x_i = x \\ +1 & \text{else} \end{cases}$$



Example:

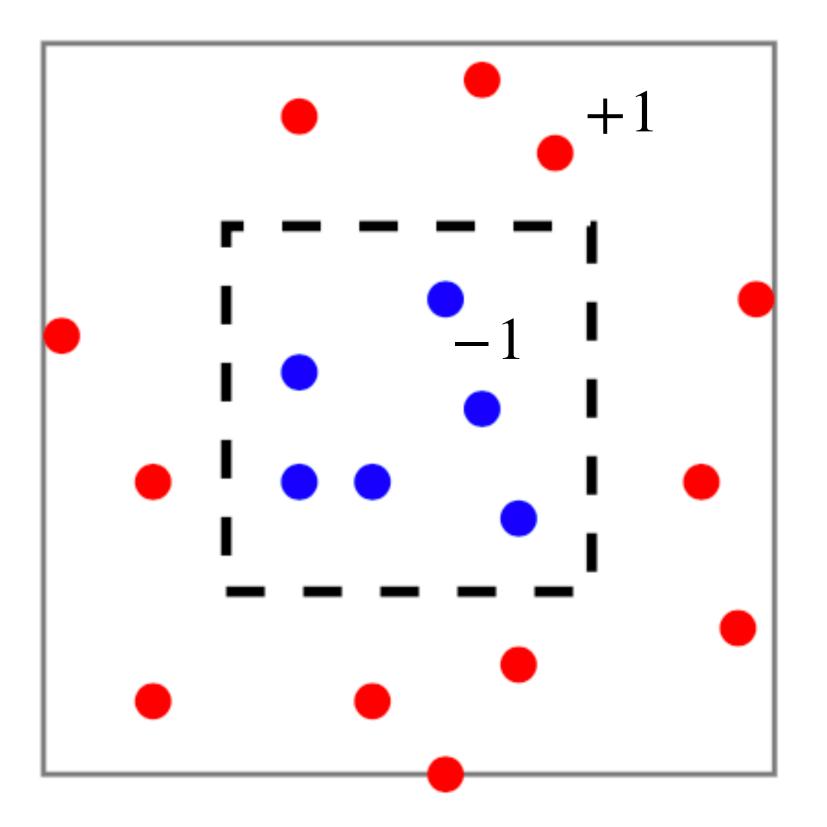
$\hat{h}(x) = \begin{cases} y_i & \text{if } \exists i, x_i = x \\ +1 & \text{else} \end{cases}$ $\implies \frac{1}{n} \sum_{i=1}^{n} \ell(\hat{h}(x_i), y_i) = 0$



Q: But what's the true expected error of this \hat{h} ?

Example:

$\hat{h}(x) = \begin{cases} y_i & \text{if } \exists i, x_i = x \\ +1 & \text{else} \end{cases}$ $\implies \frac{1}{n} \sum_{i=1}^{n} \ell(\hat{h}(x_i), y_i) = 0$



Example:

$\hat{h}(x) = \begin{cases} y_i & \text{if } \exists i, x_i = x \\ +1 & \text{else} \end{cases}$ $\implies \frac{1}{n} \sum_{i=1}^{n} \ell(\hat{h}(x_i), y_i) = 0$

Q: But what's the true expected error of this \hat{h} ?

A: area of smaller box / total area

ERM with inductive bias

A common solution is to restrict the search space (i.e., hypothesis class)

$$\hat{h}_{ERM} := \arg\min_{h \in \mathcal{H}} \frac{1}{n} \sum_{i=1}^{n} \left[\ell(h(x_i), y_i) \right]$$

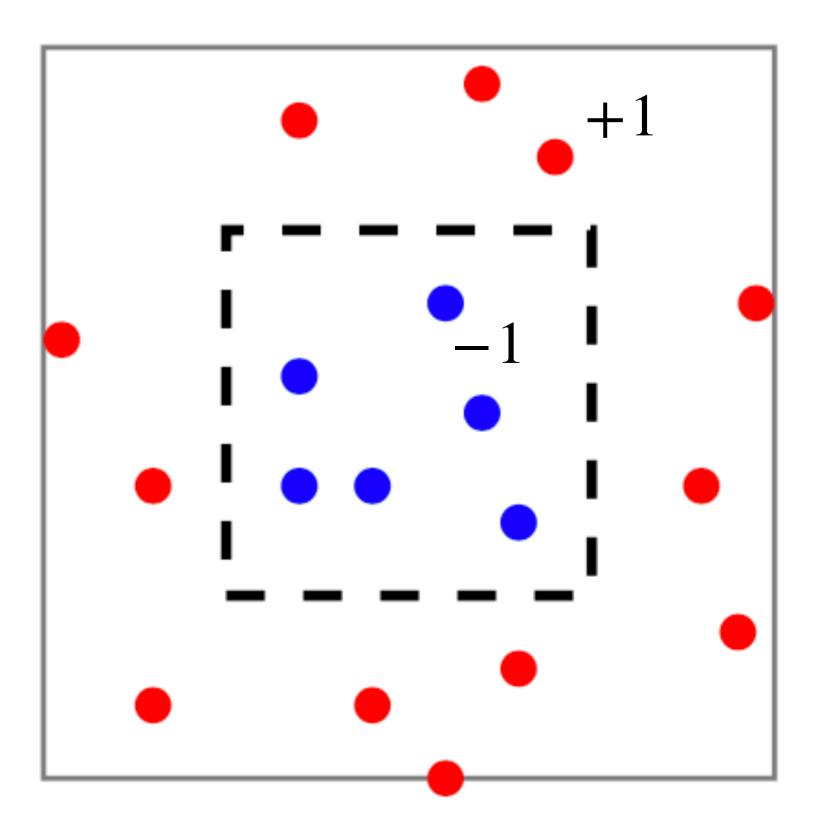
ERM with inductive bias

A common solution is to restrict the search space (i.e., hypothesis class)

$$\hat{h}_{ERM} := \arg\min_{h \in \mathscr{H}} \frac{1}{n} \sum_{i=1}^{n} \left[\ell(h(x_i), y_i) \right]$$

By restricting to \mathcal{H} , we bias towards solutions from \mathcal{H}

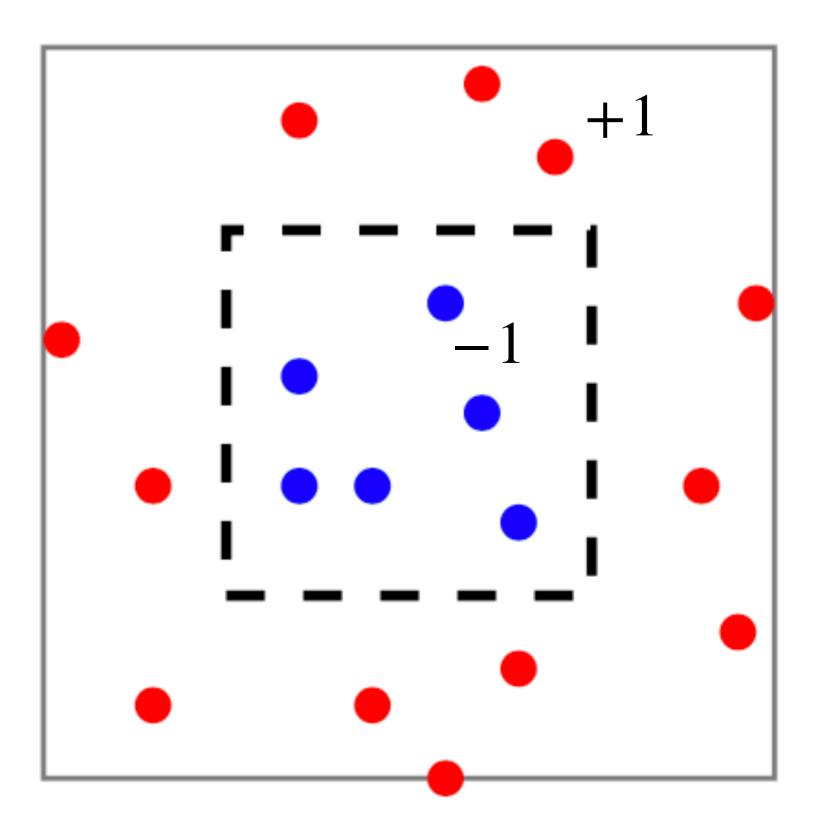




Example:

Unrestricted hypothesis class did not work;



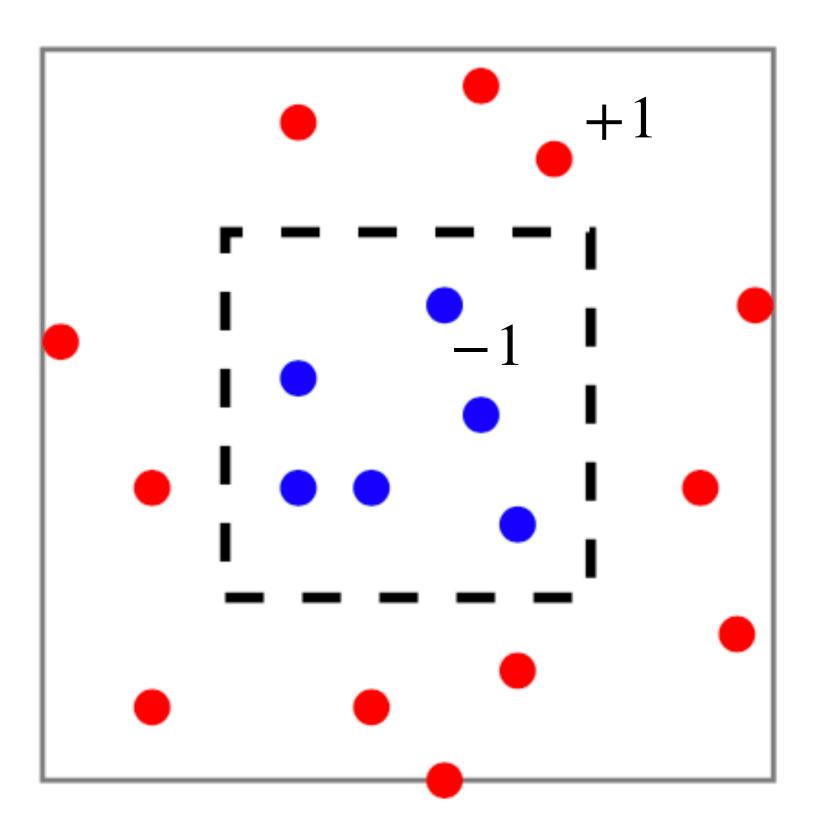


Example:

Unrestricted hypothesis class did not work;

However, if we restrict \mathscr{H} to contains ALL axis-aligned rectangles, then ERM will succeed, i.e.,





Example:

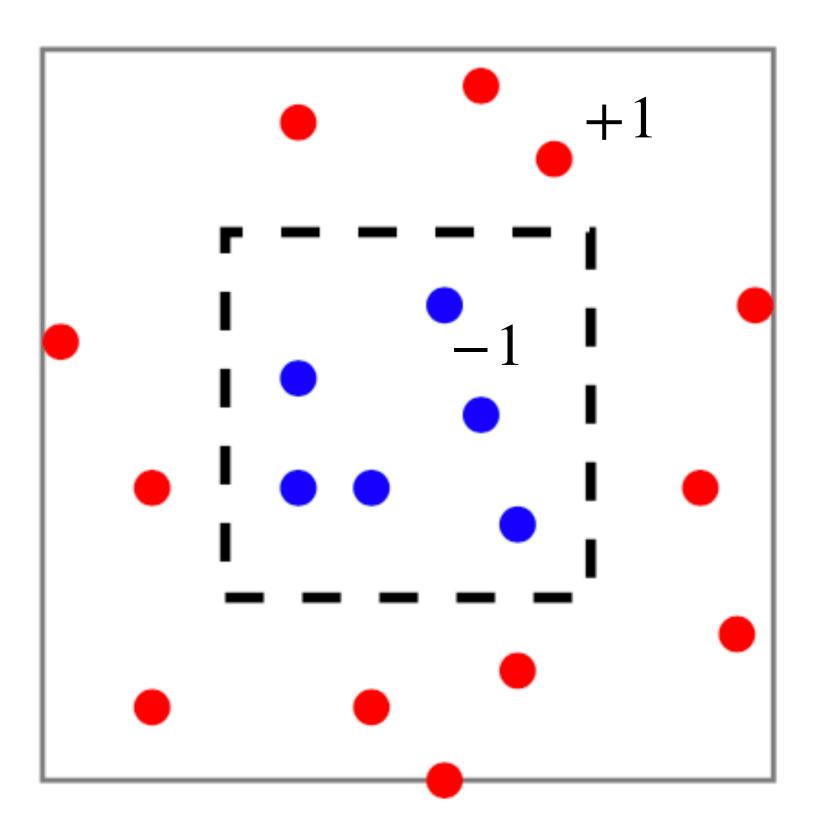
Unrestricted hypothesis class did not work;

However, if we restrict \mathscr{H} to contains ALL axis-aligned rectangles, then ERM will succeed, i.e.,

 $\mathbb{E}_{\mathcal{D}} \mid \mathbb{E}_{x, y \sim P} \mathscr{C}(\hat{h}_{ERM}(x), y)$

 $\leq \min_{h \in \mathcal{H}} \mathbb{E}_{x, y \sim P} \ell(h(x), y) + O(1/\sqrt{n})$





Example:

Unrestricted hypothesis class did not work;

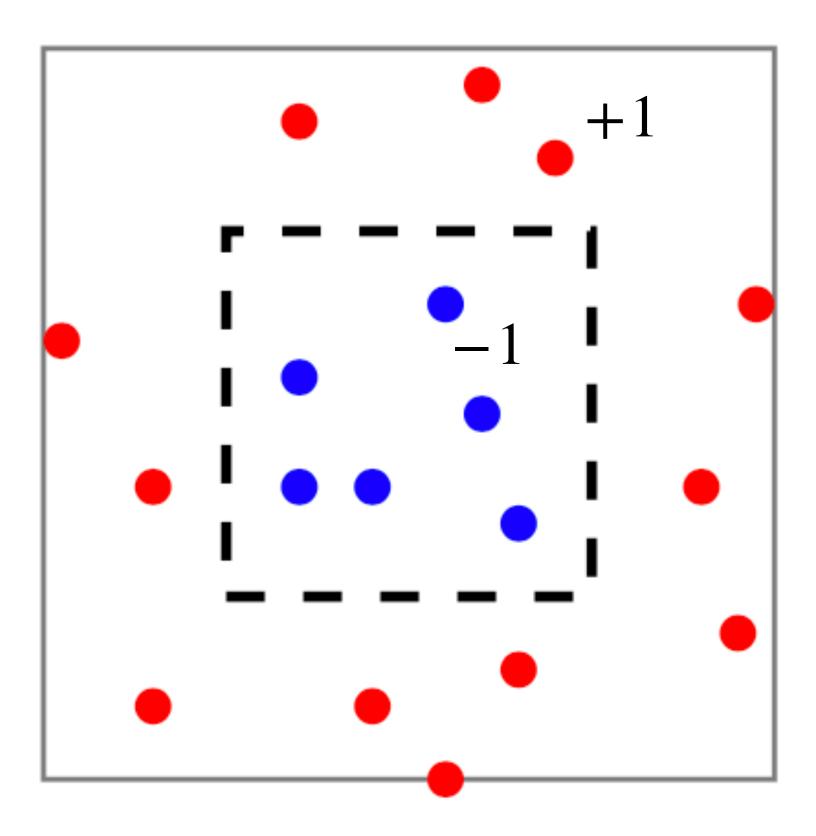
However, if we restrict \mathcal{H} to contains ALL axis-aligned rectangles, then ERM will succeed, i.e.,

