Overfitting

Bias-Variance Tradeoff

- Choice of hypothesis class introduces learning bias
  - More complex class → less bias
  - More complex class → more variance
Training set error

\[ w^* = \arg\min_w \sum_j \left( t(x_j) - \sum_i w_i h_i(x_j) \right)^2 \]

- Given a dataset (Training data)
- Choose a loss function
  - e.g., squared error (L_2) for regression
- **Training set error**: For a particular set of parameters, loss function on training data:

\[
\text{error}_{\text{train}}(w) = \frac{1}{N_{\text{train}}} \sum_{j=1}^{N_{\text{train}}} \left( t(x_j) - \sum_i w_i h_i(x_j) \right)^2
\]
Prediction error

- Training set error can be poor measure of “quality” of solution
- **Prediction error**: We really care about error over all possible input points, not just training data:

\[
\text{error}_{\text{true}}(w) = E_x \left[ \left( t(x) - \sum_i w_i h_i(x) \right)^2 \right]
\]

\[
= \int_x \left( t(x) - \sum_i w_i h_i(x) \right)^2 p(x)dx
\]

Prediction error as a function of model complexity: Bias/Variance tradeoff
Prediction error as a function of model complexity: train v. true error

\[
\text{error}_{\text{train}}(w) = \frac{1}{N_{\text{train}}} \sum_{j=1}^{N_{\text{train}}} (t(x_j) - \sum_i w_i h_i(x_j))^2
\]

\[
\text{error}_{\text{true}}(w) = \int \left( t(x) - \sum_i w_i h_i(x) \right)^2 p(x) \, dx
\]

Computing prediction error

- Computing prediction
  - Hard integral
  - May not know \( t(x) \) for every \( x \)

\[
\text{error}_{\text{true}}(w) = \int \left( t(x) - \sum_i w_i h_i(x) \right)^2 p(x) \, dx
\]

- Monte Carlo integration (sampling approximation)
  - Sample a set of i.i.d. points \( \{x_1, \ldots, x_M\} \) from \( p(x) \)
  - Approximate integral with sample average

\[
\text{error}_{\text{true}}(w) \approx \frac{1}{M} \sum_{j=1}^{M} \left( t(x_j) - \sum_i w_i h_i(x_j) \right)^2
\]
Why training set error doesn’t approximate prediction error?

- Sampling approximation of prediction error:
  \[
  \text{error}_{true}(\mathbf{w}) \approx \frac{1}{M} \sum_{j=1}^{M} \left( y_j - \sum_i w_i h_i(x_j) \right)^2
  \]

- Training error:
  \[
  \text{error}_{train}(\mathbf{w}) = \frac{1}{N_{train}} \sum_{j=1}^{N_{train}} \left( t(x_j) - \sum_i w_i h_i(x_j) \right)^2
  \]

- Very similar equations!!!
  - Why is training set a bad measure of prediction error???

  Because you cheated!!!

  Training error good estimate for a single \( \mathbf{w} \),
  But you optimized \( \mathbf{w} \) with respect to the training error,
  and found \( \mathbf{w} \) that is good for this set of samples

  Training error is a (optimistically) biased estimate of prediction error

- Very similar equations!!!
  - Why is training set a bad measure of prediction error???
Test set error

Given a dataset, **randomly** split it into two parts:
- Training data – \( \{ x_1, \ldots, x_{N_{\text{train}}} \} \)
- Test data – \( \{ x_1, \ldots, x_{N_{\text{test}}} \} \)

Use training data to optimize parameters \( w \)

**Test set error:** For the **final output** \( \hat{w} \), evaluate the error using:

\[
\text{error}_{\text{test}}(w) = \frac{1}{N_{\text{test}}} \sum_{j=1}^{N_{\text{test}}} \left( t(x_j) - \sum_i w_i h_i(x_j) \right)^2
\]
Overfitting

- **Overfitting**: a learning algorithm overfits the training data if it outputs a solution \( w \) when there exists another solution \( w' \) such that:

\[
[\text{error}_{\text{train}}(w) < \text{error}_{\text{train}}(w')] \land [\text{error}_{\text{true}}(w') < \text{error}_{\text{true}}(w)]
\]

How many points to I use for training/testing?

