CS 189 Introduction to Machine Learning
Fall 2017 HW0

This homework is due **Friday, August 25 at 10 p.m.**. Note that every homework after will be due at **noon** instead.

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?

   None. I work alone
   Comments: The time is short, not enough for even a short homework. Problem #4 needs more explanation

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. Hannah

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".

3 Eigendecomposition Review

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

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

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?
2. What if the adversary sets 2 of the ε_i?
3. How many does the adversary need to change and how would it do it?

5 Your Own Question

Write your own question, and provide a thorough solution.

Problem # 2. Sample Submission

DONE

Problem # 3. Eigendecomposition Review

$$A = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix} \qquad Ax = \lambda x \quad \text{for some } x$$

$$(A - I\lambda)x = 0$$

$$\Rightarrow \det(A - I\lambda) = 0$$

$$\begin{vmatrix} 1-\lambda & 3 \\ 3 & 1-\lambda \end{vmatrix} = 0$$

$$(1-\lambda)^2 - 9 = 0$$

$$1 - \lambda_1 = 3 \quad \text{or} \quad 1 - \lambda_2 = -3$$

$$\Rightarrow \quad \lambda_1 = -2 \qquad \lambda_2 = 4$$

$$3x_1 + 3x_2 = 0 \qquad -3x_1 + 3x_2 = 0$$

$$\Rightarrow x = \begin{bmatrix} -1 \\ 1 \end{bmatrix} \qquad \Rightarrow x = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Problem # 4. Linear regression & Adversarial Noise

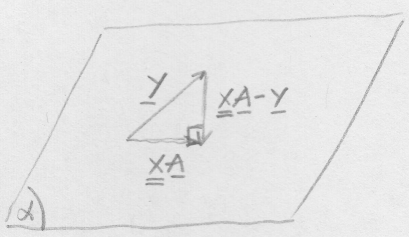
Model : $y_i = ax_i + b$

Actual : $y_i = ax_i + b + \varepsilon_i$

change of ε_i leads to change of y_i

The OLS linear regression requires $\min \| \underline{\underline{X}}\underline{A} - \underline{Y} \|$, where:

$$X = \begin{bmatrix} x_1 & 1 \\ x_2 & 1 \\ \cdots & \\ x_n & 1 \end{bmatrix} \qquad A = \begin{bmatrix} a \\ b \end{bmatrix} \qquad Y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$$



Let α is the plane generated by XA when we vary A.

$(\underline{\underline{X}}\underline{A} - \underline{Y})$ min iff $(\underline{\underline{X}}\underline{A} - \underline{Y}) \perp \alpha$

i.e $(\underline{\underline{X}}\underline{A} - \underline{Y}) \perp X_i$'s, where X_i's are the column vectors of $\underline{\underline{X}}$

$$\underline{\underline{X}}^T(\underline{\underline{X}}\underline{A} - \underline{Y}) = 0$$

$$\underline{\underline{X}}^T\underline{\underline{X}}\underline{A} - \underline{\underline{X}}^T\underline{Y} = 0$$

$$A = (\underline{\underline{X}}^T\underline{\underline{X}})^{-1}\underline{\underline{X}}^T\underline{Y}$$

$$\begin{bmatrix} a \\ b \end{bmatrix} = (\underline{\underline{X}}^T\underline{\underline{X}})^{-1}\underline{\underline{X}}^T\underline{Y}$$

We have two linear equations with unknowns a, b.

Remember $y_i = a^* x_i + b^* + \varepsilon_i$ a), where a^*, b^* are of the original model.

$$\underline{Y} = \underline{\underline{X}}\underline{A}^* + \underline{\varepsilon}$$

$$\Rightarrow \begin{bmatrix} a \\ b \end{bmatrix} = (\underline{\underline{X}}^T\underline{\underline{X}})^{-1}\underline{\underline{X}}^T(\underline{\underline{X}}\underline{A}^* + \underline{\varepsilon})$$

$$\underbrace{\begin{bmatrix} a \\ b \end{bmatrix}}_{\text{desired}} = \underbrace{(\underline{\underline{X}}^T\underline{\underline{X}})^{-1}\underline{\underline{X}}^T\underline{\underline{X}}\underline{A}^*}_{\text{constant}} + \underbrace{(\underline{\underline{X}}^T\underline{\underline{X}})^{-1}\underline{\underline{X}}^T\underline{\varepsilon}}_{\substack{\text{constant} \\ \text{full rank}}} \quad (*)$$

$\underline{\varepsilon}$: manipulate

1.) If the adversary can set exactly one of the ε_i, say ε_1

→ He solves two equations for one unknown ε_1

→ overdetermined

⇒ The adversary cannot obtain the desired a & b

2.) If the adversary can set two of the ε_i, say ε_1 & ε_2

i.e. He solves the 2-equation system (*) for two unknowns ε_1 & ε_2 → the system is exactly determined

