Lecture 6: Rank Nullity, Inverses, Intro To Inner Product

Prof. Piya Pal
ECE 269
FALL 2021

AGENDA

1. RANK NULLITY THEOREM
   - PROOF

2. PROPERTIES OF RANK

3. RIGHT, LEFT & "THE" INVERSE OF MATRIX

4. INNER PRODUCT (DEFINITION)

RANK-NULLITY THEOREM

Let $\mathcal{U}, \mathcal{V}$ be vector spaces over a field $\mathbb{F}$. Let $T: \mathcal{U} \to \mathcal{V}$ be a linear map. Suppose $\mathcal{U}$ is finite dimensional, Then.

$$\dim(R(T)) + \dim(\mathcal{N}(T)) = \dim(\mathcal{U}).$$

Proof:

$$R(T) = \{v \in \mathcal{V}, \text{ s.t. } v = T(u) \text{ for some } u \in \mathcal{U}\}$$

$$\mathcal{N}(T) = \{u \in \mathcal{U}, \text{ s.t. } T(u) = 0\}$$

$\mathcal{N}(T) \subseteq \mathcal{U}$. Let $\dim(\mathcal{U}) = n$ (n is a finite integer)

$$\dim(N(T)) \leq n.$$

Let $k = \dim(N(T)) \leq n$.

Let $\{u_1, v_2, v_3, \ldots, u_k\}$ be a basis for $N(T)$

$\Rightarrow \{u_1, u_2, \ldots, u_k\}$ is a linearly independent set in $\mathcal{U}$.

$\Rightarrow$ Recall: Any linearly independent set in a vector space is contained in some basis of the vector space.

$\Rightarrow$ There exist vectors $u_{k+1}, u_{k+2}, \ldots, u_n \in \mathcal{U}$ s.t. $\{u_1, u_2, \ldots, u_k, u_{k+1}, \ldots u_n\}$ is a basis for $\mathcal{U}$.

Consider the vectors

$$T(u_{k+1}) = v_1$$
$$T(u_{k+2}) = v_2$$
$$\vdots \qquad \vdots$$
$$T(u_n) = v_{n-k}$$

Of course $v_1, v_2, \ldots, v_{n-k} \in R(T)$.

If we can show that $v_1, v_2, \ldots, v_{n-k}$ is a "basis" for $R(T)$, then we will have

$$\boxed{\dim(R(T)) = n-k}$$

$$\Rightarrow \dim(R(T)) + k = n \qquad \dim(\mathcal{U})$$

$$\Rightarrow \dim(R(T)) + \dim(N(T)) = n.$$

Goal is therefore to show that
$v_1, v_2, \dots, v_{n-k}$ is a basis of $R(T)$

$\Leftrightarrow$ (i) $\{v_1, \dots, v_{n-k}\}$ spans $R(T)$ and
(ii) $\{v_1, \dots, v_{n-k}\}$ are linearly independent.

(i) To show $\{v_1, \dots, v_{n-k}\}$ span $R(T)$
Easy to show that $\operatorname{span}\{v_1, \dots, v_{n-k}\} \subseteq R(T)$
(why? since $v_1, \dots, v_{n-k} \in R(T)$ & $R(T)$ is a subspace)

We need to show that $R(T) \subseteq \operatorname{span}\{v_1, \dots, v_{n-k}\}$
$\Rightarrow$ we show that any vector $v \in R(T)$ can be expressed as a linear combination of $v_1, \dots, v_{n-k}$.

Let $v \in R(T)$
$\Rightarrow$ there exists $u \in \mathcal{U}$ s.t. $v = T(u)$.

