MATRIX ANALYSIS - PSI5794

MAR/18/2019
LEC # 04

3. VECTOR SPACES

Matrix analysis is LIN ALG for finite dimension vec spaces, as such they are at the heart of matrix theory.

We can have a more structured view of vec spaces if we study a few algebraic structures, such as groups, rings an fields

An algebraic structure is a set equipped with one or more ops. An op. takes two els from the set and produce a third element also in the set (closure).

3.1. Algebraic structures

GROUP is a set G with an (abstract) operation $\oplus$ and denoted $(G, \oplus)$, so that for any $a, b, c \in G$

G1) G is closed under $\oplus$, ~~if a, b ∈ G then~~ $a+b \in G$

G2) Operation $\oplus$ is associative
$(a \oplus b) \oplus c = a \oplus (b \oplus c)$

G3) there exists a neutral element e in G
$a \oplus e = e \oplus a = a$

G4) there exists an inverse element $\bar{a}^{1}$ (Additive Inverse)
$\bar{a}^{1} \oplus a = a \oplus \bar{a}^{1} = e$

Sometimes $(G, 0, \oplus)$

Examples

1) $\mathbb{Z}$, ~~under~~ $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ under the usual addition and $e=0$
ARE GROUPS

that is, "Group" generalize the usual number systems

2) the set of $A_{n \times n}$ under entrywise addition is a Group

3) Does the set of natural numbers $\mathbb{N}$ under usual addition form a group? No! $\nexists$ additive inverse

$\mathbb{N} = \{1, 2, \dots\}$

If $\mathbb{N}^*$ is considered, $\nexists$ e (neutral element)

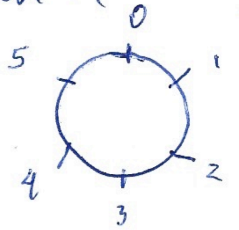
$\mathbb{N} = \{0, 1, 2, \dots\}$ some times includes 0

4) $\mathbb{Z}$ with $a \oplus b \triangleq a+b-1$ is a commutative group.

Finite Groups

Example: $\mathbb{Z}_n$ with addition mod n

$\mathbb{Z}_6$: $G = \{0, 1, 2, \dots, 5\}$



clockwise

$3 \oplus 2 = 5$

$3 \oplus 4 = 1$

Additive inverse:

$a' = n - a$

We can build the Addition table

A group is not necessarily commutative, i.e., ②

$a \oplus b \neq b \oplus a$ in general.

Example: the group of invertible matrices under usual matrix multiplication → why it has be invertible? o.w. ∄ "additive inverse"

in a non commu group

A commutative Group is called an Abelian Group (Niels Abel)

(see example 4 back of previous page)

RING is a set R with two abstract operations $\oplus, \odot$ satisfying for $a, b, c \in R$

~~R1) R is closed under~~ R1) $(R, \oplus)$ is an Abelian group

R2) R is closed under $\odot$

R3) "Multiplication" $\odot$ is associative

$$(a \odot b) \odot c = a \odot (b \odot c)$$

R4) $\odot$ is distributive over $\oplus$

$$a \odot (b \oplus c) = a \odot b \oplus a \odot c, \quad (b \oplus c) \odot a = b \odot a \oplus c \odot a$$

"Multiplication" $\odot$ is not necessarily commutative. $a \odot b \neq b \odot a$

(although $\oplus$ is: $(R, \oplus)$ is an Abelian Group).

(we didn't speak neither of multiplicative neutral element nor of multiplicative inverse, as it is analogous to the case for groups)

sometimes $(R, 0, \oplus, \odot)$

Examples

1) $(\mathbb{Z}, \oplus, \odot)$: $a \oplus b \triangleq a + b - 1$, $\boxed{a \odot b \triangleq ab + a + b}$ is A RING

2) the set of matrices $A_{N \times N}$ under entrywise addition and usual matrix multiplication is A RING

3) the ring of Quaternions $(1, i, j, k)$ PINTER 176

→ $a \odot b \triangleq ab - (a+b) + 2$ does form a ring

$a \odot b = ab + a + b$ does not!

