Book Notes

Statistical Learning with R

Jon Geiger

January 20, 2022

Tentative Schedule

Week 1: Chapter 1

Week 2: Chapter 2.1-2.2

Week 3: Chapter 4.1-4.3 (4.4 optional). Lab 4.7.1-2 (4.7.3-5 optional).

Week 4: Chapter 4.5-4.6. Lab 4.7.7.

Week 5: Chapter 5.1-5.2. Lab 5.3.1-4.

Week 6: Chapter 6.2-6.3 (6.4 optional). Lab 6.5.1-3.

Week 7: Chapter 8.1-8.2. Lab 8.3.1-5

Week 8: Chapter 12.1-12.2. Lab 12.5.1.

Week 9: Chapter 12.4. Lab 12.5.3-4

Week 10: Grace Week

Organization

Chapters get single-# headers, and sections get double-## headers.

Sub-sections (e.g. Chapter 2.1.3) are separated with horizontal lines (created with three asterisks):

Chapter 1: Introduction

Statistical Learning is split up into **supervised learning** and **unsupervised learning**.

- *Supervised learning* "involves building a statistical modeling for predicting, or estimating, an output based on one or more inputs."
- *Unsupervised learning* involves "inputs but no supervising output," allowing us to learn structure from the data.

Some Key Datasets

`Wage` Data:

- Includes a number of factors relating to wages for a specific group of men from the Atlantic region of the U.S.
- Involves predicting a *quantitative* output, useful in *regression*

`Smarket` (Stock Market) Data:

- Contains daily movements in the S&P 500 in the five-year period between 2001 and 2005
- The goal is *classification*, or to predict whether the prices will increase or decrease on a given day.

`NCI60` Gene Expression Data:

- Contains 6,830 gene expression measurements for each of 64 cancer cell lines.
- This is a *clustering* problem, and we can analyze *principal components* of the data.

Purpose of the Book

"The purpose of *An Introduction to Statistical Learning* (ISL) is to facilitate the transition of statistical learning from an academic to a mainstream field."

ISL is based on four principles:

1. Many statistical learning methods are relevant and useful in a wide range of academic and non-academic disciplines, beyond just the statistical sciences.
2. Statistical learning should not be viewed as a series of black boxes.
3. While it is important to know what job is performed by each cog, it is not necessary to have the skills to construct the machine inside the box.
4. We presume that the reader is interested in applying statistical learning methods to real-world problems.

Notation

- $\mathbf{X}$ is an $n \times p$ matrix whose (i, j)th element is x_{ij}
  - Rather than $m \times n$ for m observations of n variables, we can think of $\mathbf{X}$ as a matrix (or spreadsheet) with n rows and p columns, or n observations of p variables.
- Vectors are column vectors by default.
- x_i is the vector of **rows** of $\mathbf{X}$, with length p:

$$x_i = \begin{pmatrix} x_{i1} \\ x_{i2} \\ \vdots \\ x_{ip} \end{pmatrix}$$

- $\mathbf{x}$ is the vector of the **columns** of $\mathbf{X}$, with length n:

$$\mathbf{x}_j = \begin{pmatrix} x_{1j} \\ x_{2j} \\ \vdots \\ x_{nj} \end{pmatrix}$$

- y_i denotes the ith observation of the variable on which we wish to make predictions. We can write the set of all n observations in vector form as:

$$\mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

- A vector of length n will be denoted in lower-case bold, such as:

$$\mathbf{a} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

Chapter 2: Statistical Learning

2.1: What is Statistical Learning?

Input Variables are also called *predictors*, *independent variables*, *features*, or just *variables*, denoted by X_i's. **Output Variables** are also called *responses* or *dependent variables*, denoted using the symbol Y.

With a quantitative response Y and p predictors $X = (X_1, X_2, \ldots, X_p)$, we assume there is some relationship between Y and X which takes the general form:

$$Y = f(X) + \epsilon$$

f is an unknown function of all the X_i's, and ϵ is a random *error term*, independent of X with a zero mean. f represents the *systematic* information that X provides about Y.

Statistical Learning refers to a set of approaches for estimating f.

We estimate f for two reasons: **prediction**, and **inference**.

We can *predict* Y with $\hat{Y} = \hat{f}(X)$, where $\hat{f}(X)$ represents our estimate for f, and $\hat{Y}$ is the resulting prediction of Y. Our goal is to minimize the reducible error (the error which can be changed by modifying f), keeping in mind that ϵ cannot be reduced.

