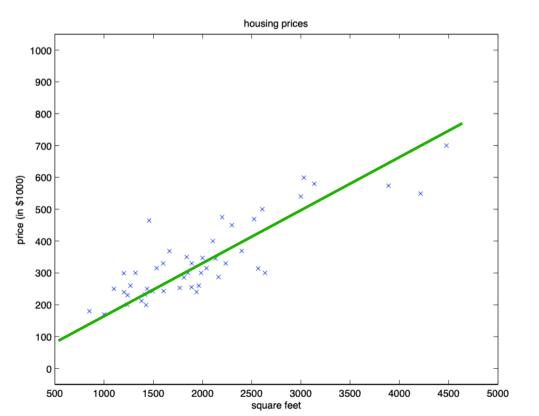
Empirical Risk Minimization

Announcements

Recap on Linear Regression

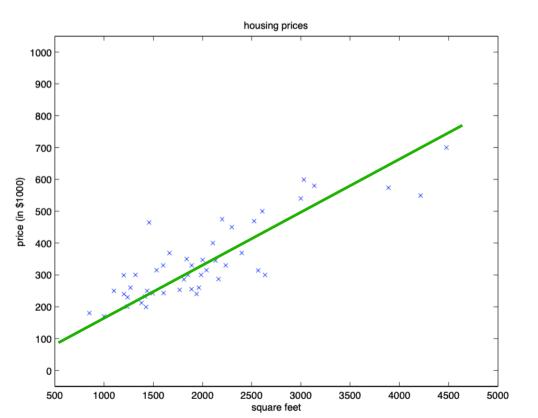
Given dataset $\mathcal{D} = \{x_i, y_i\}, x_i \in \mathbb{R}^d, y_i \in \mathbb{R}$



Recap on Linear Regression

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

2

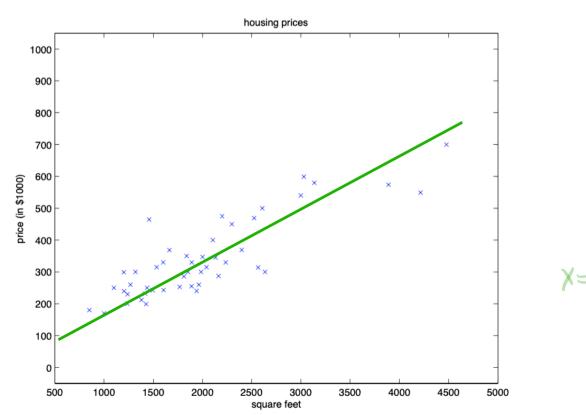


Least Regression with squared loss:

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

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:

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

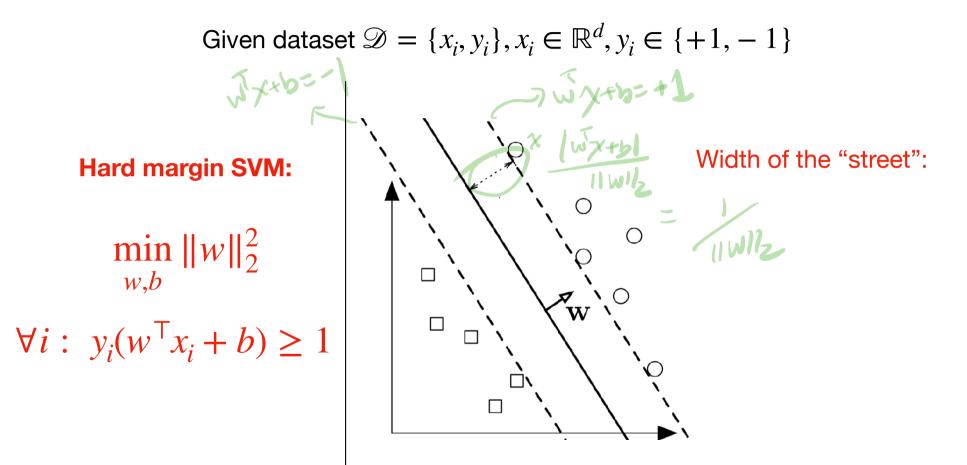
$$\nabla_w L(w) = \mathbf{x} \mathbf{x} \mathbf{w} - \mathbf{x} \mathbf{y}$$

$$\begin{bmatrix} \mathbf{x}_1 \mathbf{x}_1 \cdots \mathbf{x}_n \\ \mathbf{y}_1 \end{bmatrix} \mathbf{y} = \begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \mathbf{y}_1 \end{bmatrix}$$

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

Hard margin SVM:

$\min_{w,b} \|w\|_2^2$ $\forall i: y_i(w^{\mathsf{T}}x_i + b) \ge 1$

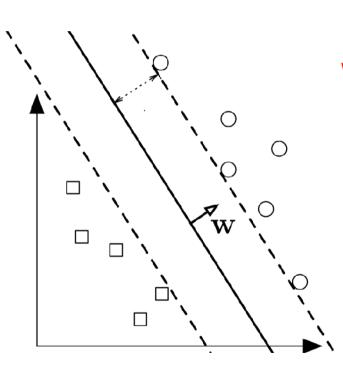


Given dataset
$$\mathcal{D} = \{x_i, y_i\}, x_i \in \mathbb{R}^d, y_i \in \{+1, -1\}$$

