Row Space, Column Space, and Null Space (IV)

Theorem (row operations & null space). Elementary row operations do not change the null space of a matrix.

Theorem (row operations & row space). Elementary row operations do not change the row space of a matrix.

Comment: row operations change the column space of a matrix. Example:

$$A = \begin{bmatrix} 1 & 3 \\ 2 & 6 \end{bmatrix} \quad \rightarrow \quad R = \begin{bmatrix} 1 & 3 \\ 0 & 0 \end{bmatrix} \quad \rightarrow \quad \begin{bmatrix} 1 \\ 2 \end{bmatrix} \text{ cannot be produced from } \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Theorem (R matrix & basis). If a matrix R is in row echelon form, then the row vectors with the leading 1's (the nonzero row vectors) form a basis for the row space of R, and the column vectors with the leading 1's of the row vectors form a basis for the column space of R.

Theorem (basis for column space). If A and B are row equivalent matrices, then:
(a) A given set of column vectors of A is linearly independent if and only if the corresponding column vectors of B are linearly independent.
(b) A given set of column vectors of A forms a basis for the column space of A if and only if the corresponding column vectors of B form a basis for the column space of B.

Row Space, Column Space, and Null Space (V)

Problem. Given a set of vectors $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ in R^n, find a subset of these vectors that forms a basis for span (S), and express each vector that is not in that basis as a linear combination of the basis vectors.

Find basis for the Space Spanned by a Set of Vectors

- **Step 1.** Form the matrix A whose columns are the vectors in the set $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$.
- **Step 2.** Reduce the matrix A to reduced echelon form R.
- **Step 3.** Denote the column vectors of R by $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k$.
- **Step 4.** Identify the columns of R that contain the leading 1's. The corrsponding column vectors of A form a basis for span (S). (first part of problem finished)
- **Step 5.** Obtain a set of dependency equations for the column vectors $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k$ of R by successively expressing each $\mathbf{w}_i$ that does not contain a leading 1 of R as a linear combination of predecessors that do.
- **Step 6.** In each dependency equation obtained in Step 5, replace the vector $\mathbf{w}_i$ by the vector $\mathbf{v}_i$ for $i = 1, 2, \ldots, k$. (second part of problem finished)

Cryptography (I)

Cryptography: The study of encoding and deconding secret messages.

A few basic definitions:

- **Plaintext:** Uncoded message.
- **Ciphertext:** Coded message.
- **Enciphering:** Process of converting a plaintext to a ciphertext.
- **Deciphering:** Process of converting a ciphertext to a plaintext.

Enciphering codes are called **Ciphers**. Examples:

- **Substitution ciphers:** each letter from the alphabet is replaced by a different letter.
- **Polygraphic systems:** plain text is divided into sets of n letters, each of which is replaced by a set of n cipher letters. A subclass of these are the Hill Ciphers (based on matrix transformations).

Table 1

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

Cryptography (II)

In the simplest Hill ciphers (Hill 2-ciphers), successively pairs of plaintext are transformed into ciphertext by the following procedure:

- **Step 1.** Choose a 2×2 matrix with integer entries to perform encoding. We will impose other conditions later (e.g. A invertible).

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

- **Step 2.** Group successive plaintext letters into pairs (adding an arbitrary "dummy" letter to fill out the last pair if the plaintext has an odd number of letters) and replace each plaintext letter by its numerical value.
- **Step 3.** Successively convert each plaintext pair $p_1\, p_2$ into a column vector

$$\mathbf{p} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

and form the product $A\mathbf{p}$. We will call $\mathbf{p}$ a **plaintext vector** and $A\mathbf{p}$ the corresponding **ciphertext vector**.

- **Step 4.** Convert each ciphertext vector into its alphabetic equivalent (see table previous slide). (*if an entry from* $A\mathbf{p}$ *is greater than 25 we replace it by the reminder resulting from dividing the entry by 26*)

Cryptography (III)

Working with reminders is at the core of a body of mathematics called **modular arithmetic**. In modular arithmetic we are given a positive integer m, called **modulus**, and any two integers whose difference is an integer multiple of the modulus are regarded as equal or equivalent.

Definition (equivalent). If m is a positive integer and a and b are any integers, then we say that a is **equivalent** to b modulo m, written

$$a = b \pmod{m}$$

if $a - b$ is an integer multiple of m. (**Ex.:** $6 = 1 \pmod 5$, $19 = 3 \pmod 2$)

Comment: For any modulus m every integer a is equivalent, modulo m, to exactly one of the integers

$$0, 1, 2, \ldots, m - 1$$

We call this integer the **residue** of a modulo m, and we write

$$Z_m = \{0, 1, 2, \ldots, m - 1\}$$

to denote the set of residues modulo m. (residues found using next theorem)

Theorem (residue). For any integer a and modulus m, let

$$R = \text{reminder of } \frac{|a|}{m}$$

Then the residue r of a modulo m is given by

$$r = \begin{cases} R & \text{if } a \geq 0 \\ m - R & \text{if } a < 0 \text{ and } R \neq 0 \\ 0 & \text{if } a < 0 \text{ and } R = 0 \end{cases}$$

Definition (reciprocal). If a is a number in Z_m, then a number a^{-1} in Z_m is called a **reciprocal** or **multiplicative inverse** of a modulo m if $aa^{-1} = a^{-1}a = 1 \pmod{m}$.

Comment: If a and m have a common prime factor, then a has no reciprocal.

Deciphering. To decipher a message we use the inverse of the enciphering matrix. If m is a positive integer, then a square matrix A with entries in Z_m is said to be **invertible modulo m** if there is a matrix B with entries in Z_m, such that

$$AB = BA = I \qquad (\text{mod } m)$$

Example: If A is an invertible matrix modulo 26 used in a Hill 2-cipher (2×2 matrix) then

$$\mathbf{c} = A\mathbf{p} \pmod{26} \qquad \rightarrow \qquad \mathbf{p} = A^{-1}\mathbf{c} \pmod{26}$$

Theorem (invertible modulo m). A square matrix A with entries in Z_m is invertible modulo m if and only if the residue of $\det(A)$ modulo m has a reciprocal modulo m.

Corollary I. A square matrix A with entries in Z_m is invertible modulo m if and only if m and the residue of $\det(A)$ modulo m have no common prime factors.

Corollary II. A square matrix A with entries in Z_{26} is invertible modulo 26 if and only if the residue of $\det(A)$ modulo 26 is not divisible by 2 or 13.

Comment: If

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

has entries in Z_{26} and the residue of $\det(A) = ad - bc$ modulo 26 is not divisible by 2 or 13, then the inverse of A (mod 26) is

$$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{26}$$

where $(ad - bc)^{-1}$ is the reciprocal of the residue of $ad - bc$ (mod 26).