In *inference*, we wish to understand the association between Y and each of the X_i's. A problem of inference could be driven by the following questions:

- Which predictors are associated with the response?
- What is the relationship between the response and the predictor?
- Can the relationship between Y and each predictor be adequately summarized using a linear equation, or is the relationship more complicated?

There are two methods to estimating f: **Parametric Methods**, and **Non-Parametric Methods**.

Parametric Methods involve a two-step, model-based approach:

1. We make an assumption about the functional form of f. One simple example might be that f is linear in X:
   $$f(X) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_p X_p$$
   With a linear model, we estimate $p + 1$ coefficients from β_0 to β_p.
2. After model selection, we need to *fit* or *train* the model. This is the process of estimating the parameters β_0 through β_p such that in the case of the linear model above,
   $$Y \approx \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_p X_p$$

The process is called *parametric* because we are *estimating parameters* to fit the model. This is generally simpler because it is easier to fit a set of parameters than it is to fit an entirely arbitrary function f. A parametric model has the disadvantage in that it typically does not match the true unknown form of f.

Non-parametric models have the advantage of not assuming a form for f, and can thus fit a wider range of possible shapes of f. These models need many more observations to work effectively. An example of a non-parametric model is a *thin-plate spline*, which can be either rough or smooth, where the roughness is analogous to overfitting data in a parametric model.

In choosing a model, there's a tradeoff between the *interpretability* of that model and the *flexibility* of that model. Generally, the more flexible a model is (bagging, boosting, SVMs, Deep Learning), the less interpretable the output is. Likewise, less flexible models (Subset Selection, Lasso, Least Squares) tend to be more interpretable.

- Choosing a more *restrictive* (less flexible) model is preferable in problems of inference, as the outcome needs to be interpretable.
- Conversely, more flexible models can be better for prediction problems when interpretability is not strictly necessary.

All examples from this past chapter have been examples of *supervised learning*. These techniques include linear regression, logistic regression, Generalized Additive Models (GAMs), boosting, Support Vector Machines (SVMs), and boosting. These all have in common that for a single observation x_i, there is an associated response measurement y_i.

Unsupervised learning tackles a different challenge, namely, that for each observation i, we have a set of measurements x_i with no associated response y_i. These types of problems are usually *cluster analysis* problems, where we try to find patterns, order, and/or groups in the data. More specifically, the goal is to figure whether or not the data fall into distinct groups, and if they do, which observations comprise those groups.

There do exist some problems which can be categorized as *semi-supervised learning* problems, namely scenarios in which our response data is incomplete. Namely, if we have both predictor and response measurements for m observations, where $m < n$, then for the remaining $m - n$ measurements we have predictor data but no response data.

Regression problems have a *quantitative response*. e.g. Least Squares.

Classification problems have a *categorical response*. e.g. Despite its name, logistic regression.

Some statistical methods, such as K-nearest neighbors (KNN) and boosting, can be used for either quantitative or categorical responses.

2.2: Assessing Model Accuracy

In evaluating statistical learning methods, we need some measure of how well its predictions match the observed data. In the case of regression, this is the *mean squared error* (MSE):

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{f}(x_i))^2$$

A "good prediction" will yield a small MSE, as the error term $(y_i - \hat{f}(x_i))$ will be small for each observation.

With the case of linear regression, though, it is quite possible to overfit the data to perfectly capture each response (thus the MSE would be zero). We don't care how our model performs on our *training data*, but rather how it performs when we feed it *test data*. Because of this, we care about fitting parameters for $\hat{f}$ that will minimize the *test MSE* rather than the *training MSE*.

Often when choosing a model, it is useful to plot the training MSE and test MSE as a function of flexibility. Typically, the most flexible models will can yield a very low training MSE but will fail to produce a low test MSE (overfitting). Similarly, the least flexible models cannot produce a low MSE in either the training nor the test data, so the best models have a training MSE and test MSE that are roughly equal.

The test MSE for a given value x_0 can always be decomposed into the sum of three fundamental quantities:

1. The *variance* of $\hat{f}(x_0)$
2. The squared *bias* of $\hat{f}(x_0)$
3. The variance of the error terms ϵ

$$E\left(y_0 - \hat{f}(x_0)\right)^2 = \text{Var}(\hat{f}(x_0)) + \left[\text{Bias}(\hat{f}(x_0))\right]^2 + \text{Var}(\epsilon)$$

In this case, $E\left(y_0 - \hat{f}(x_0)\right)^2$ is the *expected test MSE* at x_0. If our goal is to minimize the MSE, we need to estimate f such that the learning method achieves both a *low bias* and a *low variance*. This is known as the **bias-variance trade-off**.