 $\mathbb{E}_{\mathcal{D}} \mid \mathbb{E}_{x, y \sim P} \mathscr{C}(\hat{h}_{ERM}(x), y)$

 $\leq \min_{h \in \mathcal{H}} \mathbb{E}_{x, y \sim P} \ell(h(x), y) + O(1/\sqrt{n})$

 $\leq O(1/\sqrt{n})$





Example:

Unrestricted hypothesis class did not work;

However, if we restrict \mathscr{H} to contains ALL axis-aligned rectangles, then ERM will succeed, i.e.,

 $\mathbb{E}_{\mathcal{D}} \mid \mathbb{E}_{x, y \sim P} \mathscr{C}(\hat{h}_{ERM}(x), y)$

 $\leq \min_{h \in \mathcal{H}} \mathbb{E}_{x, y \sim P} \ell(h(x), y) + O(1/\sqrt{n})$

 $\leq O(1/\sqrt{n})$

(Exact proof out of the scope of this class — see CS 4783/5783)



Summary so far

To guarantee small test error, we need to restrict \mathcal{H}

ERM with unrestricted hypothesis class could fail (i.e., overfitting)

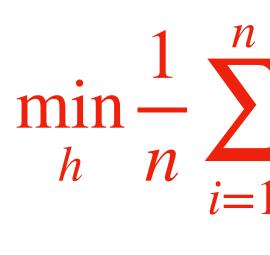
Outline for Today

3. Regularization

1. Empirical Risk Minimization

2. Examples on loss & hypothesis classes

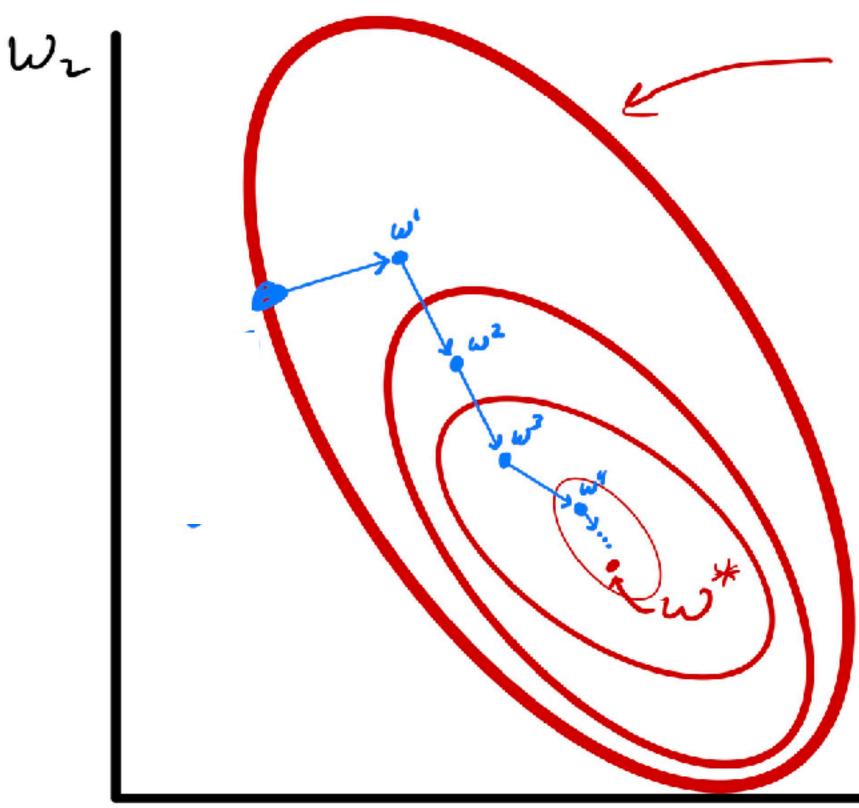
ERM with restricted hypothesis class



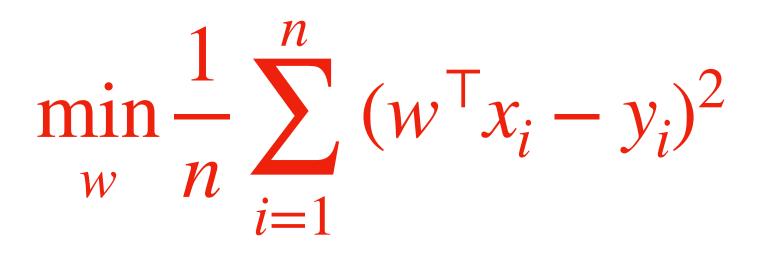
- $\min_{h} \frac{1}{n} \sum_{i=1}^{n} \left[\ell(h(x_i), y_i) \right]$
 - s.t. $h \in \mathcal{H}$

Let's go through several examples on Constraints under the linear regression context

Linear Regression: squared loss + ℓ_2 constraint

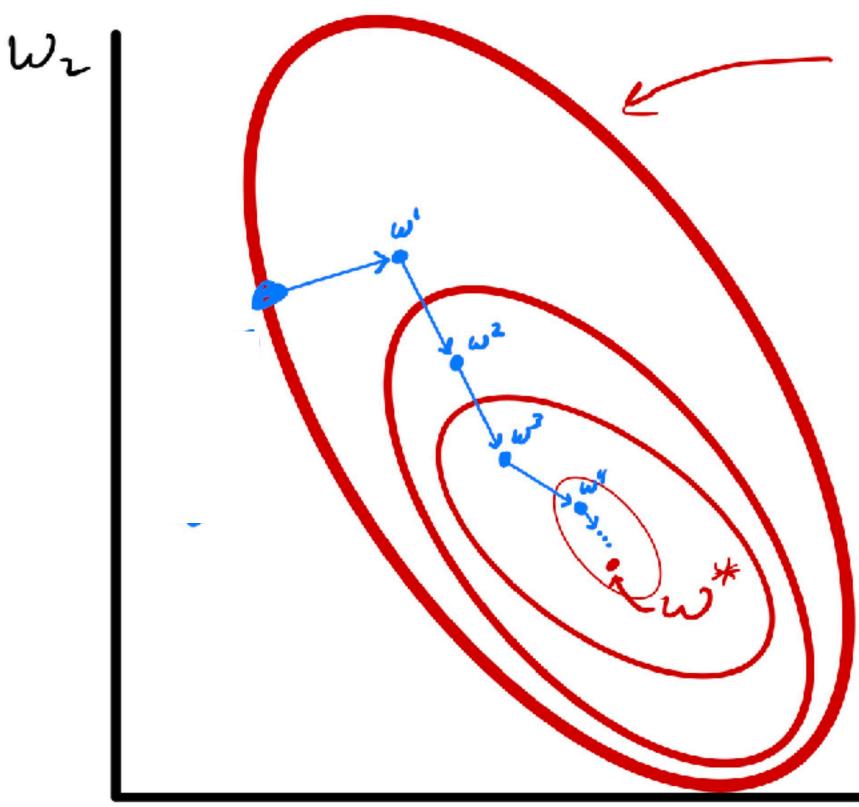


- Level sets of L(w)





Linear Regression: squared loss + ℓ_2 constraint

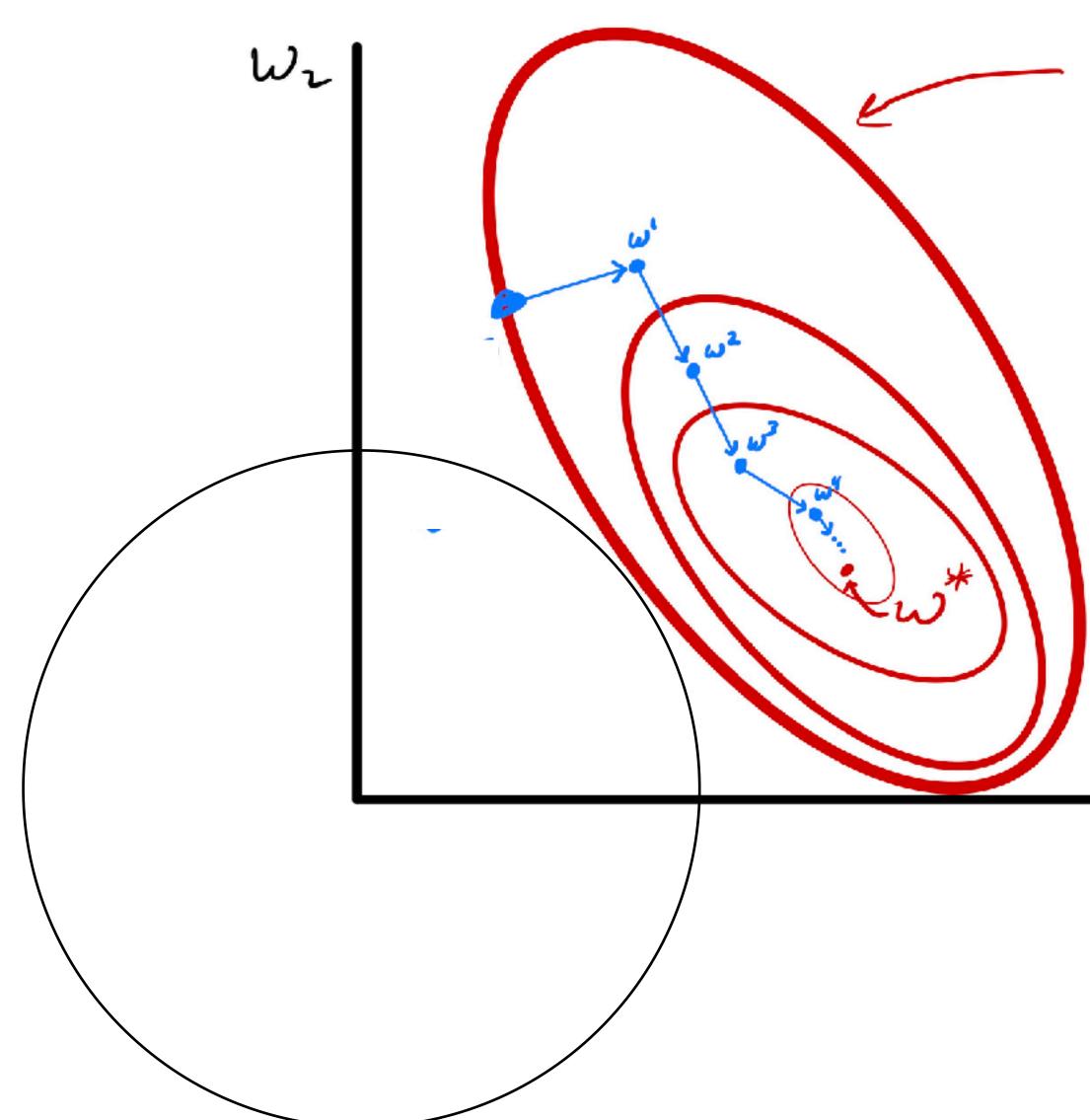


- Level sets of L(w)

$\min_{w} \frac{1}{n} \sum_{i=1}^{n} (w^{\mathsf{T}} x_{i} - y_{i})^{2}$ s.t. $||w||_{2}^{2} \leq B$

 ω

Linear Regression: squared loss + ℓ_2 constraint

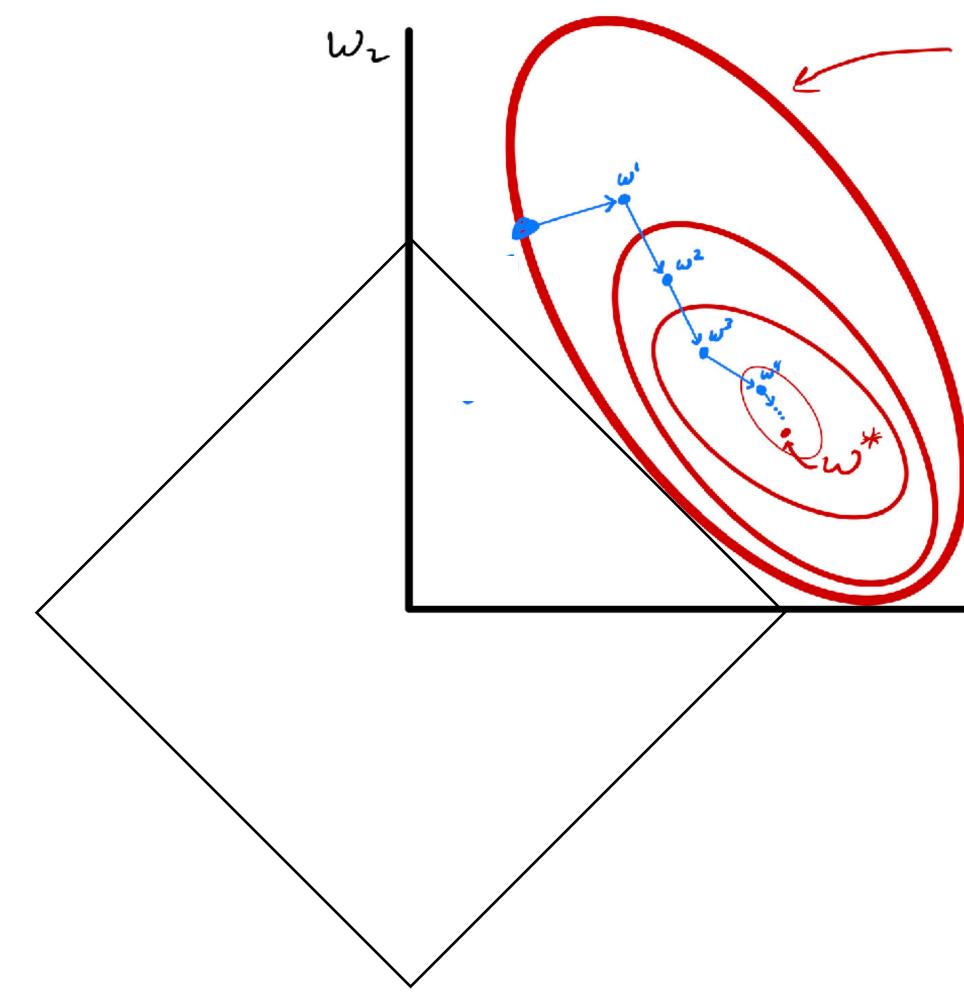


- Level sets of L(w)

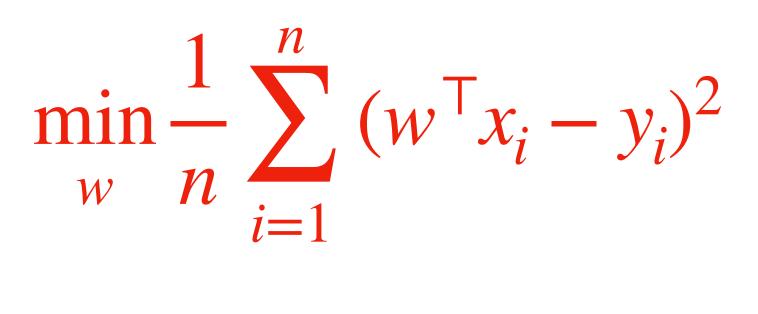
$\min_{w} \frac{1}{n} \sum_{i=1}^{n} (w^{\mathsf{T}} x_{i} - y_{i})^{2}$ s.t. $||w||_{2}^{2} \leq B$