A ring with a neutral element $\bar{e}$ for $\odot$ (multip.) is called a ring with unity: $a \odot \bar{e} = \bar{e} \odot a = a$

A ring does not necessarily have a "multiplicative" inverse for $\odot$ (ie, Not necessarily $\exists\, \bar{a}' \mid \bar{a}' \odot a = a \odot \bar{a}' = \bar{e}$)

Notação mais usual

Field is a commutative ring with unity and multiplicative inverse for every nonzero element. Or

or element $\neq e$?

Field is a set $\mathbb{F}$ with two abstract ops $\oplus, \odot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$

closure under $\odot, \oplus$

BACK

F1) $a \oplus b = b \oplus a$, $a \odot b = b \odot a$ — $\odot, \oplus$ commute

F2) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$, $(a \odot b) \odot c = a \odot (b \odot c)$ — $\oplus, \odot$ associate

F3) $\exists$ neutral element $\boxed{\overset{0}{e}} \in \mathbb{F}$ for $\oplus$: $a \oplus \boxed{\overset{0}{e}} = \boxed{\overset{0}{e}} \oplus a = a$ — identity for $\oplus$

F4) $\exists$ neutral element $\boxed{\overset{1}{\bar{e}}} \in \mathbb{F}$ for $\odot$: $a \odot \boxed{\overset{1}{\bar{e}}} = \boxed{\overset{1}{\bar{e}}} \odot a = a$ — identity for $\odot$

F5) $\exists\, \bar{a}' \in \mathbb{F} \mid \bar{a}' \oplus a = a \oplus \bar{a}' = \boxed{\overset{0}{e}}$ — additive inverse

F6) $\exists\, \bar{a}' \in \mathbb{F} \mid \bar{a}' \odot a = a \odot \bar{a}' = \boxed{\overset{1}{\bar{e}}}$, $a \in \{\mathbb{F} \setminus \{e\}\}$ — multip. inverse

F7) $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ $(= (b \oplus c) \odot a)$

sometimes $(\mathbb{F}, 0, 1, \oplus, \odot)$

Examples

1) Set $\mathbb{Q}$, quotients p/q, $p, q \in \mathbb{Z}$, $q \neq 0$ under usual addition & multiplication

2) Reals $\mathbb{R}$ under usual $+, \cdot$

3) Roots of polynomials with coeffs $\{a_k\}$ integers

$$\underbrace{a_n}_{} x^n + \underbrace{a_{n-1}}_{} x^{n-1} \cdots a_1 x + a_0 = 0$$

4) Finite Field: $\mathbb{Z}_n$ with ~~addition~~ $\oplus$ and $\odot$ modulo n for $n = $ prime

e.g., $\mathbb{Z}_3$ $\qquad$ $\text{rem}\left(\frac{ab}{n}\right)$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Counterexample: what if n is not prime?

A field is

F1) Commutative ring (with unit)

F2) 1_R

F3) multiplicative inverse: $a^{-1} \odot a = a \odot a^{-1} = 1_R$

$0,$

A field is

F1) A commutative unit ring $(R, \oplus, \odot, 1_R)$

F2) Multiplicative inverse for $\odot$: $a^{-1} \odot a = a \odot a^{-1} = 1_R$

Notation: $(R, \oplus, 0_R, \odot, 1_R)$.

Basically, a field is an algebraic structure in which we find solutions for any lin eq in one variable

No!

$ax+b=0$

$ax+b+(-b)=0-b$

$ax+0=-b$

$ax=-b$

$a^{-1}a\,x=-a^{-1}b$

$x=-a^{-1}b$

$ax=b$

$a^{-1}\cdot ax=a^{-1}\cdot b$

$1\cdot x=a^{-1}\cdot b$

$x=a^{-1}\cdot b$

that's why we drawn scalars/numbers from $\mathbb{F}$: to build vec spaces, to perform elimination techniques over matrices (GE, GJ)

In this course we get scalar from $\mathbb{F}=\mathbb{R}$ or $\mathbb{F}=\mathbb{C}$.

