29 October 2020 17:14

Linear algebraic methods in combinatorics

Introduction to Linear Algebra

Group - an algebraic structure

$(A, *)$ — A: set, $*$: binary operation on A.

We say $(A, *)$ is a group if

→ closure $a * b \in A$, $\forall a, b \in A$

→ associativity $a * (b * c) = (a * b) * c$, $\forall a, b, c \in A$

→ identity : $\exists$ an identity element $e \in A$ s.t.

$e * a = a * e = a$.

→ inverse : $\forall a \in A$, $\exists b \in A$ s.t.

$a * b = b * a = e$.

In addition, if

commutativity i.e. $a * b = b * a$, $\forall a, b \in A$

then $(A, *)$ is a commutative group or an Abelian group.

Field.

$(A, +, \cdot)$ — A: set; $+, \cdot$: two binary operations defined on elements of A.

$(A, +, \cdot)$ is a field if

→ $(A, +)$ is an Abelian group

→ $(A \setminus \{0\}, \cdot)$ is an Abelian group, where $0 \in A$ is the identity element of $(A, +)$

→ Distributive law

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Examples . .

Groups . .

(i) $(\mathbb{Z}, +)$ — Abelian group ($\mathbb{Z}$: integers)

(ii) $(\mathbb{Z}_n, +)$ — $+$: modulo n addition

$n = 5$ $(\{0,1,2,3,4\}, +)$.

(iii) $(\mathbb{Z}_p, \cdot)$ → multiplication modulo p.

p → prime

Fields.

(i) $(\mathbb{R}, +, \cdot)$ — reals

(ii) $(\mathbb{C}, +, \cdot)$ — complex nos

(iii) $(\mathbb{Z}_p, +, \cdot)$

p → prime

Vector Spaces :

vectors — represent multidimensional data.

$(\ , \ , \ , \ - - \ , \ )$

A vector space V over a field $\mathbb{F}$ is an Abelian group with a scalar product $\alpha \cdot v$ for all $\alpha, \beta \in \mathbb{F}$, $u, v \in V$ satisfying the following axioms:

(i) $\alpha(\beta v) = (\alpha\beta) v$

(ii) $(\alpha + \beta) v = \alpha v + \beta v$

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

(iv) $\underbrace{1}_{\text{multiplicative identity of } \mathbb{F}} \cdot v = v$

Elements of V are called vectors, elements of $\mathbb{F}$ are scalars.

Examples ...

(i) $\mathbb{R}^n$ over $\mathbb{R}$

$$u = (\overbrace{u_1, u_2}^{\mathbb{R}}, \ldots, u_n) \in \mathbb{R}^n$$

$$v = (v_1, v_2, \ldots, v_n) \in \mathbb{R}^n$$

$$w = (w_1, w_2, \ldots, w_n) \in \mathbb{R}^n$$

$\alpha, \beta, \gamma \in \mathbb{R}$.

$u + v \in \mathbb{R}^n$ (closure)

$u + (v + w) = (u + v) + w$ (associativity)

$u + (0, 0, \ldots, 0) = u$ (identity

$u + (0, 0, \ldots, 0) = u$ (identity)

$(u_1, u_2, \ldots, u_n) + (-u_1, -u_2, \ldots, -u_n) = 0$
(inverse)

$u + v = v + u$ (commutativity)

$= (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n)$

$= (v_1 + u_1, v_2 + u_2, \ldots, v_n + u_n)$

$\alpha(\beta u) = \alpha(\beta u_1, \beta u_2, \ldots, \beta u_n)$

$= (\alpha\beta u_1, \alpha\beta u_2, \ldots, \alpha\beta u_n)$

$= (\alpha\beta) u$

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

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

$1 \cdot u = u.$

(ii) If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$

(ii) If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$

polynomials whose coefficients come from $\mathbb{F}$

is a vector space over $\mathbb{F}$.

$$\mathbb{R}[x]$$

$$p(x) = 5x^2 + 3x + 7$$

$$q(x) = 6x^3 + 3x^2 + 2x$$

$$6x^3 + 8x^2 + 5x + 7 \in \mathbb{R}[x]$$

(iii) $MAT_{m \times n}(\mathbb{F}) \rightarrow$ $m \times n$ matrices with elements from a field $\mathbb{F}$.

