Bias-Variance Tradeoff & Model Selection

Announcements

HW5 and P5 are coming out

Denote $h_{\mathcal{D}}$ as the ERM solution on dataset \mathcal{D} w/ squared loss $\ell(h, x, y) = (h(x) - y)^2$

Denote $h_{\mathcal{D}}$ as the ERM solution on dataset \mathcal{D} w/ squared loss $\ell(h, x, y) = (h(x) - y)^2$

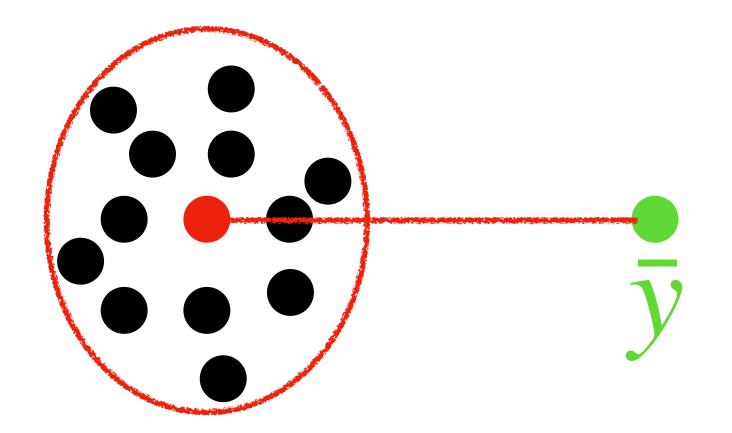
What we have shown is the Bias-Variance decomposition:

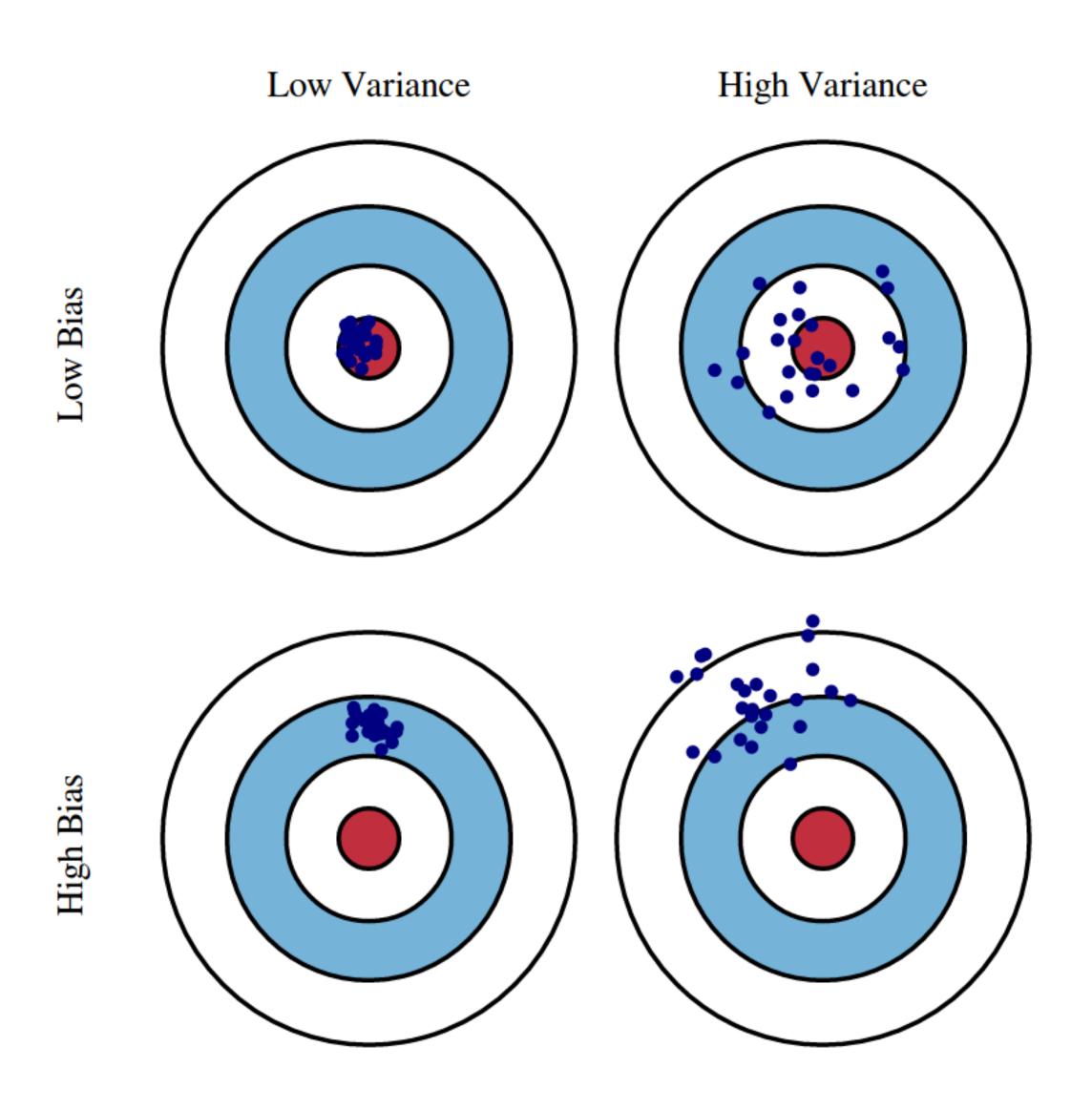
$$\mathbb{E}_{\mathcal{D},x,y}(h_{\mathcal{D}}(x)-y)^2 = \mathbb{E}_{\mathcal{D},x}(h_{\mathcal{D}}(x)-\bar{h}(x))^2 + \mathbb{E}_x(\bar{h}(x)-\bar{y}(x))^2 + \mathbb{E}_{x,y}(\bar{y}(x)-y)^2$$

Denote $h_{\mathcal{D}}$ as the ERM solution on dataset \mathcal{D} w/ squared loss $\ell(h, x, y) = (h(x) - y)^2$

What we have shown is the Bias-Variance decomposition:

$$\mathbb{E}_{\mathcal{D},x,y}(h_{\mathcal{D}}(x)-y)^2 = \mathbb{E}_{\mathcal{D},x}(h_{\mathcal{D}}(x)-\bar{h}(x))^2 + \mathbb{E}_x(\bar{h}(x)-\bar{y}(x))^2 + \mathbb{E}_{x,y}(\bar{y}(x)-y)^2$$





Outline of Today

1. Bias & Variance tradeoff demo on Ridge Linear Regression

2. Derivation of Bias / Variance for Ridge LR

2. Model selection in practice (re-visit Cross Validation)

Let us consider the case where features are fixed, i.e., x_1, \ldots, x_n fixed (no randomness)

Let us consider the case where features are fixed, i.e., x_1, \ldots, x_n fixed (no randomness)

But
$$y_i \sim (w^*)^T x_i + \epsilon_i$$
, $\epsilon_i \sim \mathcal{N}(0,1)$

Let us consider the case where features are fixed, i.e., x_1, \ldots, x_n fixed (no randomness)

But
$$y_i \sim (w^*)^T x_i + \epsilon_i$$
, $\epsilon_i \sim \mathcal{N}(0,1)$

(This is called LR w/ fixed design)

Let us consider the case where features are fixed, i.e., x_1, \ldots, x_n fixed (no randomness)

But
$$y_i \sim (w^*)^T x_i + \epsilon_i$$
, $\epsilon_i \sim \mathcal{N}(0,1)$

(This is called LR w/ fixed design)

(So the only randomness of our dataset $\mathcal{D} = \{x_i, y_i\}$ is coming from the noises ϵ_i)

Ridge Linear Regression formulation

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

Ridge Linear Regression formulation

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

What we will show now:

Larger λ (model becomes "simpler") => larger bias, but smaller variance

Ridge Linear Regression formulation

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

What we will show now:

Larger λ (model becomes "simpler") => larger bias, but smaller variance

(Q: think about the case where $\lambda \to \infty$, what happens to \hat{w} ?)