3.2. VECTOR SPACES $(V,\mathbb{F})$ → two sets

Vec spaces are the most basic objects in Lin Algebra

Def: A vector space over a field $\mathbb{F}$ is a set V with two ops $+$ and $\cdot$ called vector addition and scalar multiplication, so that

V1) $(V,+)$ is an abelian group (= commutative group)

V2) For any $\alpha, \beta \in \mathbb{F}$ and $u,v\in V$, form the scalar product $\alpha v\in V$

a) $\alpha(u+v)=\alpha u+\alpha v$

b) $(\alpha+\beta)u=\alpha u+\beta u$

c) $\alpha(\beta u)=(\alpha\beta)u$

d) $1u=u$

the elements of V are called vectors and the elements of $\mathbb{F}$ are called scalars.

Examples

1) set $\mathbb{F}^n$ of n-tuples (vectors coordinates) usual $+,\cdot$ for $\mathbb{R}$, $\mathbb{C}$

2) $(\mathbb{R}^{m\times n}, \mathbb{R})$ is a vec space $v+w$ and αv entriwise

3.3. Subspaces

Def: Let $(V, \mathbb{F})$ be a vector space. then a non-empty subset S of V is a subspace over $\mathbb{F}$ under the same $+, \cdot$ ops iff

1) $\mathbf{x}, \mathbf{y} \in S \Rightarrow \mathbf{x}+\mathbf{y} \in S$
2) $\mathbf{x} \in S \Rightarrow \alpha \mathbf{x} \in S \;\forall\; \alpha \in \mathbb{F}$

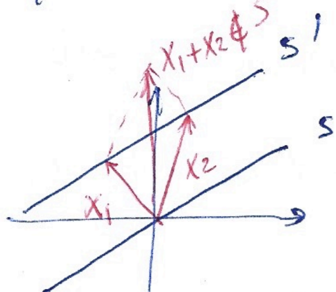
why we don't to check all the axioms? because $V, \mathbb{F}$ is already a vec space. superposition must hold

Remarks

1) Vector 0 must always be in S
2) All lines / hyperplanes crossing the origin are subspaces

Examples

1) "Lines" in $\mathbb{R}^2$



Vecs in S form a vec space
Vecs in S' don't

2) $(V, \mathbb{F}) = (\mathbb{R}^{n\times n}, \mathbb{R})$. $W = \{A \in \mathbb{R}^{n\times n} \mid A = A^T\}$ is a subspace $B = \alpha_1 A_1 + \alpha_2 A_2 = B^T$ ✓

3.4. Operations with Subspaces

Def: Spanning Sets: for a set $V = \{v_1, \ldots, v_N\}$ the subspace generated by all lin combos over V is called the space spanned by V

$$Sp(V) = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_N v_N$$

If a vecspace $U = Sp(V)$, we say V is a spanning set for U.

Def: Let V be a vecspc and R and S subspaces of V, i.e., $S, R, \subseteq V$.

1) Sum of R, S: $R + S \triangleq \{ r + s \mid r \in R, s \in S \}$
2) Intersection of R, S: $R \cap S \triangleq \{ v \mid v \in R, v \in S \}$
3) Direct sum $T \triangleq R \oplus S$ of R, S if
   a) $R \cap S = 0$
   b) $T = R + S$

R, S are said to be complements in T

Remark: the union $R \cup S$ of subspaces is not necessarily a subspace. $R+S$ and $R \cap S$ always are.