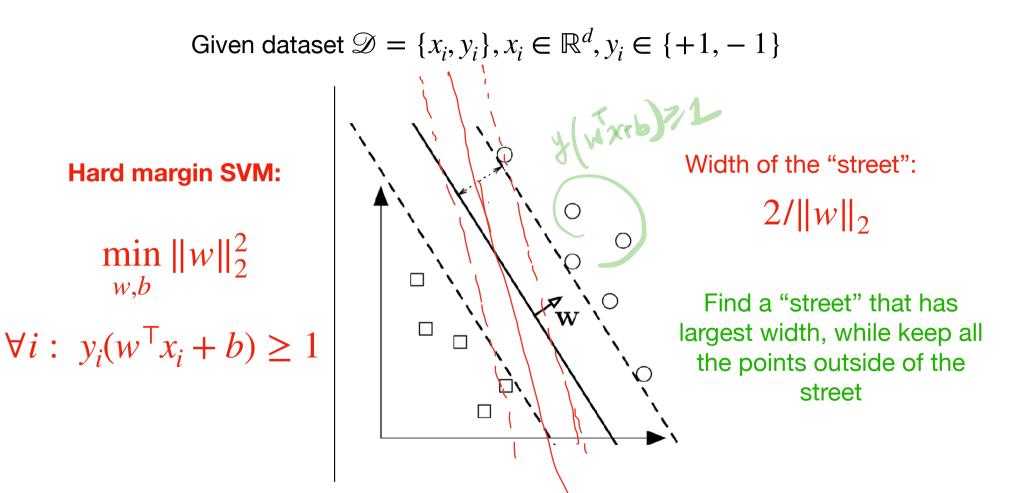
Hard margin SVM:

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

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



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



Outline for Today

1. Empirical Risk Minimization

2. Examples on loss & hypothesis classes

3. Regularization

Recall the general supervised learning setting:

Recall the general supervised learning setting:

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

Recall the general supervised learning setting:

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., $x_i, y_i \sim P$

Recall the general supervised learning setting:

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 $\mathcal{H} := \{h\} \subset \mathcal{X} \mapsto \mathbb{R}$

Recall the general supervised learning setting:

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., $x_i, y_i \sim P$

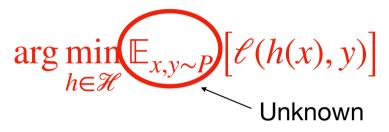
Hypothesis $h : \mathcal{X} \to \mathbb{R}$, & hypothesis class $\mathcal{H} := \{h\} \subset \mathcal{X} \mapsto \mathbb{R}$

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

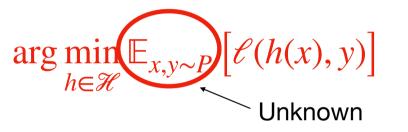
The ultimate objective function:

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

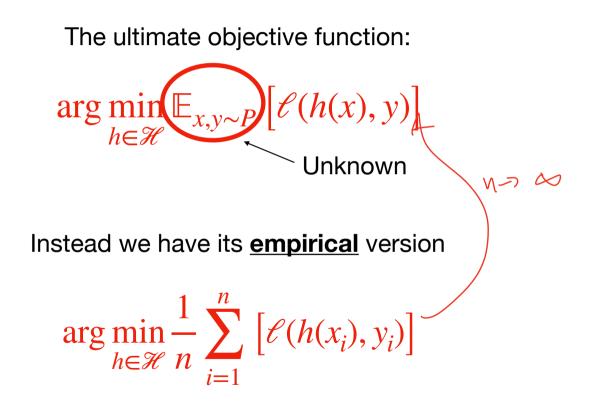
The ultimate objective function:



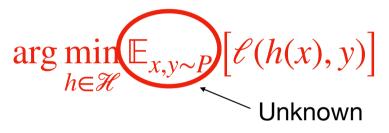
The ultimate objective function:



Instead we have its empirical version



The ultimate objective function:



Instead we have its empirical version

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

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} :

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

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

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

Trank Pator

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

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

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

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

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

We often are interested in the true performance of \hat{h}_{ERM} : $\mathbb{E}_{\mathcal{D}}\left[\mathbb{E}_{x,y\sim P}\ell(\hat{h}_{ERM}(x),y)\right]$

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

e.g., In LR: $\hat{w} = (XX^{\top})^{-1}XY$.

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

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

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

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

The Minimum expected loss we could get if we knew P

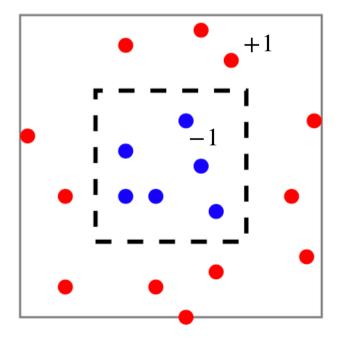
Ideally, we want the true loss of ERM to be small:

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

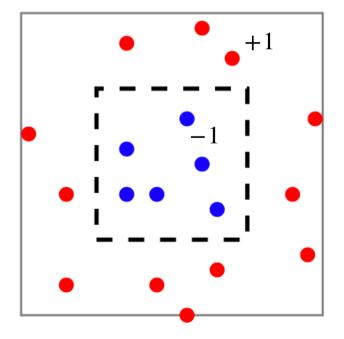
The Minimum expected loss we could get if we knew P

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

P: *x* uniformly distribution over the square; Label: blue if inside the smaller square, else red

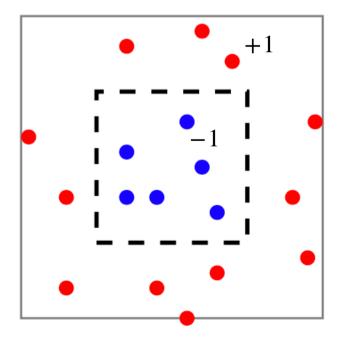


P: *x* uniformly distribution over the square; Label: blue if inside the smaller square, else red