The **variance** of a statistical learning method refers to the amount by which $\hat{f}$ would change if we estimated it using a different training data set. Ideally, the estimate for f should not vary much between training sets. This would be a *low variance*. In general, more flexible statistical methods have higher variance (overfitting to the training data).

The **bias** of a statistical learning method refers to the error that is introduced by approximating a real-life problem (usually very complicated) by a much simpler model. It's unlikely that a real-life problem actually has a linear relationship (as an example), so performing linear regression will result in some bias in estimating f.

It's very easy to achieve a model with low bias and high variance (draw a line that goes through every data point), as well as a model with high bias and low variance (fit a horizontal line through the data). Minimizing the test MSE is the key to finding the perfect bias-variance trade-off.

The bias-variance tradeoff also applies to the classification setting. In the case of classification, we assess our estimate of f with the training **error rate**, or the proportion of mistakes that are made if we apply our estimate to the training observations:

$$\frac{1}{n}\sum_{i=1}^{n} I(y_i \neq \hat{y}_i) \quad \text{where} \quad I = \begin{cases} 1 & \text{if } y_i \neq \hat{y}_i \\ 0 & \text{if } y_i = \hat{y}_i \end{cases}$$

In other words, I makes a binary indication of whether or not a classification error was made. Applying a classification method to test data, then, the *test error rate* with a set of test observations (x_0, y_0) is given by

$$\text{Ave}(I(y_0 \neq \hat{y}_0))$$

A good classifier is one for which the test error is minimized.

The **Bayes Classifier** is one which utilizes conditional probability to classify points in a two-class problem. Particularly, it seeks to find $Pr(Y = j|X = x_0)$, or "given that the observation is x_0, what's the probability that it belongs to class j?"

- The *Bayes error rate* is given by $1 - \max_j Pr(Y = j|X = x_0)$
- In general, the overall Bayes error rate is given by $1 - E\left(\max_j \Pr(Y = j|X = x_0)\right)$

The K**-Nearest Neighbors Classifier** (KNN) allows us to construct a decision boundary based on real data. It accomplishes this by choosing a test observation x_0, identifying the K closest points ($\mathcal{N}_0$), then estimates the conditional probability that x_0 would be in class j as the fraction of points whose response values equal j:

$$\Pr(Y = j|X = x_0) = \frac{1}{K} \sum_{i \in \mathcal{N}_0} I(y_i = j)$$

Similar to regression methods from earlier sections, KNN can be very flexible with low values of K, and for any set of training data, it can be important to optimize the value of K selected to minimize the test error.

Chapter 4: Classification

Classification is a statistical method used with a *qualitative* response variable.

Some classifiers covered in this chapter include logistic regression, linear discriminant analysis, quadratic discriminant analysis, naive Bayes, and K-nearest neighbors. These topics are used to segue into Generalized Linear Models and Poisson Regression.

4.1: An Overview of Classification

The `Default` data set will be used extensively, in predicting whether an individual will default on their credit card payment, on the basis of their annual income and monthly credit card balance.

We'll be building a model to predict `default` from `balance` (X_1) and `income` (X_2).

4.2: Why Not Linear Regression?

Linear regression doesn't work for classification problems because in order to predict an outcome, we need to *numerically encode* the categories as a quantitative response variable. This doesn't work because the categories rarely ever have any logical order.

In the case of predicting medical diagnoses, a response variable might look like:

$$Y = \begin{cases} 1 & \text{if } \texttt{stroke}, \\ 2 & \text{if } \texttt{drug overdose}, \\ 3 & \text{if } \texttt{epileptic seizure}. \end{cases}$$

The situation improves slightly if we choose to use the *dummy variable* approach, where we code a response variable which looks like:

$$Y = \begin{cases} 0 & \text{if } \texttt{stroke}; \\ 1 & \text{if } \texttt{drug overdose}. \end{cases}$$

In this case, we could have some estimates outside of the $[0, 1]$ range, which leads to difficulty interpreting probabilities.

Overall: (1) regression cannot accommodate non-binary classification, and (b) regression methods will not provide meaningful estimates of $\Pr(Y|X)$, even with just two classes.

4.3: Logistic Regression

Consider the binary classification problem, namely with the `Default` data set.

Logistic regression models the *probability* that Y belongs to a particular class, rather than modeling the classification directly.