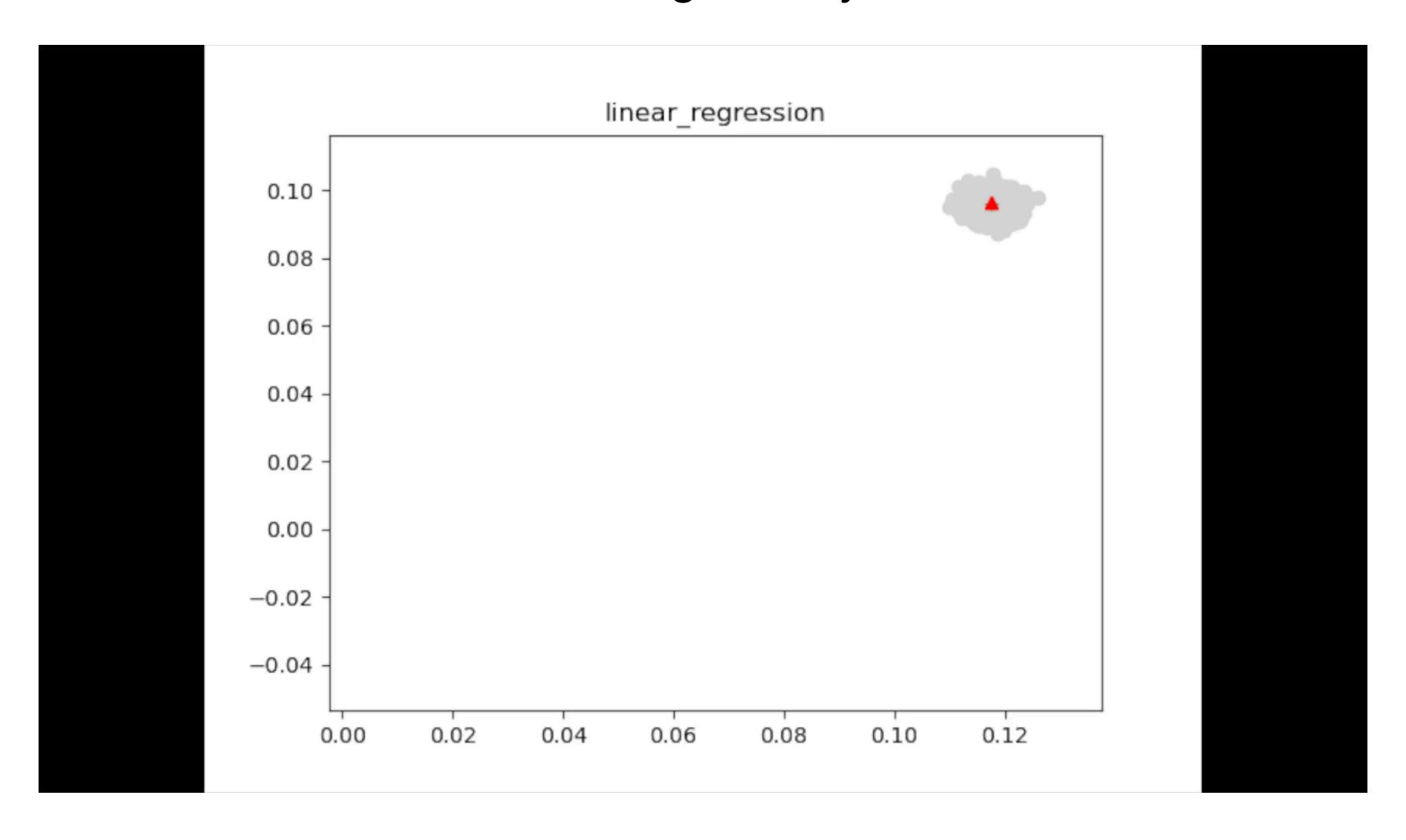
Demonstration for 2d ridge linear regression

- 1. We create 5000 datasets: $\mathcal{D}_1, \mathcal{D}_2, ..., \mathcal{D}_{5000}$,
- 2. For a given λ , solve Ridge LR for each dataset, get $\hat{w}_1, \dots, \hat{w}_{5000}$

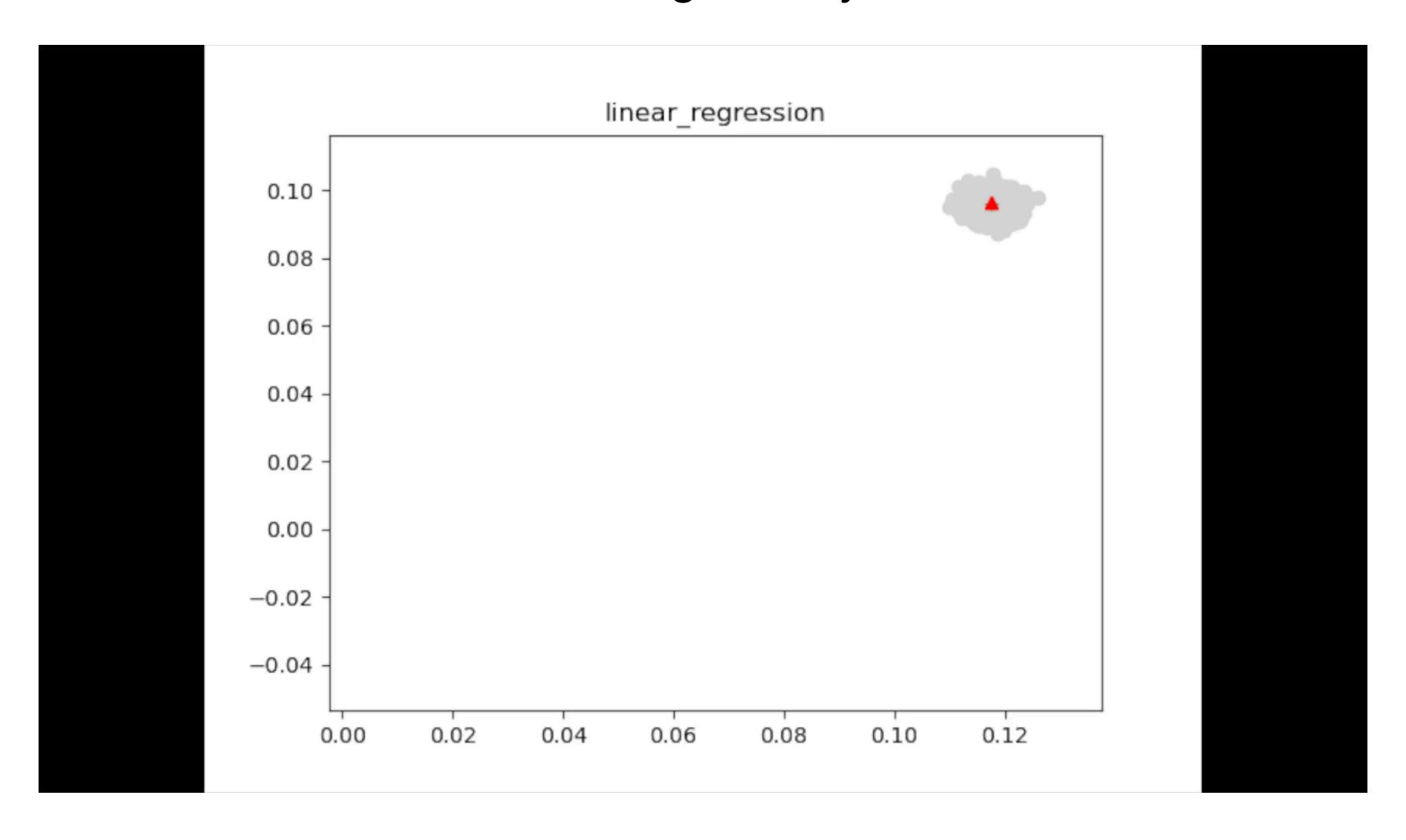
3. Estimate the mean
$$\bar{w} = \sum_{i} \hat{w}_{i}/5000$$

4. Plot $\hat{w}_1, \dots, \hat{w}_{5000}$, and mean \bar{w} , and the optimal w^*

We start with $\lambda = 0$, and gradually increase λ to $+\infty$:



We start with $\lambda = 0$, and gradually increase λ to $+\infty$:



Outline of Today

1. Bias & Variance tradeoff demo on Ridge Linear Regression

2. Derivation of Bias / Variance for Ridge LR

2. Model selection in practice (re-visit Cross Validation)

Derivation of Bias and Variance for Ridge Linear regression

Denote
$$X = [x_1, ..., x_n] \in \mathbb{R}^{d \times n}, Y = [y_1, ..., y_n]^\top \in \mathbb{R}^n, \epsilon = [\epsilon_1, ..., \epsilon_n]^\top \in \mathbb{R}^n$$