Consider a hypothesis class \mathscr{H} contains ALL mappings from $x \to y$

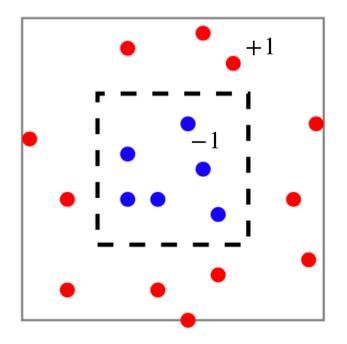
P: *x* uniformly distribution over the square; Label: blue if inside the smaller square, else red



Consider a hypothesis class \mathscr{H} contains ALL mappings from $x \to y$

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

P: *x* uniformly distribution over the square; Label: blue if inside the smaller square, else red

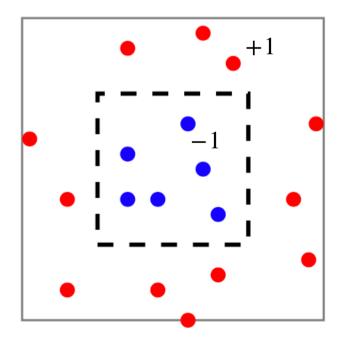


Consider a hypothesis class \mathscr{H} contains ALL mappings from $x \to y$

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

Let us consider this solution that memorizes data:

P: *x* uniformly distribution over the square; Label: blue if inside the smaller square, else red



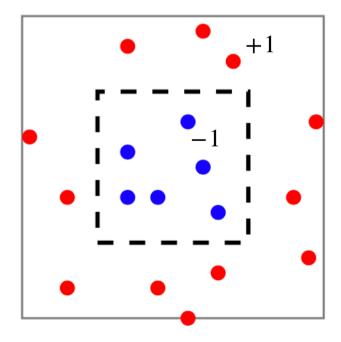
Consider a hypothesis class \mathscr{H} contains ALL mappings from $x \to y$

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

Let us consider this solution that memorizes data:

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

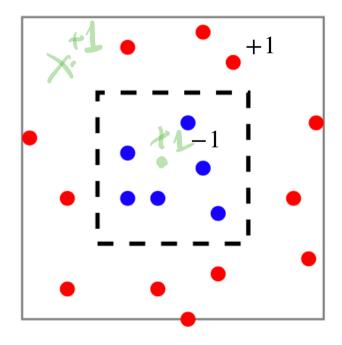
P: *x* uniformly distribution over the square; Label: blue if inside the dashed square, else red



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

$$\implies \frac{1}{n} \sum_{i=1}^{n} \ell(\hat{h}(x_i), y_i) = 0$$

P: *x* uniformly distribution over the square; Label: blue if inside the dashed square, else red

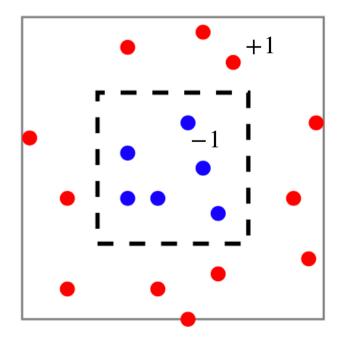


$$\hat{h}(x) = \begin{cases} y_i & \text{if } \exists i, x_i = x \\ +1 & \text{else} \end{cases}$$

$$\implies \frac{1}{n} \sum_{i=1}^{n} \ell(\hat{h}(x_i), y_i) = 0$$

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

P: *x* uniformly distribution over the square; Label: blue if inside the dashed square, else red



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

$$\implies \frac{1}{n} \sum_{i=1}^{n} \ell(\hat{h}(x_i), y_i) = 0$$

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)

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

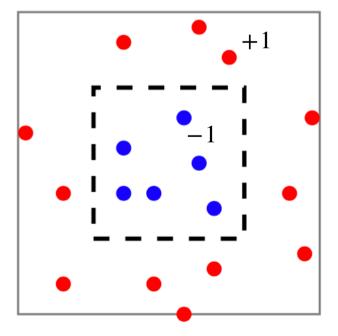
ERM with inductive bias

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

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

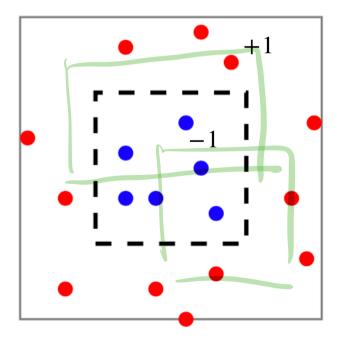
By restricting to \mathcal{H} , we bias towards solutions from \mathcal{H}

P: *x* uniformly distribution over the square; Label: blue if inside the dashed square, else red



Unrestricted hypothesis class did not work;

P: *x* uniformly distribution over the square; Label: blue if inside the dashed square, else red



Unrestricted hypothesis class did not work;

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

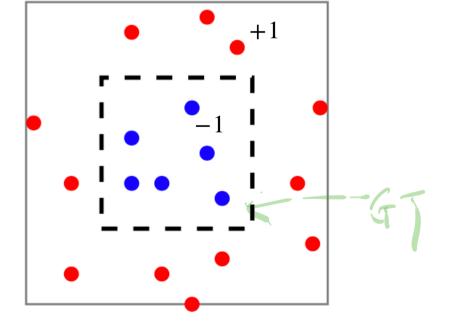
P: *x* uniformly distribution over the square; Label: blue if inside the dashed square, else red

Unrestricted hypothesis class did not work; However, if we restrict $\mathscr H$ to contains ALL

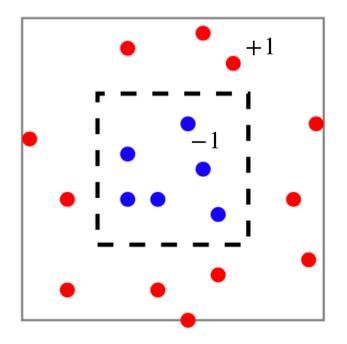
axis-aligned rectangles, then ERM will succeed, i.e.,

$$\mathbb{E}_{\mathcal{D}}\left[\mathbb{E}_{x,y\sim P}\mathcal{C}(\hat{h}_{ERM}(x),y)\right]$$