 ω

Linear Regression: squared loss + ℓ_1 constraint



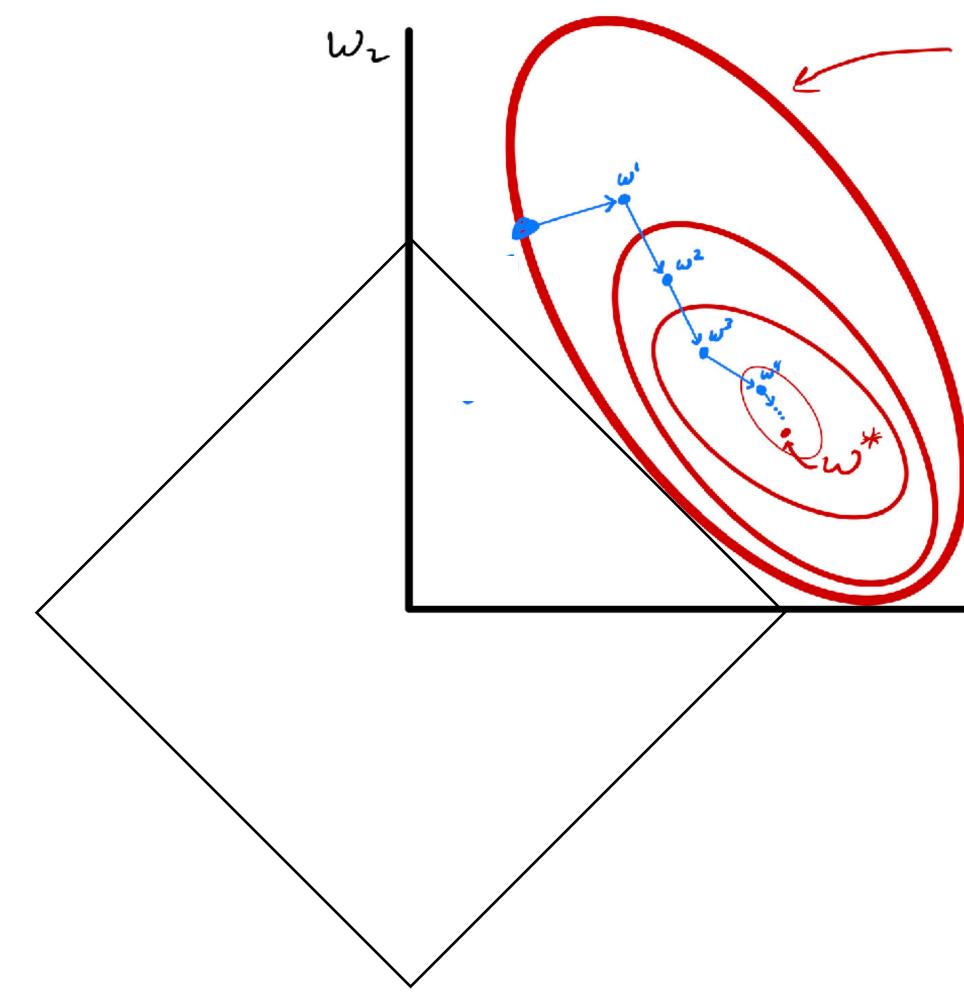
- Level sets of L(w)



s.t. $\|w\|_1 \le B$

W

Linear Regression: squared loss + ℓ_1 constraint



- Level sets of L(w)

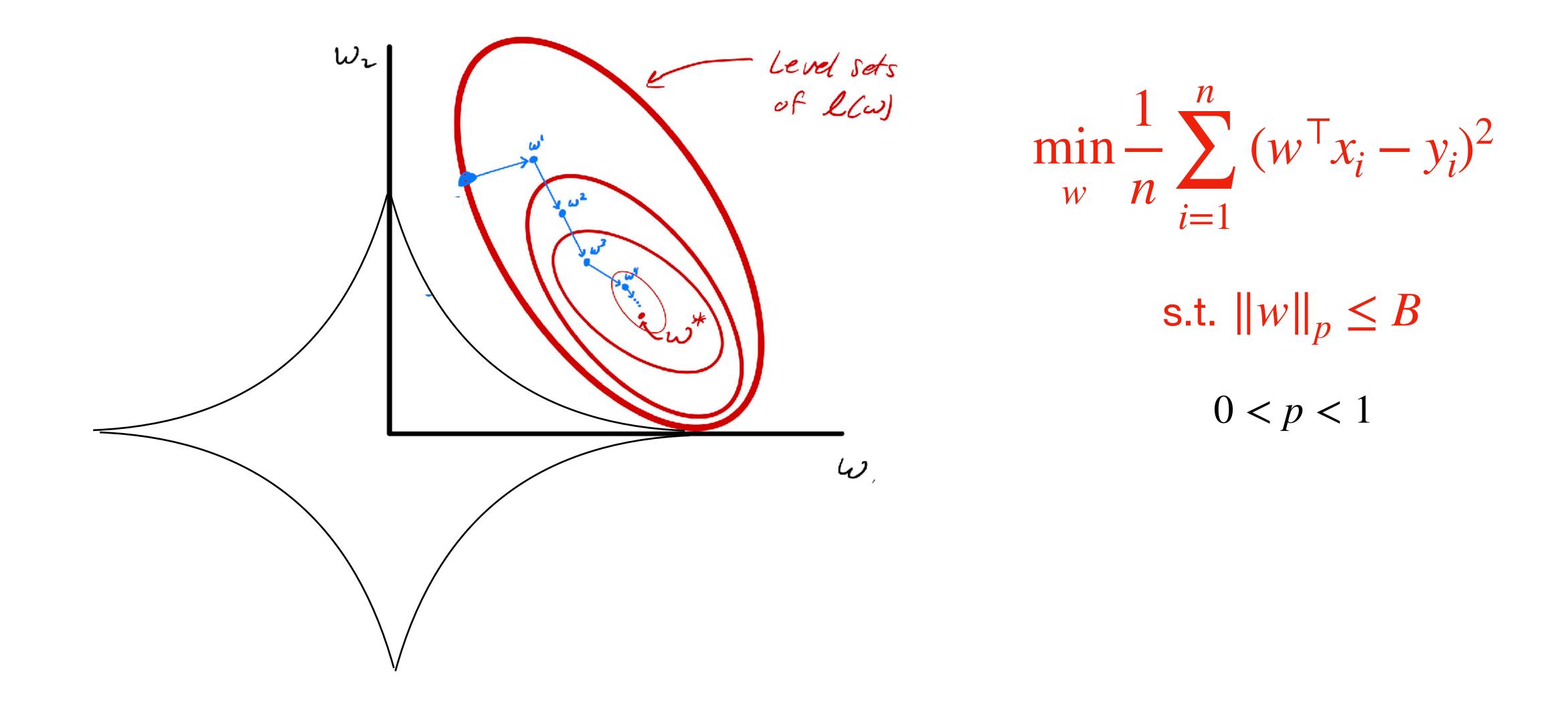
$$\min_{w} \frac{1}{n} \sum_{i=1}^{n} (w^{\mathsf{T}} x_{i} - y_{i})^{2}$$

