Math 554

Hemanshu Kaul

kaul@iit.edu

Review of Linear Algebra (& Algebra)

Field $(\mathbb{F}, +, *)$ binary operators "+" addition
"*" multiplication

with all the nice properties we see
in $\mathbb{R}$ → "0", "1", $-x$, $1/x$, distribution laws.

e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$,

$\mathbb{F}_p$ finite field of order p (prime) $\{0, 1, .., p-1\}$
modular arithmetic
modulo p

$\mathbb{F}_q$ finite field of order $q = p^k$ (prime power)

This is not $\{0, 1, \ldots, q-1\}$

Vector Space V over field $\mathbb{F}$

$\vec{u}+\vec{v}$ vector addition, $\lambda\vec{v}$ scalar multiplication and their properties.

examples

- $\mathbb{F}^n$ over $\mathbb{F}$, e.g. $\mathbb{R}^n$ over $\mathbb{R}$, $(\mathbb{F}_2)^n$ over $\mathbb{F}_2$
  $\mathbb{F}^n = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) : \alpha_i \in \mathbb{F}\}$
- $\mathbb{F}^{k\times n}$, $k\times n$ matrices whose entries come from $\mathbb{F}$, over $\mathbb{F}$
- $\mathbb{F}^{\Omega}$, set of all functions $\Omega \to \mathbb{F}$ for some set Ω, over $\mathbb{F}$
- $\mathbb{F}[x_1, \ldots, x_n]$, "Ring" of all polynomials with coefficients from $\mathbb{F}$ & indeterminates $x_1, x_2, \ldots, x_n$

  we express multivariate polynomials as sum of monomials $\rightarrow$
  $\sum_{\alpha} c_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ with $\deg(c_\alpha x_1^{\alpha_1} \ldots x_n^{\alpha_n}) = \sum_{i=1}^{n} \alpha_i$

Question What is degree of the polynomial

$$3x_1^5x_3^2 + 2x_1x_2x_3 - 6x_1^7 \,?$$

7 over $\mathbb{Q}$ (or $\mathbb{R}$)

3 over $\mathbb{F}_3$

Question What is degree of the polynomial
$3x_1^5x_3^2 + 2x_1x_2x_3 - 6x_1^7$?

7 over $\mathbb{Q}$ (or $\mathbb{R}$)
3 over $\mathbb{F}_3$

Recall dimension of a vector sp. V, $\dim(V) = \#$vectors in a basis
$\rightarrow$ spanning set of vectors
$\hookrightarrow$ linearly independent set of vectors

max # vectors in lin. ind. set $= \dim V =$ min # vectors in a spanning set

Question What is the dimension of $V = \{$all 1-var. poly. of degree at most $k\}$

$\{1, x, \dots, x^k\}$ lin. ind. & spanning set
$\therefore \dim V = k+1$

Question What is degree of the polynomial
$$3x_1^5x_3^2 + 2x_1x_2x_3 - 6x_1^7 \ ?$$

7 over $\mathbb{Q}$ (or $\mathbb{R}$)

3 over $\mathbb{F}_3$

Recall dimension of a vector sp. V, $\dim(V) = \#$vectors in a basis

→ spanning set of vectors

↪ linearly independent set of vectors

Proposition ① If $v_1, \dots, v_m$ are vectors over some finite field $\mathbb{F}_q$ then $|\mathrm{span}\{v_1, \dots, v_m\}| \leq q^m$.

Equality holds iff ??

② If $v_1, \dots, v_m$ are lin. ind. in a vector space V of dimension k, then $m \leq k$.

Question What is degree of the polynomial

$$3x_1^5x_3^2 + 2x_1x_2x_3 - 6x_1^7 \,?$$

7 over $\mathbb{Q}$ (or $\mathbb{R}$)

3 over $\mathbb{F}_3$

Recall dimension of a vector sp. V, $\dim(V) = \#$vectors in a basis

→ spanning set of vectors

→ linearly independent set of vectors

Proposition ① If $v_1, \ldots, v_m$ are vectors over some finite field $\mathbb{F}_q$ then $|\mathrm{span}\{v_1, \ldots, v_m\}| \leq q^m$.

Equality holds iff $\{v_1, \ldots, v_m\}$ is lin. ind.