Now, $\{u_1, \dots, u_k, u_{k+1}, \dots, u_n\}$ is a basis of $\mathcal{U}$

$$\Rightarrow \quad u = \sum_{i=1}^{n} \alpha_i u_i \qquad (\alpha_i \in \mathbb{F})$$

$$\Rightarrow \quad v = T(u) = T\left(\sum_{i=1}^{n} \alpha_i u_i\right)$$

linearity of T

$$= \sum_{i=1}^{n} \alpha_i T(u_i)$$

$$= \underbrace{\sum_{i=1}^{k} \alpha_i T(u_i)}_{=0} + \sum_{i=k+1}^{n} \alpha_i T(u_i)$$

$$= \sum_{i=k+1}^{n} \alpha_i T(u_i) = \sum_{i=1}^{n-k} \alpha_{i+k} v_i$$

$\Rightarrow$ v is a linear combination of $v_1, \dots, v_{n-k}$

$$\Rightarrow \boxed{\begin{array}{l} v \in \operatorname{span}\{v_1, v_2, \dots, v_{n-k}\} \\ \Rightarrow \{v_1, v_2, \dots, v_{n-k}\} \text{ spans } R(T) \end{array}}$$

(ii) To show $\{v_1, v_2, \ldots, v_{n-k}\}$ are linearly independent.

Suppose $\sum_{i=1}^{n-k} \alpha_i v_i = 0$ for some $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{F}$

$$\Rightarrow \sum_{i=1}^{n-k} \alpha_i v_i = 0 \Rightarrow \sum_{i=1}^{n-k} \alpha_i T(u_{k+i}) = 0$$

Linearity of T

$$\Rightarrow T\left(\sum_{i=1}^{n-k} \alpha_i u_{k+i}\right) = 0$$

$$\Rightarrow \sum_{i=1}^{n-k} \alpha_i u_{k+i} \in N(T)$$

Since $\{u_1, u_2, \ldots, u_k\}$ is a basis of $N(T)$

$\Rightarrow$ There exist $\beta_1, \beta_2, \ldots, \beta_k$ s.t.

$$\sum_{i=1}^{n-k} \alpha_i u_{k+i} = \sum_{i=1}^{k} \beta_i u_i$$

$$\Rightarrow \underbrace{\sum_{i=1}^{k} \beta_i u_i - \sum_{i=1}^{n-k} \alpha_i u_{k+i}}_{\text{Linear combination of } \{u_1, u_2, \ldots, u_k, u_{k+1}, \ldots, u_n\}} = 0$$

But $\{u_1, u_2, \ldots, u_k, u_{k+1}, u_{k+2}, \ldots, u_n\}$ are linearly independent.

$$\Rightarrow \alpha_1 = 0, \alpha_2 = 0, \ldots, \alpha_{n-k} = 0, \beta_1 = 0, \ldots, \beta_k = 0$$

Since $\alpha_1 = \alpha_2 = \cdots = \alpha_{n-k} = 0$, the vectors $\{v_1, v_2, \ldots, v_{n-k}\}$ must be linearly independent.

Properties Of Rank

① Let $A \in \mathbb{F}^{m\times n}$

Then $\boxed{\text{rank}(A) \leq \min(m,n)}$.

Proof: $\text{rank}(A) =$ max. # linearly independent columns in A

$\leq$ total # columns of A.

$\Rightarrow \text{rank}(A) \leq n$.

Now, $\text{rank}(A) = \dim(R(A))$.

Now $R(A) \subseteq \mathbb{F}^m$.

$\Rightarrow \dim(R(A)) \leq \dim(\mathbb{F}^m) = m$.

[Follows from the following property:- if S_1, S_2 are subspaces, s.t. $S_1 \subseteq S_2$ then, $\dim(S_1) \leq \dim(S_2)$.

Proof: See Discussion 3]

$\therefore \text{rank}(A) \leq m$

Putting them together

$$\text{rank}(A) \leq \min(m,n).$$

2. $\text{Rank}(A) = \text{Rank}(A^T)$.

(in other words, column-rank(A) = row-rank(A))

Proof: Let $r = \text{rank}(A)$, $A = [a_1\ a_2 \cdots a_n]$

Then there exists a basis $\{b_1, b_2, \dots, b_r\}$ of $R(A)$.

