The road ahead

Thus far we have seen how we can select and evaluate predictive models using the train-validate-test methodology. This approach works well if we have “enough” data.

What if we don’t have enough data to blindly train and validate models? We have to understand the behavior of prediction error well enough to intelligently explore the space of models.
The road ahead

Starting with this lecture:

- We characterize exactly how prediction error behaves through the ideas of bias and variance.
- We develop measures of model complexity that we can use to help us effectively search for “good” models.
- We develop methods of evaluating models using limited data.

A word of caution: All else being equal, more data leads to more robust model selection and evaluation! So these techniques are not “magic bullets”.
Conditional expectation
Conditional expectation

Given the population model for $\vec{X}$ and $Y$, suppose we are allowed to choose any predictive model $\hat{f}$ we want. What is the best one?

$$\text{minimize } \mathbb{E}[(Y - \hat{f}(\vec{X}))^2].$$

(Here expectation is over $(\vec{X}, Y)$.)

**Theorem**

*The predictive model that minimizes squared error is $\hat{f}(\vec{X}) = \mathbb{E}[Y | \vec{X}]$.***
Conditional expectation

Proof:

\begin{align*}
\mathbb{E}[(Y - \hat{f}(\vec{X}))^2] \\
= \mathbb{E}[(Y - \mathbb{E}[Y|\vec{X}]) + \mathbb{E}[Y|\vec{X}] - \hat{f}(\vec{X}))^2] \\
= \mathbb{E}[(Y - \mathbb{E}[Y|\vec{X})^2] + \mathbb{E}[(\mathbb{E}[Y|\vec{X}] - \hat{f}(\vec{X}))^2] \\
+ 2\mathbb{E}[(Y - \mathbb{E}[Y|\vec{X}]) (\mathbb{E}[Y|\vec{X}] - \hat{f}(\vec{X})].
\end{align*}

The first two terms are positive, and minimized if \( \hat{f}(\vec{X}) = \mathbb{E}[Y|\vec{X}] \).

For the third term, using the tower property of conditional expectation:

\begin{align*}
\mathbb{E}[(Y - \mathbb{E}[Y|\vec{X}]) (\mathbb{E}[Y|\vec{X}] - \hat{f}(\vec{X}))] \\
= \mathbb{E} \left[ \mathbb{E}[Y - \mathbb{E}[Y|\vec{X}]|\vec{X}] (\mathbb{E}[Y|\vec{X}] - \hat{f}(\vec{X}) \right] = 0.
\end{align*}

So the squared error minimizing solution is to choose \( \hat{f}(\vec{X}) = \mathbb{E}[Y|\vec{X}] \).
Why don’t we just choose $E[Y|\vec{X}]$ as our predictive model?

*Because we don’t know the distribution of $(\vec{X}, Y)$!*

Nevertheless, the preceding result is a useful guide:

- It provides the benchmark that every squared-error-minimizing predictive model is striving for: approximate the conditional expectation.
- It provides intuition for why linear regression approximates the conditional mean.
Population model

For the rest of the lecture write:

\[ Y = f(\vec{X}) + \varepsilon, \]

where \( \mathbb{E}[\varepsilon|\vec{X}] = 0 \). In other words, \( f(\vec{X}) = \mathbb{E}[Y|\vec{X}] \).

We make the assumption that \( \text{Var}(\varepsilon|\vec{X}) = \sigma^2 \) (i.e., it does not depend on \( \vec{X} \)).

We will make additional assumptions about the population model as we go along.
Prediction error revisited
A note on prediction error and conditioning

When you see “prediction error”, it typically means:

$$\mathbb{E}[(Y - \hat{f}(\vec{X}))^2 | (*))],$$

where (*) can be one of many things:

- $X, Y, \vec{X}$;
- $X, Y$;
- $X, \vec{X}$;
- $X$;
- nothing.

As long we don’t condition on both $\vec{X}$ and $Y$, the model is random!
Models and conditional expectation

So now suppose we have data \(X, Y\), and use it to build a model \(\hat{f}\).