② If $v_1, \ldots, v_m$ are lin. ind. in a vector space V of dimension k, then $m \leq k$.

Question What is degree of the polynomial
$$3x_1^5x_3^2 + 2x_1x_2x_3 - 6x_1^7 ?$$
7 over $\mathbb{Q}$ (or $\mathbb{R}$)
3 over $\mathbb{F}_3$

Recall dimension of a vector sp. V, $\dim(V) = \#$vectors in a basis
→ spanning set of vectors
→ linearly independent set of vectors

Proposition ① If $v_1, \ldots, v_m$ are vectors over some finite field $\mathbb{F}_q$ then $|\text{span}\{v_1, \ldots, v_m\}| \leq q^m$.
Equality holds iff $\{v_1, \ldots, v_m\}$ is lin. ind.

② $\boxed{\text{If } v_1, \ldots, v_m \text{ are lin. ind. and } v_i \in \text{span}\{u_1, \ldots, u_k\}\ \forall i, \text{ then } m \leq k.}$

Eventown vs. Oddtown

A town with n people is considering forming clubs such that

→ Any two clubs must have an <u>even</u> number of common members

and in addition they are evaluating following two rules and picking one of them:

<u>Eventown rule</u> Each club has even # of members

<u>Oddtown rule</u> Each club has odd # of members

Which rule is "better"?

Consider constructing clubs under each rule.

Eventown vs. Oddtown

A town with n people is considering forming clubs such that

→ Any two clubs must have an even number of common members

and in addition they are evaluating following two rules and picking one of them:

<u>Eventown rule</u> Each club has even # of members

<u>Oddtown rule</u> Each club has odd # of members

Which rule is "better"?

Consider constructing clubs under each rule.

Eventown: Pair up people so that each pair joins or not joins a club together, so we can construct $2^{\lfloor n/2 \rfloor}$ such clubs.

Eventown vs. Oddtown

A town with n people is considering forming clubs such that

→ Any two clubs must have an <u>even</u> number of common members

and in addition they are evaluating following two rules and picking one of them:

<u>Eventown rule</u> Each club has even # of members

<u>Oddtown rule</u> Each club has odd # of members

Which rule is "better"?

Consider constructing clubs under each rule.

Oddtown: Form n clubs by each club being a single person.

Is it possible to form more clubs in Oddtown?

Theorem [Oddtown thm; Berlekamp 1969]

If $\mathcal{F}$ is a family of odd-sized subsets of $[n]$ whose pairwise intersection has even-size, then $|\mathcal{F}| \leq n$.

Theorem [Oddtown thm; Berlekamp 1969]

If $\mathcal{F}$ is a family of odd-sized subsets of $[n]$ whose pairwise intersection has even-size, then $|\mathcal{F}| \leq n$.

Proof Suppose $\mathcal{F} = \{F_1, \ldots, F_m\}$

For each F_i, associate an incidence vector $u^{(i)}$ as

$$u_j^{(i)} = \begin{cases} 0 & \text{if } j \notin F_i \\ 1 & \text{if } j \in F_i \end{cases}, \quad j = 1, 2, \ldots, n$$

$$u^{(i)} \cdot u^{(i)} = ?$$

$$u^{(i)} \cdot u^{(j)} = ?$$

for $i \neq j$

Theorem [Oddtown thm; Berlekamp 1969]

If $\mathcal{F}$ is a family of odd-sized subsets of $[n]$ whose pairwise intersection has even-size, then $|\mathcal{F}| \leq n$.

Proof Suppose $\mathcal{F} = \{F_1, \dots, F_m\}$

For each F_i, associate an incidence vector $u^{(i)}$ as

$$u^{(i)}_j = \begin{cases} 0 & \text{if } j \notin F_i \\ 1 & \text{if } j \in F_i \end{cases}, \quad j = 1, 2, \dots, n$$

$$u^{(i)} \cdot u^{(i)} = |F_i| = \text{odd } \# \equiv 1 \pmod 2$$

$$u^{(i)} \cdot u^{(j)} = |F_i \cap F_j| = \text{even } \# \equiv 0 \pmod 2$$

for $i \neq j$

so think of $u^{(i)}$ as vectors in $(\mathbb{F}_2)^n$ with $u^{(i)} \cdot u^{(j)} = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$

Theorem [Oddtown thm; Berlekamp 1969]

If $\mathcal{F}$ is a family of odd-sized subsets of $[n]$ whose pairwise intersection has even-size, then $|\mathcal{F}| \leq n$.