$\Rightarrow$ Each column a_i of A is a linear combination of $\{b_1, b_2, \dots, b_r\}$

$$\Rightarrow a_1 = \sum_{i=1}^{r} c_{1i} b_i, \quad a_2 = \sum_{i=1}^{r} c_{2i} b_i, \dots\dots$$

$$a_n = \sum_{i=1}^{r} c_{ni} b_i$$

$$\Rightarrow [a_1\ a_2 \cdots a_n] = [b_1\ b_2 \cdots b_r] \underbrace{\begin{bmatrix} c_{11} & \cdots & c_{n1} \\ c_{12} & \cdots & c_{n2} \\ \vdots & & \vdots \\ c_{1r} & \cdots & c_{nr} \end{bmatrix}}_{\text{call it } C}$$

$\Rightarrow$ Each row of A is a linear combination of rows of C.

C has "r" rows.

$\Rightarrow$ dimension of row-span of $A \leq r$.

$\Rightarrow \dim(R(A^T)) \leq r = \text{rank}(A)$.

$\Rightarrow \text{rank}(A^T) \leq \text{rank}(A)$, for all A — (1)

Applying this to A^T, we get

$$\operatorname{rank}\left((A^T)^T\right) \leq \operatorname{rank}(A^T).$$

$$\text{ie } \operatorname{rank}(A) \leq \operatorname{rank}(A^T) \quad \text{--- } (2).$$

Combining (1) & (2) we get

$$\operatorname{rank}(A) = \operatorname{rank}(A^T)$$

[Also see Discussion 3]

RIGHT INVERSE OF A

1. $A \in \mathbb{F}^{m \times n}$, suppose $n \geq m$

Does there exist a matrix $C \in \mathbb{F}^{n \times m}$

s.t.
$$AC = I_{m \times m} \quad ?$$

(i) Suppose $\text{rank}(A) = m$.

$\{a_1, a_2, \dots, a_n\}$ is spanning set for $R(A)$. (range space of A).

Since $\text{rank}(A) = m$

$\Rightarrow$ There exists a set of "m" linearly independent columns of A.

Suppose they are $a_1, a_2, \dots, a_m$ (without loss of generality)

$a_1 \in \mathbb{F}^m$, $a_2 \in \mathbb{F}^m$, ... $a_m \in \mathbb{F}^m$

$\dim(\mathbb{F}^m) = m$.

$\Rightarrow \{a_1, \dots, a_m\}$ are a set of m linearly independent vectors in $\mathbb{F}^m$.

$\Rightarrow \{a_1, \dots, a_m\}$ is a basis of $\mathbb{F}^m$.

$\Rightarrow$ We can represent every vector in $\mathbb{F}^m$ as a linear combination of $\{a_1, \dots, a_m\}$

Notice,

$$\underset{m\times m}{I} = \begin{bmatrix} e_1 & e_2 & \cdots & e_m \end{bmatrix}, \quad e_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \end{bmatrix} \rightarrow i\text{th}.$$

$e_i \in \mathbb{F}^m$.

There exists coefficients c_{ij}

$$\sum_{i=1}^{m} a_i c_{i1} = e_1$$

$$\vdots \qquad\qquad \vdots$$

$$\sum_{i=1}^{m} a_i c_{im} = e_m$$

(since $\{a_1, \dots, a_m\}$ is a basis of $\mathbb{F}^m$).

For $i = 1, 2, \dots, m$, define $c_i \in \mathbb{F}^n$ as $[c_i]_j = \begin{cases} c_{ji} & , j \le m \\ 0 & , \text{else} \end{cases}$

$\Rightarrow$ There exists a matrix C such that

$$A \begin{bmatrix} c_1 & c_2 & \cdots & c_m \end{bmatrix} = \begin{bmatrix} e_1 & e_2 & \cdots & e_m \end{bmatrix}$$

(ii) Rank$(A) < m$; $\operatorname{rank}(I_{m\times m}) = m$

But $\operatorname{rank}(AC) \le \operatorname{rank}(A) < m$

This is because $R(AC) \subseteq R(A) \Rightarrow \dim(R(AC)) \le \operatorname{rank}(A)$

$\Rightarrow$ C cannot exist

When $\text{rank}(A) = m$, there exists a matrix $C \in \mathbb{F}^{n \times m}$ s.t.

$$AC = I_{m \times m}$$

Such a C is called a "right inverse" of A.

