CS 189: Introduction to Machine Learning

Fall 2017

•

Homework 0

Due on Friday, August 25th, 2017 at 10 p.m.

•

Solutions by

Jinhong Du

3033483677

Problem 1: Getting Started

1. Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. In case of course events, just describe the group. How did you work on this homework? Any comments about the homework?

   Jinhong Du
   jaydu@berkeley.edu

2. Please copy the following statement and sign next to it:
   I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.

   I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up. Jinhong Du

3. How many hours did the homework take you to finish?
   ◯ 1 ◯ 2 ☑ 3 ◯ 4 ◯ 5 ◯ 6 ◯ 7 ◯ 8 ◯ 9 ◯ 10+

Problem 2: Sample Submission

Please submit a plain text file to the Gradescope programming assignment “Homework 0 Test Set”:

1. Containing 5 rows, where each row has only one value “1”.
2. No spaces or miscellaneous characters.
3. Name it “submission.txt”.

Problem 3: Eigendecomposition Review

Compute eigenvectors and eigenvalues for the following matrix. Show your work.

$$\begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}$$

Proof.

$$A = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}$$

Let

$$\begin{aligned} |\lambda I - A| &= \begin{vmatrix} \lambda - 1 & -3 \\ -3 & \lambda - 1 \end{vmatrix} \\ &= (\lambda - 1)^2 - 9 \\ &= \lambda^2 - 2\lambda - 8 \\ &= (\lambda - 4)(\lambda + 2) \\ &= 0 \end{aligned}$$

We got $\lambda_1 = 4,\ \lambda_2 = -2$

$$\begin{aligned} (4I - A)u &= \begin{bmatrix} 3 & -3 \\ -3 & 3 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \\ &= 0 \end{aligned}$$

We get $u_4 = (1, 1)^T$.

$$\begin{aligned} (-2I - A)u &= \begin{bmatrix} -3 & -3 \\ -3 & -3 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \\ &= 0 \end{aligned}$$

We get $u_{-2} = (-1, 1)^T$. $\square$

Problem 4: Linear Regression and Adversarial Noise

Suppose we have training data consisting of n points (x_i, y_i), which we have modeled as coming from $y_i = ax_i + b$. We will do standard linear ordinary least-squares regression on the data to recover estimates for a and b. Say that y_i are actually coming from $y_i = ax_i + b + \varepsilon_i$, for some unknown disturbance process ε_i.

1. Can an adversary force the linear regression to recover any desired a, b by setting exactly 1 of the ε_i to be a selected non-zero value?

(1)

$$\begin{aligned} Q &= \sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \\ &= \sum_{i=1}^{n}(y_i - ax_i - b)^2 \end{aligned}$$

Let

$$\begin{cases} \dfrac{\partial Q}{a} = -2\sum\limits_{i=1}^{n} x_i(y_i - ax_i - b) = 0 \\ \dfrac{\partial Q}{b} = 2\sum\limits_{i=1}^{n}(y_i - ax_i - b) = 0 \end{cases}$$

i.e.

$$\begin{cases} \hat{a} = \dfrac{\sum\limits_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sum\limits_{i=1}^{n}(x_i - \overline{x})^2} \\ \hat{b} = \overline{y} - \hat{a}\overline{x} \end{cases}$$

Suppose that $y_1' = y_1 + \epsilon_1 (\epsilon_1 \neq 0)$, then $\overline{y}' = \overline{y} + \dfrac{1}{n}\epsilon_1$,

$$\begin{aligned} \hat{a}' &= \frac{(x_1 - \overline{x}) \cdot \dfrac{n-1}{n}\epsilon_1 + \sum\limits_{i=2}^{n}(x_i - \overline{x})\left(y_i - \overline{y} - \dfrac{1}{n}\epsilon_1\right)}{\sum\limits_{i=1}^{n}(x_i - \overline{x})^2} \\ &= \frac{(x_1 - \overline{x})\epsilon_1 + \sum\limits_{i=2}^{n}(x_i - \overline{x})(y_i - \overline{y}) - \dfrac{1}{n}\sum\limits_{i=1}^{n}(x_i - \overline{x})\epsilon_1}{\sum\limits_{i=1}^{n}(x_i - \overline{x})^2} \\ &= \frac{(x_1 - \overline{x})(y_1 - \overline{y}) + \sum\limits_{i=2}^{n}(x_i - \overline{x})(y_i - \overline{y}) - 0}{\sum\limits_{i=1}^{n}(x_i - \overline{x})^2} \\ &= \hat{a} + \frac{(x_1 - \overline{x})(\epsilon_1 + \overline{y} - y_1)}{\sum\limits_{i=1}^{n}(x_i - \overline{x})^2} \end{aligned}$$

Solution (cont.)