What is the prediction error if we see a new \(X'\)?

\[
E[(Y - \hat{f}(X'))^2 | X, Y, X']
= E[(Y - f(X'))^2 | X']
+ (\hat{f}(X') - f(X'))^2
= \sigma^2 + (\hat{f}(X') - f(X'))^2.
\]

I.e.: When minimizing mean squared error, “good” models should behave like conditional expectation.\(^1\)

Our goal: understand the second term.

\(^{1}\)This is just another way of deriving that the prediction-error-minimizing solution is the conditional expectation.
Models and conditional expectation [*]

Proof of preceding statement:
The proof is essentially identical to the earlier proof for conditional expectation:

\[
\begin{align*}
\mathbb{E}[(Y - \hat{f}(\vec{X}))^2|\mathbf{X}, \mathbf{Y}, \vec{X}] &= \mathbb{E}[(Y - f(\vec{X}) + f(\vec{X}) - \hat{f}(\vec{X}))^2|\mathbf{X}, \mathbf{Y}, \vec{X}] \\
&= \mathbb{E}[(Y - f(\vec{X}))^2|\vec{X}] + (f(\vec{X}) - \hat{f}(\vec{X}))^2 \\
&\quad + 2\mathbb{E}[Y - f(\vec{X})|\vec{X}](f(\vec{X}) - \hat{f}(\vec{X})) \\
&= \mathbb{E}[(Y - f(\vec{X}))^2|\vec{X}] + (f(\vec{X}) - \hat{f}(\vec{X}))^2,
\end{align*}
\]

because \( \mathbb{E}[Y - f(\vec{X})|\vec{X}] = \mathbb{E}[Y - \mathbb{E}[Y|\vec{X}]|\vec{X}] = 0. \)
A thought experiment

Our goal is to understand:

$$\left( \hat{f}(\mathbf{X}) - f(\mathbf{X}) \right)^2.$$  \hfill (**) 

Here is one way we might think about the quality of our modeling approach:

- Fix the design matrix $\mathbf{X}$.
- Generate data $\mathbf{Y}$ many times (parallel “universes”).
- In each universe, create a $\hat{f}$.
- In each universe, evaluate (**).
A thought experiment

Our goal is to understand:

\[(\hat{f} (\vec{X}) - f (\vec{X}))^2. \quad (**)

What kinds of things can we evaluate?

- If \(\hat{f} (\vec{X})\) is “close” to the conditional expectation, then on average in our universes, it should look like \(f (\vec{X})\).

- \(\hat{f} (\vec{X})\) might be close to \(f (\vec{X})\) on average, but still vary wildly across our universes.

The first is *bias*. The second is *variance*.
Let's carry out some simulations with a synthetic model.

*Population model:*

- We generate $X_1, X_2$ as i.i.d. $\mathcal{N}(0, 1)$ random variables.
- Given $X_1, X_2$, the distribution of $Y$ is given by:

$$Y = 1 + X_1 + 2X_2 + \varepsilon,$$

where $\varepsilon$ is an independent $\mathcal{N}(0, 5)$ random variable.

Thus $f(X_1, X_2) = 1 + X_1 + 2X_2$. 
Example: Parallel universes

Generate a design matrix $\mathbf{X}$ by sampling 1000 i.i.d. values of $(X_1, X_2)$.

Now we run $m = 500$ simulations. These are our “universes.” In each simulation, generate data $\mathbf{Y}$ according to:

$$Y_i = f(X_i) + \varepsilon_i,$$

where $\varepsilon_i$ are i.i.d. $N(0, 5)$ random variables.

*In each simulation, what changes is the specific values of the $\varepsilon_i$. This is what it means to condition on $\mathbf{X}$. 
Example: OLS in parallel universes

In each simulation, given the design matrix $X$ and $Y$, we build a fitted model $\hat{f}$ using ordinary least squares.

Finally, let $\tilde{X}$ denote a fixed matrix of 1000 i.i.d. test values of $(X_1, X_2)$. (We use the same test data $\tilde{X}$ across all the universes.)

In each universe we evaluate:

$$\text{MSE} = \frac{1}{1000} \sum_{i=1}^{1000} (\hat{f}(\tilde{X}_{i1}, \tilde{X}_{i2}) - f(\tilde{X}_{i1}, \tilde{X}_{i2}))^2.$$  

(This is an estimate of $\mathbb{E}[(\hat{f}(\vec{X}) - f(\vec{X}))^2|X, Y]$ in the given universe.)