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



P: *x* uniformly distribution over the square; Label: blue if inside the dashed square, else red



Unrestricted hypothesis class did not work;

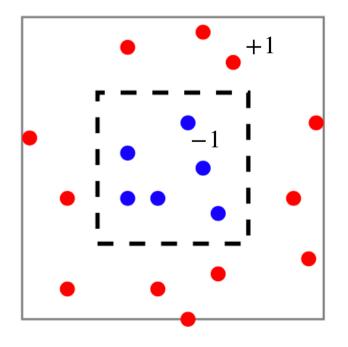
However, if we restrict \mathscr{H} to contains ALL axis-aligned rectangles, then ERM will succeed, i.e.,

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

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

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

P: *x* uniformly distribution over the square; Label: blue if inside the dashed square, else red



Unrestricted hypothesis class did not work;

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

$$\Xi_{\mathscr{D}}\left[\mathbb{E}_{x,y\sim P}\mathscr{C}(\hat{h}_{ERM}(x),y)\right]$$

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

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

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

Summary so far

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

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

Outline for Today

1. Empirical Risk Minimization

2. Examples on loss & hypothesis classes

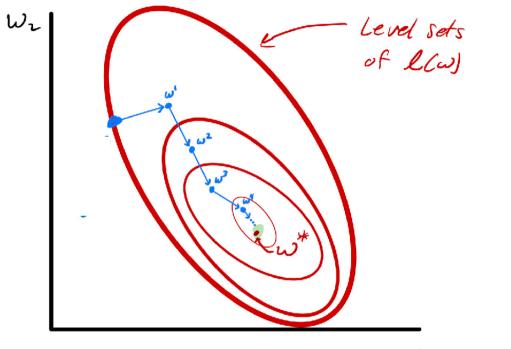
3. Regularization

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

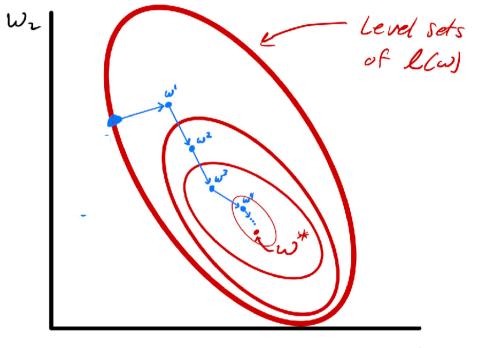
Linear Regression: squared loss + ℓ_2 constraint



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

W

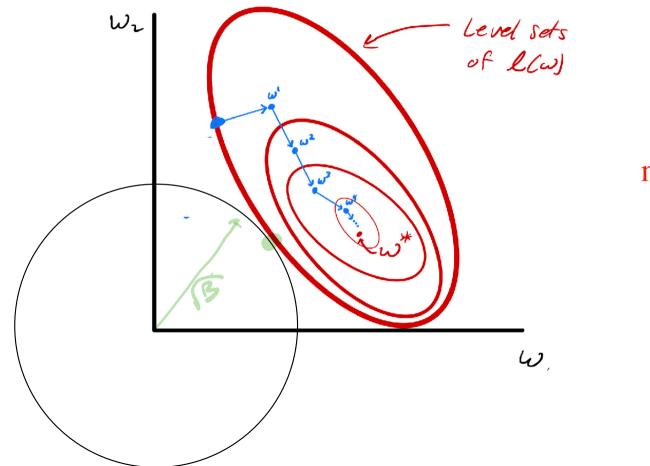
Linear Regression: squared loss + ℓ_2 constraint



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

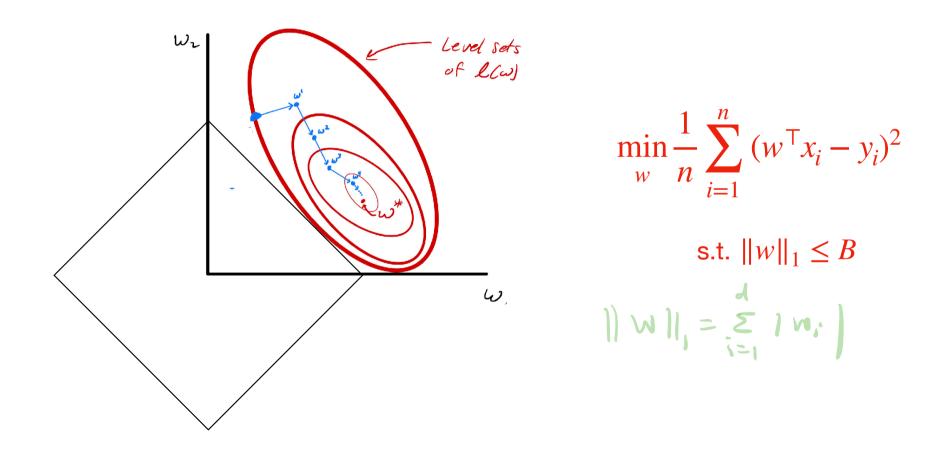
 ω

Linear Regression: squared loss + ℓ_2 constraint

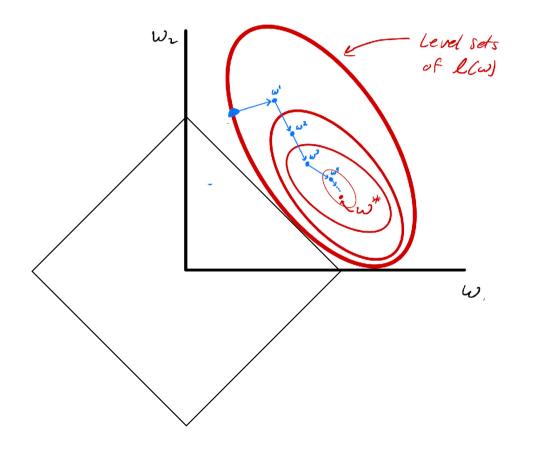


$$\min_{w} \frac{1}{n} \sum_{i=1}^{n} (w^{\mathsf{T}} x_{i} - y_{i})^{2}$$
s.t. $||w||_{2}^{2} \le B$