Proof Suppose $\mathcal{F} = \{F_1, \ldots, F_m\}$

For each F_i, associate an incidence vector $u^{(i)}$ as

$$u^{(i)}_j = \begin{cases} 0 & \text{if } j \notin F_i \\ 1 & \text{if } j \in F_i \end{cases}, \quad j = 1, 2, \ldots, n$$

$$u^{(i)} \cdot u^{(i)} = |F_i| = \text{odd } \# \equiv 1 \pmod 2$$

$$u^{(i)} \cdot u^{(j)} = |F_i \cap F_j| = \text{even } \# \equiv 0 \pmod 2$$

for $i \neq j$

so think of $u^{(i)}$ as vectors in $(\mathbb{F}_2)^n$ with $u^{(i)} \cdot u^{(j)} = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$

Claim $\{u^{(1)}, \ldots, u^{(m)}\}$ is lin. ind. in $(\mathbb{F}_2)^n$

Pf. ?

$\therefore$ $m \leq \dim((\mathbb{F}_2)^n) = n$. ∎

Theorem [Oddtown thm; Berlekamp 1969]

If $\mathcal{F}$ is a family of odd-sized subsets of $[n]$ whose pairwise intersection has even-size, then $|\mathcal{F}| \leq n$.

Proof Suppose $\mathcal{F} = \{F_1, \ldots, F_m\}$

For each F_i, associate an incidence vector $u^{(i)}$ as

$$u_j^{(i)} = \begin{cases} 0 & \text{if } j \notin F_i \\ 1 & \text{if } j \in F_i \end{cases}, \quad j = 1, 2, \ldots, n$$

$$u^{(i)} \cdot u^{(i)} = |F_i| = \text{odd \#} \equiv 1 \pmod 2$$

$$u^{(i)} \cdot u^{(j)} = |F_i \cap F_j| = \text{even \#} \equiv 0 \pmod 2$$

for $i \neq j$

so think of $u^{(i)}$ as vectors in $(\mathbb{F}_2)^n$ with $u^{(i)} \cdot u^{(j)} = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$

Claim $\{u^{(1)}, \ldots, u^{(m)}\}$ is lin. ind. in $(\mathbb{F}_2)^n$

Pf. $\sum_{j=1}^{m} c_j u^{(j)} = 0 \Rightarrow u^{(i)} \cdot \sum c_j u^{(j)} = 0 \Rightarrow \sum c_j (u^{(i)} \cdot u^{(j)}) = 0$

$\Rightarrow c_i = 0 \quad \forall i$

$\therefore m \leq \dim((\mathbb{F}_2)^n) = n.$ ∎

Read later

Another way of proving the oddtown theorem:

Let M be the incidence matrix of $\mathcal{F} = \{F_1, \dots, F_m\}$, ie., $M_{m \times n}$ over $\mathbb{F}_2$ defined as $m_{ij} = \begin{cases} 1 & \text{if } j \in F_i \\ 0 & \text{if } j \notin F_i . \end{cases}$ $\begin{array}{l} i = 1, \dots, n \\ j = 1, \dots, m \end{array}$

We know $\text{rank}(M) \leq n$ (rank of matrix can't exceed either of its dimensions)

Define $A = MM^T$, $m \times m$ matrix over $\mathbb{F}_2$

with $a_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$ AH!! $A = I_m$

So, $\text{rank}(A) = m$.

We know for any two $m \times n$ & $n \times m$ matrices C & D,

$\text{rank}(CD) \leq \text{rank}(C)$ and $\leq \text{rank}(D)$

$\therefore$ $m = \text{rank}(A) \leq \text{rank}(M) \leq n$, so $m \leq n$. $\blacksquare$

Diagonal Criterion

usually multivariate polynomials

For $i = 1, \dots, m$, let $f_i : \Omega \to \mathbb{F}$ be functions and $a_i \in \Omega$ such that

$$f_i(a_j) \neq 0 \text{ if } i = j$$

$$\text{and } f_i(a_j) = 0 \text{ if } i \neq j$$

Then $f_1, \dots, f_m$ are linearly independent in the space $\mathbb{F}^{\Omega}$.