s.t. $||w||_{1} \le B$

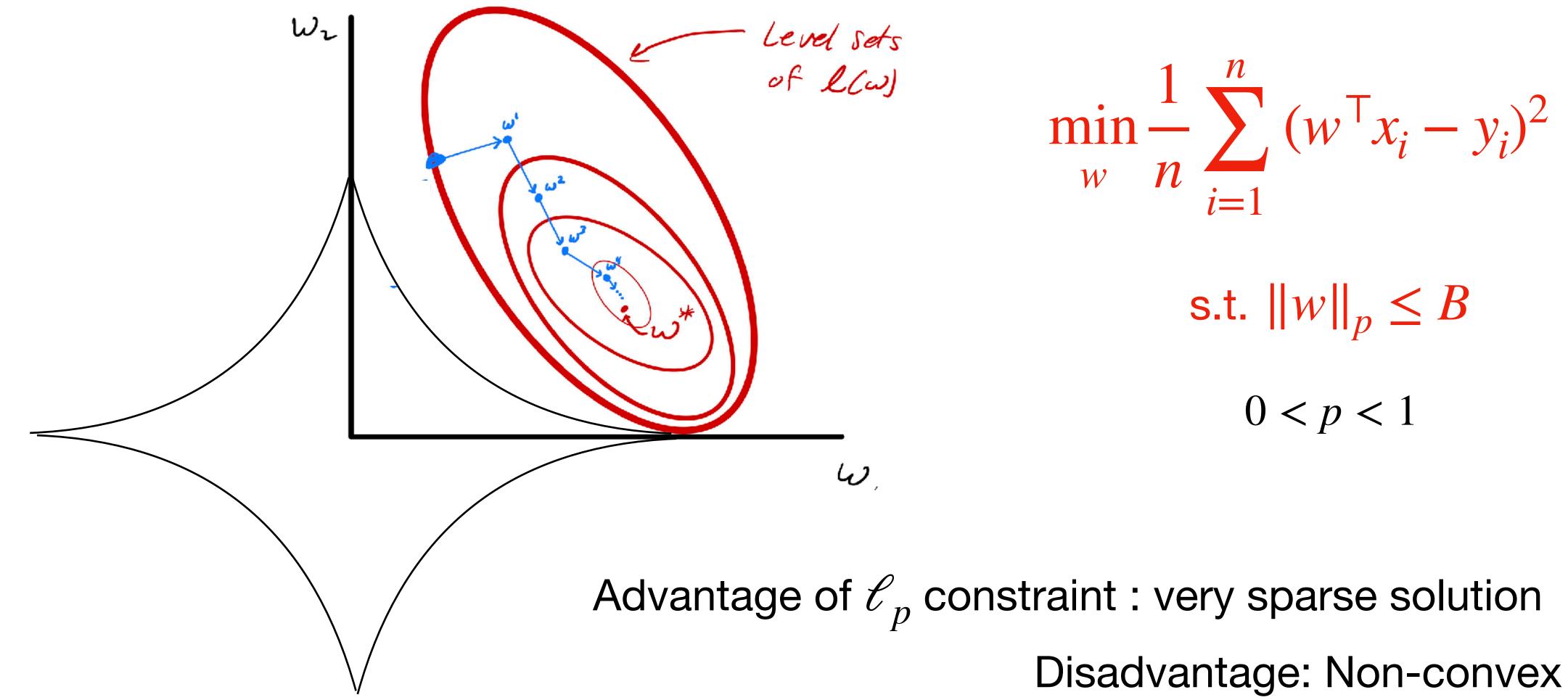
 ω_{j}

Advantage: give sparse solution

Linear Regression: squared loss + ℓ_p constraint

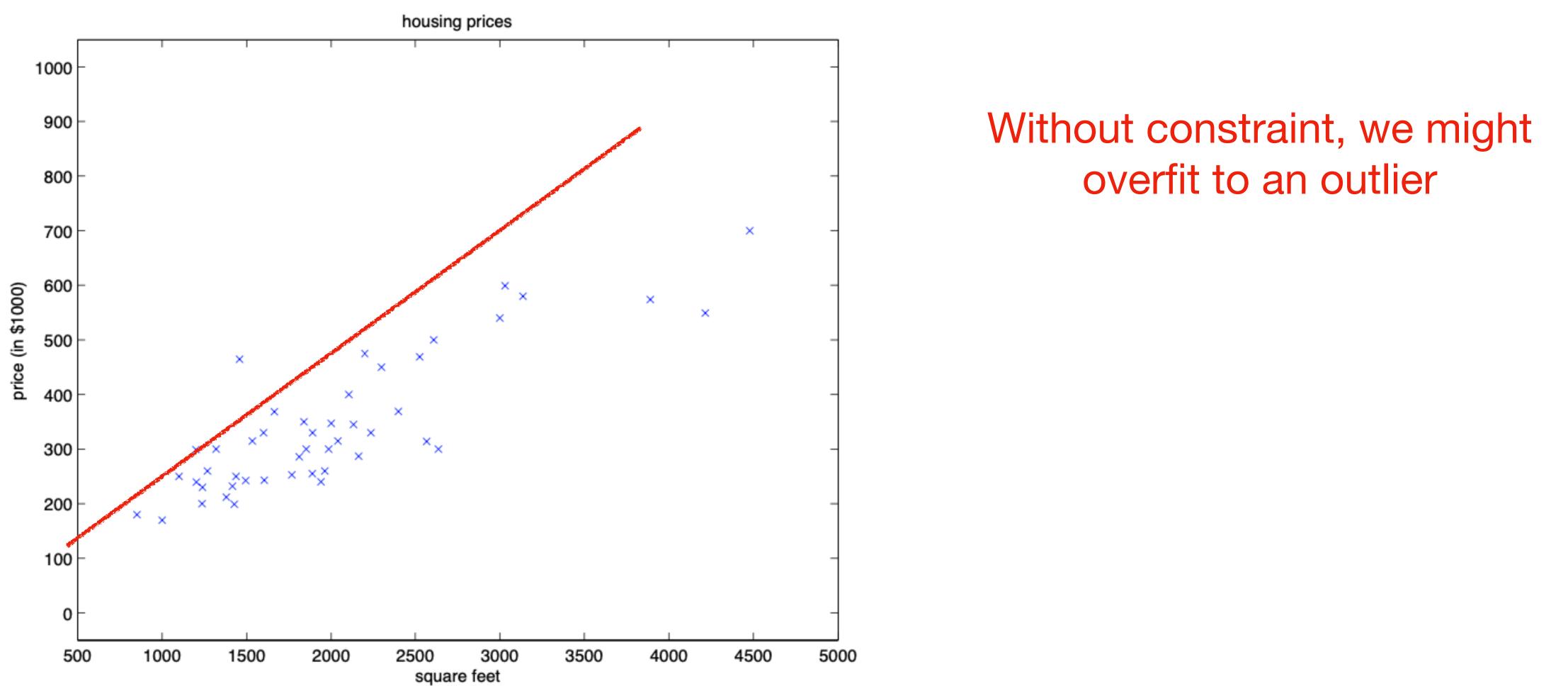


Linear Regression: squared loss + ℓ_p constraint

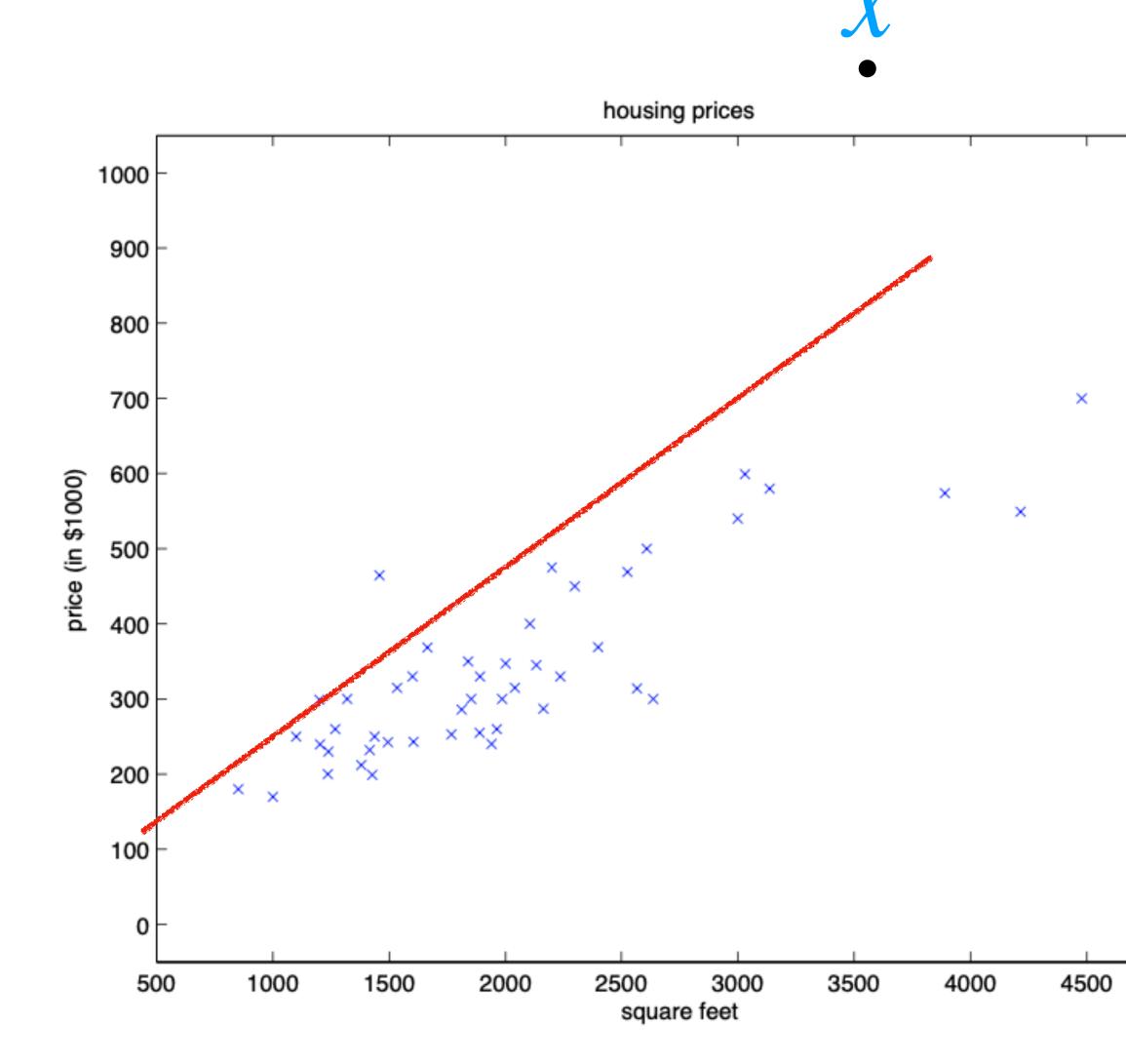


Disadvantage: Non-convex

X



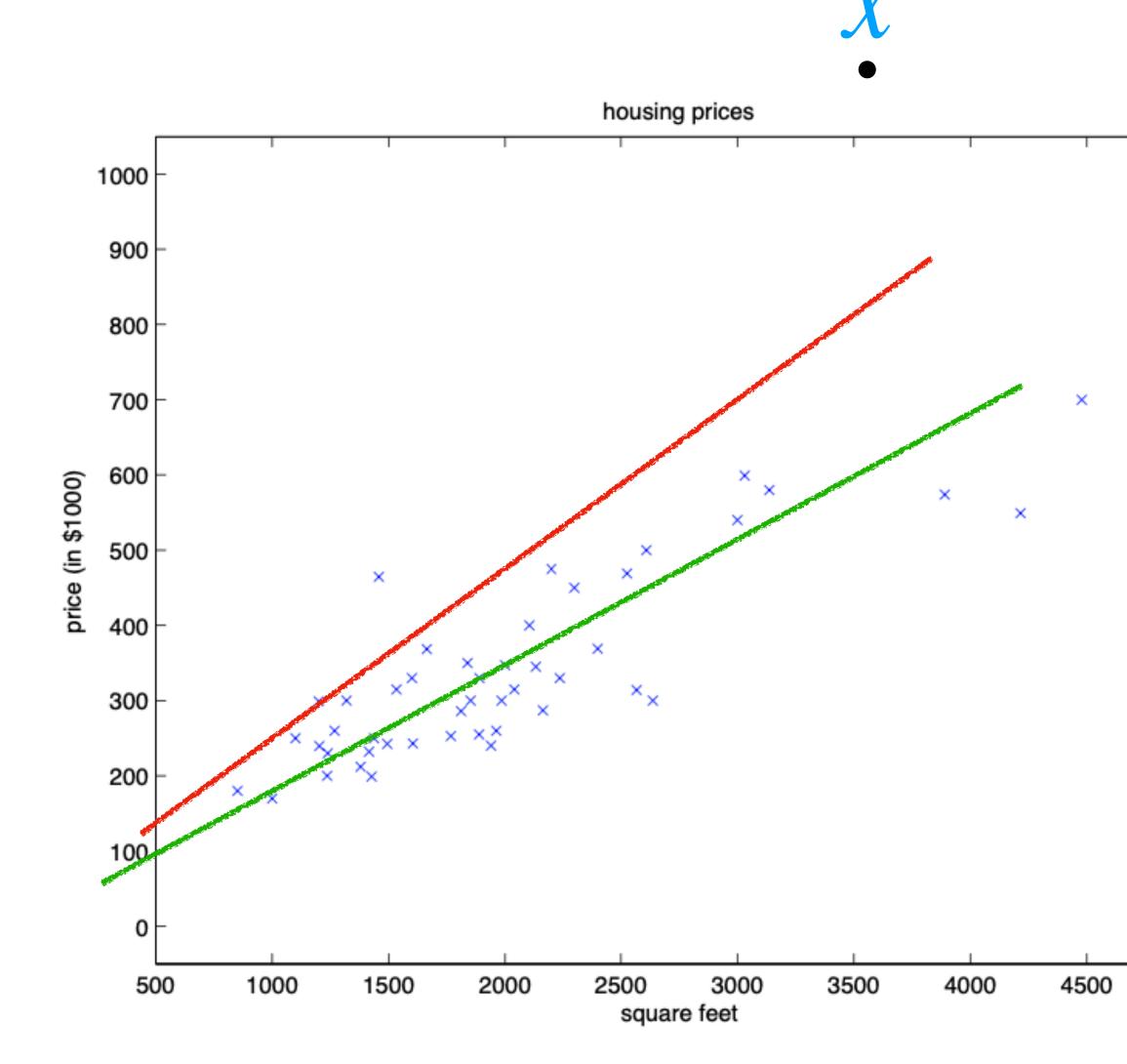
5000





With constraint $||w||_2^2 \le B$, we can avoid overfitting (i.e., force us to not pay too much attention to minimizing loss)

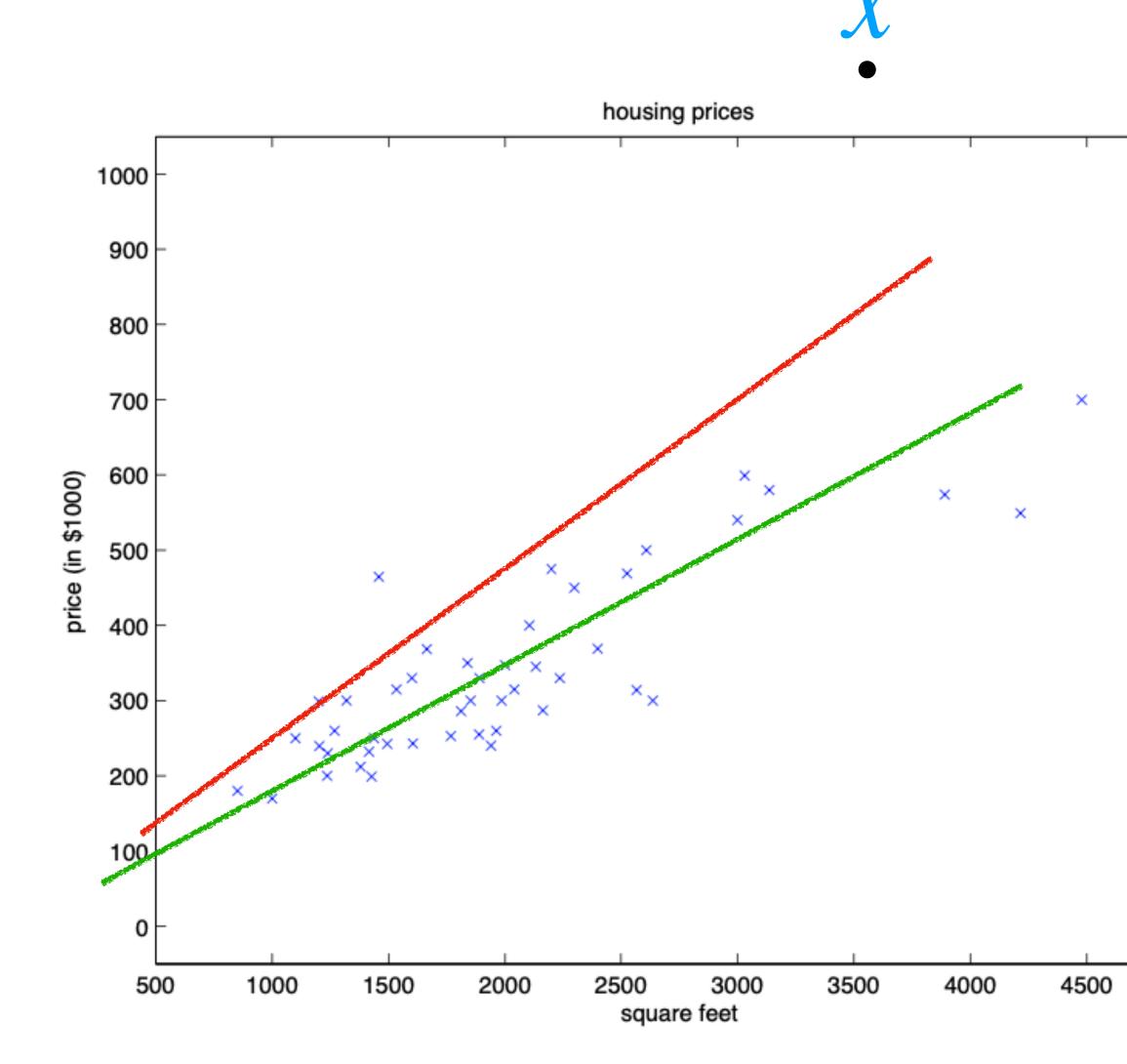
5000





With constraint $||w||_2^2 \le B$, we can avoid overfitting (i.e., force us to not pay too much attention to minimizing loss)

5000



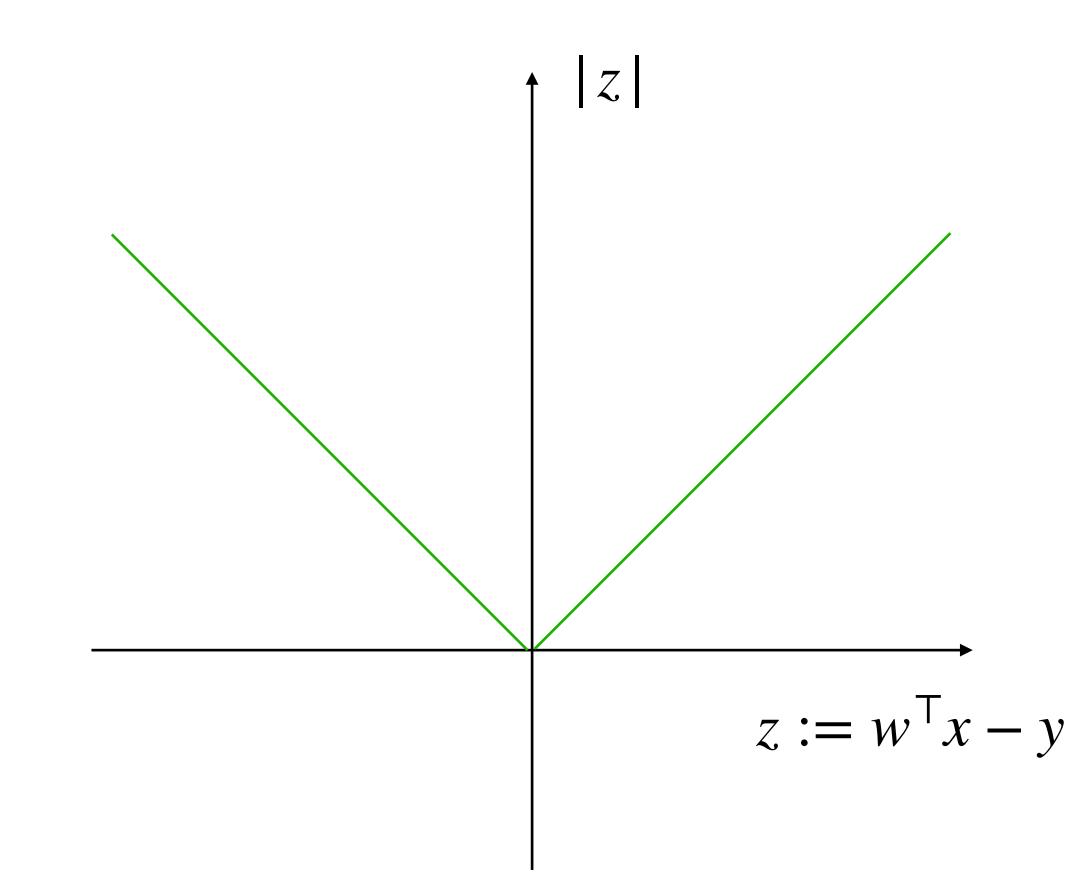


With constraint $||w||_2^2 \leq B$, we can avoid overfitting (i.e., force us to not pay too much attention to minimizing loss)

(More details in next lecture)

Absolute loss:

$$\min_{w} \frac{1}{n} \sum_{i=1}^{n} |w^{\mathsf{T}} x_{i} - y_{i}|$$
s.t. $R(w) \leq B$

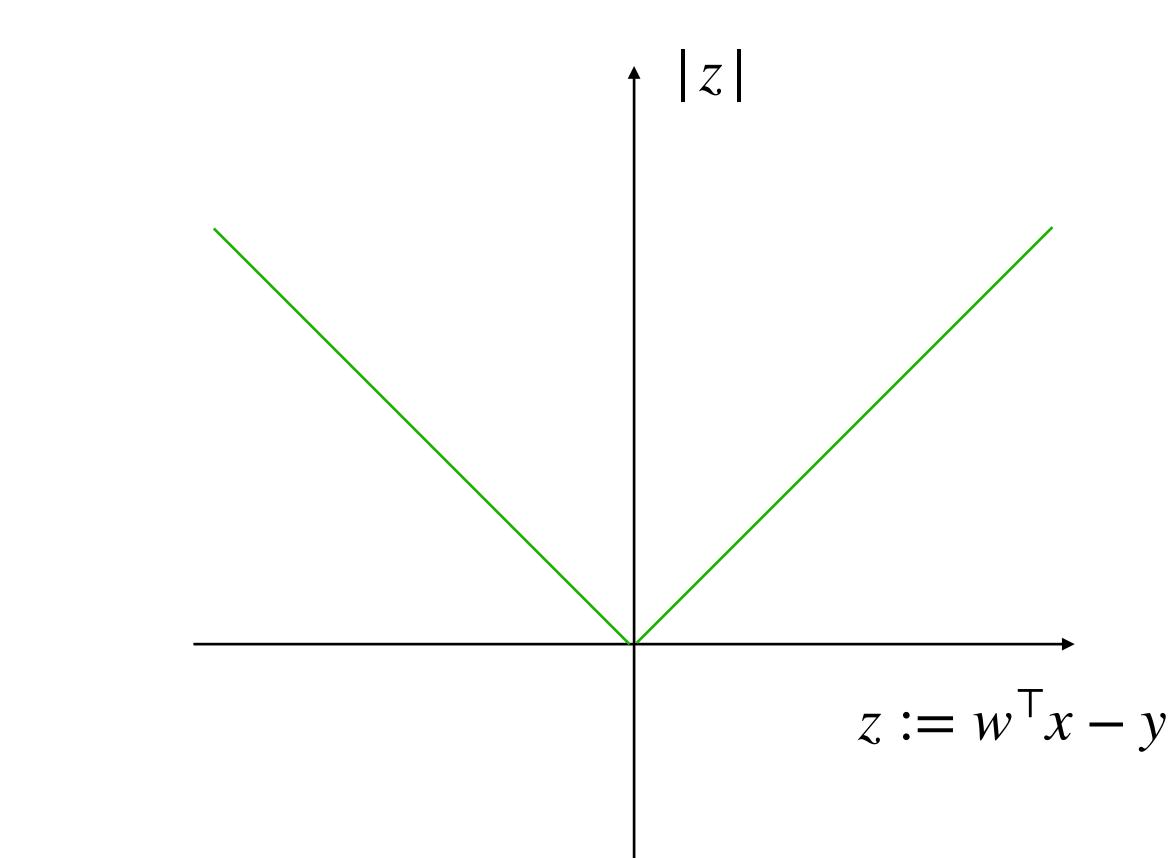




Absolute loss:

$$\min_{w} \frac{1}{n} \sum_{i=1}^{n} |w^{\mathsf{T}} x_{i} - y_{i}|$$
s.t. $R(w) \leq B$