Linear Regression: squared loss + ℓ_1 constraint



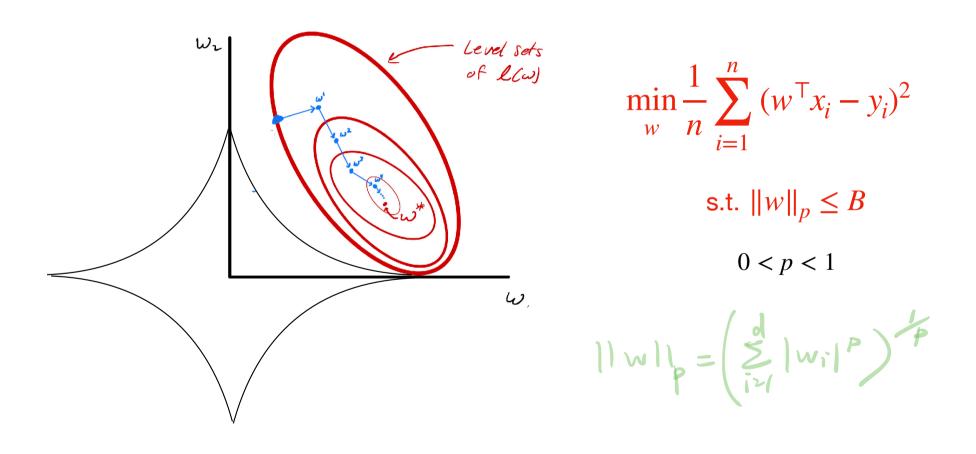
Linear Regression: squared loss + ℓ_1 constraint



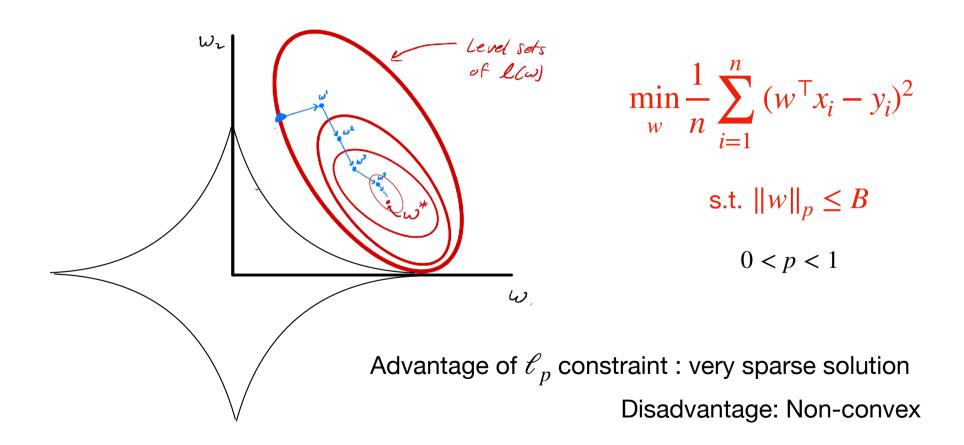
$$\min_{w} \frac{1}{n} \sum_{i=1}^{n} (w^{\top} x_{i} - y_{i})^{2}$$
s.t. $||w||_{1} \le B$

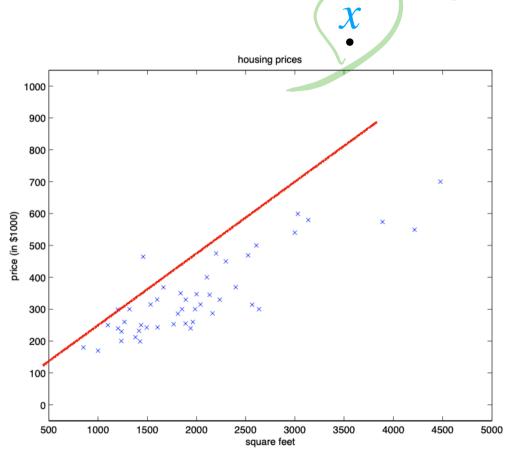
Advantage: give sparse solution

Linear Regression: squared loss + \mathcal{C}_p constraint



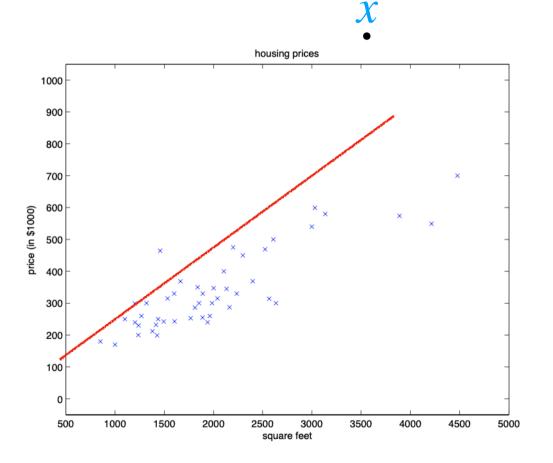
Linear Regression: squared loss + \mathcal{C}_p constraint