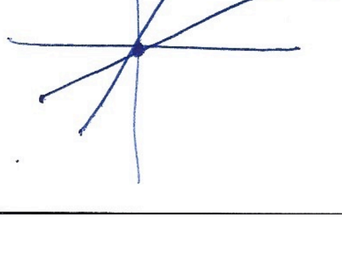
Example

1) $V = \mathbb{R}^2$

$R + S = \mathbb{R}^2$

$R \cap S = \{0\}$

$R \oplus S = \mathbb{R}^2$



2) $V = \mathbb{R}^3$, S, R different planes crossing the origin

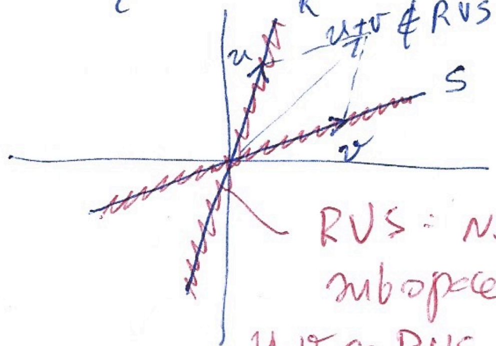
R: 2 vecs LI
S: 2 vecs LI

$R + S = \mathbb{R}^3$

$R \cap S \neq \{0\}$ (it is a line crossing origin)

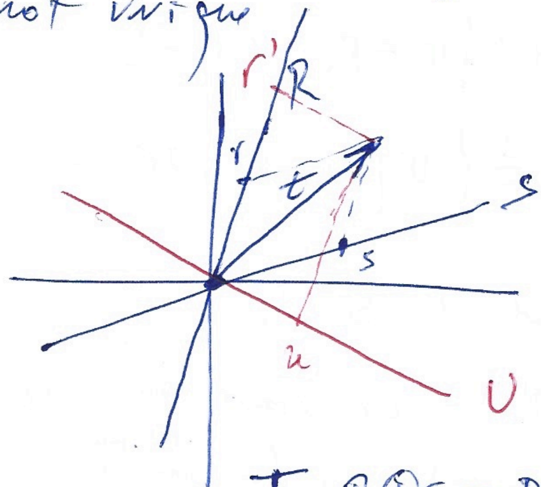
$R \oplus S$ is not defined

3) Let $u \in R$, $v \in S$. $u+v$ may not lie in $R \cup S$



$R \cup S$: Not subspace.
$u, v \in R \cup S$ but
$u+v \notin R \cup S$

Remark: If $T = R \oplus S$, then any $t \in T$ can be written uniquely as $t = r + s$ $(r \in R, s \in S)$.
However, the complement of R (or S) in T is not unique



$t = r + s$
$t = r' + u$

U is another complement of R in T (or S)

$T = R \oplus S = R \oplus U = \mathbb{R}^2$

What is the definition of R (S) in T?
It is in the red box within item (3) in previous page.

3.5. LINEAR INDEPENDENCE (LI)

A set $S = \{V_1, V_2, \dots, V_N\}$ is said to be LI

if $\alpha_1 V_1 + \alpha_2 V_2 + \cdots + \alpha_N V_N = 0 \quad \alpha_i \in \mathbb{F} \quad (I)$

is only satisfied by the trivial solution $\alpha_i = 0 \; \forall i$

On the other hand, if (I) admits a nontrivial solution, i.e., a set $\{\alpha_i\}$ not all zeroes, then the set is said to be LINEAR DEPENDENT (LD).

Examples

1) $S = \{3$ non colinear vecs in $\mathbb{R}^3\}$ is LI

2) $R = \{v_1, v_2, v_3\}$ with $v_1 = v_2$

$$\left.\begin{array}{l} \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0 \\ \alpha_1 v_1 + \alpha_2 (v_1) + \alpha_3 v_3 = 0 \end{array}\right\}$$ nontrivial sols of the form $(\alpha, -\alpha, 0)$ $\therefore$ R is LD

We are actually considering the solution of a ~~non~~ homogeneous system

$$\underbrace{V}_{\substack{\text{Matrix} \\ \text{of vecs} \\ \text{coordinates}}} \cdot \underbrace{\alpha}_{\substack{\text{lin} \\ \text{combines}}} = 0$$

Trivial sol → V is LI

Non trivial sol → V is LD

Remarks: 1) If a set $S = \{v_1, v_2, \dots, v_N\}$ is LI, any sub set of S is also LI

2) What if we add a new vector z to an LI set S?