Proof $\displaystyle\sum_{i=1}^{m} \lambda_i f_i(x) = 0 \Rightarrow \sum_{i=1}^{m} \lambda_i f_i(a_j) = 0 \Rightarrow \lambda_j f_j(a_j) = 0$

$\Rightarrow \lambda_j = 0 \quad \forall j$

Diagonal Criterion

usually multivariate polynomials

For $i=1,\dots,m$, let $f_i:\Omega\to\mathbb{F}$ be functions and $a_i\in\Omega$ such that

$$f_i(a_j)\neq 0 \text{ if } i=j$$
$$\text{and } f_i(a_j)=0 \text{ if } i\neq j$$

Then $f_1,\dots,f_m$ are linearly independent in the space $\mathbb{F}^{\Omega}$.

Proof $\sum_{i=1}^{m}\lambda_i f_i(x)=0 \Rightarrow \sum_{i=1}^{m}\lambda_i f_i(a_j)=0 \Rightarrow \lambda_j f_j(a_j)=0$
$\Rightarrow \lambda_j=0 \quad \forall j$

Triangular Criterion

For $i=1,\dots,m$, let $f_i:\Omega\to\mathbb{F}$ be functions and $a_i\in\Omega$ such that

$$f_i(a_j)\neq 0 \text{ if } i=j$$
$$f_i(a_j)=0 \text{ if } i<j$$

Then $f_1,f_2,\dots,f_m$ are lin. independent in the space $\mathbb{F}^{\Omega}$

k-distance set is a set of points in $\mathbb{R}^n$ such that distances between pairs of points belong to set of atmost k numbers.

1-distance set How many distinct points can we place in $\mathbb{R}^n$ such that all points will be equidistant?

$n=2$: 3 pt.s / corners of equilateral Triangle.

$n=3$: 4 corners of a tetrahedron.

$n+1$ corners of a regular simplex in $\mathbb{R}^n$.

k-distance set is a set of points in $\mathbb{R}^n$ such that distances between pairs of points belong to set of atmost k numbers.

1-distance set How many distinct points can we place in $\mathbb{R}^n$ such that all points will be equidistant?

$n=2$: 3 pt.s / corners of equilateral Triangle.

$n=3$: 4 corners of a tetrahedron.

$n+1$ corners of a regular simplex in $\mathbb{R}^n$.

2-distance set $X \subseteq \mathbb{R}^n$ is a 2-distance set if $\exists\, d_1, d_2 > 0$ s.t. $\|x-y\| \in \{d_1, d_2\}$ $\forall x \neq y$ in X.

Let $\underline{m(n)}$ be the max # points in such a set.

2-distance sets in $\mathbb{R}^n$

$m(1) \geqslant$

$m(2) \geqslant$

2-distance sets in $\mathbb{R}^n$

$m(1) \geq 3$ 

$m(2) \geq 5$  corners of a regular pentagon

Let $S \subseteq \mathbb{R}^{n+1}$ be set of $\binom{n+1}{2}$ binary vectors containing exactly 2 ones. This is a 2-distance set with only 2 & $\sqrt{2}$ as possible distances.

All points of S belong to the n-dim hyperplane $x_1 + x_2 + \dots + x_{n+1} = 2$

This hyperplane can be projected down to $\mathbb{R}^n$ while preserving distances (isometrically) to get a 2-distance set S' of $\binom{n+1}{2}$ points in $\mathbb{R}^n$.

$$m(n) \geq \binom{n+1}{2} = \frac{n^2}{2} + \Theta(n)$$

Upper Bound ?

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S = \{v^{(1)}, v^{(2)}, \ldots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$

Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = \left(\|x - v^{(i)}\|^2 - \lambda_1^2\right)\left(\|x - v^{(i)}\|^2 - \lambda_2^2\right)$ for $i = 1, \ldots, m$

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S = \{v^{(1)}, v^{(2)}, \ldots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$

Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = (\|x - v^{(i)}\|^2 - \lambda_1^2)(\|x - v^{(i)}\|^2 - \lambda_2^2)$ for $i = 1, \ldots, m$

Then $f_i(v^{(j)}) = 0$ if $i \neq j$

$f_i(v^{(i)}) = \lambda_1^2 \lambda_2^2 \neq 0$ in $\mathbb{R}$.