We then create a density plot of these mean squared errors across the 500 universes.
Example: Results

We go through the process with three models: A, B, C.

The three we try are:

- $Y \sim 1 + X_1$.
- $Y \sim 1 + X_1 + X_2$.
- $Y \sim 1 + X_1 + X_2 + \ldots + I(X_1^4) + I(X_2^4)$.

Which is which?
Example: Results

Results:

![MSE density model A B C graph]
A thought experiment: Aside

This is our first example of a frequentist approach:

- The population model is fixed.
- The data is random.
- We reason about a particular modeling procedure by considering what happens if we carry out the same procedure over and over again (in this case, fitting a model from data).
Examples: Bias and variance

Suppose you are predicting, e.g., wealth based on a collection of demographic covariates.

- Suppose we make a constant prediction: \( \hat{f}(X_i) = c \) for all \( i \). Is this biased? Does it have low variance?

- Suppose that every time you get your data, you use enough parameters to fit \( Y \) exactly: \( \hat{f}(X_i) = Y_i \) for all \( i \). Is this biased? Does it have low variance?
The bias-variance decomposition

We can be more precise about our discussion.

\[
\mathbb{E}[(Y - \hat{f}(\vec{X}))^2|\vec{X}, \vec{X}]
= \sigma^2 + \mathbb{E}[(\hat{f}(\vec{X}) - f(\vec{X}))^2|\vec{X}, \vec{X}]
= \sigma^2 + \left(f(\vec{X}) - \mathbb{E}[\hat{f}(\vec{X})|\vec{X}, \vec{X}]\right)^2
+ \mathbb{E}\left[\left(\hat{f}(\vec{X}) - \mathbb{E}[\hat{f}(\vec{X})|\vec{X}, \vec{X}]\right)^2|\vec{X}, \vec{X}\right].
\]

The first term is *irreducible error*.

The second term is $\text{BIAS}^2$.

The third term is $\text{VARIANCE}$. 


The bias-variance decomposition

The bias-variance decomposition measures how sensitive prediction error is to changes in the training data (in this case, $Y$).

- If there are systematic errors in prediction made regardless of the training data, then there is high bias.
- If the fitted model is very sensitive to the choice of training data, then there is high variance.
The bias-variance decomposition: Proof [*]

*Proof:* We already showed that:

$$
\mathbb{E}[(Y - \hat{f}(\bar{X}))^2|X, Y, \bar{X}] = \sigma^2 + (\hat{f}(\bar{X}) - f(\bar{X}))^2 .
$$

Take expectations over $Y$:

$$
\mathbb{E}[(Y - \hat{f}(\bar{X}))^2|X, \bar{X}] = \sigma^2 + \mathbb{E}[(\hat{f}(\bar{X}) - f(\bar{X}))^2|X, \bar{X}] .
$$

Add and subtract $\mathbb{E}[\hat{f}(\bar{X})|X, \bar{X}]$ in the second term:

$$
\mathbb{E}[(\hat{f}(\bar{X}) - f(\bar{X}))^2|X, \bar{X}] \\
= \mathbb{E}\left[\left(\hat{f}(\bar{X}) - \mathbb{E}[\hat{f}(\bar{X})|X, \bar{X}]\right)^2\right] + \mathbb{E}[\hat{f}(\bar{X})|X, \bar{X}] - f(\bar{X})]^2|X, \bar{X}]
$$
The bias-variance decomposition: Proof [*]

Proof (continued): Cross-multiply:

$$\mathbb{E}[(\hat{f}(\vec{X}) - f(\vec{X}))^2 | \mathbf{X}, \vec{X}]$$

$$= \mathbb{E} \left[ \left( \hat{f}(\vec{X}) - \mathbb{E}[\hat{f}(\vec{X}) | \mathbf{X}, \vec{X}] \right)^2 | \mathbf{X}, \vec{X} \right]$$

$$+ \left( \mathbb{E}[\hat{f}(\vec{X}) | \mathbf{X}, \vec{X}] - f(\vec{X}) \right)^2$$

$$+ 2\mathbb{E} \left[ \left( \hat{f}(\vec{X}) - \mathbb{E}[\hat{f}(\vec{X}) | \mathbf{X}, \vec{X}] \right) \left( \mathbb{E}[\hat{f}(\vec{X}) | \mathbf{X}, \vec{X}] - f(\vec{X}) \right) | \mathbf{X}, \vec{X} \right].$$

(The conditional expectation drops out on the middle term, because given $\mathbf{X}$ and $\vec{X}$, it is no longer random.)