Ridge LR in matrix / vector form:

Derivation of Bias and Variance for Ridge Linear regression

Denote
$$X = [x_1, ..., x_n] \in \mathbb{R}^{d \times n}, Y = [y_1, ..., y_n]^\top \in \mathbb{R}^n, \epsilon = [\epsilon_1, ..., \epsilon_n]^\top \in \mathbb{R}^n$$

Ridge LR in matrix / vector form:

$$\hat{w} = \arg\min_{w} \|X^{\mathsf{T}}w - Y\|_{2}^{2} + \lambda \|w\|_{2}^{2}$$

Derivation of Bias and Variance for Ridge Linear regression

Denote
$$X = [x_1, ..., x_n] \in \mathbb{R}^{d \times n}, Y = [y_1, ..., y_n]^\top \in \mathbb{R}^n, \epsilon = [\epsilon_1, ..., \epsilon_n]^\top \in \mathbb{R}^n$$

Ridge LR in matrix / vector form:

$$\hat{w} = \arg\min_{w} \|X^{\mathsf{T}}w - Y\|_{2}^{2} + \lambda \|w\|_{2}^{2}$$

Since
$$y_i = (w^*)^T x_i + \epsilon_i$$
 we have $Y = X^T w^* + \epsilon$

Recall we have closed form solution for Ridge LR

$$\hat{w} = (XX^{\mathsf{T}} + \lambda I)^{-1}XY = (XX^{\mathsf{T}} + \lambda I)^{-1}X(X^{\mathsf{T}}w^{\star} + \epsilon)$$

Recall we have closed form solution for Ridge LR

$$\hat{w} = (XX^\top + \lambda I)^{-1}XY = (XX^\top + \lambda I)^{-1}X(X^\top w^\star + \epsilon)$$
 Source of the randomness of



Recall we have closed form solution for Ridge LR

$$\hat{w} = (XX^{\top} + \lambda I)^{-1}XY = (XX^{\top} + \lambda I)^{-1}X(X^{\top}w^{\star} + \epsilon)$$
 Source of the randomness of



Recall we have closed form solution for Ridge LR

$$\hat{w} = (XX^{\top} + \lambda I)^{-1}XY = (XX^{\top} + \lambda I)^{-1}X(X^{\top}w^{\star} + \epsilon)$$
 Source of the randomness of

$$\mathbb{E}_{\epsilon}[\hat{w}] = (XX^{\mathsf{T}} + \lambda I)^{-1}X[X^{\mathsf{T}}w^{\star} + \mathbb{E}_{\epsilon}[\epsilon]]$$



Recall we have closed form solution for Ridge LR

$$\hat{w} = (XX^{\top} + \lambda I)^{-1}XY = (XX^{\top} + \lambda I)^{-1}X(X^{\top}w^{\star} + \epsilon)$$
 Source of the randomness of

 \hat{W}

$$\mathbb{E}_{\epsilon}[\hat{w}] = (XX^{\mathsf{T}} + \lambda I)^{-1}X[X^{\mathsf{T}}w^{\star} + \mathbb{E}_{\epsilon}[\epsilon]]$$
$$= (XX^{\mathsf{T}} + \lambda I)^{-1}XX^{\mathsf{T}}w^{\star}$$

Recall we have closed form solution for Ridge LR

$$\hat{w} = (XX^{\top} + \lambda I)^{-1}XY = (XX^{\top} + \lambda I)^{-1}X(X^{\top}w^{\star} + \epsilon)$$
 Source of the randomness of

 \hat{W}

$$\mathbb{E}_{\epsilon}[\hat{w}] = (XX^{\top} + \lambda I)^{-1}X[X^{\top}w^{*} + \mathbb{E}_{\epsilon}[\epsilon]]$$

$$= (XX^{\top} + \lambda I)^{-1}XX^{\top}w^{*}$$

$$= (XX^{\top} + \lambda I)^{-1}(XX^{\top} + \lambda I - \lambda I)w^{*}$$

Recall we have closed form solution for Ridge LR

$$\hat{w} = (XX^{\top} + \lambda I)^{-1}XY = (XX^{\top} + \lambda I)^{-1}X(X^{\top}w^{\star} + \epsilon)$$
 Source of the randomness of

 \hat{W}

$$\mathbb{E}_{\epsilon}[\hat{w}] = (XX^{\top} + \lambda I)^{-1}X[X^{\top}w^{*} + \mathbb{E}_{\epsilon}[\epsilon]]$$
$$= (XX^{\top} + \lambda I)^{-1}XX^{\top}w^{*}$$

$$= (XX^{\top} + \lambda I)^{-1}(XX^{\top} + \lambda I - \lambda I)w^{\star} = w^{\star} - \lambda(XX^{\top} + \lambda I)^{-1}w^{\star}$$

$$\bar{w} = \mathbb{E}[\hat{w}] = w^* - \lambda (XX^T + \lambda)^{-1} \lambda w^*$$

Bias term:
$$\sum_{i=1}^{n} ((\bar{w} - w^*)^T x_i)^2$$

$$\bar{w} = \mathbb{E}[\hat{w}] = w^* - \lambda (XX^T + \lambda)^{-1} \lambda w^*$$

Bias term:
$$\sum_{i=1}^{n} ((\bar{w} - w^*)^{\mathsf{T}} x_i)^2$$

$$= \sum_{i=1}^{n} \left((\lambda (XX^{\mathsf{T}} + \lambda)^{-1} w^{\star})^{\mathsf{T}} x_i \right)^2$$

$$\bar{w} = \mathbb{E}[\hat{w}] = w^* - \lambda (XX^T + \lambda)^{-1} \lambda w^*$$

Bias term:
$$\sum_{i=1}^{n} ((\bar{w} - w^*)^T x_i)^2$$

$$= \sum_{i=1}^{n} \left((\lambda (XX^{\mathsf{T}} + \lambda)^{-1} w^{\star})^{\mathsf{T}} x_i \right)^2$$

$$= \lambda^{2}(w^{\star})^{\mathsf{T}}(XX^{\mathsf{T}} + \lambda I)^{-1}XX^{\mathsf{T}}(XX^{\mathsf{T}} + \lambda I)^{-1}w^{\star}$$

Bias =
$$\lambda^2 (w^*)^\top (XX^\top + \lambda I)^{-1} XX^\top (XX^\top + \lambda I)^{-1} w^*$$

Bias =
$$\lambda^2 (w^*)^\top (XX^\top + \lambda I)^{-1} XX^\top (XX^\top + \lambda I)^{-1} w^*$$

Eigendecomposition on $XX^{\mathsf{T}} = U\Sigma U^{\mathsf{T}}$

Bias =
$$\lambda^2 (w^*)^\top (XX^\top + \lambda I)^{-1} XX^\top (XX^\top + \lambda I)^{-1} w^*$$

Eigendecomposition on $XX^{\top} = U\Sigma U^{\top}$

$$= (w^{\star})^{\top} U \begin{bmatrix} \frac{\sigma_1}{(\sigma_1/\lambda + 1)^2} & 0 & 0 \dots \\ 0 & \frac{\sigma_2}{(\sigma_2/\lambda + 1)^2} & 0 \dots \\ 0, & \dots & \frac{\sigma_d}{(\sigma_d/\lambda + 1)^2} \end{bmatrix} U^{\top} w^{\star}$$

Bias =
$$\lambda^2 (w^*)^\top (XX^\top + \lambda I)^{-1} XX^\top (XX^\top + \lambda I)^{-1} w^*$$

Eigendecomposition on $XX^{\top} = U\Sigma U^{\top}$

$$= (w^{\star})^{\mathsf{T}} U \begin{bmatrix} \frac{\sigma_1}{(\sigma_1/\lambda + 1)^2} & 0 & 0 \dots \\ 0 & \frac{\sigma_2}{(\sigma_2/\lambda + 1)^2} & 0 \dots \\ 0, & \dots & \frac{\sigma_d}{(\sigma_d/\lambda + 1)^2} \end{bmatrix} U^{\mathsf{T}} w^{\star}$$
 Q: how does bias behave when $\lambda \to +\infty$