Advantage: less sensitive to outliers





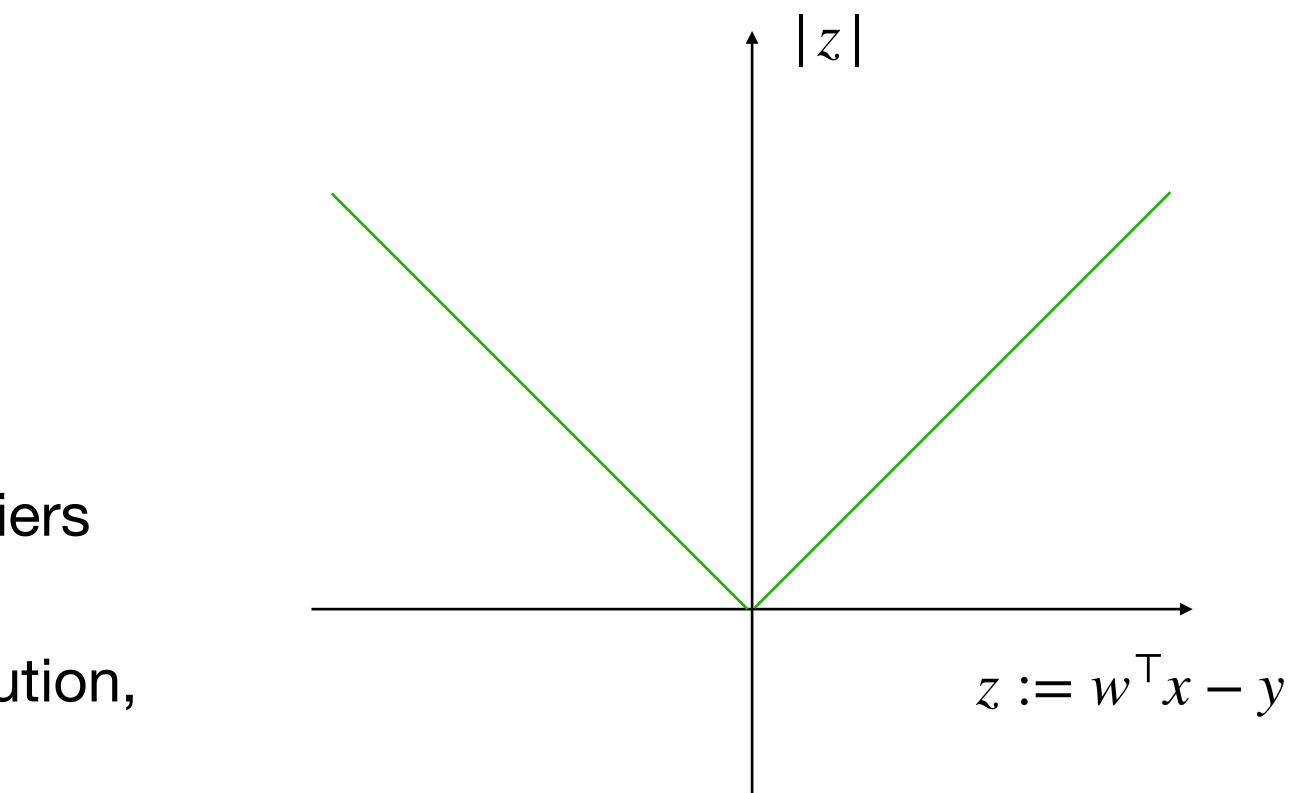
Absolute loss:

$$\min_{w} \frac{1}{n} \sum_{i=1}^{n} |w^{\mathsf{T}} x_{i} - y_{i}|$$

s.t. $R(w) \leq B$

Advantage: less sensitive to outliers

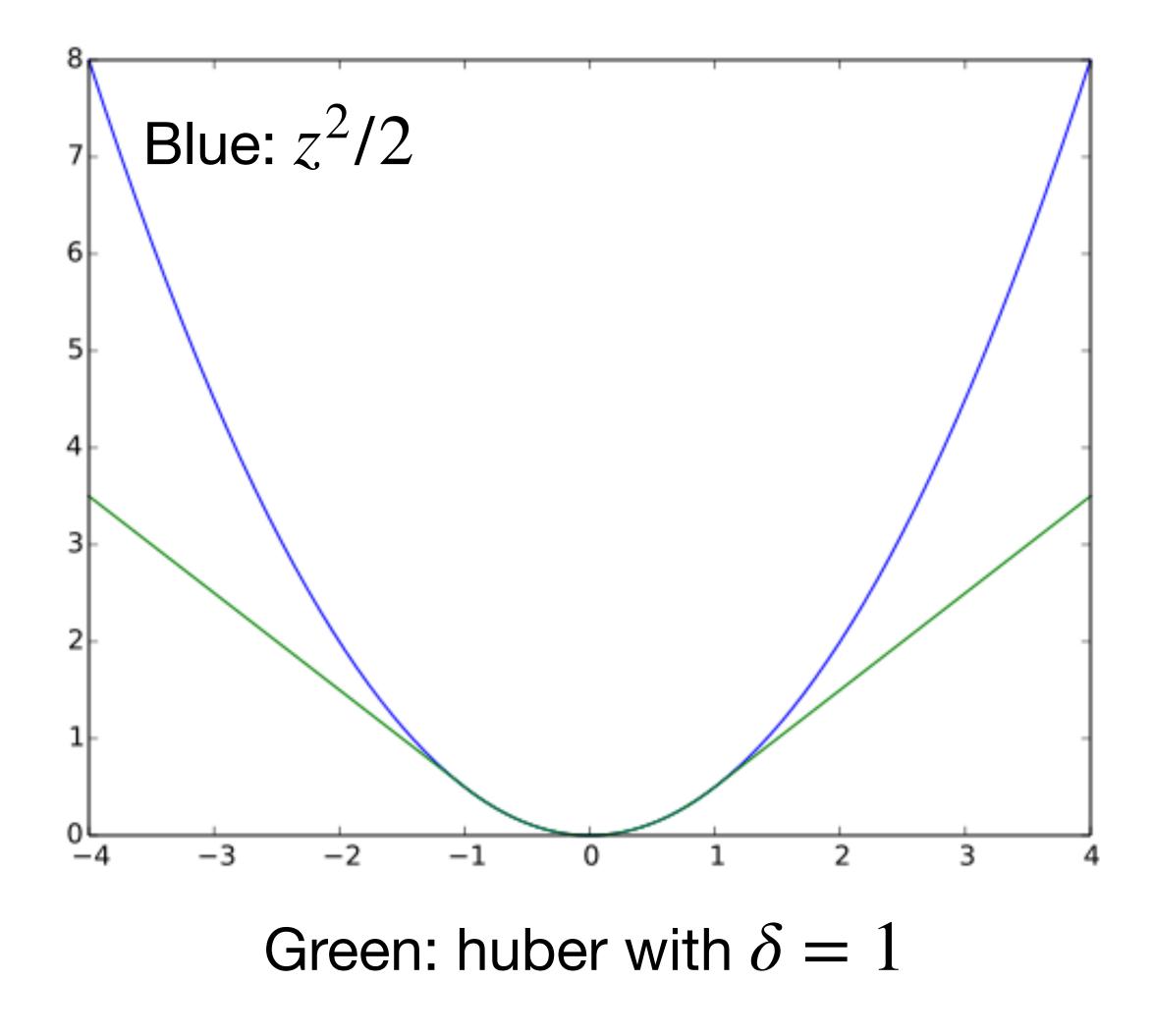
Disadvantage: no closed-form solution, non-differentiable at 0





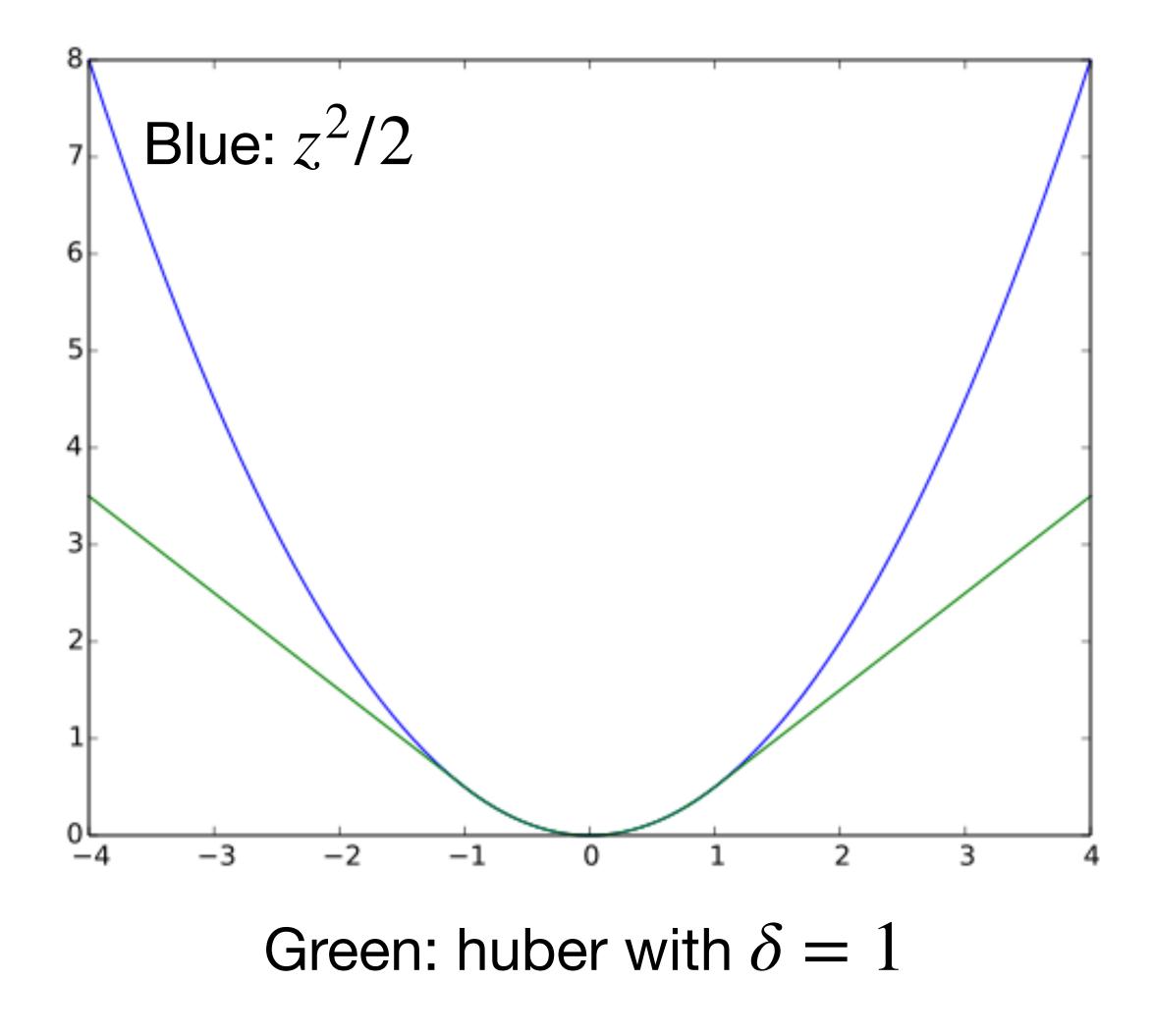
Huber loss: $\min_{w} \frac{1}{n} \sum_{i=1}^{n} L_{\delta}(w^{\mathsf{T}}x - y)$ s.t. $R(w) \leq B$

Where $L_{\delta}(z) = \begin{cases} z^2/2 & |z| \le \delta \\ \delta(|z| - \delta/2) & \text{else} \end{cases}$



Huber loss: $\min_{w} \frac{1}{n} \sum_{i=1}^{n} L_{\delta}(w^{\mathsf{T}}x - y)$ s.t. $R(w) \leq B$ Where $L_{\delta}(z) = \begin{cases} z^2/2 & |z| \le \delta \\ \delta(|z| - \delta/2) & \text{else} \end{cases}$

Advantage: best of both worlds

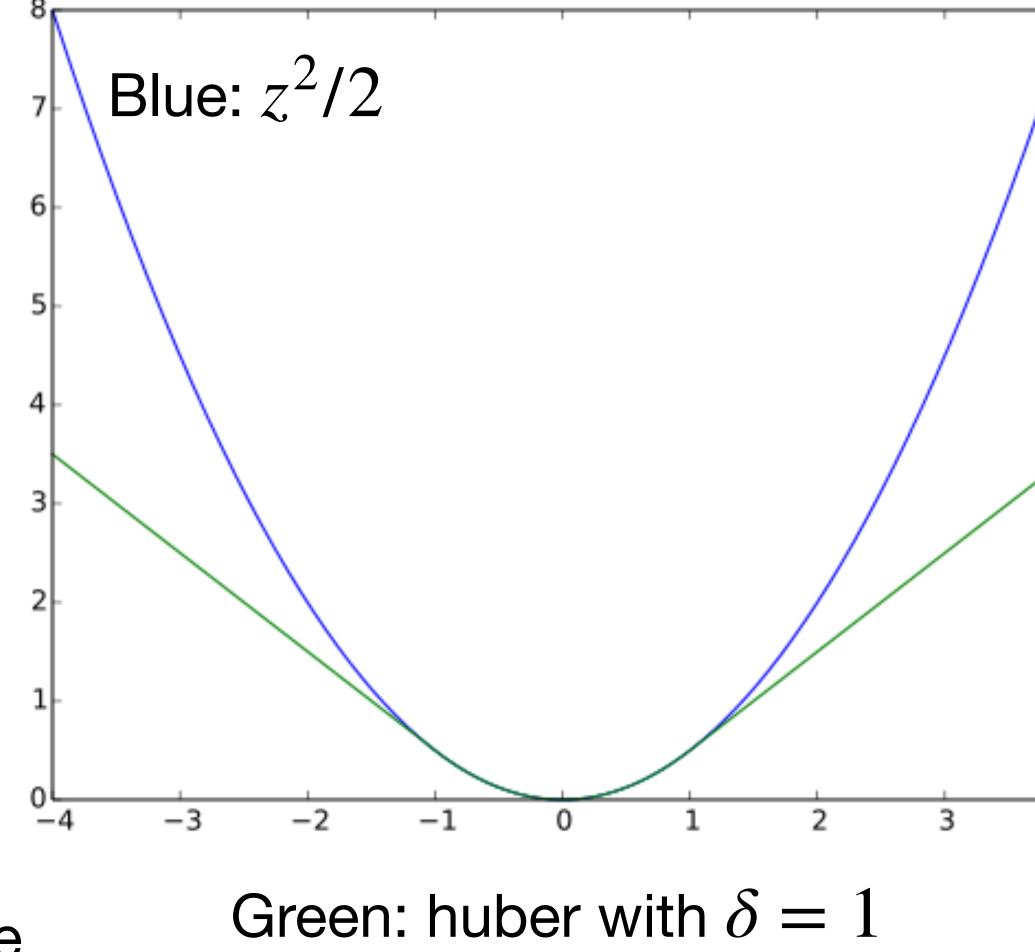


Huber loss: $\min_{w} \frac{1}{n} \sum_{i=1}^{n} L_{\delta}(w^{\mathsf{T}}x - y)$ s.t. $R(w) \leq B$ Where

$$L_{\delta}(z) = \begin{cases} z^2/2 & |z| \le \delta \\ \delta(|z| - \delta/2) & \text{else} \end{cases}$$