Therefore, when $\epsilon_1 + \overline{y} - y_1 = 0$,

$$\hat{b}' = \hat{b}$$

Therefore, only in special cases, an adversary force the linear regression to recover any desired a, b by setting exactly 1 of the ϵ_i to be a selected non-zero value

2. What if the adversary sets 2 of the ε_i?

(2) Suppose that $y_1' = y_1 + \epsilon_1,\ y_2' = y_2 + \epsilon_2 (\epsilon_1, \epsilon_2 \neq 0)$, then $\overline{y}' = \overline{y} + \frac{1}{n}(\epsilon_1 + \epsilon_2)$,

$$\begin{aligned}
\hat{a}' &= \frac{(x_1 - \overline{x}) \cdot \left(\frac{n-1}{n}\epsilon_1 - \frac{1}{n}\epsilon_2\right) + (x_2 - \overline{x}) \cdot \left(\frac{n-1}{n}\epsilon_1 - \frac{1}{n}\epsilon_2\right) + \sum_{i=3}^{n}(x_i - \overline{x})\left(y_i - \overline{y} - \frac{1}{n}(\epsilon_1 + \epsilon_2)\right)}{\sum_{i=1}^{n}(x_i - \overline{x})^2} \\
&= \frac{(x_1 - \overline{x})\epsilon_1 + (x_2 - \overline{x})\epsilon_2 + \sum_{i=2}^{n}(x_i - \overline{x})(y_i - \overline{y}) - \frac{1}{n}\sum_{i=1}^{n}(x_i - \overline{x})(\epsilon_1 + \epsilon_2)}{\sum_{i=1}^{n}(x_i - \overline{x})^2} \\
&= \hat{a} + \frac{(x_1 - \overline{x})(\epsilon_1 + \overline{y} - y_1)}{\sum_{i=1}^{n}(x_i - \overline{x})^2} + \frac{(x_2 - \overline{x})(\epsilon_2 + \overline{y} - y_2)}{\sum_{i=1}^{n}(x_i - \overline{x})^2}
\end{aligned}$$

Therefore, when $\epsilon_1 + \overline{y} - y_1 = \epsilon_2 + \overline{y} - y_2 = 0$, or $(x_1 - \overline{x})(\epsilon_1 + \overline{y} - y_1) + (x_2 - \overline{x})(\epsilon_2 + \overline{y} - y_2) = 0$

$$\hat{b}' = \hat{b}$$

Therefore, only in special cases, an adversary force the linear regression to recover any desired a, b by setting exactly 1 of the ϵ_i to be a selected non-zero value

3. How many does the adversary need to change and how would it do it?

(3)It depends on the datas. If $\epsilon_i (i = 1, 2 \cdots, n)$ are symmetrical to the original line, then the adversary can force the linear regression to recover desired a, b. On the contrary, if the adversary all lie in the same side of the original line, the it will change the value of linear regression estimators.

Problem 5: Your Own Question

Write your own question, and provide a thorough solution.

Question

How to evaluate a linear regreesion model?

Solution

(1) Plot

We can use scatter plot, box plot, pair plot or coplot to analyse the datas and the regression line. It's intuitive, however, it may be too subjective to draw a conclusion about the linear regression model.

(2) The F-test

The F-test evaluates the null hypothesis that all regression coefficients are equal to zero versus the alternative that at least one does not.

(3) Goodness-of-fit

The square of the correlation between the observed Y values and the predicted $\hat{Y}$ values summarize how well a linear model fits datas by calculating

$$R^2 = \frac{\sum_{i=1}^{n}(\hat{Y}_i - \overline{Y})^2}{\sum_{i=1}^{n}(Y_i - \overline{Y})^2}$$

If R^2 is closer to 1, then the model is better fitted.

(4) SSE or MSE or RMSE

Sum of the squared residuals(SSE) is defined by

$$SSE = \sum_{i=1}^{n}(Y_i - EY_i)^2$$

Mean of the squared residuals(SSE) is defined by

$$MSE = \frac{1}{n-2}\sum_{i=1}^{n}(Y_i - EY_i)^2$$

The square root of the variance of the residuals(RMSE) is defined by

$$RMSE = \sqrt{MSE}$$

If the SSE or MSE or RMSE is smaller, the model is better fitted.