Bias =
$$\lambda^2 (w^*)^\top (XX^\top + \lambda I)^{-1} XX^\top (XX^\top + \lambda I)^{-1} w^*$$

Eigendecomposition on $XX^{\top} = U\Sigma U^{\top}$

$$= (w^{\star})^{\mathsf{T}} U \begin{bmatrix} \frac{\sigma_1}{(\sigma_1/\lambda + 1)^2} & 0 & 0 \dots \\ 0 & \frac{\sigma_2}{(\sigma_2/\lambda + 1)^2} & 0 \dots \\ 0, & \dots & \frac{\sigma_d}{(\sigma_d/\lambda + 1)^2} \end{bmatrix} U^{\mathsf{T}} w^{\star}$$
 Q: how does bias behave when $\lambda \to +\infty$ Q: how does bias behave when $\lambda \to 0$

$$\bar{w} = \mathbb{E}[\hat{w}] = (XX^{\mathsf{T}} + \lambda I)^{-1}XX^{\mathsf{T}}w^{\star}$$

$$\bar{w} = \mathbb{E}[\hat{w}] = (XX^{\mathsf{T}} + \lambda I)^{-1}XX^{\mathsf{T}}w^{\star}$$

Variance term:
$$\sum_{i=1}^{n} \mathbb{E}(\hat{w}^{\mathsf{T}} x_i - \bar{w}^{\mathsf{T}} x_i)^2$$

$$\bar{w} = \mathbb{E}[\hat{w}] = (XX^{\mathsf{T}} + \lambda I)^{-1}XX^{\mathsf{T}}w^{\mathsf{T}}$$

Variance term:
$$\sum_{i=1}^{n} \mathbb{E}(\hat{w}^{\mathsf{T}} x_i - \bar{w}^{\mathsf{T}} x_i)^2$$

$$= \sum_{i=1}^{d} \sigma_i^2 / (\sigma_i + \lambda)^2$$

$$\bar{w} = \mathbb{E}[\hat{w}] = (XX^{\mathsf{T}} + \lambda I)^{-1}XX^{\mathsf{T}}w^{\star}$$

Variance term:
$$\sum_{i=1}^{n} \mathbb{E}(\hat{w}^{\mathsf{T}} x_i - \bar{w}^{\mathsf{T}} x_i)^2$$

$$= \sum_{i=1}^{d} \sigma_i^2 / (\sigma_i + \lambda)^2$$

(Optional — tedious but basic computation, see note)

$$\bar{w} = \mathbb{E}[\hat{w}] = (XX^{\mathsf{T}} + \lambda I)^{-1}XX^{\mathsf{T}}w^{\mathsf{*}}$$

Variance term:
$$\sum_{i=1}^{n} \mathbb{E}(\hat{w}^{\mathsf{T}} x_i - \bar{w}^{\mathsf{T}} x_i)^2$$

$$= \sum_{i=1}^{d} \sigma_i^2 / (\sigma_i + \lambda)^2$$

(Optional — tedious but basic computation, see note)

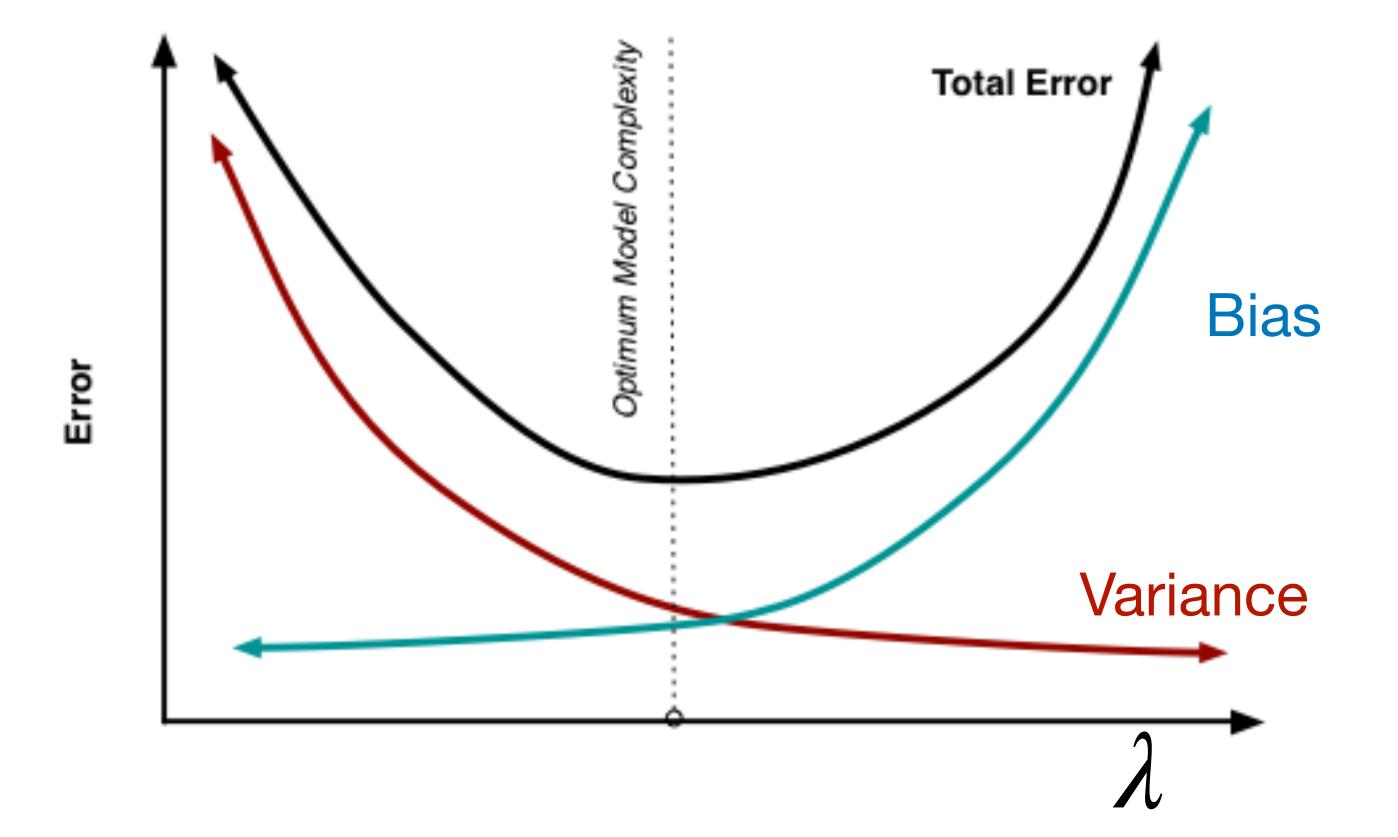
Q: how does Var behave when $\lambda \to + \infty$

Q: how does Var behave when $\lambda \to 0$

Ridge Linear regression

Tuning λ allows us to control the generalization error of Ridge LR solution:

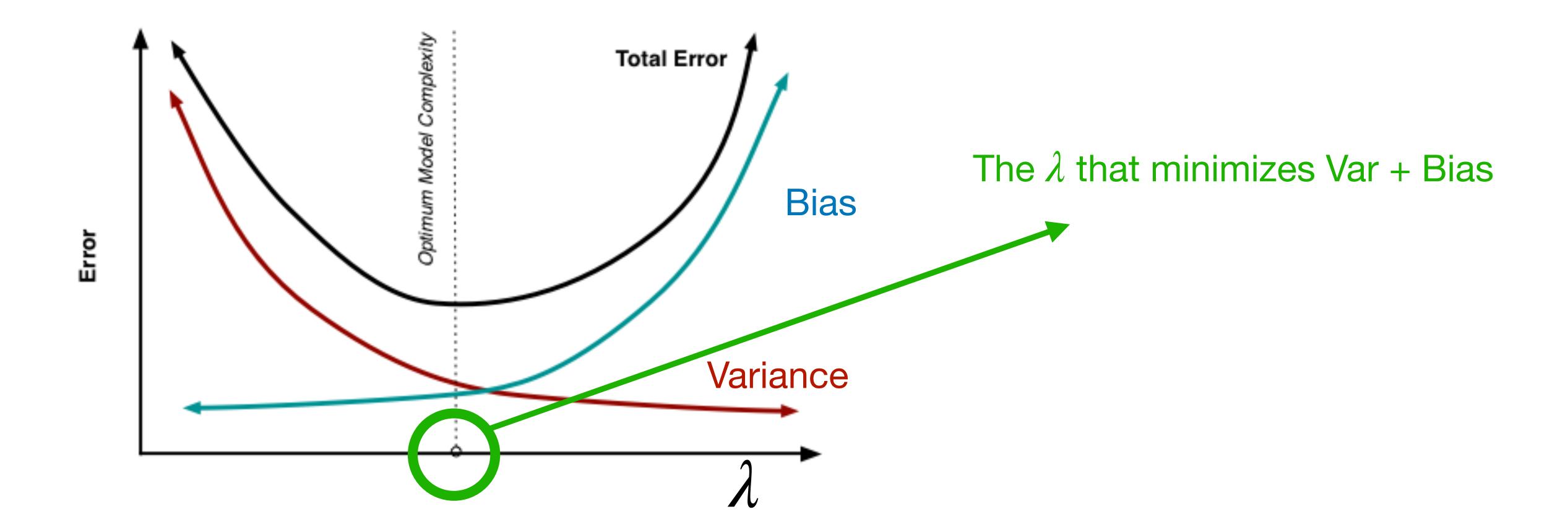
$$\mathbb{E}(\hat{w}^{\mathsf{T}}x - y)^2 = \text{Variance} + \text{Bias} + \text{Inherent noise}$$