Advantage: best of both worlds

Disadvantage: additional parameter δ to tune

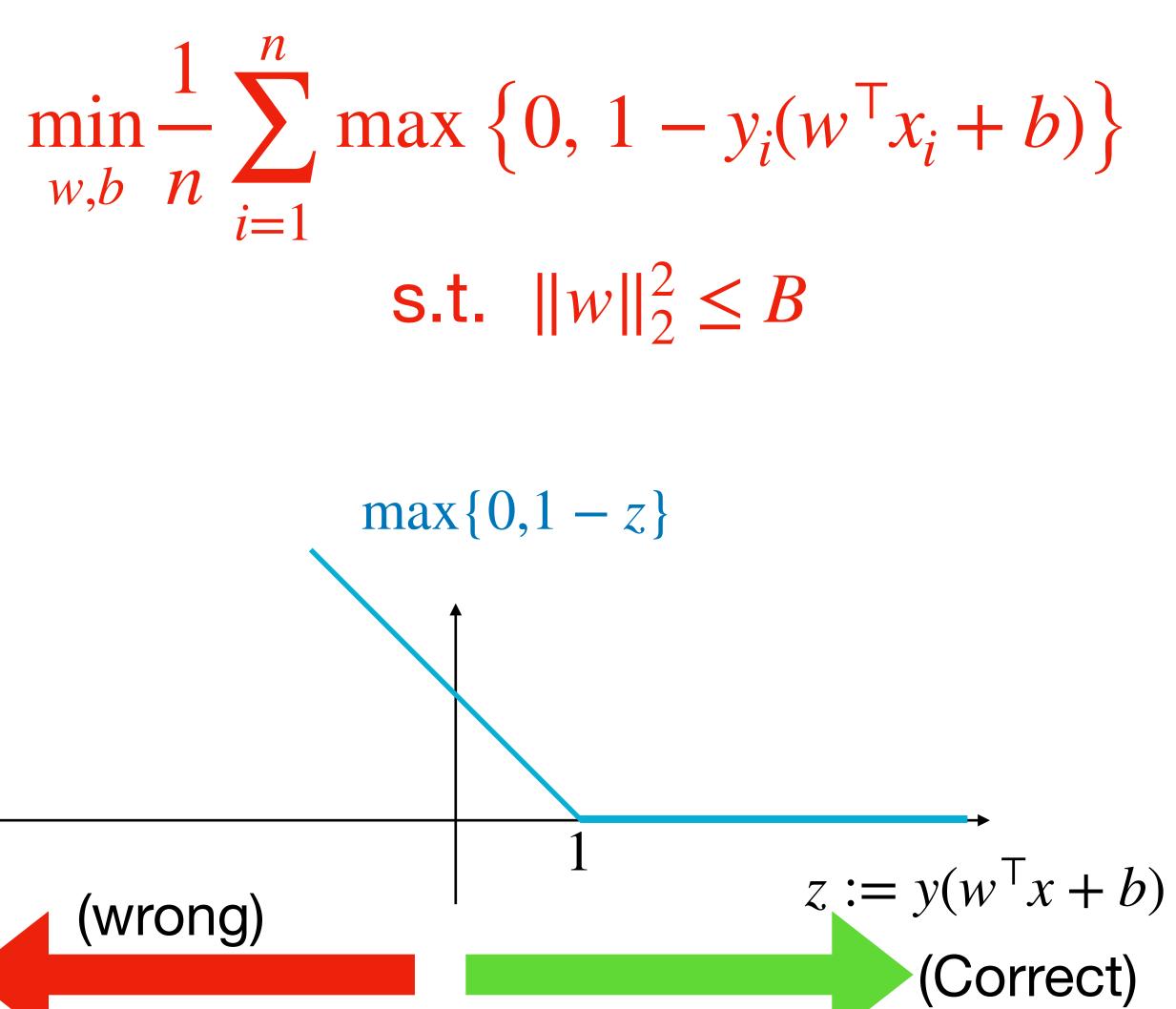




Linear classification: Hinge loss + constraint

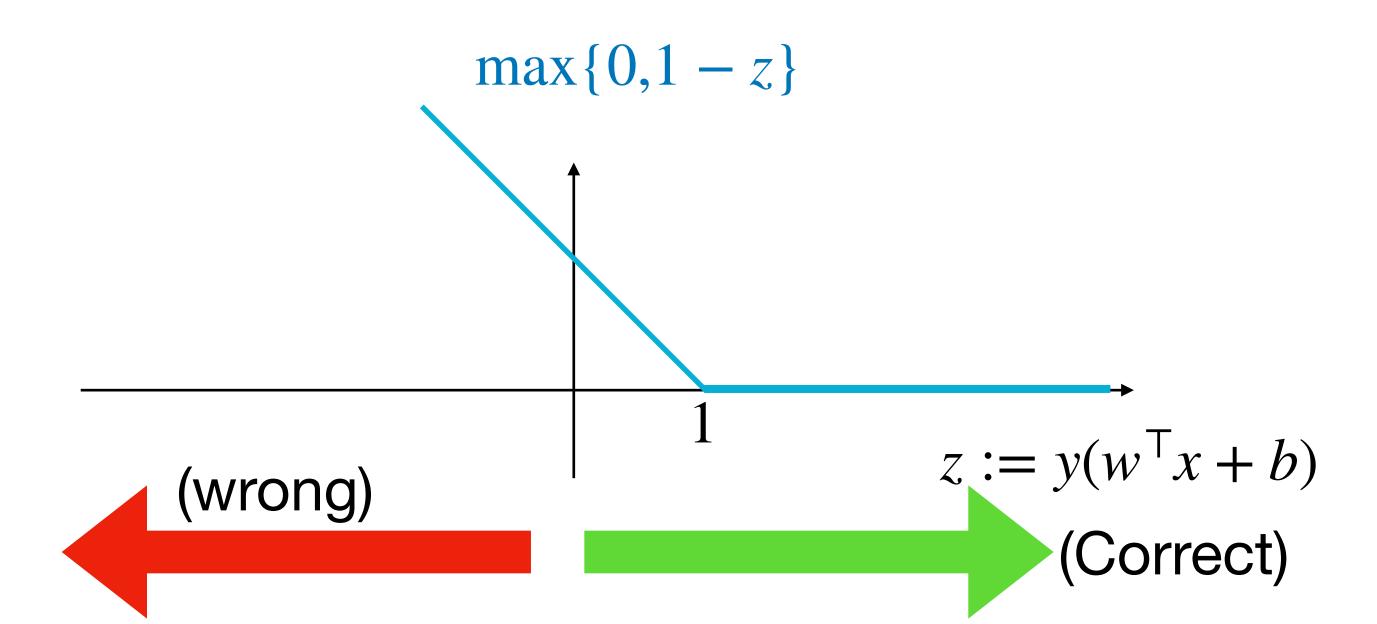
 $\min_{w,b} \frac{1}{n} \sum_{i=1}^{n} \max\left\{0, 1 - y_i(w^{\mathsf{T}}x_i + b)\right\}$ **s.t.** $||w||_2^2 \le B$

Linear classification: Hinge loss + constraint

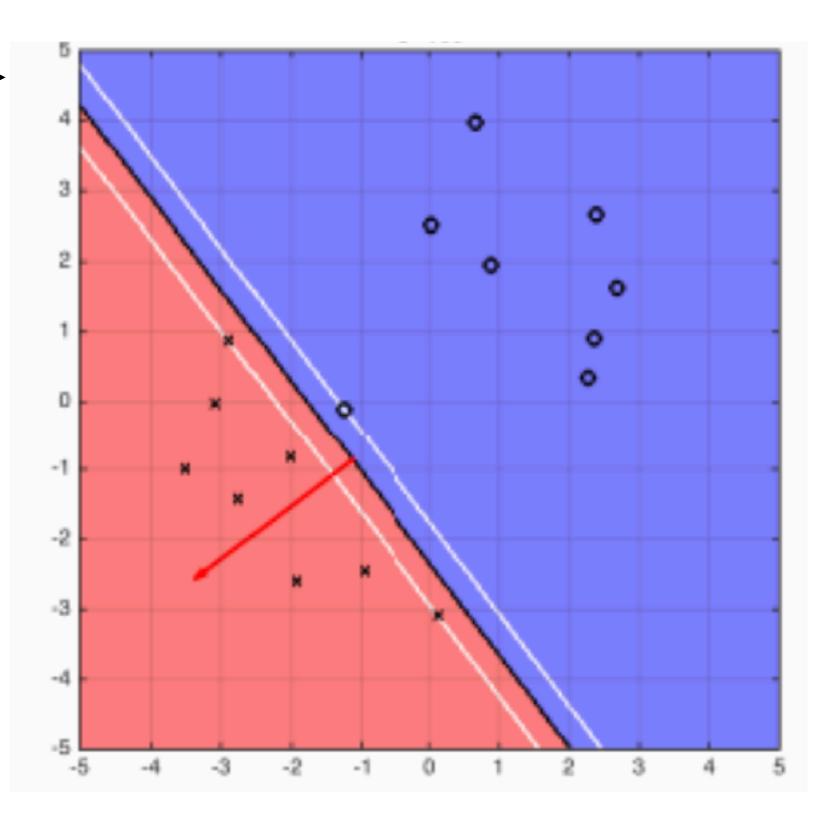


Linear classification: Hinge loss + constraint

$$\min_{w,b} \frac{1}{n} \sum_{i=1}^{n} \max\left\{0, \ 1 - y_i(w^{\top}x_i + b)\right\}$$
s.t. $||w||_2^2 \le B$



Constraint avoids overfit: (Recall: small $||w||_2$ should have large street width)

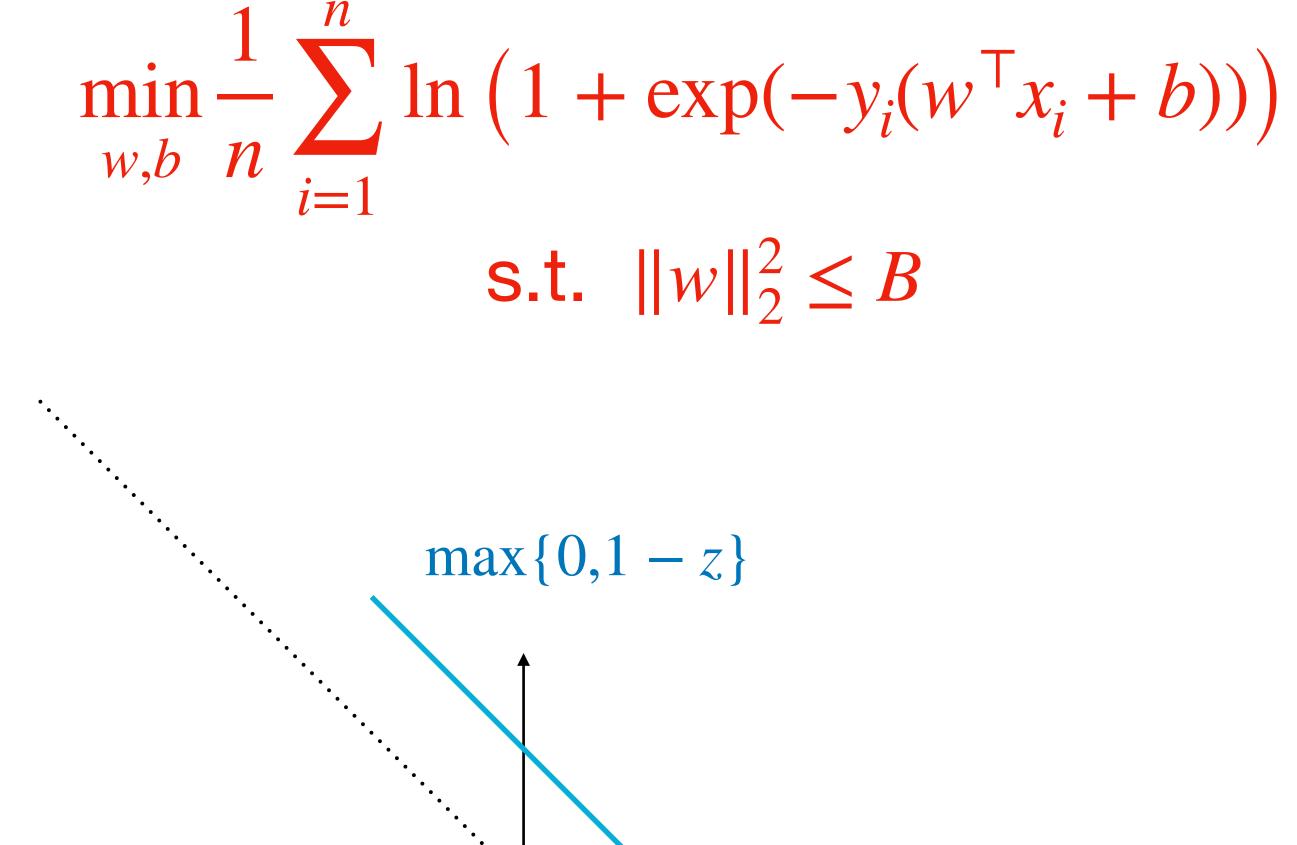


Linear classification: Log-loss + constraints

 $\min_{w,b} \frac{1}{n} \sum_{i=1}^{n} \ln\left(1 + \exp(-y_i(w^{\mathsf{T}}x_i + b))\right)$

