Assignment 1: Hill Cipher

2019 Fall EECS205002 Linear Algebra

Due: 2019/10/16

The main idea of Hill cipher is to encode message with an invertible matrix and modulus operation [1]. Here we remove the modulus operation to simplify the task, so the remaining part is to encrypt the message x with a given invertible matrix A. The cipher text is then $y = Ax$. To decode the message, one could compute $A^{-1}y$ to obtain plain text x.

For example, let the matrix A be

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 2 & 3 & 2 \end{bmatrix}.$$

and the message is $x = [1\ 2\ 3]^T$. The encoded message is

$$y = Ax = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 2 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 8 \\ 21 \\ 14 \end{bmatrix}.$$

To decode the message, one can compute

$$A^{-1} = \begin{bmatrix} 1 & -1 & 1 \\ 2 & 0 & -1 \\ -4 & 1 & 1 \end{bmatrix}.$$

The decoded message is

$$x = A^{-1}y = \begin{bmatrix} 1 & -1 & 1 \\ 2 & 0 & -1 \\ -4 & 1 & 1 \end{bmatrix} \begin{bmatrix} 8 \\ 21 \\ 14 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}.$$

To ensure A^{-1} is also an integer matrix, one requirement is $\det(A) = \pm 1$, based on the formula given in textbook 2.3.

1 Assignment in Python

1. Design a Hill cipher matrix which contains all the digits of your student ID. Those digits must be in the first row and in the first column. The first row and the first column cannot contain more than two zeros. The matrix size n should be $n = 5$.

2. Give one or two examples to show it can correctly encode and decode integer messages. Compute the matrix inverse use the formula in textbook and `numpy.linalg.inv`.

3. Use the `abssum` to compare the original message and the decoded message. Is the answer zero? If not, explain why. How about using the inversion derived by the formula?

2 Submission

1. Write a report in PDF file that includes (a) your Hill cipher matrix A indicating where are the digits of your student ID, (b) the derivation of A and A^{-1}, and (c) the answers to question 3.

2. Python code of the second problem.

3. Zip them and submit to iLMS system

3 Hint of algorithm

The algorithm to find an integer matrix A of $\det(A) = \pm 1$ is sketched as follows.

1. Decide the matrix size n, and put the digits of your student ID on the $n \times n$ matrix A.

2. Assign two unused elements as unknowns, say a and b, in the matrix A, and add necessary elements to make A's determinate nonzero.

3. Compute the determinate $\det(A) = 1$ or $\det(A) = -1$ as a linear Diophantine equation of a an b.

4. Solve linear Diophantine equation [2].

5. If the equation above has no solution, go to 2 and find different assignments of unknowns.

6. If cannot construct A with $\det(A) = \pm 1$, go to 1 and enlarge n.

References

[1] ccjou *Hill Cipher.* `https://ccjou.wordpress.com/2013/09/10/%E5%B8%8C%E7%88%BE%E5%AF%86%E7%A2%BC/?fbclid=IwAR175SK34eqCXJfhOsDnlk_0cEQ4bLSDG1BSSsd36JQSMaq436LxlpJoIok`

[2] wikiHow Staff *How to Solve a Linear Diophantine Equation.* `https://www.wikihow.com/Solve-a-Linear-Diophantine-Equation`