Ridge Linear regression

Tuning λ allows us to control the generalization error of Ridge LR solution:

$$\mathbb{E}(\hat{w}^{\mathsf{T}}x - y)^2 = \text{Variance} + \text{Bias} + \text{Inherent noise}$$



Outline of Today

1. Bias & Variance tradeoff demo on Ridge Linear Regression

2. Derivation of Bias / Variance for Ridge LR

2. Model selection in practice (re-visit Cross Validation)

Examples:

1. Select the right order of polynomials for regression

Examples:

1. Select the right order of polynomials for regression

2. Select the right ridge regularization weight λ

Examples:

1. Select the right order of polynomials for regression

2. Select the right ridge regularization weight λ

3. Select the right penalty for slack variables in soft SVM (i.e., the C parameter)

Examples:

1. Select the right order of polynomials for regression

2. Select the right ridge regularization weight λ

3. Select the right penalty for slack variables in soft SVM (i.e., the C parameter)

Cross Validation revisit:

Split the data into K folds

Cross Validation revisit:

Split the data into K folds

$$\hat{w}_k = \text{Ridge LR}(\mathcal{D}_{-i}, \lambda),$$

Cross Validation revisit:

Split the data into K folds

$$\hat{w}_k = \text{Ridge LR}(\mathcal{D}_{-i}, \lambda),$$

$$\epsilon_{vad;k} = \sum_{x,y \in \mathcal{D}_i} (\hat{w}_i^\mathsf{T} x - y)^2 / \|\mathcal{D}_i\|$$

Cross Validation revisit:

Split the data into K folds

$$\hat{w}_k = \text{Ridge LR}(\mathcal{D}_{-i}, \lambda),$$

$$\epsilon_{vad;k} = \sum_{x,y \in \mathcal{D}_i} (\hat{w}_i^\intercal x - y)^2 / |\mathcal{D}_i|$$
 Output avg validation error
$$\bar{\epsilon}_{\lambda} = \sum_{i=1}^K \epsilon_{vad;i} / K$$

Cross Validation revisit:

Split the data into K folds

$$\begin{split} \hat{w}_k &= \operatorname{Ridge} \operatorname{LR}(\mathcal{D}_{-i}, \lambda), \\ e_{vad;k} &= \sum_{x,y \in \mathcal{D}_i} (\hat{w}_i^\mathsf{T} x - y)^2 / \|\mathcal{D}_i\| \end{split}$$

Output avg validation error
$$\bar{e}_{\lambda} = \sum_{i=1}^{K} \epsilon_{vad;i} / K$$

$$\approx \mathbb{E}_{x,y\sim P}(\hat{w}_i^\mathsf{T} x - y)^2$$
, i.e., test error of \hat{w}_i

Cross Validation revisit:

Split the data into K folds

$$\hat{w}_k = \operatorname{Ridge} \operatorname{LR}(\mathcal{D}_{-i}, \lambda),$$

$$\epsilon_{vad;k} = \sum_{x,y \in \mathcal{D}_i} (\hat{w}_i^{\mathsf{T}} x - y)^2 / |\mathcal{D}_i|$$
 Output avg validation error $\bar{\epsilon}_{\lambda} = \sum_{i=1}^K \epsilon_{vad;i} / K$

Output avg validation error
$$\bar{\epsilon}_{\lambda} = \sum_{i=1}^{K} \epsilon_{vad;i} / K$$

$$\approx \mathbb{E}_{x,y\sim P}(\hat{w}_i^\mathsf{T} x - y)^2$$
, i.e., test error of \hat{w}_i

$$\approx \mathbb{E}_{\mathcal{D}}\left[\mathbb{E}_{x,y\sim P}(\hat{w}_{\mathcal{D}}^{\mathsf{T}}x-y)^{2}\right], \text{ i.e.,}$$
 Generalization error of Ridge LR w/ λ

By numerating a set of possible $\lambda \in \mathbb{R}^+$, we select the one that has the smallest Cross-Valid error:

By numerating a set of possible $\lambda \in \mathbb{R}^+$, we select the one that has the smallest Cross-Valid error:

By numerating a set of possible $\lambda \in \mathbb{R}^+$, we select the one that has the smallest Cross-Valid error:

Split the data into K folds For i = 1 to K:
$$| \hat{w}_k = \text{Ridge LR}(\mathcal{D}_{-i}, \lambda), \\ e_{vad;k} = \sum_{x,y \in \mathcal{D}_i} (\hat{w}_i^{\mathsf{T}} x - y)^2 / |\mathcal{D}_i|$$
 Output avg validation error $\bar{e}_{\lambda} = \sum_{i=1}^K e_{vad;i} / K$

By numerating a set of possible $\lambda \in \mathbb{R}^+$, we select the one that has the smallest Cross-Valid error:

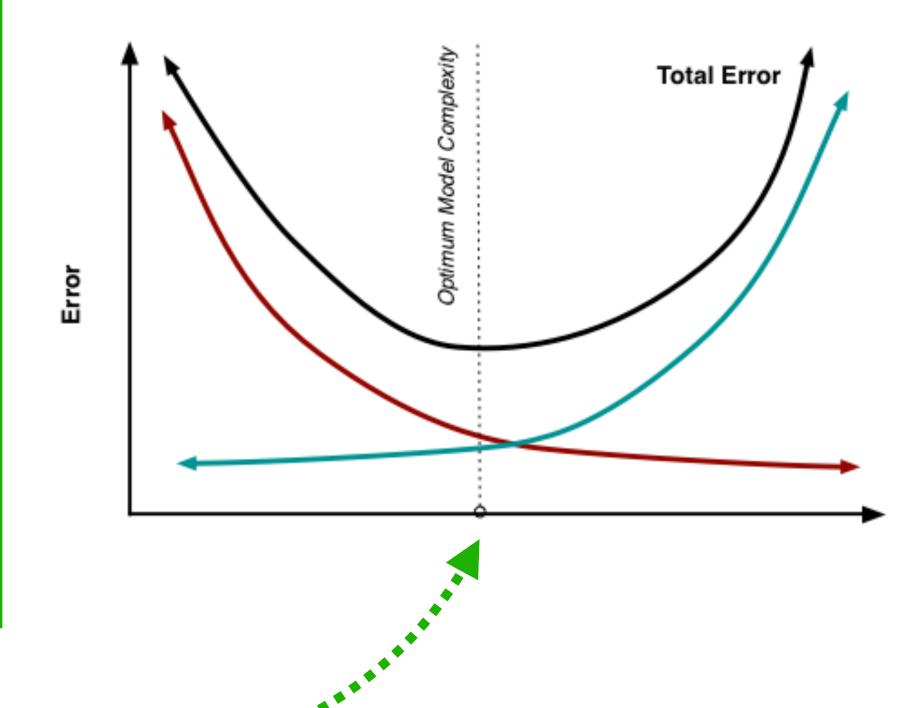
Split the data into K folds For i = 1 to K:
$$|\hat{w}_k = \text{Ridge LR}(\mathcal{D}_{-i}, \lambda), \\ e_{vad;k} = \sum_{x,y \in \mathcal{D}_i} (\hat{w}_i^{\mathsf{T}} x - y)^2 / |\mathcal{D}_i|$$
 Output avg validation error $\bar{e}_{\lambda} = \sum_{i=1}^K e_{vad;i} / K$