- **s.t.** $||w||_2^2 \le B$

Linear classification: Log-loss + constraints



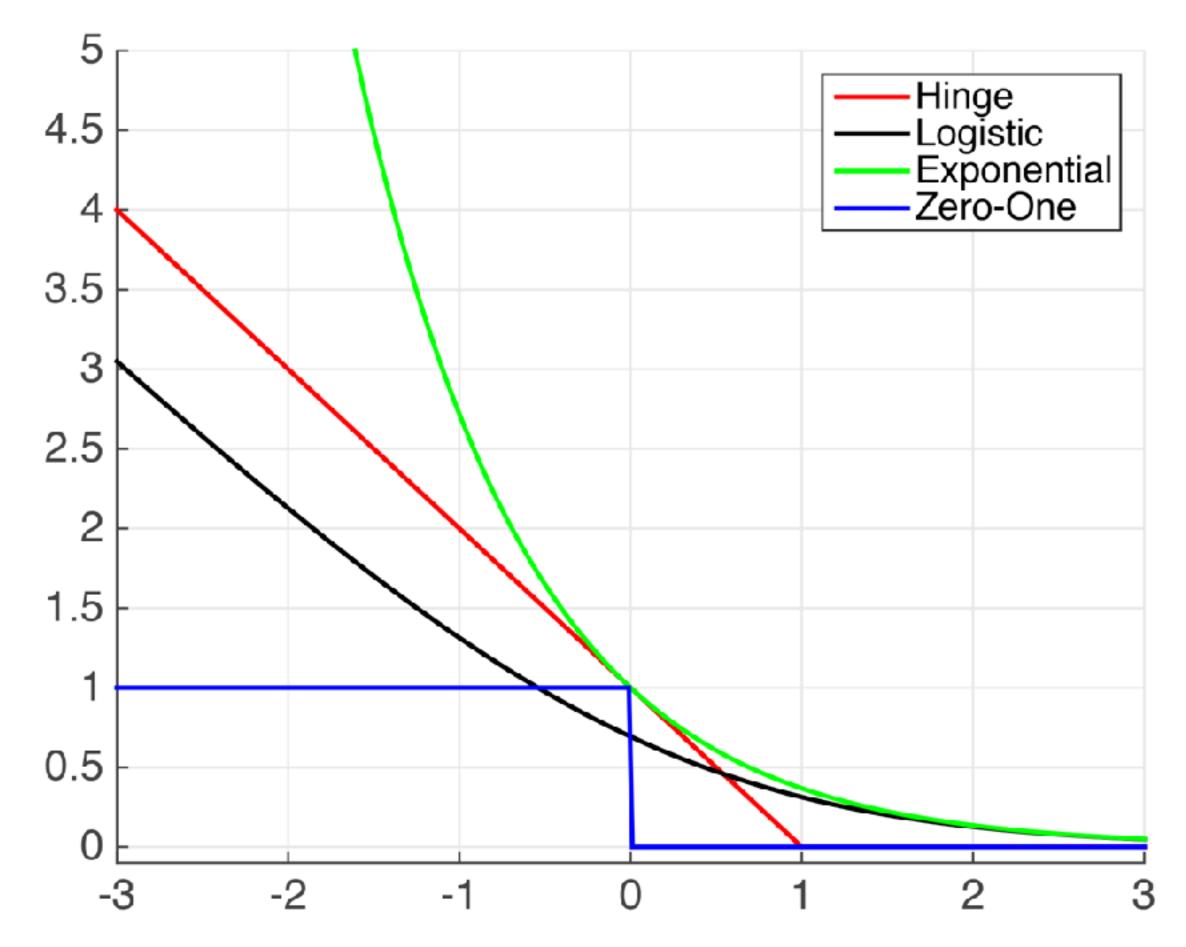
- **s.t.** $||w||_2^2 \le B$

 $z := y(w^{\top}x + b)$

Linear classification: Exponential loss + constraints

$$\min_{w,b} \frac{1}{n} \sum_{i=1}^{n} \exp\left(-y_i(w^{\mathsf{T}}x_i+b)\right)$$

s.t. $||w||_2^2 \le B$

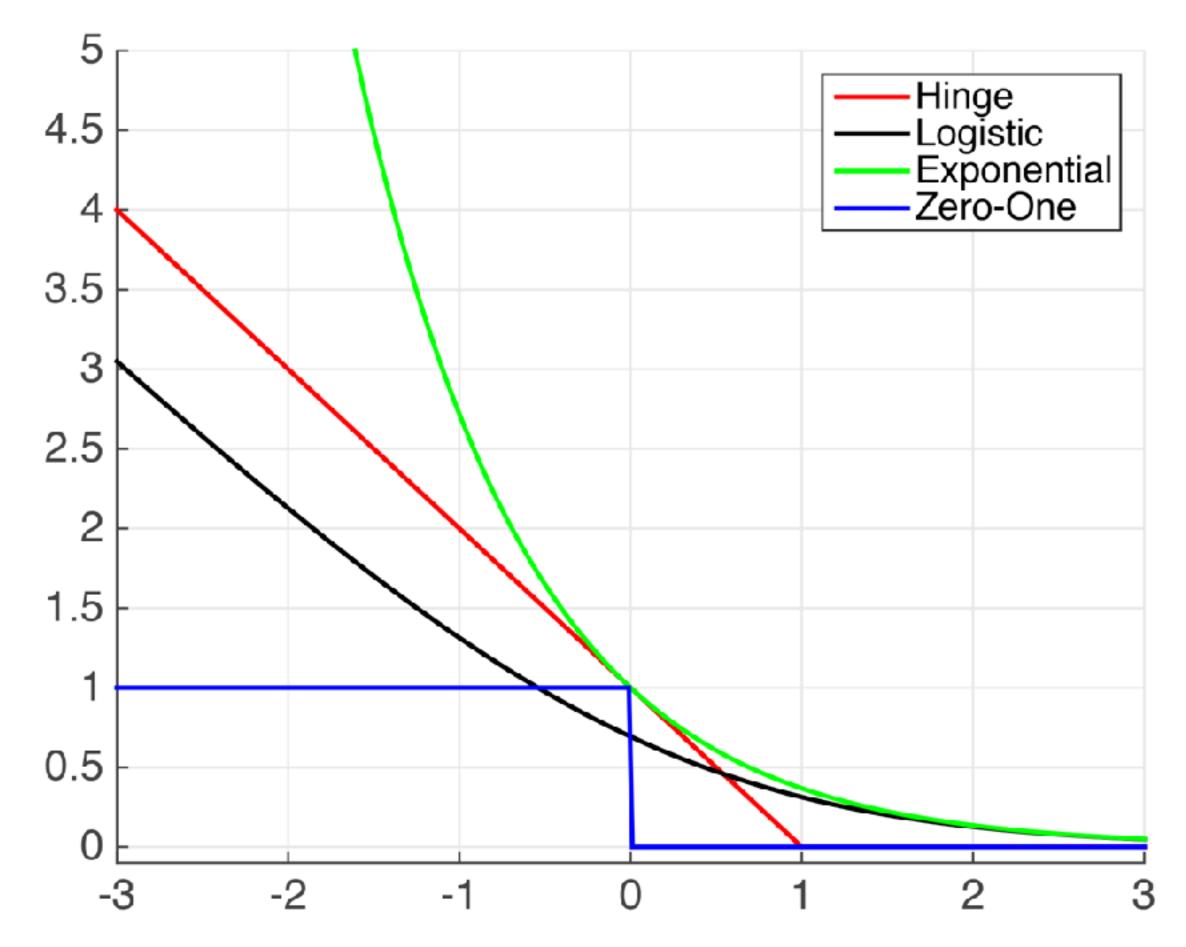


Linear classification: Exponential loss + constraints

$$\min_{w,b} \frac{1}{n} \sum_{i=1}^{n} \exp\left(-y_i(w^{\mathsf{T}}x_i+b)\right)$$

s.t. $||w||_2^2 \le B$

(Later, AdaBoost uses this loss)



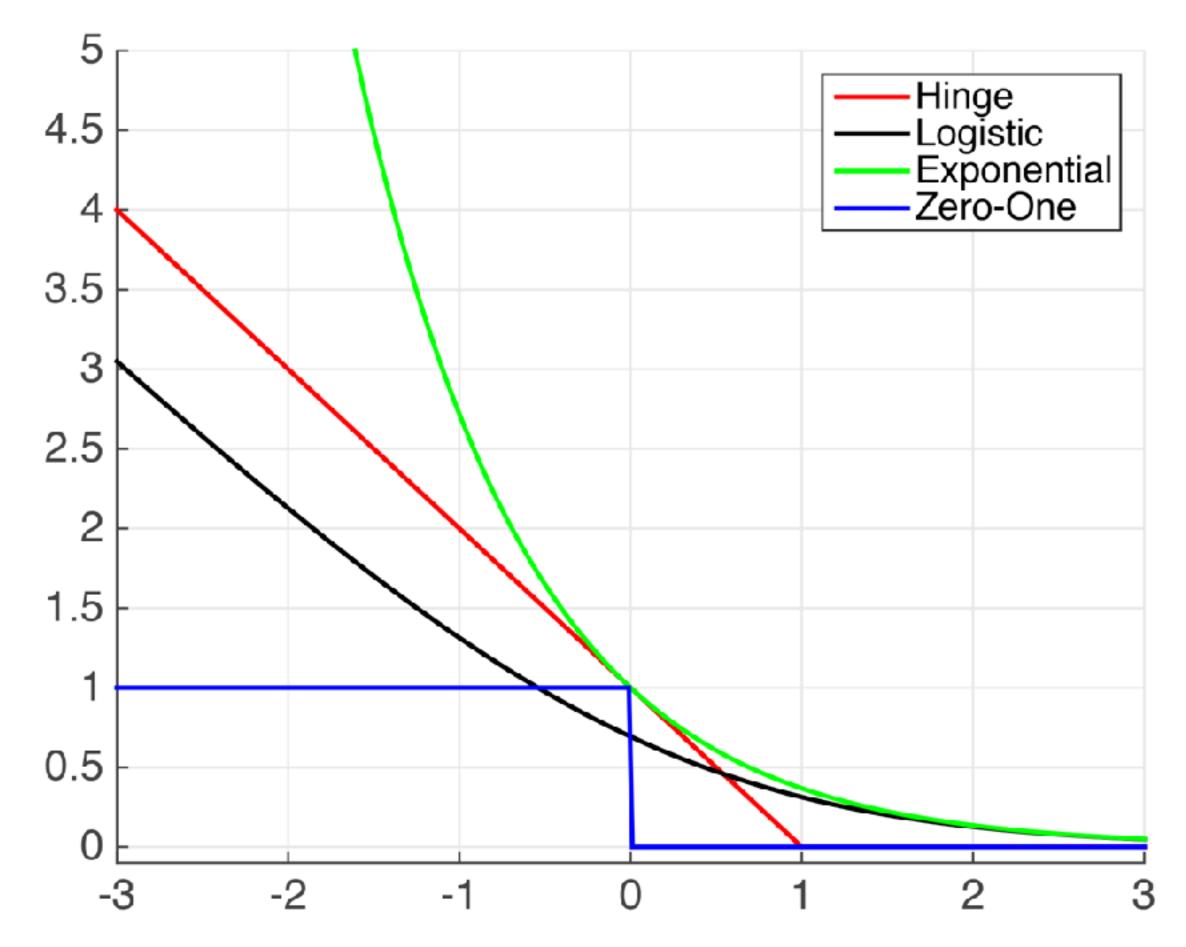
Linear classification: Exponential loss + constraints

$$\min_{w,b} \frac{1}{n} \sum_{i=1}^{n} \exp\left(-y_i(w^{\mathsf{T}}x_i+b)\right)$$

s.t. $||w||_2^2 \le B$

(Later, AdaBoost uses this loss)

Very aggressive loss (but may overfit w/ noisy data)



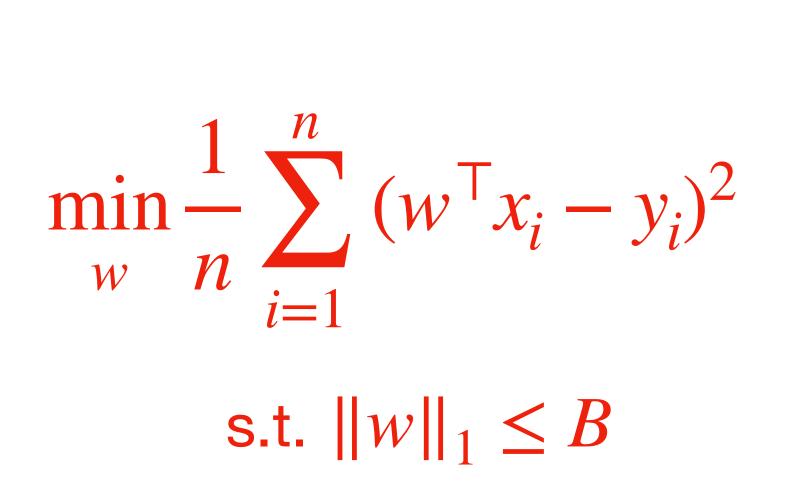
Outline for Today

1. Empirical Risk Minimization

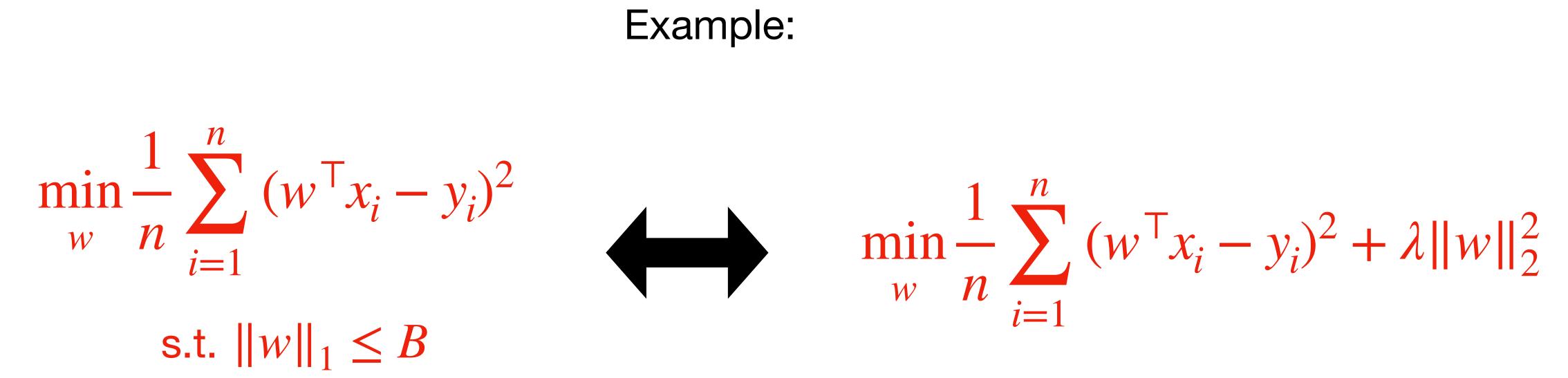
2. Examples on loss & hypothesis classes

3. Regularization

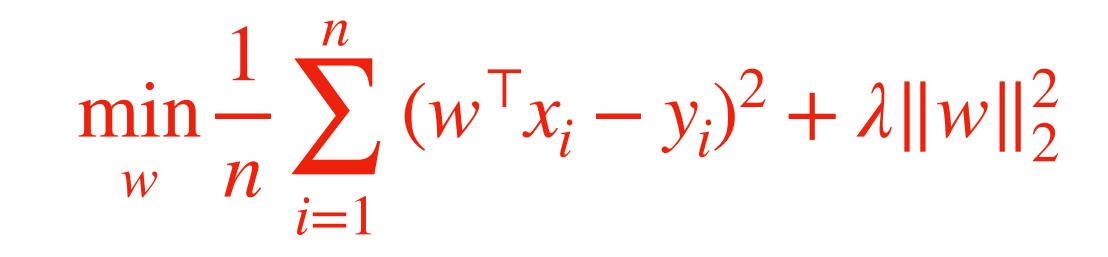
We can turn constraint optimization problem into unconstrained using Lagrange multiplier