The first term is the VARIANCE. The second term is the BIAS$^2$. We have to show the third term is zero.
The bias-variance decomposition: Proof [*]

Proof (continued). We have:

\[
\mathbb{E}\left[ \left( \hat{f}(\tilde{X}) - \mathbb{E}[\hat{f}(\tilde{X})|X, \tilde{X}] \right) \left( \mathbb{E}[\hat{f}(\tilde{X})|X, \tilde{X}] - f(\tilde{X}) \right) \bigg| X, \tilde{X} \right]
\]

\[
= \left( \mathbb{E}[\hat{f}(\tilde{X})|X, \tilde{X}] - f(\tilde{X}) \right) \mathbb{E}\left[ \left( \hat{f}(\tilde{X}) - \mathbb{E}[\hat{f}(\tilde{X})|X, \tilde{X}] \right) \bigg| X, \tilde{X} \right]
\]

\[
= 0,
\]

using the tower property of conditional expectation.
Example: $k$-nearest-neighbor fit

Generate data the same way as before:

We generate 1000 $X_1, X_2$ as i.i.d. $N(0, 1)$ random variables.

We then generate 1000 $Y$ random variables as:

$$Y_i = 1 + 2X_{i1} + 3X_{i2} + \varepsilon_i,$$

where $\varepsilon_i$ are i.i.d. $N(0, 5)$ random variables.
Example: $k$-nearest-neighbor fit

Using the first 500 points, we create a $k$-nearest-neighbor ($k$-NN) model: For any $\vec{X}$, let $\hat{f}(\vec{X})$ be the average value of $Y_i$ over the $k$ nearest neighbors $X_{(1)}, \ldots, X_{(k)}$ to $\vec{X}$ in the training set.

How does this fit behave as a function of $k$?
Example: \( k \)-nearest-neighbor fit

The graph shows root mean squared error (RMSE) as a function of \( k \):
Given $\mathbf{X}$ and $\mathbf{X}$, let $X_1, \ldots, X_k$ be the $k$ closest points to $\mathbf{X}$ in the data. You will show that:

$$
\text{BIAS} = f(\mathbf{X}) - \frac{1}{k} \sum_{i=1}^{k} f(X_i),
$$

and

$$
\text{VARIANCE} = \frac{\sigma^2}{k}.
$$

This type of result is why we often refer to a “tradeoff” between bias and variance.
Linear regression: Linear population model

Now suppose the population model itself is linear:\(^2\)

\[
Y = \beta_0 + \sum_{j} \beta_j X_j + \varepsilon, \quad \text{i.e.} \quad Y = \tilde{X} \beta + \varepsilon,
\]

for some fixed parameter vector \(\beta\).

The errors \(\varepsilon\) are i.i.d. with \(E[\varepsilon_i|X] = 0\) and \(\text{Var}(\varepsilon_i|X) = \sigma^2\).

Also assume errors \(\varepsilon\) are uncorrelated across observations. So for our given data \(X, Y\), we have \(Y = X\beta + \varepsilon\), where:

\[
\text{Var}(\varepsilon|X) = \sigma^2 I.
\]

\(^2\)Note: Here \(\tilde{X}\) is viewed as a row vector \((1, X_1, \ldots, X_p)\).
Linear regression

Suppose we are given data $\mathbf{X}, \mathbf{Y}$ and fit the resulting model by ordinary least squares. Let $\hat{\beta}$ denote the resulting fit:

$$\hat{f}(\vec{X}) = \beta_0 + \sum_j \hat{\beta}_j X_j$$

with $\hat{\beta} = (\mathbf{X}^\top \mathbf{X})^{-1} \mathbf{X}^\top \mathbf{Y}$.