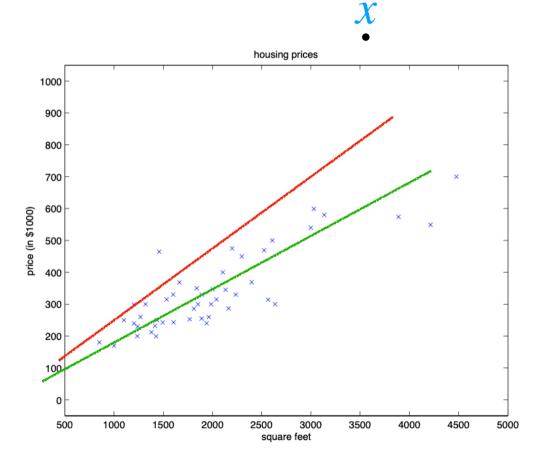
Without constraint, we might overfit to an outlier





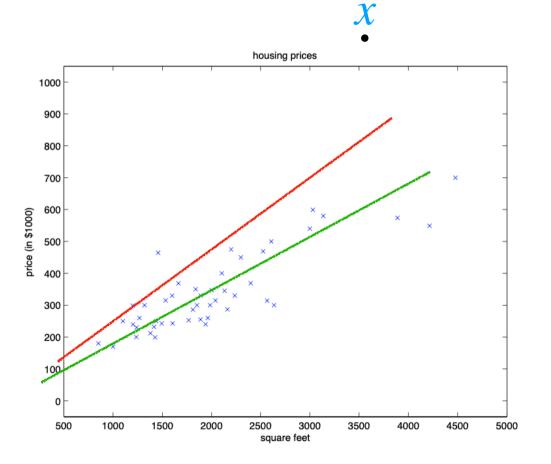
Without constraint, we might overfit to an outlier

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



Without constraint, we might overfit to an outlier

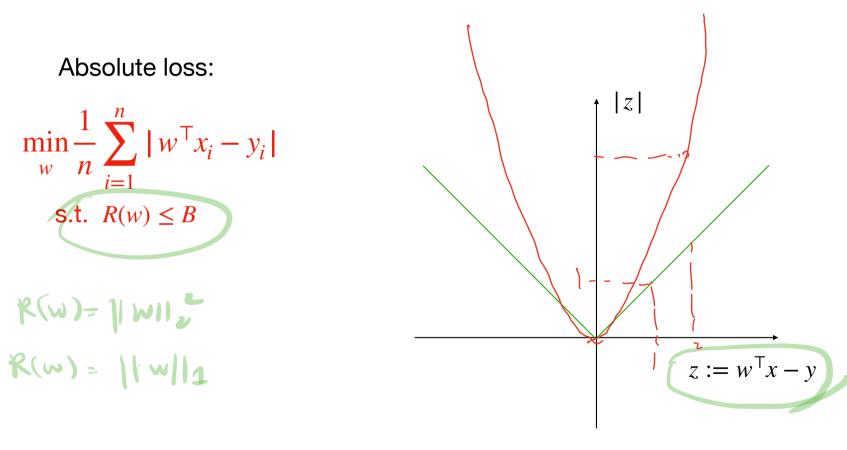
With constraint $||w||_2^2 \le B$, we can avoid overfitting (i.e., force us to not pay too much attention to minimizing loss)



Without constraint, we might overfit to an outlier

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

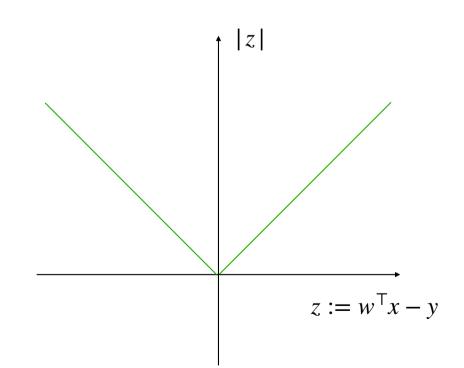
(More details in next lecture)



Absolute loss:

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

Advantage: less sensitive to outliers



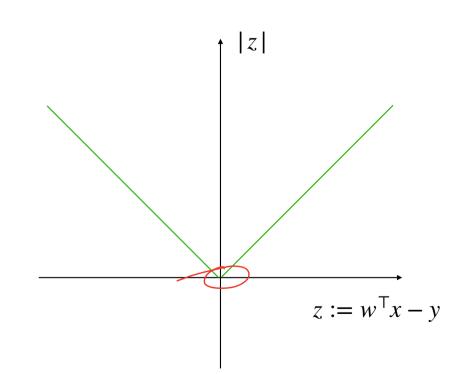
Absolute loss:

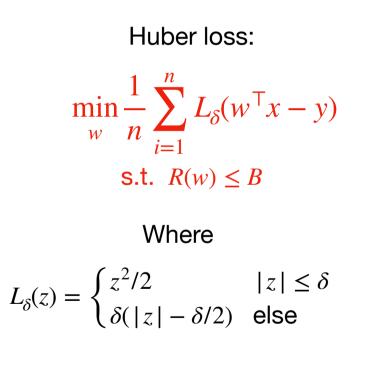
$$\min_{w} \frac{1}{n} \sum_{i=1}^{n} |w^{\mathsf{T}} x_{i} - y_{i}|$$

