1ZC3 Engineering Math II-B (Linear Algebra I)

(WS 19 C03) Lecture 35

Last Time Row Space, Column Space, Null Space of A

To find bases for these:

- Reduce A to its RREF R
- For null(A): solve $A\bar{x} = \bar{0}$ i.e. $[A \mid 0]$ i.e. $[R \mid 0]$
- For row(A): use the non-zero rows of R
- For col(A): use the columns of A corresponding to the pivot columns of R (with leading 1s)

Note Dependence structure amongst columns same for A and R.

10.14 Cryptography – enciphering & deciphering messages

Given letters, first encode as #s:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Hill n-Cipher

↙ original message

- Convert "plaintext" into #s (see chart above)
- Split up string of #s into n-tuples called plaintext vectors

$$\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

(Repeat last letter/digit enough times that length is a multiple of n.)

- We fix in background a matrix A, nxn, enciphering matrix (needs to satisfy a rule - see later)
- Replace each plaintext vector with $A\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$

$$\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

- another n-tuple
- called a ciphertext vector

- Change back to text, ciphertext (see below)
- Send ciphertext.

We'll only look at 2-ciphers.

Example Encipher ENCODE using the Hill 2-cipher & matrix

$$A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}.$$

Solution ENCODE

5 14 3 15 4 5

↓ plaintext vectors $\begin{bmatrix} 5 \\ 14 \end{bmatrix}, \begin{bmatrix} 3 \\ 15 \end{bmatrix}, \begin{bmatrix} 4 \\ 5 \end{bmatrix}$

↓ ciphertext vectors

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 5 \\ 14 \end{bmatrix} = \begin{bmatrix} 15 \\ 19 \end{bmatrix} \begin{matrix} 0 \\ S \end{matrix}$$

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 3 \\ 15 \end{bmatrix} = \begin{bmatrix} 9 \\ 18 \end{bmatrix} \begin{matrix} I \\ R \end{matrix}$$

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 12 \\ 9 \end{bmatrix} \begin{matrix} L \\ I \end{matrix}$$

Send OSIRLI.

Example Encipher END using $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$.

Solution 3 letters : so add D on end ENDD

$$\begin{bmatrix} 5 \\ 14 \end{bmatrix}\begin{bmatrix} 4 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 5 \\ 14 \end{bmatrix} = \begin{bmatrix} 15 \\ 19 \end{bmatrix} \begin{matrix} 0 \\ S \end{matrix}$$

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 4 \\ 4 \end{bmatrix} = \begin{bmatrix} 12 \\ 8 \end{bmatrix} \begin{matrix} L \\ H \end{matrix}$$

Send OSLH.

Potential Problem Encipher GET OUT using $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$.

GE TO UT

$\begin{bmatrix}7\\5\end{bmatrix}$ $\begin{bmatrix}20\\15\end{bmatrix}$ $\begin{bmatrix}21\\20\end{bmatrix}$

$$\begin{bmatrix}3&0\\1&1\end{bmatrix}\begin{bmatrix}7\\5\end{bmatrix}=\begin{bmatrix}21\\12\end{bmatrix}\begin{matrix}U\\L\end{matrix}$$

differ by a multiple of 26 (same for all 4 blue arrows)

$$\begin{bmatrix}3&0\\1&1\end{bmatrix}\begin{bmatrix}20\\15\end{bmatrix}=\begin{bmatrix}60\\35\end{bmatrix}\equiv\begin{bmatrix}8\\9\end{bmatrix}\begin{matrix}H\\I\end{matrix}$$

"is equivalent to"

$$\begin{bmatrix}3&0\\1&1\end{bmatrix}\begin{bmatrix}21\\20\end{bmatrix}=\begin{bmatrix}63\\41\end{bmatrix}\equiv\begin{bmatrix}11\\15\end{bmatrix}\begin{matrix}K\\O\end{matrix}$$

Send ULHIKO.

Modular Arithmetic If m is a positive integer, a, b integers, we say "a is equivalent to b modulo m" written $a = b \pmod m$ if

$a - b$ is a multiple of m.

Examples $6 = 2 \pmod 4 = 10 \pmod 4 = -14 \pmod 4$

$6-2=4$ $\quad 6-10=-4$ $\quad 6-(-14)=20$

So ∞-many #s $= 6$ modulo 4.

Define the residue of a modulo m to be

the $b \in \mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ with $a = b \pmod m$. [It is a Fact that there is only one.]

Examples The residue of 6 modulo 4 is 2 (2 is the only # in $\{0,1,2,3\}$ equivalent to 6 modulo 4).

[If $a = b \pmod m$ then $b = a \pmod m$ as $b - a = -(a-b)$ so is also a multiple of m.]

The residue of 63 modulo 26 is 11

" " " -7 " 26 is 19 ← so the residue is not quite the remainder, which here would be -7 — need to be in $\mathbb{Z}_{26}$.

How do we work this out? Add / subtract multiples of m till we land in $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

[$\mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$.]

Use Fact For any integer k

$$a = (a \pm km) \pmod m$$

True since $a - (a \pm km) = \pm km$ multiple of m.

We can also multiply #s ...

Examples

$3 \times 4 = 12 = 12 \pmod{26}$

$5 \times 7 = 35 = (35-26) \pmod{26} = 9 \pmod{26}$

$11 \times 19 = 209 = (209 - 208) \pmod{26} = 1 \pmod{26}$

We can multiply "big" #s and still get 1.

T.B.C.

We'll use this next time to decipher.

You should subtract "convenient" or "easy" multiples of 26

Here you could have done any of the following & it still would have been just fine, just a bit more time consuming:

$$209 = (209-104) \pmod{26}$$
$$= 105 \pmod{26}$$
$$= 1 \pmod{26}$$

or
$$209 = (209-52) \bmod 26$$
$$= 157 \pmod{26}$$
$$= 105 \pmod{26}$$
$$= 53 \pmod{26}$$
$$= 27 \pmod{26}$$
$$= 1 \pmod{26}$$

It will probably help to remember 26, 52, (78), 104, 130, 156, (182), 208, all multiples of 26 (the ones in parentheses are not so easy to work with).