The probability of defaulting given a certain balance can be expressed as

$$\Pr(\texttt{balance} = \texttt{Yes}|\texttt{balance}) \equiv p(\texttt{balance})$$

In general, we notate that $p(X) = \Pr(Y = 1|X)$. In logistic regression, we use the logistic function, which we can rearrange to create a linear regression problem.

$$p(X) = \frac{e^{\beta_0+\beta_1 X}}{1 + e^{\beta_0+\beta_1 X}} \quad \text{Logistic Function}$$

$$\therefore \quad \frac{p(X)}{1 - p(X)} = e^{\beta_0+\beta_1 X} \quad \text{Odds}$$

$$\log\left(\frac{p(X)}{1 - p(X)}\right) = \beta_0 + \beta_1 X \quad \text{Log Odds / Logit}$$

Odds close to zero indicate low probabilities of default, and values close to ∞ indicate high probabilities of default. Interpreting this final equation is a bit tricky, as a one-unit increase in X will yield a β_1 increase in the log odds.

The coefficients β_0 and β_1 must be estimated to best fit our training data. This is done using *maximum likelihood estimation*. The likelihood function is:

$$\ell(\beta_0, \beta_1) = \prod_{i:y_i=1} p(x_i) \prod_{i':y_{i'}=0} (1 - p(x_{i'}))$$

The estimates $\hat{\beta}_0$ and $\hat{\beta}_1$ are chosen to maximize this likelihood function.

In a problem of inference looking for association between `default` and `balance`, our null hypothesis would be $H_0 : \beta_1 = 0$, which makes sense because a one-unit increase in X should not affect Y at all. So the null logistic function will be $p(X) = \frac{e^{\beta_0}}{1+e^{\beta_0}}$. Similarly to linear regression, the z-statistic associated with β_1 is $z = \hat{\beta}_1/\text{SE}(\hat{\beta}_1)$.

For making predictions, we plug our estimates into the logistic function, so we have the equation:

$$\hat{p}(X) = \frac{e^{\hat{\beta}_0+\hat{\beta}_1 X}}{1 + e^{\hat{\beta}_0+\hat{\beta}_1 X}}$$

Multiple Logistic Regression extends nicely out from simple logistic regression, where we can generalize our log odds equation from earlier:

$$\log\left(\frac{p(X)}{1 - p(X)}\right) = \beta_0 + \beta_1 X_1 + \cdots + \beta_p X_p$$

Where we have p predictors. This also means that our logistic equation for making predictions becomes:

$$p(X) = \frac{e^{\beta_0+\beta_1 X_1+\cdots+\beta_p X_p}}{1 + e^{\beta_0+\beta_1 X_1+\cdots+\beta_p X_p}}$$

We would also use maximum likelihood estimation to estimate all the coefficients $\beta_0, \beta_1, \ldots, \beta_p$.

What happens when we want to classify something which has more than one outcome? In the previous section we dealt with the three classes being `stroke`, `drug overdose`, and `epileptic seizure`. This is a problem of **multinomial logistic regression**. We select a single class to act as the *baseline*, then we say that:

$$\Pr(Y = k|X = x) = \begin{cases} \dfrac{e^{\beta_{k0}+\beta_{k1}x_1+\cdots+\beta_{kp}x_p}}{1+\sum_{l=1}^{K-1} e^{\beta_{l0}+\beta_{l1}x_1+\cdots+\beta_{lp}x_p}} & \text{for } k = 1, \ldots, K-1, \\ \dfrac{1}{1+\sum_{l=1}^{K-1} e^{\beta_{l0}+\beta_{l1}x_1+\cdots+\beta_{lp}x_p}} & \text{for } k = K. \end{cases}$$

Additionally, it can be shown that

$$\log\left(\frac{\Pr(Y = k|X = x)}{\Pr(Y = K|X = x)}\right) = \beta_{k0} + \beta_{k1}x_1 + \cdots + \beta_{kp}x_p$$

An alternative coding for multinomial logistic regression is known as *softmax* coding, where, rather than selecting a baseline class, we treat all K classes symmetrically, and assume that for $k = 1, \ldots, K$,

$$\Pr(Y = k|X = x) = \frac{e^{\beta_{k0}+\beta_{k1}x_1+\cdots+\beta_{kp}x_p}}{1+\sum_{l=1}^{K} e^{\beta_{l0}+\beta_{l1}x_1+\cdots+\beta_{lp}x_p}}$$

So, we actually estimate coefficients for all K classes rather than just for $K-1$ classes. As a result of this, the log odds ratio between the kth and k'th classes is

$$\log\left(\frac{\Pr(Y = k|X = x)}{\Pr(Y = k'|X = x)}\right) = (\beta_{k0} - \beta_{k'0}) + (\beta_{k1} - \beta_{k'1})x_1 + \cdots + (\beta_{kp} - \beta_{k'p})x_p$$