$\alpha_1 v_1 + \cdots + \alpha_N v_N + \alpha_{N+1} z = 0$

$\bar{\alpha}_1 v_1 + \cdots + \bar{\alpha}_N v_N = -z$ → $\exists$ sol → LD; $\nexists$ sol → LI

$\bar{\alpha}_k = \dfrac{\alpha_k}{\alpha_{N+1}}$

3.6. BASIS AND DIMENSION

One of the most useful properties of vec spaces is that they possess bases. That is, for any vec space V, a set of $\{v_k\}$ LI vecs that $V = Sp(\{v_k\})$ describes uniquely any other vec in V via a Lin comb. It is a "fingerprint", or signature of V.

A basis of a vec space V is the minimal set of LI vecs that spans / generate V. that is because there may be redundancy in the vec set, i.e., $\{\underbrace{v_1, v_2, \dots, v_n}_{LI}, \underbrace{v_{n+1}, \dots, v_{n+k}}_{\text{may be LD of } \{v_1, \dots, v_n\}}\}$ generates V but it is not LI.

Def: A set of vecs $\{v_1, v_2, \dots, v_n\}$ is a basis for a vec space V if

1) $\{v_k\}$ is LI   2) $V = Sp\{v_k\}$

Def: the dimension of V is the maximum number of LI vecs in V.

"basis is a maximal LI set (cannot be made larger without losing lin-independence). A basis is also a minimal spanning LI set (it cannot be made smaller and still span the space of interest)" STRANG 70

BACK

3.7. Basis Expansion and Vector Coordinates

Given a vec space V, if $B_V = \{v_1, \dots, v_N\}$ is an ordered basis for V, then any vec v has an unique expansion over B_V

$$v = \sum_{j=1}^{N} \alpha_j v_j = \alpha_1 v_1 + \dots + \alpha_k v_k + \dots + \cancel{v}\alpha_N v_N$$

Component in B_V — Coordinate of v in B_V — basis vec

We are free to choose any B_V, but once chosen, ~~and~~ the coordinates $\{\alpha_j\}$ are unique.

<u>Proof</u>: $v = \sum_{j=1}^{N} \alpha_j v_j$. ~~Let~~ Assume $v = \sum_j \gamma_j v_j$ is ~~be~~ another basis expansion for v.

$$v = \sum_j \alpha_j v_j$$

$$- \quad v = \sum_j \gamma_j v_j$$

$$0 = \sum_j (\alpha_j - \gamma_j) v_j$$

$$(\alpha_1 - \gamma_1) v_1 + \dots + (\alpha_k - \gamma_k) v_k + \dots + (\alpha_N - \gamma_N) v_N = 0$$

$\{v_j\}$ is an LI set, then the only sol is the trivial sol $(\alpha_k - \gamma_k) = 0$ or $\alpha_k = \gamma_k$, $k = 1, N$.

3.8. CHANGE OF BASIS

Why should we change basis? Find a Basis in which description of vecs is simpler. 9

~~texto~~

If vec v is represented in basis $B_v = \{v_1, \ldots, v_N\}$ and we need its representation in another basis $B_z = \{z_1, \ldots, z_N\}$, proceed as follows.