(2) Given $A \in \mathbb{F}^{m\times n}$, if $\text{rank}(A) = n$ there exists a matrix B such that

$$BA = I_{n\times n}.$$

Such a matrix B is called "a left inverse of A".

If $\text{rank}(A) < n$, no left inverse of A exists.

Uniqueness? If $\text{rank}(A) = n = m$, the left inverse is unique.

If $m > n$ ($\text{rank}(A) = n$) then infinite left inverses exist (if $\mathbb{F}$ not a finite field).

The Inverse of A

Can a matrix $A \in \mathbb{F}^{m \times n}$ have both right & left inverses ?

Suppose A has both left and right inverse.

$\Rightarrow$ there exists B s.t. $BA = I_{n \times n}$

and " " C " $AC = I_{m \times m}$

Notice,

$$(BA)C = I.C = C$$

$$BAC = C$$

$$\Rightarrow \underset{n\times m}{B} = \underset{n\times m}{C} \quad (\because AC = I)$$

Q is $n = m$?

Suppose not. Then either $n > m$ or $m > n$. If $n > m$, $\text{rank}(A) < n$.

$\Rightarrow$ no left inverse of A exists

Similarly if $m > n$, $\operatorname{rank}(A) < m$

$\Rightarrow$ no right inverse of A exists.

If A has both left and right inverses, then the left & right inverse must be the same matrix and we must have $m = n = \operatorname{rank}(A)$

Such an inverse of A, which is both left & right inverse of A is called "the inverse of A".

We call such a matrix with

$$m = n = \operatorname{rank}(A)$$

as an "<u>invertible matrix</u>"

The inverse of A in this case is often denoted by the symbol A^{-1}.

A^{-1} is matrix, $A^{-1} \in \mathbb{F}^{n \times n}$ s.t.

$$A^{-1}A = I = AA^{-1}$$

There is a unique matrix A^{-1} which satisfies the above.

$$A \in \mathbb{F}^{m \times n}$$

if $\operatorname{rank}(A) = m$	if $\operatorname{rank}(A) = n$	$\operatorname{rank}(A) = m = n$
$\Rightarrow$ Right inverse of A exists.	$\Rightarrow$ Left inverse of A exists	$\Rightarrow$ A is invertible
$\Rightarrow$ Non unique if $n > m$ (If $\mathbb{F}$ not finite) infinite right inverses exist	$\Rightarrow$ Non unique if $m > n$ (If $\mathbb{F}$ not finite) infinite left inverses exist	$\Rightarrow$ Inverse is unique
$\Rightarrow$ Unique if $n = m$.	$\Rightarrow$ Unique if $m = n$.	

INNER PRODUCT

Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. A vector space $\mathcal{V}$ over $\mathbb{F}$ is said to be an inner-product space if it is equipped with a function called inner product

$$\langle \cdot , \cdot \rangle : \mathcal{V} \times \mathcal{V} \to \mathbb{F} \quad (\mathbb{F} = \mathbb{R} \text{ or } \mathbb{C}).$$

which satisfies the following properties.

(i) $\langle u+v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$, $\forall u, v, w \in \mathcal{V}$.

(ii) $\langle \alpha u, v \rangle = \alpha . \langle u, v \rangle$, $\forall u, v \in \mathcal{V}, \alpha \in \mathbb{F}$.

multiplication of real or complex numbers

(iii) $\langle u, v \rangle = \overline{\langle v, u \rangle}$ $\forall u, v \in \mathcal{V}$ ($\bar{\alpha}$ represents complex conjugate of α)

(iv) $\langle u, u \rangle \geq 0$, $\forall u \in \mathcal{U}$. Moreover, $\langle u, u \rangle = 0$ if and only if $u = 0$