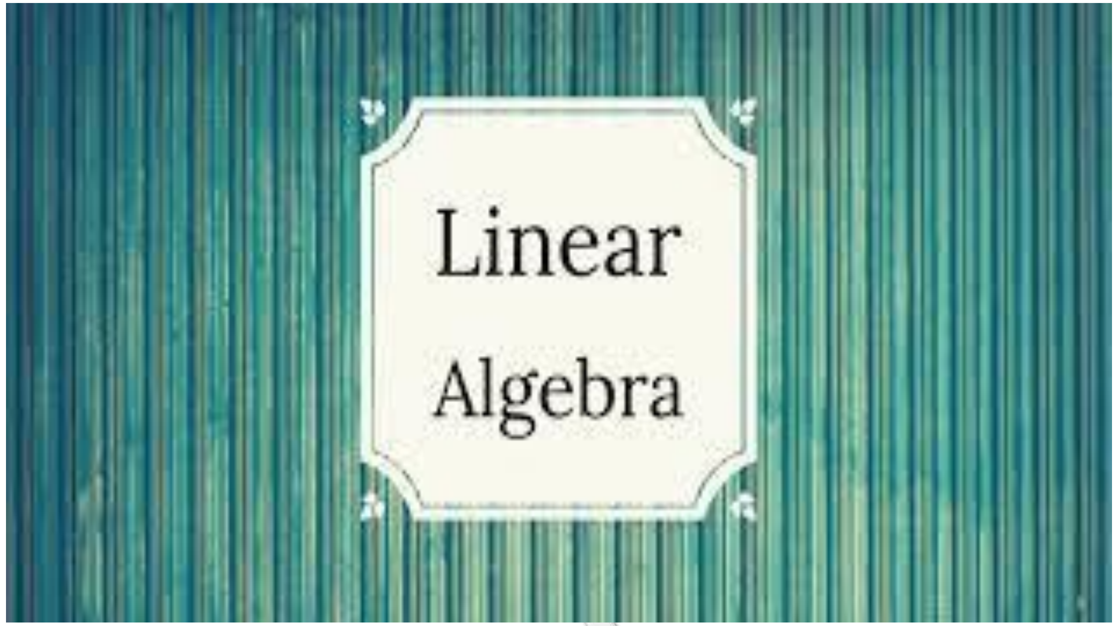

Lecture 9

Date: 21/09/2020

Note: These PPTs are for student’s reference, for detailed content(practice), students are advised to use text-books and reference books mentioned in the syllabus.

Topic: Solution of system of linear algebraic equations, by

Application of matrix to Encoding & Decoding

Examples on Encoding & Decoding

Inverse of matrix A under modulo n

- Step-I Find inverse of A by usual manner
- Step-II Write multiplicative inverse for det(A) under given modulo n
- Step-III Multiply by multiplicative inverse inside the matrix A
- Step-IV Convert all numbers of A under given modulo n

Demonstration of inverse of A under modulo n

Find inverse of A=$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$ under modulo 26

Consider A^{-1} = $\frac{1}{3}\begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix}$

Note that multiplicative inverse of 3 under (mod 26) is 9

Hence, A^{-1} = 9 $\begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix}$ (mod 26)

= $\begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix}$ (mod 26)

=$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}$ (mod 26)

One can easily verify that A. A^{-1}= A^{-1}.A=I

As, $\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$. $\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}$= $\begin{bmatrix} 53 & 234 \\ 26 & 105 \end{bmatrix}$= $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $(mod\ 26)$

Thus, $\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}^{-1}$ = $\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}$ under (mod 26)

For encoding and decoding one should know the Cipher table which is given as follows

Cryptography

To begin, you need to assign a number to each letter in the alphabet (with 0 assigned to a blank space), as follows.

0 = _	9 = I	18 = R
1 = A	10 = J	19 = S
2 = B	11 = K	20 = T
3 = C	12 = L	21 = U
4 = D	13 = M	22 = V
5 = E	14 = N	23 = W
6 = F	15 = O	24 = X
7 = G	16 = P	25 = Y
8 = H	17 = Q	26 = Z

Process of Encoding & Decoding

Consider that if A is given (security) key matrix and B is the message matrix then encoded message matrix is given by,

$$C=A.B(\text{mod } n)$$

On the other hand decoded message is obtained by using the operation

$$B=A^{-1}.C(\text{mod } n)$$

Where A is key matrix and C is encoded message matrix.

Steps for Encoding the given text message

Step-I Convert the text message to a number message using Cipher table

Step-II For the given key matrix write the number message into matrix form such that number of columns of key matrix A should be equal to number of rows of message matrix say B**. Note that while putting the elements in matrix one should put it over the columns of message matrix B.**

Step-III If matrix B is not getting complete matrix then assume blank spaces at the end of text message, hence entries in the matrix will be "zeros" at those places (as 0 is assigned for blank spaces in cipher table)

Step-IV If we call encoded message matrix say C then C= A.B

Step-V Convert the numbers to given modulo n for matrix C

Step-VI Write the encoded message by converting the numbers into letters again. **Note that while writing message one should put the letters over the columns of C.**

Example on encoding the message with the help of given key matrix over given modulo n

Encode the message "SECRET_CODE" using key matrix $\begin{bmatrix} 1 & 1 \\ 2 & 6 \end{bmatrix}$ under modulo 27

Note that A has 2 columns, hence B will have order 2Xm

We convert the given text message to number message using Cipher table as follows,

19,5,3,18,5,20,0,3,15,4,5,0 (As blank space between the words considered '0' , and to complete the matrix added '0' at the end of the message, hence m=6)

Hence, the message matrix will be

B=$\begin{bmatrix} 19 & 3 & 5 & 0 & 15 & 5 \\ 5 & 18 & 20 & 3 & 4 & 0 \end{bmatrix}$, putting the number over columns of matrix B.