- Very hard question to answer!
  - Too few training points, learned \( w \) is bad
  - Too few test points, you never know if you reached a good solution
- Bounds, such as Hoeffding’s inequality can help:
  \[
P(\hat{\theta} - \theta^* \geq \epsilon) \leq 2e^{-2N\epsilon^2}
\]
- More on this later this quarter, but still hard to answer
- Typically:
  - If you have a reasonable amount of data, pick test set “large enough” for a “reasonable” estimate of error, and use the rest for learning
  - If you have little data, then you need to pull out the big guns…
    - e.g., bootstrapping
Error estimators

\[ \text{error}_{\text{train}}(w) = \int \left( t(x) - \sum_i w_i h_i(x) \right)^2 p(x) \, dx \]

\[ \text{error}_{\text{train}}(w) = \frac{1}{N_{\text{train}}} \sum_{i=1}^{N_{\text{train}}} \left( t(x_i) - \sum_i w_i h_i(x_i) \right)^2 \]

\[ \text{error}_{\text{test}}(w) = \frac{1}{N_{\text{test}}} \sum_{i=1}^{N_{\text{test}}} \left( t(x_i) - \sum_i w_i h_i(x_i) \right)^2 \]

Error as a function of number of training examples for a fixed model complexity

little data \quad \text{infinite data}
Error estimators

Be careful!!!

Test set only unbiased if you never never ever ever do any any any any any learning on the test data

For example, if you use the test set to select the degree of the polynomial… no longer unbiased!!! (We will address this problem later in the quarter)

$$
\text{Err}_{\text{test}}(w) = \frac{1}{N_{\text{test}}} \sum_{j=1}^{N_{\text{test}}} \left( f(x_j) - \sum_i w_i h_i(x_j) \right)^2
$$

What you need to know

- True error, training error, test error
  - Never learn on the test data
  - Never learn on the test data
  - Never learn on the test data
  - Never learn on the test data
  - Never learn on the test data
  - Never learn on the test data
- Overfitting
Regularization in Linear Regression

- Overfitting usually leads to very large parameter choices, e.g.:
  
  \[-2.2 + 3.1 X - 0.30 X^2\]  \[-1.1 + 4,700,910.7 X - 8,585,638.4 X^2 + \ldots\]

- Regularized or penalized regression aims to impose a “complexity” penalty by penalizing large weights
  
  “Shrinkage” method
Ridge Regression

- Ameliorating issues with overfitting:

- New objective:

\[ \hat{w}_{\text{ridge}} = \arg\min_w \sum_{j=1}^N \left( t(x_j) - (w_0 + \sum_{i=1}^k w_i h_i(x_j)) \right)^2 + \lambda \sum_{i=1}^k w_i^2 \]

\[ = \arg\min_w (Hw - t)^T (Hw - t) + \lambda w^T I_{0+k} w \]

Ridge Regression in Matrix Notation

\[ \hat{w}_{\text{ridge}} = \arg\min_w \sum_{j=1}^N \left( t(x_j) - (w_0 + \sum_{i=1}^k w_i h_i(x_j)) \right)^2 + \lambda \sum_{i=1}^k w_i^2 \]

\[ = \arg\min_w (Hw - t)^T (Hw - t) + \lambda w^T I_{0+k} w \]

residual error

\[ H = \begin{bmatrix} h_0 & \ldots & h_K \end{bmatrix} \quad \text{N data points} \]

\[ w = \begin{bmatrix} \end{bmatrix} \quad \text{K+1 basis functions} \]

\[ t = \begin{bmatrix} \end{bmatrix} \quad \text{N data points} \]
Minimizing the Ridge Regression Objective

\[ \hat{w}_{\text{ridge}} = \arg \min_w \sum_{j=1}^{N} \left( t(x_j) - (w_0 + \sum_{i=1}^{k} w_i h_i(x_j)) \right)^2 + \lambda \sum_{i=1}^{k} w_i^2 \]

\[ = (Hw - t)^T (Hw - t) + \lambda w^T I_{0+k} w \]

Shrinkage Properties

\[ \hat{w}_{\text{ridge}} = (H^T H + \lambda I_{0+k})^{-1} H^T t \]

- If orthonormal features/basis: \( H^T H = I \)
Ridge Regression: Effect of Regularization

\[ \hat{w}_{\text{ridge}} = \arg \min_w \sum_{j=1}^{N} \left( t(x_j) - \left( w_0 + \sum_{i=1}^{k} w_i h_i(x_j) \right) \right)^2 + \lambda \sum_{i=1}^{k} w_i^2 \]

- Solution is indexed by the regularization parameter \( \lambda \)
- Larger \( \lambda \)
- Smaller \( \lambda \)
- As \( \lambda \to 0 \)
- As \( \lambda \to \infty \)

Ridge Coefficient Path

- Typical approach: select \( \lambda \) using cross validation, more on this later in the quarter

From Kevin Murphy textbook
Error as a function of regularization parameter for a fixed model complexity

\[
\text{error}_{\text{train}}(\mathbf{w}) = \frac{1}{N_{\text{train}}} \sum_{i=1}^{N_{\text{train}}} \left( f(x_i) - \sum_{j=1}^{N} w_j u_j(x_i) \right)^2 
\]

\[\lambda = \infty \quad \lambda = 0\]

What you need to know...

- Regularization
  - Penalizes for complex models
- Ridge regression
  - L₂ penalized least-squares regression
  - Regularization parameter trades off model complexity with training error