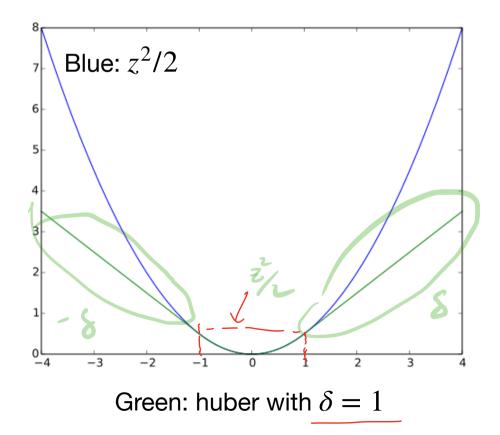
s.t. $R(w) \le B$

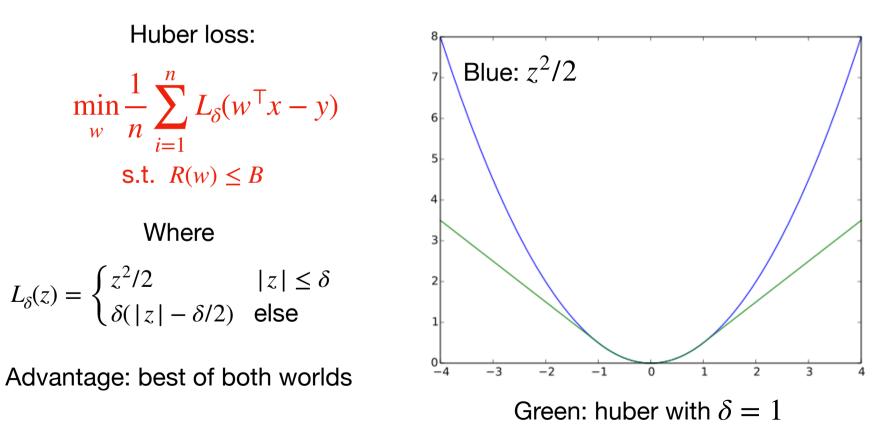
Advantage: less sensitive to outliers

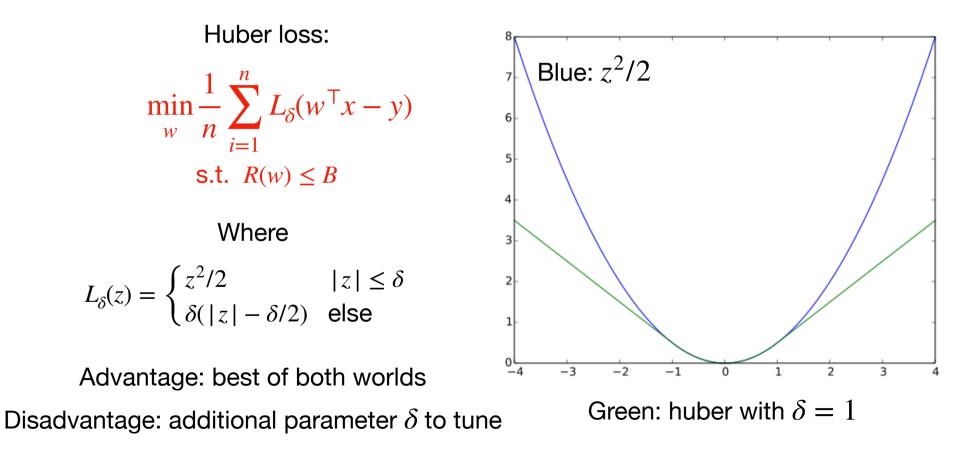
Disadvantage: no closed-form solution, non-differentiable at 0











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

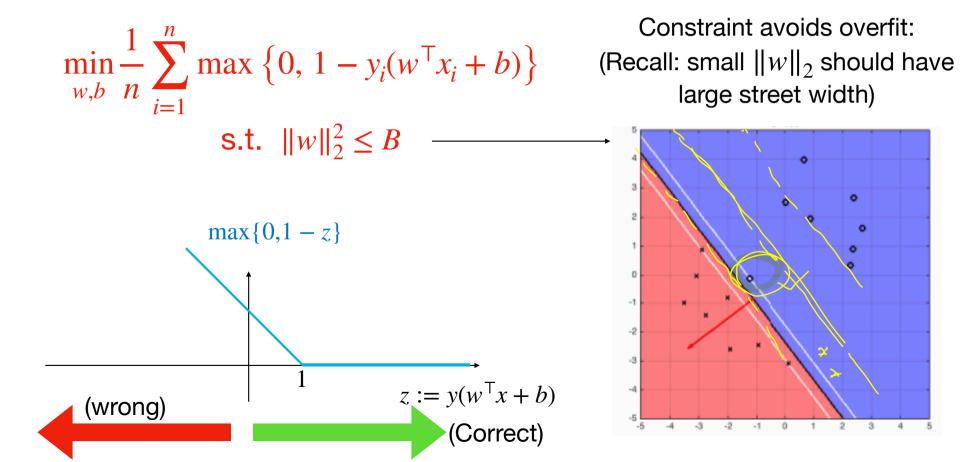
(Correct)

$$\min_{w,b} \frac{1}{n} \sum_{i=1}^{n} \max\left\{0, 1 - y_{i}(w^{\mathsf{T}}x_{i} + b)\right\}$$
s.t. $||w||_{2}^{2} \leq B$

$$\max\{0, 1 - z\}$$
(wrong)
$$z := y(w^{\mathsf{T}}x + b)$$

(wrong)