Let A be a given key matrix.

Hence, to find encoded message consider C=A.B

$$C = \begin{bmatrix} 1 & 1 \\ 2 & 6 \end{bmatrix} . \begin{bmatrix} 19 & 3 & 5 & 0 & 15 & 5 \\ 5 & 18 & 20 & 3 & 4 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 24 & 21 & 25 & 3 & 19 & 5 \\ 68 & 114 & 130 & 18 & 54 & 10 \end{bmatrix}$$

$$= \begin{bmatrix} 24 & 21 & 25 & 3 & 19 & 5 \\ 14 & 6 & 22 & 18 & 0 & 10 \end{bmatrix} \pmod{27}$$

Converting this to message “XNUFYVCRS_EJ”

This will be encoded message for “SECRET_CODE” under modulo 27 for given A

Steps for Decoding the given text message

- **Step-I** Convert the encoded message to a number message using Cipher table.

- **Step-II** Write the number message into matrix form such that number of columns of key matrix should be equal to number of rows of encoded message matrix say C**. Note that while putting the elements in matrix one should put it over the columns of encoded message matrix C.**

- **Step-III** If matrix C is not getting complete then assume blank spaces at the end of text message, hence entries in the matrix will be "zeros" at those places

- **Step-IV** Find inverse of key matrix(A) say A^{-1} and find A^{-1}.C=B(say)

- **Step-V** Convert the numbers to given modulo n for matrix B

- **Step-VI** Write the decoded message by converting the numbers into letters again. **Note that while writing message one should put the letters over the columns of B.**

Example on encoding the message with the help of given key matrix over given modulo n

Decode the message “XNUFYVCRS_EJ” using key matrix $\begin{bmatrix} 1 & 1 \\ 2 & 6 \end{bmatrix}$ under modulo 27

Note that A has 2 columns, hence C will have order 2Xm

We convert the given encoded message to number message using Cipher table as follows,

24,14,21,6,25,22,3,18,19,0,5,10

Hence, the encoded message matrix will be

C=$\begin{bmatrix} 24 & 21 & 25 & 3 & 19 & 5 \\ 14 & 6 & 22 & 18 & 0 & 10 \end{bmatrix}$, hence number of columns of C will be 6 i.e. m=6.

Let A be a given key matrix.

Hence, to find decoded message consider B=$A^{-1}C$

We first find A^{-1} under modulo 27

A= $\begin{bmatrix} 1 & 1 \\ 2 & 6 \end{bmatrix}$

$$A^{-1} = \frac{1}{4}\begin{bmatrix} 6 & -1 \\ -2 & 1 \end{bmatrix}$$

$$= 7\begin{bmatrix} 6 & -1 \\ -2 & 1 \end{bmatrix} \text{(mod 27)} \quad \text{....as } 4^{-1} = 7 under\ (mod\ 27)$$

$$= \begin{bmatrix} 42 & -7 \\ -14 & 7 \end{bmatrix} \text{(mod 27)}$$

$$= \begin{bmatrix} 15 & 20 \\ 13 & 7 \end{bmatrix} \text{(mod 27)}$$

Hence, consider B= A^{-1}.C

$$= \begin{bmatrix} 15 & 20 \\ 13 & 7 \end{bmatrix} . \begin{bmatrix} 24 & 21 & 25 & 3 & 19 & 5 \\ 14 & 6 & 22 & 18 & 0 & 10 \end{bmatrix}$$

Therefore B=

$$\begin{bmatrix} 640 & 435 & 815 & 405 & 285 & 275 \\ 410 & 315 & 479 & 165 & 247 & 135 \end{bmatrix}$$

$$= \begin{bmatrix} 19 & 3 & 5 & 0 & 15 & 5 \\ 5 & 18 & 20 & 3 & 4 & 0 \end{bmatrix} (\text{mod } 27)$$

Converting into text message we get the message as “SECRET_CODE_”

Hence, decoded message for “XNUFYVCRS_EJ” is “SECRET_CODE_“ for given key matrix A under modulo 27.

Exercise

1. Encode following text messages for key matrix $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ under modulo 27

(i) MOVE

(ii) INDIA

2. Decode the following messages for key matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ under modulo 27

BOW_LTYDY_

3. Decode BUQFYBUE for key matrix $\begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$ under modulo 26

4. Consider encoded message 7,7,4,16,5,8,9,13,20,3, decode this for key matrix $\begin{bmatrix} 1 & 0 \\ 4 & 13 \end{bmatrix}$ under modulo 27

5. Decode the message 41,26,33,34,29,29,67,48,57,19,19,38 for key matrix $\begin{bmatrix} 1 & 2 & 1 \\ 1 & 1 & 1 \\ 2 & 1 & 1 \end{bmatrix}$ under modulo 27

Answers

1.(i) MAV_

(ii) IWDMAA

2. NOW_STUDY_

3. SUPERMAN

4.GOD_EXISTS

5. GOD_EXISTS__