Select
$$\lambda^* = \arg\min_{\lambda} \bar{\epsilon}_{\lambda}$$

By numerating a set of possible $\lambda \in \mathbb{R}^+$, we select the one that has the smallest Cross-Valid error:

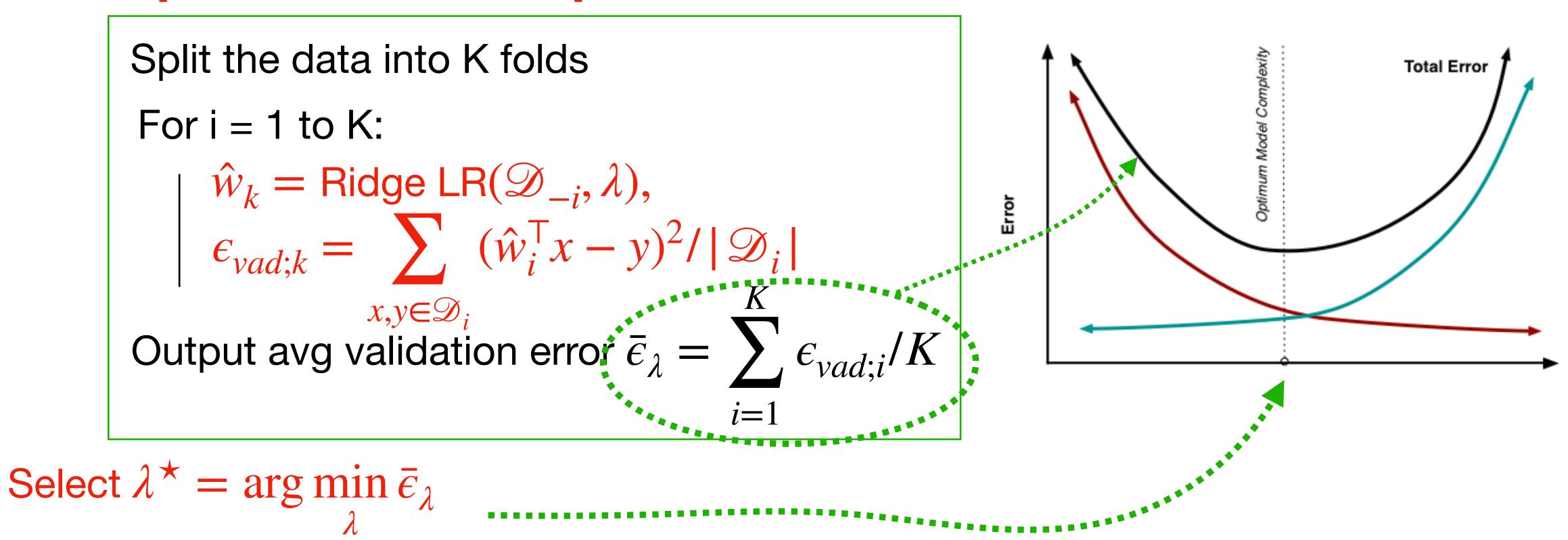
For λ in [1e-5, 1e-4, ... 1e4,1e5]:

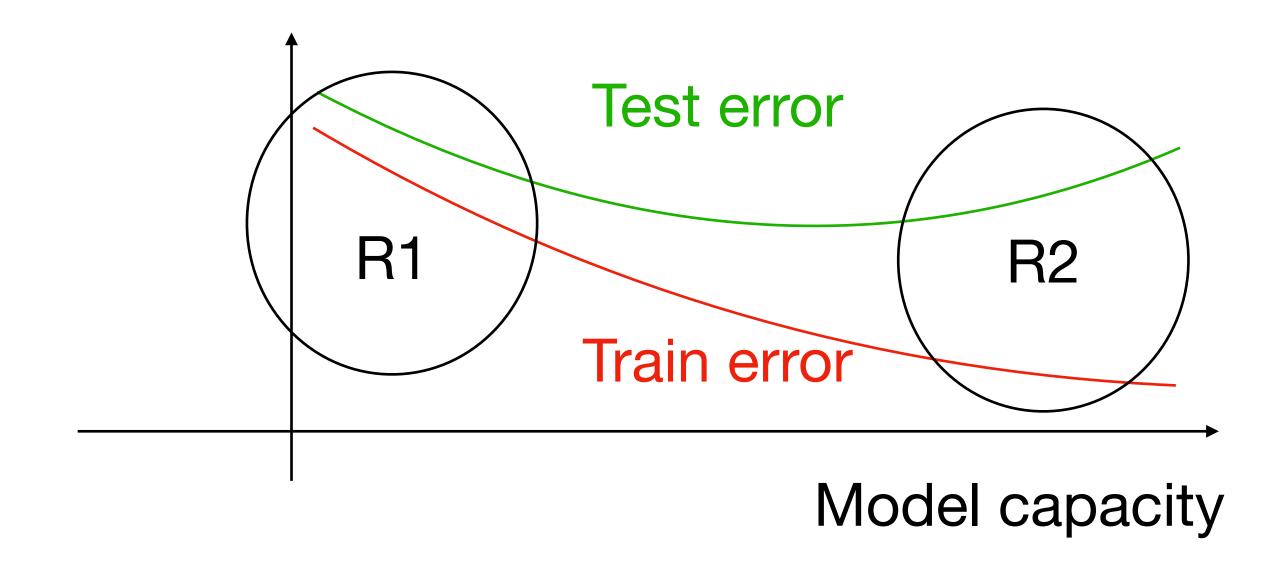
Split the data into K folds For i = 1 to K: $|\hat{w}_k = \text{Ridge LR}(\mathcal{D}_{-i}, \lambda), \\ \epsilon_{vad;k} = \sum_{x,y \in \mathcal{D}_i} (\hat{w}_i^{\intercal} x - y)^2 / |\mathcal{D}_i|$ Output avg validation error $\bar{\epsilon}_{\lambda} = \sum_{i=1}^K \epsilon_{vad;i} / K$

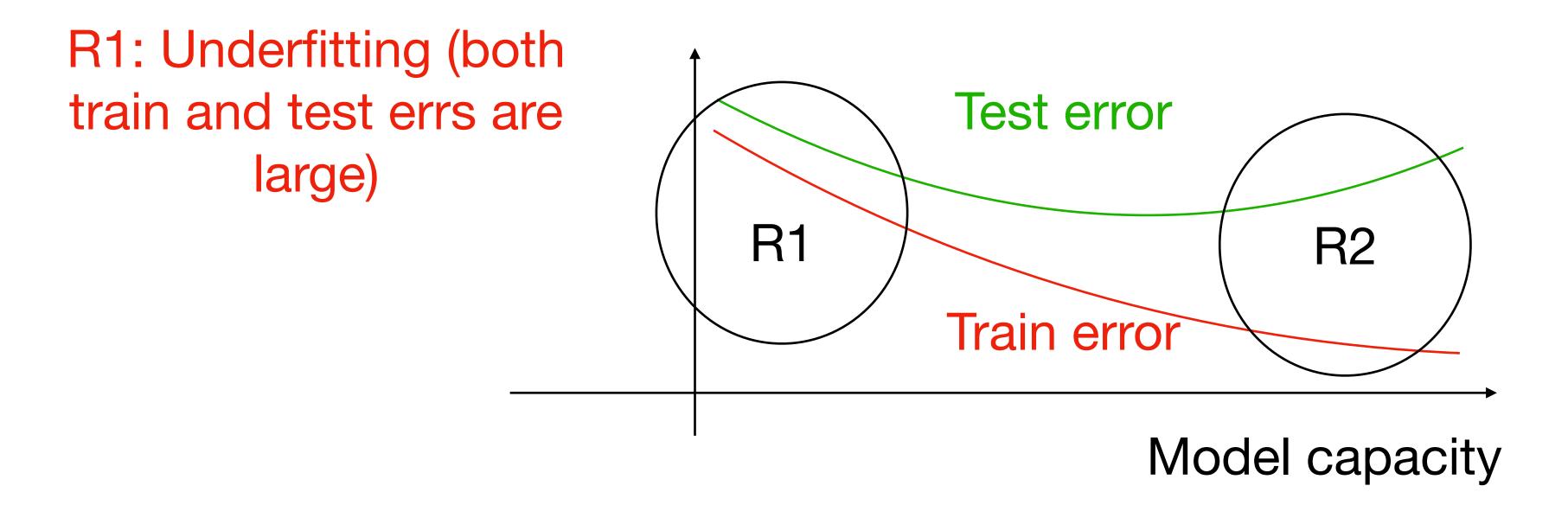


Select $\lambda^* = \arg\min_{\lambda} \bar{\epsilon}_{\lambda}$

By numerating a set of possible $\lambda \in \mathbb{R}^+$, we select the one that has the smallest Cross-Valid error:



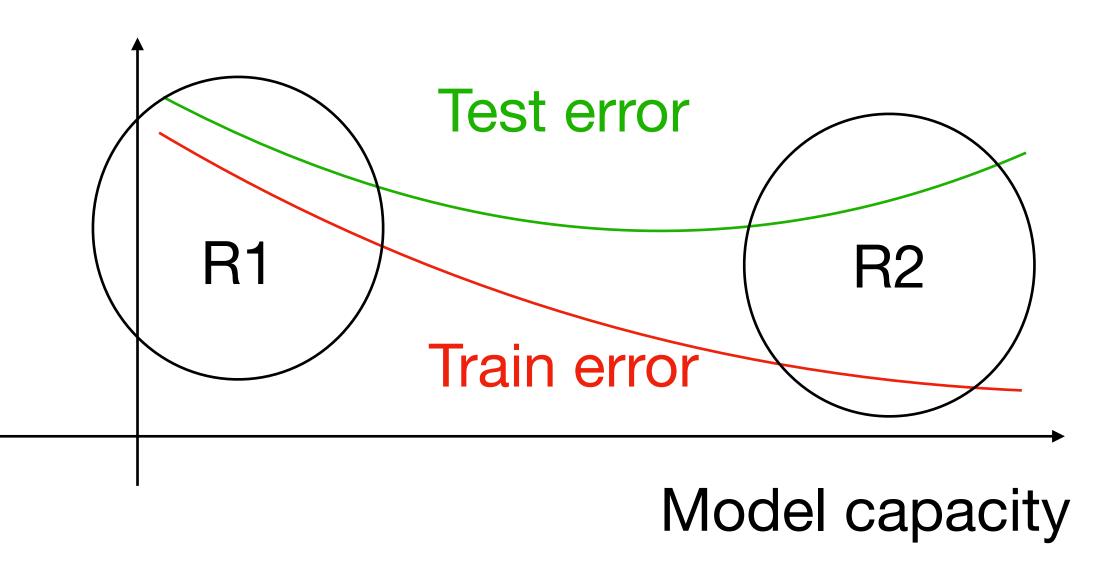




R1: Underfitting (both train and test errs are large)

Suggestions:

1. Increase complexity of models

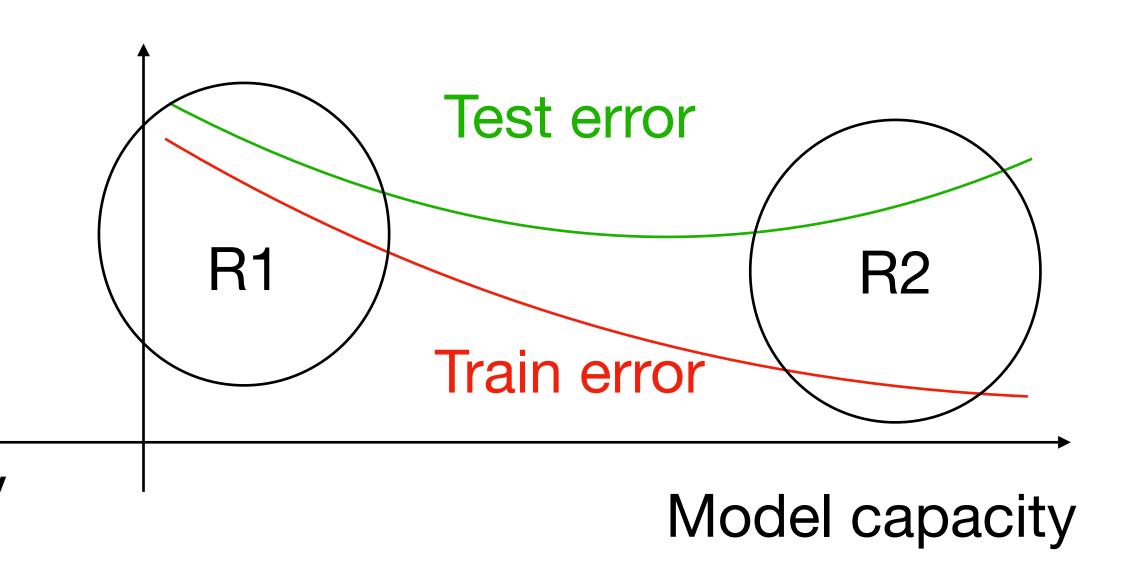


R1: Underfitting (both train and test errs are large)

Suggestions:

1. Increase complexity of models

2. More features



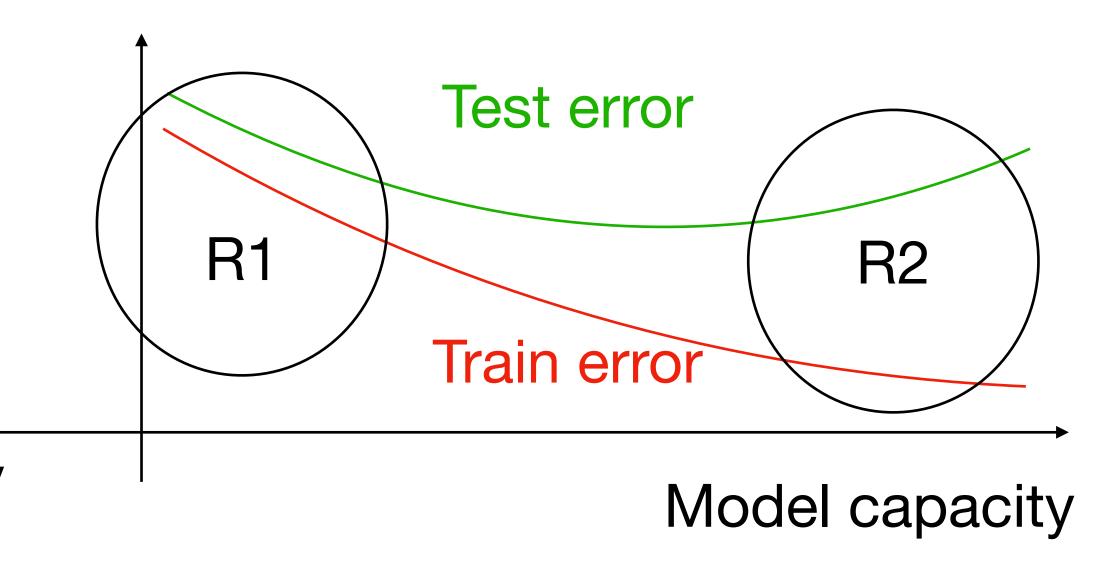
R1: Underfitting (both train and test errs are large)

Suggestions:

1. Increase complexity of models

2. More features

3. Using Boosting (we will see it later)



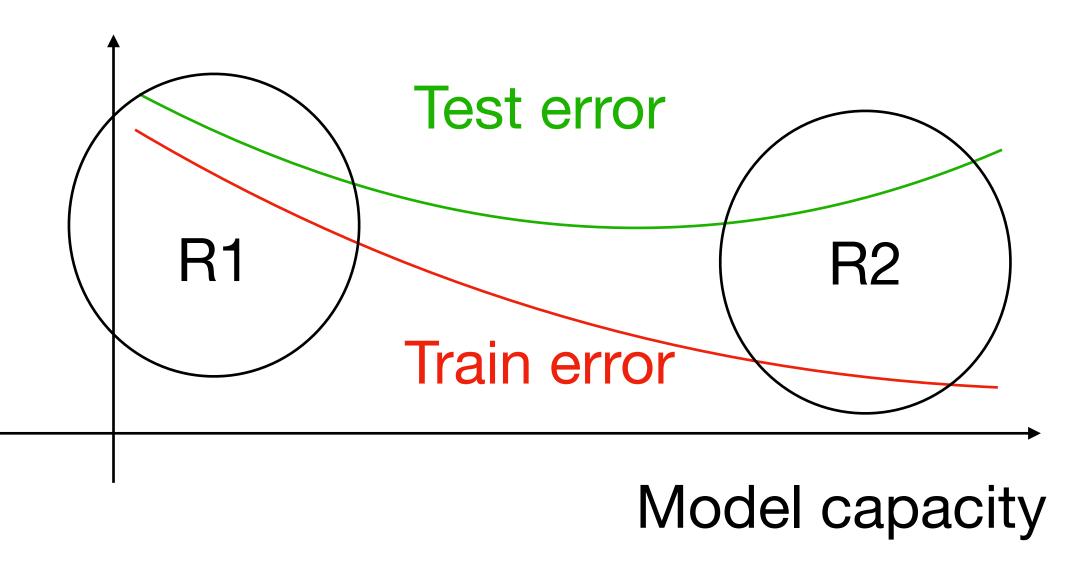
R1: Underfitting (both train and test errs are large)

Suggestions:

1. Increase complexity of models

2. More features

3. Using Boosting (we will see it later)

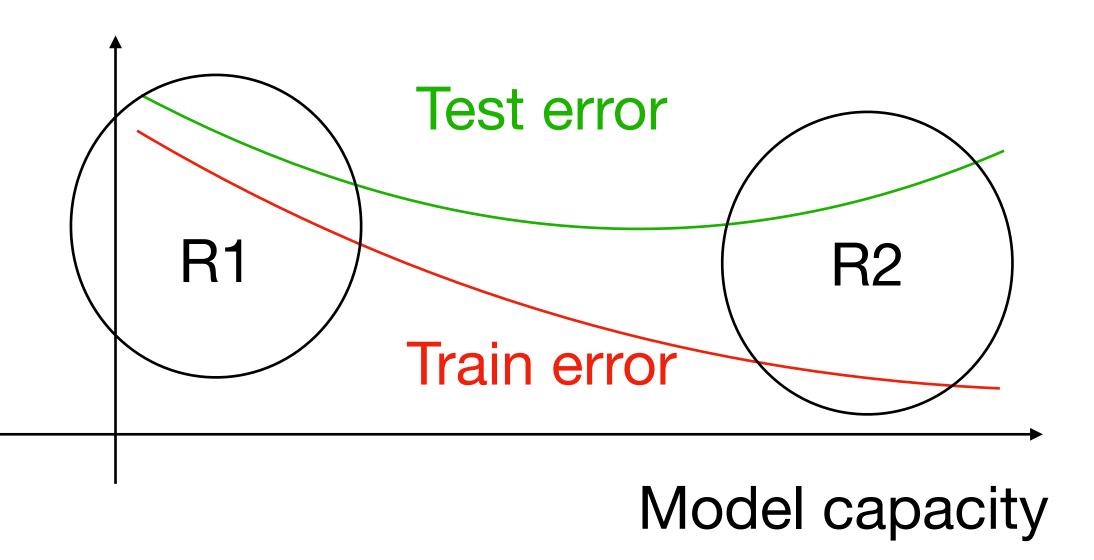


R2: overfitting (small train err but large test err)

R1: Underfitting (both train and test errs are large)

Suggestions:

- 1. Increase complexity of models
 - 2. More features
- 3. Using Boosting (we will see it later)



R2: overfitting (small train err but large test err)

Suggestions:

1. More train data

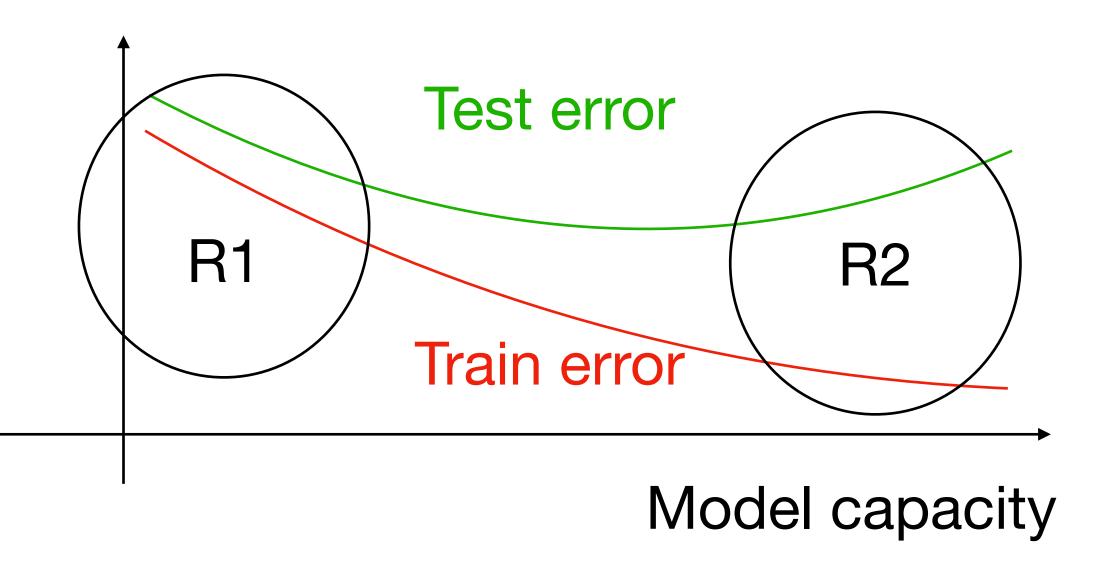
R1: Underfitting (both train and test errs are large)

Suggestions:

1. Increase complexity of models

2. More features

3. Using Boosting (we will see it later)



R2: overfitting (small train err but large test err)

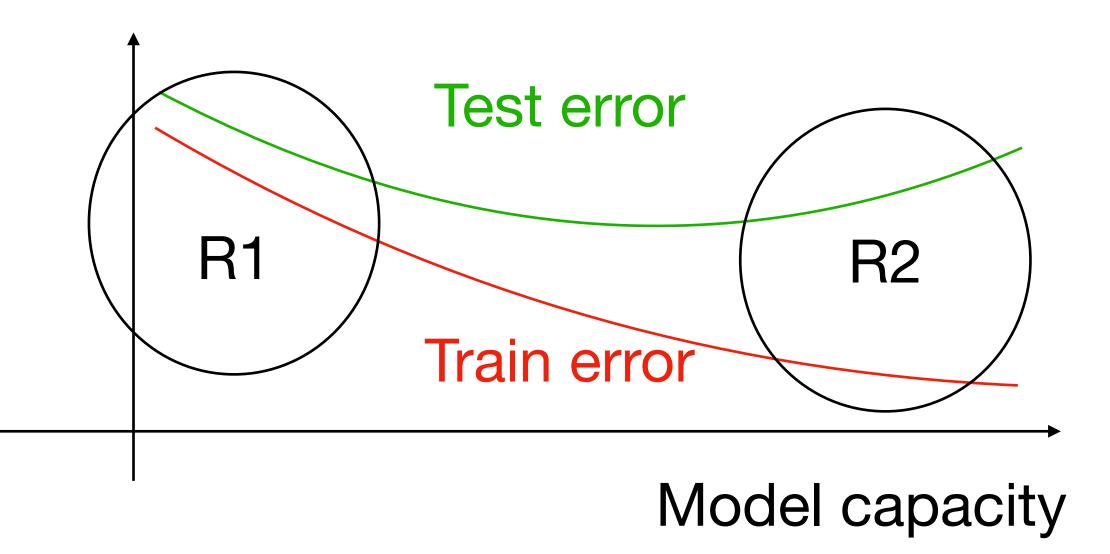
Suggestions:

- 1. More train data
- 2. Reduce model capacity

R1: Underfitting (both train and test errs are large)

Suggestions:

- 1. Increase complexity of models
 - 2. More features
- 3. Using Boosting (we will see it later)



R2: overfitting (small train err but large test err)

Suggestions:

- 1. More train data
- 2. Reduce model capacity
 - 3. Using Bagging (we will see it later)