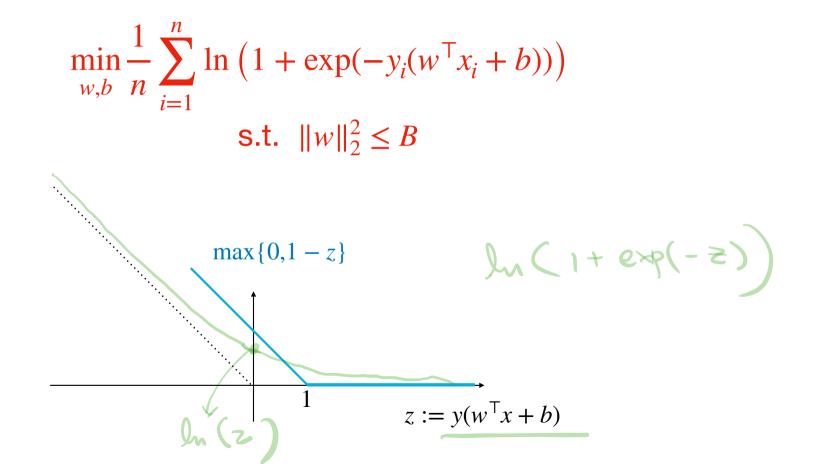
Linear classification: Hinge loss + constraint



Linear classification: Log-loss + constraints

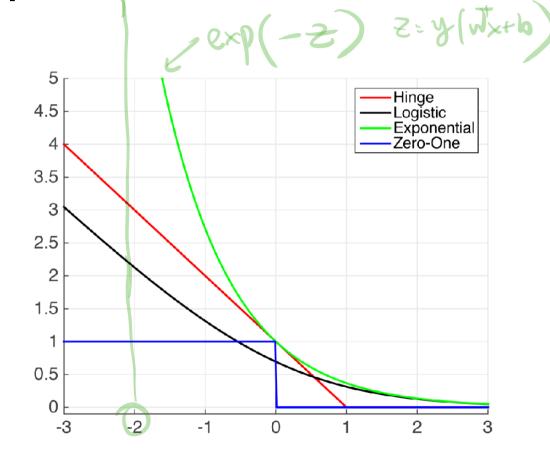
$$\min_{w,b} \frac{1}{n} \sum_{i=1}^{n} \ln\left(1 + \exp(-y_i(w^{\mathsf{T}}x_i + b))\right) \\
\text{s.t. } \|w\|_2^2 \le B$$

Linear classification: Log-loss + constraints



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

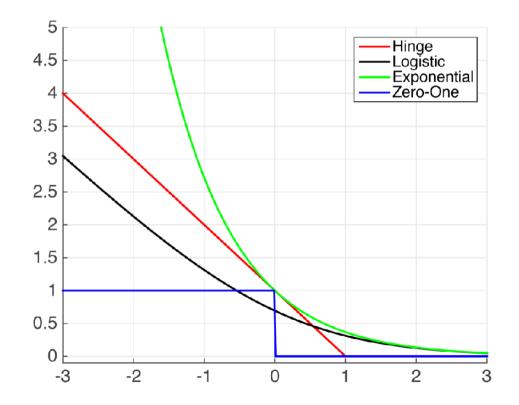


Linear classification: Exponential loss + constraints

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

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

(Later, AdaBoost uses this loss)



Linear classification: Exponential loss + constraints

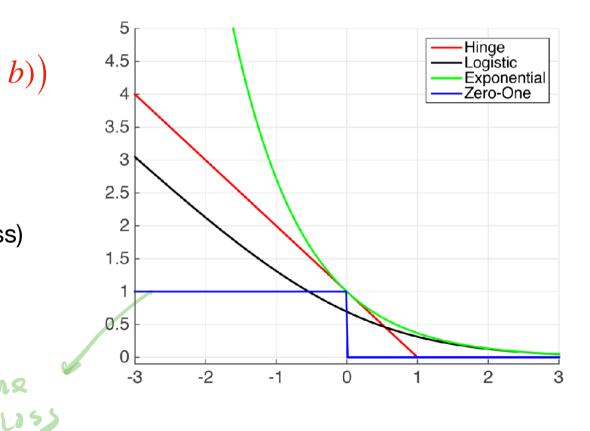
$$\min_{w,b} \frac{1}{n} \sum_{i=1}^{n} \exp\left(-y_i(w^{\mathsf{T}}x_i + b)\right)$$

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

(Later, AdaBoost uses this loss)

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

7210-042



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

Example:

We can turn constraint optimization problem into unconstrained using Lagrange multiplier

Example:

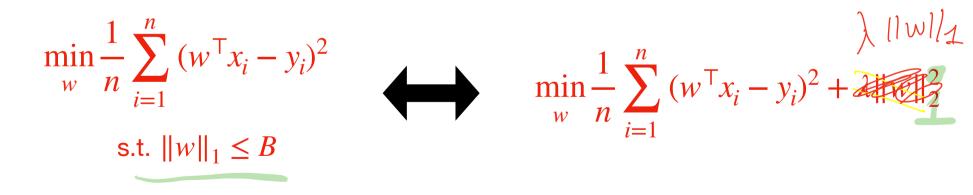
$$\min_{w} \frac{1}{n} \sum_{i=1}^{n} (w^{\mathsf{T}} x_i - y_i)^2$$
s.t. $||w||_1 \le B$

We can turn constraint optimization problem into unconstrained using Lagrange multiplier

Example:

We can turn constraint optimization problem into unconstrained using Lagrange multiplier

Example:



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

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

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

Ridge Linear Regression

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

Lasso:

$$\min_{w} \sum_{i=1}^{n} (w^{\top} x_{i} - y_{i})^{2} + \lambda \|w\|_{1}$$

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

Ridge Linear Regression

$$\min_{w} \sum_{i=1}^{n} (w^{\top} x_i - y_i)^2 + \lambda \|w\|_2^2$$

Lasso:
$$\min_{w} \sum_{i=1}^{n} (w^{\mathsf{T}} x_{i} - y_{i})^{2} + \lambda ||w||_{1}$$

Returned solution is often sparse!

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

Ridge Linear Regression

$$\min_{w} \sum_{i=1}^{n} (w^{\top} x_i - y_i)^2 + \lambda \|w\|_2^2$$

Lasso:

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

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