→ always possible

3.) The adversary need to change at least 2 of the ε_i. Without the loss of generality, he assumes those are ε_1 & ε_2. Rewriting $\underline{\varepsilon}$ gives:

$$\underline{\varepsilon} = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \varepsilon_3 \\ \vdots \\ \varepsilon_n \end{bmatrix} + \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \underbrace{\begin{bmatrix} 0 \\ 0 \\ \varepsilon_3 \\ \vdots \\ \varepsilon_n \end{bmatrix}}_{\underline{\varepsilon}_0} + \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ \cdots & \\ 0 & 0 \end{bmatrix}}_{\underline{\underline{I}}_\varepsilon} \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \end{bmatrix} \quad (**)$$

He can determine ε_0 by using the actual equation (1):

$$y_i = a^* x_i + b^* + \varepsilon_i$$

$$\Rightarrow \quad \varepsilon_i = y_i - a^* x_i - b^* \qquad \forall i \neq 1, 2$$

Substitute (**) into (*):

$$\begin{bmatrix} a \\ b \end{bmatrix} = (\underline{\underline{X}}^T \underline{\underline{X}})^{-1} \underline{\underline{X}}^T \underline{\underline{X}} \underline{A}^* + (\underline{\underline{X}}^T \underline{\underline{X}})^{-1} \underline{\underline{X}}^T \left(\underline{\varepsilon}_0 + \underline{\underline{I}}_\varepsilon \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \end{bmatrix} \right)$$

$$\begin{bmatrix} a \\ b \end{bmatrix} = (\underline{\underline{X}}^T \underline{\underline{X}})^{-1} \underline{\underline{X}}^T \underline{\underline{X}} \underline{A}^* + (\underline{\underline{X}}^T \underline{\underline{X}})^{-1} \underline{\underline{X}}^T \underline{\varepsilon}_0 + (\underline{\underline{X}}^T \underline{\underline{X}})^{-1} \underline{\underline{X}}^T \underline{\underline{I}}_\varepsilon \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \end{bmatrix} = \left((\underline{\underline{X}}^T \underline{\underline{X}})^{-1} \underline{\underline{X}}^T \underline{\underline{I}}_\varepsilon \right)^{-1} \left(\begin{bmatrix} a \\ b \end{bmatrix} - (\underline{\underline{X}}^T \underline{\underline{X}})^{-1} \underline{\underline{X}}^T \underline{\underline{X}} \underline{A}^* - (\underline{\underline{X}}^T \underline{\underline{X}})^{-1} \underline{\underline{X}}^T \underline{\varepsilon}_0 \right)$$

$\uparrow$ ε_1 & ε_2 to be set

$\uparrow$ desired

Problem #5

Find the inverse of the matrix $A = \begin{bmatrix} 1 & 2 & 2 \\ 4 & 5 & 6 \\ 3 & 7 & 5 \end{bmatrix}$

Solution

$$\det(A) = \begin{vmatrix} 1 & 2 & 2 \\ 4 & 5 & 6 \\ 3 & 7 & 5 \end{vmatrix} = 1\begin{vmatrix} 5 & 6 \\ 7 & 5 \end{vmatrix} - 2\begin{vmatrix} 4 & 6 \\ 3 & 5 \end{vmatrix} + 2\begin{vmatrix} 4 & 5 \\ 3 & 7 \end{vmatrix}$$

$$= -17 - 4 + 26 = 5$$

$$M_{11} = \begin{vmatrix} 5 & 6 \\ 7 & 5 \end{vmatrix} = -17 \qquad M_{12} = \begin{vmatrix} 4 & 6 \\ 3 & 5 \end{vmatrix} = 2 \qquad M_{13} = \begin{vmatrix} 4 & 5 \\ 3 & 7 \end{vmatrix} = 13$$

$$M_{21} = \begin{vmatrix} 2 & 2 \\ 7 & 5 \end{vmatrix} = -4 \qquad M_{22} = \begin{vmatrix} 1 & 2 \\ 3 & 5 \end{vmatrix} = -1 \qquad M_{23} = \begin{vmatrix} 1 & 2 \\ 3 & 7 \end{vmatrix} = 1$$

$$M_{31} = \begin{vmatrix} 2 & 2 \\ 5 & 6 \end{vmatrix} = 2 \qquad M_{32} = \begin{vmatrix} 1 & 2 \\ 4 & 6 \end{vmatrix} = -2 \qquad M_{33} = \begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix} = -3$$

$$\rightarrow \begin{bmatrix} -17 & 2 & 13 \\ -4 & -1 & 1 \\ 2 & -2 & -3 \end{bmatrix} \rightarrow \begin{bmatrix} -17 & -2 & 13 \\ 4 & -1 & -1 \\ 2 & 2 & -3 \end{bmatrix} \rightarrow \begin{bmatrix} -17 & 4 & 2 \\ -2 & -1 & 2 \\ 13 & -1 & -3 \end{bmatrix}$$

$$\Rightarrow \quad A^{-1} = \frac{1}{5}\begin{bmatrix} -17 & 4 & 2 \\ -2 & -1 & 2 \\ 13 & -1 & -3 \end{bmatrix}$$