What can we say about bias and variance?
Linear regression

Let’s look at bias:

\[
\mathbb{E}[f(\bar{X})|\bar{X}, X] = \mathbb{E}[\bar{X}\hat{\beta}|\bar{X}, X] \\
= \mathbb{E}[\bar{X}(X^\top X)^{-1}(X^\top Y)|\bar{X}, X] \\
= \bar{X}(X^\top X)^{-1}(X^\top (\mathbb{E}[X\beta + \epsilon|\bar{X}, X])) \\
= \bar{X}(X^\top X)^{-1}(X^\top X)\beta = \bar{X}\beta = f(\bar{X}).
\]

In other words: the ordinary least squares solution is unbiased!
Linear regression: The Gauss-Markov theorem

In fact: among all *unbiased linear models*, the OLS solution has *minimum variance*.

This famous result in statistics is called the *Gauss-Markov* theorem.

**Theorem**

Assume a linear population model with uncorrelated errors. Fix a (row) covariate vector \( \vec{X} \), and let \( \gamma = \vec{X} \beta = \sum_j \beta_j X_j \).

Given data \( X, Y \), let \( \hat{\beta} \) be the OLS solution. Let

\[
\hat{\gamma} = \vec{X} \hat{\beta} = \vec{X} (X^\top X)^{-1} X^\top Y.
\]

Let \( \hat{\delta} = g(X, \vec{X}) Y \) be any other estimator for \( \gamma \) that is linear in \( Y \) and unbiased for all \( X \): \( \mathbb{E}[\hat{\delta}|X, \vec{X}] = \gamma \).

Then \( \text{Var}(\hat{\delta}|X, \vec{X}) \geq \text{Var}(\hat{\gamma}|X, \vec{X}) \), with equality if and only if \( \hat{\delta} = \hat{\gamma} \).
The Gauss-Markov theorem: Proof [\(*\)]

*Proof:* We compute the variance of \( \hat{\delta} \).

\[
\mathbb{E}[(\hat{\delta} - \mathbb{E}[\hat{\delta}|\vec{X}, X])^2|\vec{X}, X]
= \mathbb{E}[(\hat{\delta} - \vec{X}\beta)^2|\vec{X}, X]
= \mathbb{E}[(\hat{\delta} - \hat{\gamma} + \hat{\gamma} - \vec{X}\beta)^2|\vec{X}, X]
= \mathbb{E}[(\hat{\delta} - \hat{\gamma})^2|\vec{X}, X]
\quad + \mathbb{E}[(\hat{\gamma} - \vec{X}\beta)^2|\vec{X}, X]
\quad + 2\mathbb{E}[(\hat{\delta} - \hat{\gamma})(\hat{\gamma} - \vec{X}\beta)|\vec{X}, X].
\]

Look at the last equality: If we can show the last term is zero, then we would be done, because the first two terms are uniquely minimized if \( \hat{\delta} = \hat{\gamma} \).
The Gauss-Markov theorem: Proof [*]

Proof continued: For notational simplicity let $c = g(X, \tilde{X})$. We have:

$$
E[(\hat{\delta} - \hat{\gamma})(\hat{\gamma} - \tilde{X}\beta)|\tilde{X}, X] = E[(cY - \tilde{X}\hat{\beta})^2(\tilde{X}\hat{\beta} - \tilde{X}\beta)|\tilde{X}, X].
$$

Now using the fact that $\hat{\beta} = (X^T X)^{-1}X^T Y$, that $Y = X\beta + \varepsilon$, and the fact that $E[\varepsilon\varepsilon^T|\tilde{X}, X] = \sigma^2 I$, the last quantity reduces (after some tedious algebra) to:

$$
\sigma^2 \tilde{X}(X^T X)^{-1}(X^T c^T - \tilde{X}^T).
$$
Proof continued: To finish the proof, notice that from unbiasedness we have:

\[ \mathbb{E}[cY|X, \tilde{X}] = \tilde{X}\beta. \]

But since \( Y = X\beta + \varepsilon \), where \( \mathbb{E}[\varepsilon|X, \tilde{X}] = 0 \), we have:

\[ cX\beta = \tilde{X}\beta. \]

Since this has to hold true for every \( X \), we must have \( cX = \tilde{X} \), i.e., that:

\[ X^\top c^\top - \tilde{X}^\top = 0. \]

This concludes the proof.
Linear regression: Variance of OLS

We can explicitly work out the variance of OLS in the linear population model.

\[
\text{Var}(\hat{f}(\vec{X}) | X, \vec{X}) = \text{Var}(\vec{X}(X^\top X)^{-1}X^\top Y | X, \vec{X}) = \vec{X}(X^\top X)^{-1}X^\top \text{Var}(Y|X)X(X^\top X)^{-1} \vec{X}.
\]

Now note that \(\text{Var}(Y|X) = \text{Var}(\varepsilon|X) = \sigma^2 I\) where \(I\) is the \(n \times n\) identity matrix.