We have
$$v = \sum_{i=1}^{N} \alpha_i v_i \quad (i) \qquad \text{We want} \quad v = \sum_{j=1}^{N} \beta_j z_j \quad (ii)$$

Describe each New basis vec z_j in the old basis

Coordinates of z_j in B_v

$$z_j = \sum_{i=1}^{N} p_{ij} v_i \qquad j = 1, N \qquad (iii)$$

(iii) → (ii)

$$v = \sum_{j=1}^{N} \beta_j \left(\sum_{i=1}^{N} p_{ij} v_i \right) = \sum_j \sum_i p_{ij} \beta_j v_i$$

$$v = \sum_i \underbrace{\boxed{\sum_j p_{ij} \beta_j}}_{\alpha_i} v_i$$

compare to (i)

Comparing to (i) and by unicity of coordinates under the same basis

$$\alpha_i = \sum_{j=1}^{N} p_{ij} \beta_j \qquad i = 1, N$$

$$\left.\begin{aligned}
\alpha_1 &= p_{11}\beta_1 + \cdots + p_{1k}\beta_k + \cdots + p_{1N}\beta_N \\
&\vdots \\
\alpha_i &= p_{i1}\beta_1 + \cdots + p_{ik}\beta_k + \cdots + p_{iN}\beta_N \\
&\vdots \\
\alpha_N &= p_{N1}\beta_1 + \cdots + p_{Nk}\beta_k + \cdots + p_{NN}\beta_N
\end{aligned}\right\}$$

in matrix form

$$\boxed{\alpha = P\beta} \qquad [v]_{B_z}$$

$$\boxed{\beta = P^{-1}\alpha} \qquad [v]_{B_v} = P_{B_v B_z}$$

3.9 ABSTRACT AND CONCRETE VECTORS

See LOEHR ch.6 for details

Any abstract vector v from an N-dim abstract vec-space $(V, \mathbb{F})$ can be represented by a concrete $N \times 1$ col vector (N-tuples) with entries in $\mathbb{F}$:

$$\underbrace{B_V = \{v_1, \dots, v_N\}}_{N \text{ LI vecs from } V} \iff \underbrace{B_V = [v_1 \ \cdots \ v_N]}_{N \text{ LI vecs from } \mathbb{F}^N} \quad N \times N \text{ matrix}$$

In other words $(V, \mathbb{F}) \iff (\mathbb{F}^N, \mathbb{F})$. By doing so, we can conveniently rewrite $v = \sum_j \alpha_j v_j$

abstract vecs — Col vecs (Nx1)

$$v = \alpha_1 v_1 + \dots + \alpha_N v_N \iff v = \alpha_1 v_1 + \dots + \alpha_N v_N$$

Lin Comb Coeffs — Lin Comb Coeffs

BACK

$$v = [v_1 \ \cdots \ v_N] \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{bmatrix}$$

$$\boxed{v = \underbrace{B_V}_{\substack{N \times N \\ \text{basis} \\ \text{matrix}}} \underbrace{\alpha}_{\substack{\text{Coordinates} \\ \text{of } v \text{ in} \\ B_V}}} \quad \text{or} \quad \boxed{[v]_{B_V} = \alpha}$$

α is the "signature" of v in basis B_V

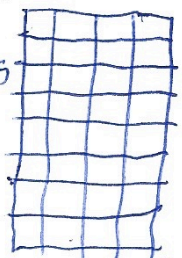
We can freely talk about ~~an~~ abstract vects or concrete vecs interchangeably, as convenient.

3.10 Range and Null spaces

For matrices, there are two "special" spaces that are omnipresent, in terms of lin. comb. of ~~their~~ their cols (rows). They are directly related to the solution of lin sys we covered earlier.

Def: the Range space of a matrix A_{mn} is

$$R(A) = \{Ax \mid x \in \mathbb{F}^n\} \subseteq \mathbb{F}^m$$



Also known as the col space of A

Also convenient; row space of A: $x^T A \Leftrightarrow A^T x$

which is the col space of A^T ($T \to *$ for $\mathbb{C}^n$)

col space ≡ right range, row space ≡ left range

Def: the Null space of a matrix A_{mn} is

$$N(A) = \{x \mid Ax = 0\} \subseteq \mathbb{F}^n$$

that is, it is the solution space of the Homogeneous system $Ax = 0$

right null space: $Ax = 0$

left null space: $x^T A = 0 \Leftrightarrow A^T x = 0$