$\therefore$ $F = \{f_1(x), f_2(x), \ldots, f_m(x)\}$ is lin. ind. in $\mathbb{R}[x_1, x_2, \ldots, x_n]$.

2- distance sets in $\mathbb{R}^n$

Theorem [Larman – Rogers – Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S = \{v^{(1)}, v^{(2)}, \ldots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$

Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = (\|x - v^{(i)}\|^2 - \lambda_1^2)(\|x - v^{(i)}\|^2 - \lambda_2^2)$ for $i = 1, \ldots, m$

Then $f_i(v^{(j)}) = 0$ if $i \neq j$

$f_i(v^{(i)}) = \lambda_1^2 \lambda_2^2 \neq 0$ in $\mathbb{R}$.

$\therefore$ $F = \{f_1(x), f_2(x), \ldots, f_m(x)\}$ is lin. ind. in $\mathbb{R}[x_1, x_2, \ldots, x_n]$.

Let $W = \text{span}(F)$, then $m \leq \dim W$

So, to get an upper bound on m, we need an u.b. on $\dim W$ which can found by a "small" spanning set for F.

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S = \{v^{(1)}, v^{(2)}, \ldots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$

Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = (\|x - v^{(i)}\|^2 - \lambda_1^2)(\|x - v^{(i)}\|^2 - \lambda_2^2)$ for $i = 1, \ldots, m$

Expand the expression of each $f_i(x_1, x_2, \ldots, x_n)$ to get the monomial terms of the expansion:

degree 4 term : $(\sum x_k^2)^2$ # possibilities : ?

degree 3 term : $x_j \sum x_k^2$ # possibilities : ?

degree 2 term : $x_i x_j$ # possibilities : ?

degree 1 term : x_i # possibilities : ?

degree 0 term : 1 # possibilities : ?

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S = \{v^{(1)}, v^{(2)}, \ldots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$.

Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = (\|x - v^{(i)}\|^2 - \lambda_1^2)(\|x - v^{(i)}\|^2 - \lambda_2^2)$ for $i = 1, \ldots, m$

Expand the expression of each $f_i(x_1, x_2, \ldots, x_n)$ to get the monomial terms of the expansion:

degree 4 term : $\left(\sum x_k^2\right)^2$ # possibilities : 1

degree 3 term : $x_j \sum x_k^2$ # possibilities : n

degree 2 term : $x_i x_j$ # possibilities : $\binom{n}{2} + n = \frac{n(n+1)}{2}$

degree 1 term : x_i # possibilities : n

degree 0 term : 1 # possibilities : 1

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S = \{v^{(1)}, v^{(2)}, \dots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$

Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = (\|x - v^{(i)}\|^2 - \lambda_1^2)(\|x - v^{(i)}\|^2 - \lambda_2^2)$ for $i = 1, \dots, m$

$F = \{f_1(x), \dots, f_m(x)\}$ lin. ind. in $\mathbb{R}[x_1, \dots, x_n]$

and F has a spanning set with $1 + n + \frac{n(n+1)}{2} + n + 1$ monomials

$$\therefore \quad m \le \dim(\mathrm{span}(F)) \le 1 + n + \frac{n(n+1)}{2} + n + 1 = (n+1)\left(2 + \frac{n}{2}\right) = \frac{(n+1)(n+4)}{2}$$

$\blacksquare$

Polynomial / Lin. Algebra Method

To show $|S| \leq n$

Step 1. Define a polynomial associated with each element of S.

Step 2. Show these polynomials are lin. ind.

Step 3. Show these polynomials are spanned by a set of n (simpler) polynomials.

Polynomial / Lin. Algebra Method

To Show $|S| \leq n$

Step 1. Define a polynomial associated with each element of S.

say, $S = \{s_1, s_2, \dots, s_m\}$ & $s_i \to P_i$, $i = 1, \dots, m$

Step 2. Show these polynomials are lin. ind.

$\{P_1, \dots, P_m\}$ lin. ind.

Step 3. Show these polynomials are spanned by a set of n (simpler) polynomials.

$\mathrm{span}(\{P_1, \dots, P_m\}) \subseteq \mathrm{span}(\{r_1, r_2, \dots, r_n\})$, so $m \leq n$