Therefore:

\[
\text{Var}(\hat{f}(\vec{X}) | X, \vec{X}) = \sigma^2 \vec{X}(X^\top X)^{-1} \vec{X}^\top.
\]
Linear regression: In-sample prediction error

The preceding formula is not particularly intuitive. To get more intuition, evaluate in-sample prediction error:

\[
\text{Err}_{\text{in}} = \frac{1}{n} \sum_{i=1}^{n} \mathbb{E}[(Y - \hat{f}(\bar{X}))^2 | X, Y, \bar{X} = X_i].
\]

This is the prediction error if we received new samples of \(Y\) corresponding to each covariate vector in our existing data. Note that the only randomness in the preceding expression is in the new observations \(Y\).
Linear regression: In-sample prediction error [\(*\)]

Taking expectations over \(Y\) and using the bias variance decomposition on each term of \(Err_{in}\), we have:

\[
E[(Y - \hat{f}(\vec{X}))^2 | X, \vec{X} = X_i] = \sigma^2 + 0^2 + \sigma^2 X_i (X^\top X)^{-1} X_i.
\]

First term is irreducible error; second term is zero because OLS is unbiased; and third term is variance when \(\vec{X} = X_i\).

Now note that:

\[
\sum_{i=1}^{n} X_i (X^\top X)^{-1} X_i = \text{Trace}(H),
\]

where \(H = X(X^\top X)^{-1} X^\top\) is the hat matrix.

It can be shown that the \(\text{Trace}(H) = p\) (see appendix).
Therefore we have:

$$\mathbb{E}[\text{Err}_{in}|X] = \sigma^2 + 0^2 + \frac{p}{n}\sigma^2.$$ 

This is the bias-variance decomposition for linear regression:

- As before $\sigma^2$ is the irreducible error.
- $0^2$ is the BIAS$^2$: OLS is unbiased.
- The last term, $(p/n)\sigma^2$, is the VARIANCE. It increases with $p$. 
It was very important in the preceding analysis that the covariates we used were the same as in the population model!

This is why:

- The bias is zero.
- The variance is \( \frac{p}{n} \sigma^2 \).

On the other hand, with a large number of potential covariates, will we want to use all of them?
What happens if we use a subset of covariates $S \subset \{0, \ldots, p\}$?

- In general, the resulting model will be *biased*, if the omitted variables are correlated with the covariates in $S$.

- It can be shown that the same analysis holds:

$$
\mathbb{E}[\text{Err}_{in}|X] = \sigma^2 + \frac{1}{n} \sum_{i=1}^{n} (X_i \beta - \mathbb{E}[\hat{f}(X_i)|X])^2 + \frac{|S|}{n} \sigma^2.
$$

(Second term is $\text{BIAS}^2$.)

So bias increases while variance decreases.

---

$^3$This is called the *omitted variable bias* in econometrics.
What happens if we introduce a new covariate that is uncorrelated with the existing covariates and the outcome?

- The bias remains zero.
- However, now the variance increases, since $VARIANCE = (p/n)\sigma^2$. 
Appendix: Trace of $H$ [*]

Why does $H$ have trace $p$?

- The trace of a (square) matrix is the sum of its eigenvalues.
- Recall that $H$ is the matrix that projects $Y$ into the column space of $X$. (See Lecture 2.)
- Since it is a projection matrix, for any $v$ in the column space of $X$, we will have $Hv = v$.
- This means that 1 is an eigenvalue of $H$ with multiplicity $p$.
- On the other hand, the remaining eigenvalues of $H$ must be zero, since the column space of $X$ has rank $p$.

So we conclude that $H$ has $p$ eigenvalues that are 1, and the rest are zero.