Some Properties

Let V be a vector space over a field $(\mathbb{F}, +, \cdot)$. Let 0 denote the identity element of $(\mathbb{F}, +)$. Let $\bigcirc$ denote the zero vector. (i.e. $\bigcirc$ is the identity element of $(V,+)$)

1. $0 \cdot v = \mathcal{O}$

2. $\alpha \mathcal{O} = \mathcal{O}$, $\forall \alpha \in \mathbb{F}$

3. if $\alpha v = \mathcal{O}$, then either $\alpha = 0$ or
$v = \mathcal{O}$

4. $(-1)v = -v$, $\forall v \in V$

5. $-(\alpha v) = (-\alpha)v = \alpha(-v)$, $\forall \alpha \in \mathbb{F}$,
$v \in V$

<u>Subspace</u>: Let V be a vector space over a field $\mathbb{F}$. Let $W \subseteq V$. Then W is a <u>subspace</u> of V if W is closed under vector addition and scalar multiplication. That is, $u, v \in W$, and $\alpha \in \mathbb{F}$, then both $u+v$ and αu are also in W.

Example.

(i) Let $W = \{(x, 3x) : x \in \mathbb{R}\}$.

Then, W is a subspace of the vector space $\mathbb{R}^2$ over $\mathbb{R}$.

(ii) W is a subset of polynomials of $\mathbb{F}[x]$ with no odd power terms.

$\hookrightarrow$ if $p(x)$ and $q(x)$ have no odd power terms, then neither $p(x) + q(x)$, nor $\alpha p(x)$ have odd power terms.

Linear Combination.

Let $v_1, v_2, \ldots, v_n$ be vectors of a vector space V over a field $\mathbb{F}$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}$. An expression of the type

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

is called a linear combination of

$v_1, v_2, \ldots, v_n$.

Proposition: Let $S \subseteq V$, where V is a vector space over a field $\mathbb{F}$.
Then span(S) is a subspace of V.

span$(\{v_1, v_2, \ldots, v_n\})$: set of all vectors obtained from all possible linear combinations of $v_1, v_2, \ldots, v_n$.

Proof: Let $S = \{v_1, v_2, \ldots, v_n\}$

To show span(S) is a subspace of V,

(i)

$$\underbrace{(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n)}_{\in \text{span}(S)} + \underbrace{(\beta_1 v_1 + \cdots + \beta_n v_n)}_{\in \text{span}(S)}$$

$= (\ldots$

$$= \underbrace{(\alpha_1+\beta_1)v_1 + \cdots + (\alpha_n+\beta_n)v_n}_{\in \text{span}(S)}$$

span(S) is closed under vector addition

(ii)

$$\beta(\underbrace{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n}_{\in \text{span}(S)}) = \beta\alpha_1 v_1 + \beta\alpha_2 v_2 + \cdots + \beta\alpha_n v_n$$

$\in$ span(S)

Thus span(S) is closed under scalar multiplication.

$\square$

Linear Independence

Let $S = \{v_1, v_2, \ldots, v_n\}$ be a set of vectors in a V.S. V over a field $\mathbb{F}$. If there exist scalars $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}$ such that not all α_is are zero and

some $\alpha_i \neq 0$.

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$$

then, S is said to be a linearly dependent set of vectors.

If S is not linearly dependent, then S is called linearly independent.

That is, if S is lin independent, then

$$\left(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0 \right) \Longrightarrow \left(\alpha_1 = 0, \alpha_2 = 0, \ldots, \alpha_n = 0 \right)$$

Basis.

A set $S = \{v_1, v_2, \ldots, v_n\}$ of vectors in a vector space V over a field $\mathbb{F}$ is called a basis for V if

S is a linearly independent set that spans V.

$\to \operatorname{span}(S) = V$

Example:

$\{(1,0,0), (0,1,0), (0,0,1)\}$ forms a basis for $\mathbb{R}^3$ over $\mathbb{R}$.

$\to$ (i) linearly independent.

(ii) $(3, 5, -2)$

$\to 3(1,0,0) + 5(0,1,0) + (-2)(0,0,1)$.

Lemma: Let $S = \{v_1, v_2, \ldots, v_n\}$ and $S' = \{u_1, u_2, \ldots, u_m\}$ be two bases for V. Then, $m = n$.

Proof Outline: Suppose not.

Without loss of generality, assume $m < n$.

$$v_1 = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_m u_m$$

$$\alpha_1 u_1 = \alpha_2 u_2 + \cdots + \alpha_m u_m - v_1$$

$$u_1 = \alpha_1^{-1}\alpha_2 u_2 + \cdots + \alpha_1^{-1}\alpha_m u_m - \alpha_1^{-1} v \longrightarrow (1)$$

Similarly,

u_2 as a lin comb. of

$u_3, u_4, \cdots, u_m, v_1, v_2$

$\vdots$

u_m as a lin comb of

$v_1, v_2, \ldots, v_m$