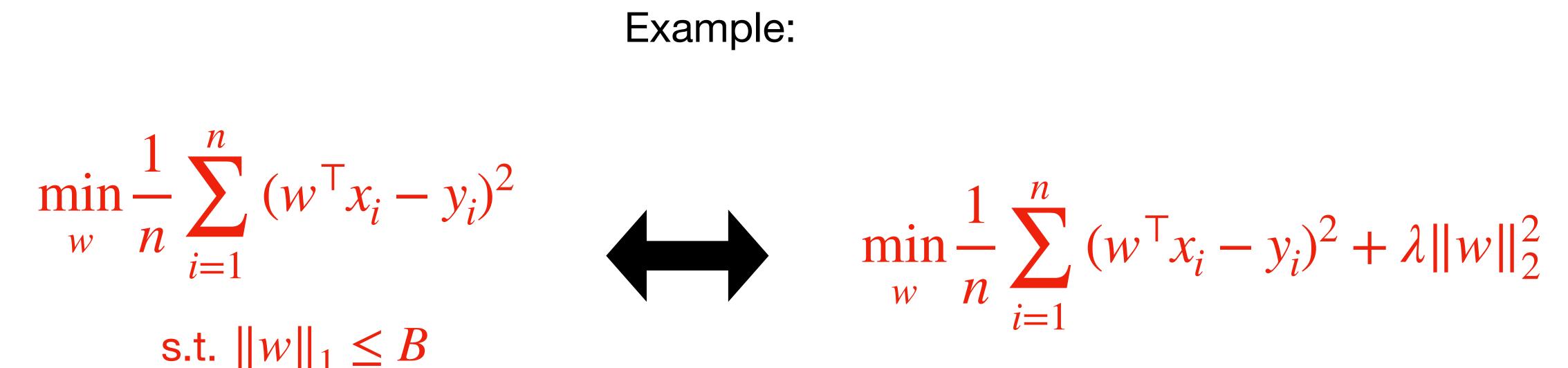


We can turn constraint optimization problem into unconstrained using Lagrange multiplier



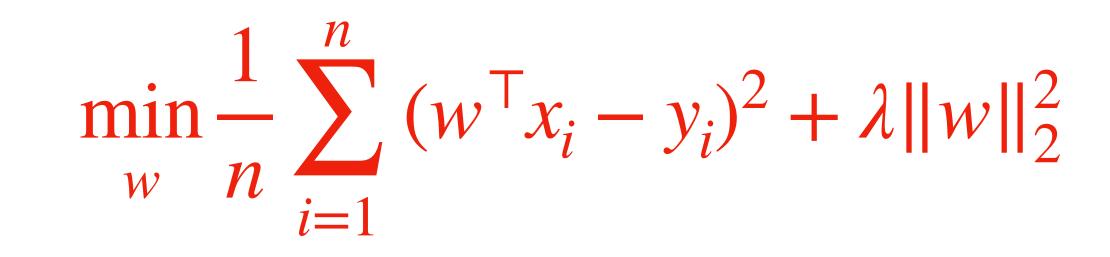
We can turn constraint optimization problem into unconstrained using Lagrange multiplier





(More details about Lagrange multiplier in Anil's optimization class CS4220)

We can turn constraint optimization problem into unconstrained using Lagrange multiplier

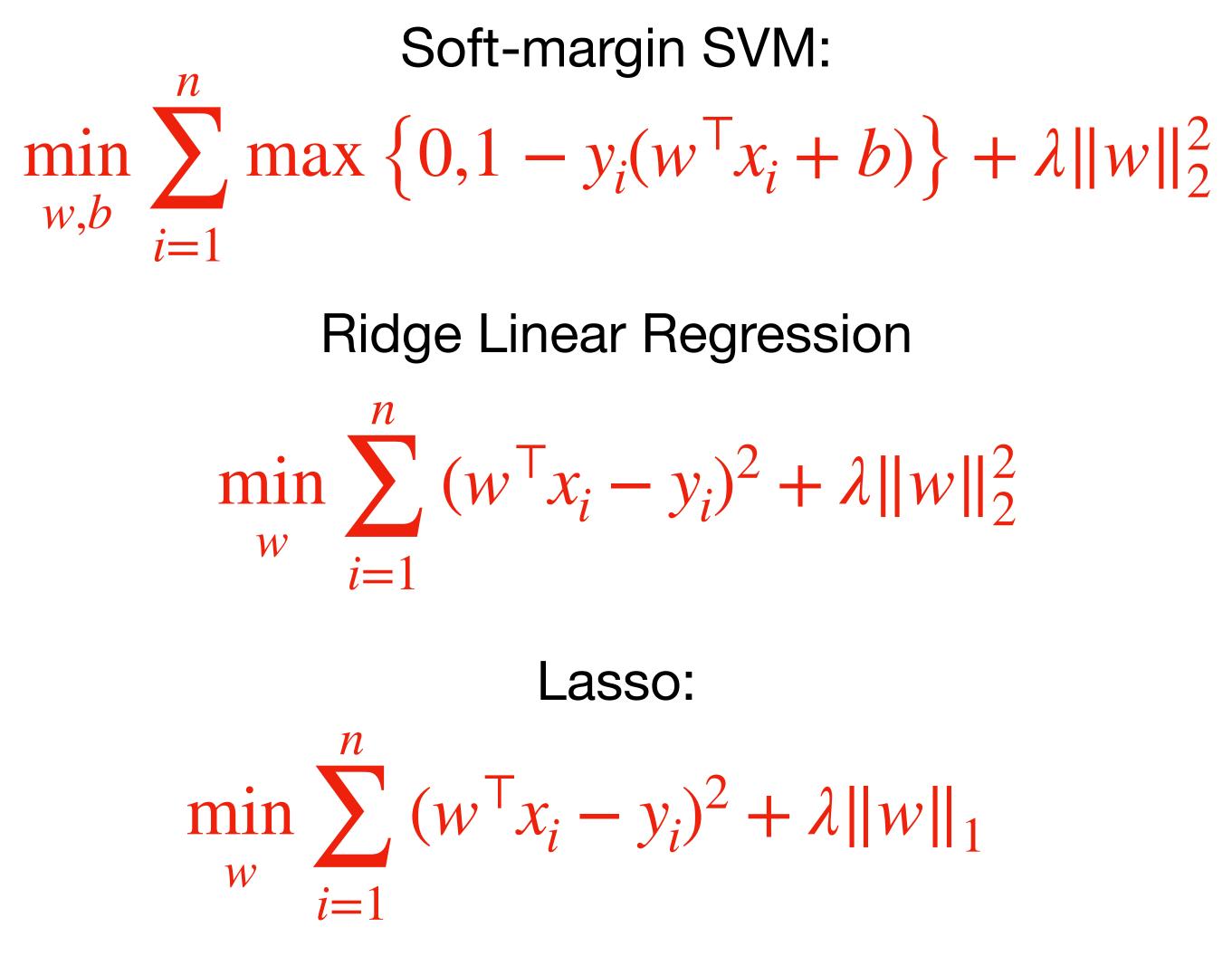


$\min_{w,b} \sum_{i=1}^{n} \max\left\{0, 1 - y_i(w^{\mathsf{T}}x_i + b)\right\} + \lambda \|w\|_2^2$

Soft-margin SVM:

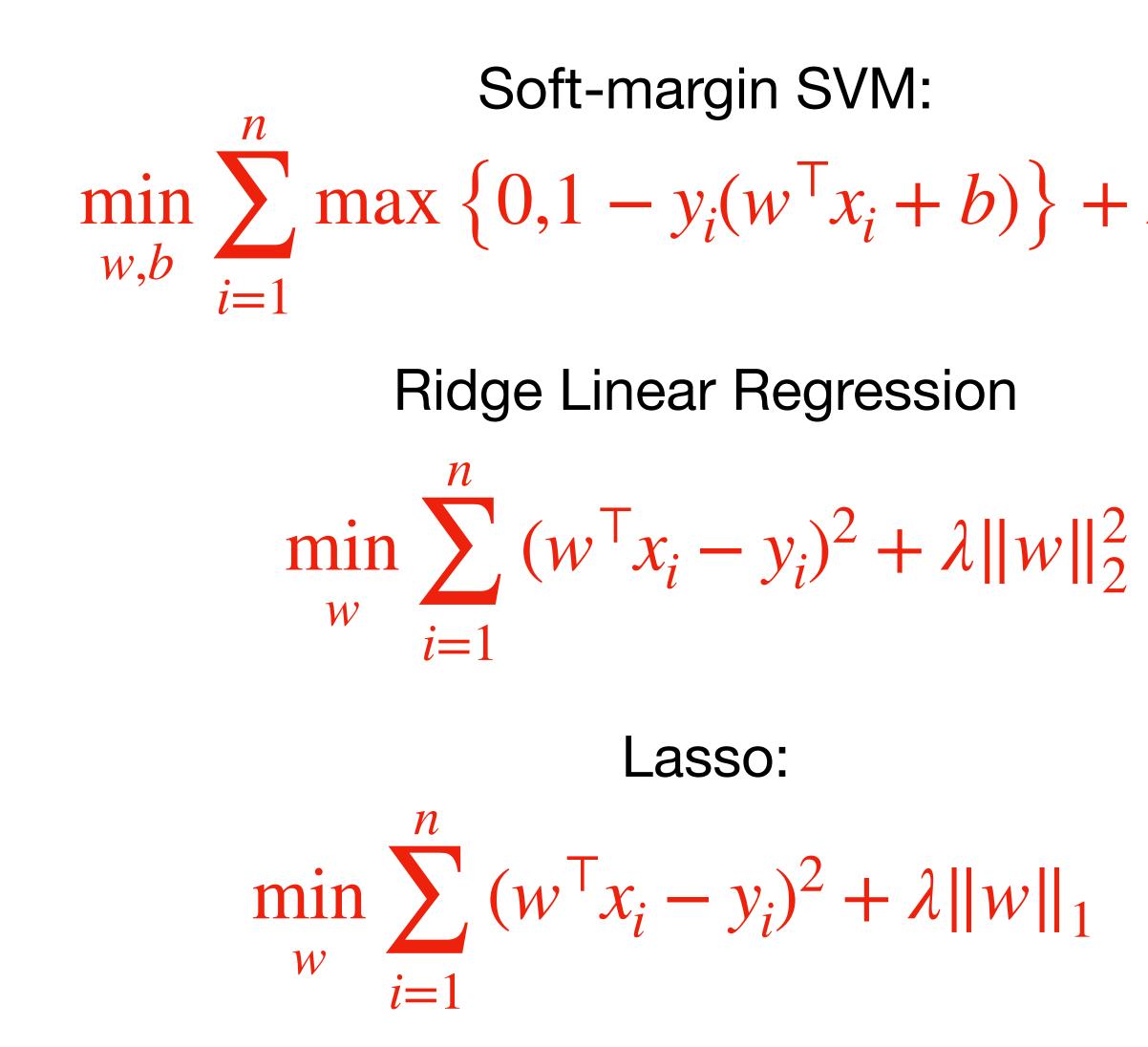
Soft-margin SVM: $\min_{w,b} \sum_{i=1}^{n} \max\left\{0, 1 - y_i(w^{\mathsf{T}}x_i + b)\right\} + \lambda ||w||_2^2$ $\min_{w} \sum_{i=1}^{n} (w^{\mathsf{T}} x_i - y_i)^2 + \lambda \|w\|_2^2$

Ridge Linear Regression



Ridge Linear Regression

Lasso:

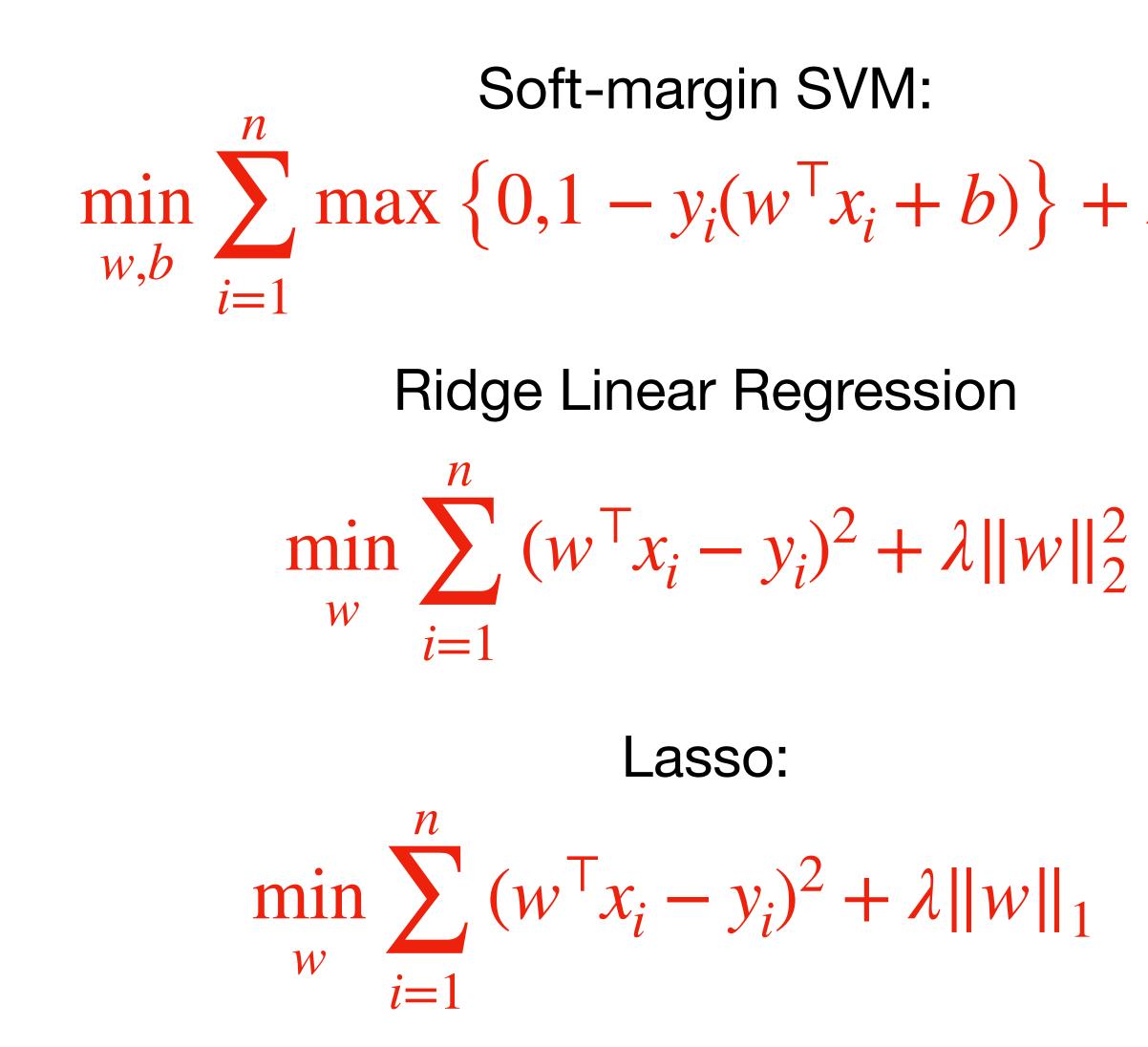


$$-y_i(w^{\mathsf{T}}x_i + b) \} + \lambda ||w||_2^2$$

Ridge Linear Regression

- Lasso:

Returned solution is often sparse!



$$-y_i(w^{\mathsf{T}}x_i + b) \} + \lambda ||w||_2^2$$

Ridge Linear Regression

- Lasso:
- $(w^{\mathsf{T}}x_i y_i)^2 + \lambda \|w\|_1$

Returned solution is often sparse!

Good for feature selection!

Summary for today

1. Empirical risk minimization framework

Summary for today

1. Empirical risk minimization framework

2. Need to restrict our hypothesis class:

Select hypothesis that is simple while can also explain the data reasonably well

Summary for today

1. Empirical risk minimization framework

2. Need to restrict our hypothesis class:

Select hypothesis that is simple while can also explain the data reasonably well

3. Examples of loss functions & Regularizations