Combinatorics, 2016 Fall, USTC

Week 15, Dec 13 & 15

Applications of Linear Algebra

While the probabilistic method is usually useful to construct examples (by randomness) and obtain lower bounds, a common application of linear algebra is to prove an upper bound, where we show that objects satisfying certain properties cannot be too large. To do so, usually we place the objects by vectors in a linear space of a certain dimension, and we show the vectors are linearly independent. Thus, the number of objects is at least the number of dimension.

Odd/Even-town

A town has n residents. They want to form some clubs according to the following rules:

(i) Each club has an odd number of members.

(ii) Every 2 clubs must share an even number of members.

Question. How many clubs can they form?

Examples. (a) $A_i = \{i\}$ for $i \in [n] \Rightarrow n$ clubs.

(b) $n =$even, $A_i = [n] \setminus \{i\} \Rightarrow n$ clubs.

(c) $n =$even, $A_1 = [n]\setminus\{1\}$, $A_2 = [n]\setminus\{2\}$, $A_i = \{1, 2, i\}$ for $i \in \{3, ..., n\} \Rightarrow$ n clubs.

Theorem 1 (Odd/Even-town)**.** *Let $\mathscr{F} \subseteq 2^{[n]}$ be a family satisfying:*

(i) $|A|$ *is odd for all* $A \in \mathscr{F}$*,*

(ii) $|A \cap B|$ *is even, for all* $A \neq B \in \mathscr{F}$*. Then* $|\mathscr{F}| \leq n$*.*

Proof. For all $A \in \mathscr{F}$, define $\mathbf{1}_A$ to be the vector in $\mathbb{F}_2^n = \{0,1\}^n$, s.t.

$$\mathbf{1}_A(i) = \begin{cases} 1, & \text{if } i \in A \\ 0, & \text{if } i \notin A, \end{cases}$$

where $\mathbb{F}_2$ is viewed as a finite field. Then, the conditions become

$$\begin{cases} \mathbf{1}_A \cdot \mathbf{1}_A = 1, & \forall A \in \mathscr{F} \\ \mathbf{1}_A \cdot \mathbf{1}_B = 0, & \forall A \neq B \in \mathscr{F}. \end{cases} \tag{1}$$

Let $|\mathscr{F}| = m$, so we have m vectors satisfying (1). Next we show all such vectors in $\mathbb{F}_2^n$ are linearly independent.

Let $\alpha_A \in \{0,1\}$, s.t. $\sum_{A \in \mathscr{F}} \alpha_A \mathbf{1}_A = \mathbf{0}$.

$$\Rightarrow \forall A \in \mathscr{F},\ \mathbf{1}_A \cdot \left(\sum_{A \in \mathscr{F}} \alpha_A \mathbf{1}_A \right) = \mathbf{0} \cdot \mathbf{1}_A = 0 \Rightarrow \alpha_A = 0.$$

This shows that $\{\mathbf{1}_A : A \in \mathscr{F}\}$ is linearly independent. Thus $|\mathscr{F}| = m \leq \#$ dimension in $\mathbb{F}_2^n = n$. ∎

Even/Odd-town

Let $\mathscr{F} \subseteq 2^n$ be s.t.:

(i) $|A|$ =even, for all $A \in \mathscr{F}$,

(ii) $|A \cap B|$ =odd, for all $A \neq B \in \mathscr{F}$.

Fact 1: Such $|\mathscr{F}| \leq n+1$.

Proof. Adding a new element $n+1$ to each set $A \in \mathscr{F}$ to get a new family $\mathscr{F}^*$. It is easy to see $\mathscr{F}^*$ satisfies Odd/Even-town condition. So $|\mathscr{F}| = |\mathscr{F}^*| \leq n+1$ ∎

Theorem 2 (Even/Odd-town)**.** *Such* $|\mathscr{F}| \leq n$.

Proof. It suffices to prove that $|\mathscr{F}| \neq n+1$. Suppose for a contradiction that $|\mathscr{F}| = n+1$. For each $A \in \mathscr{F}$, define $\mathbf{1}_A \in \mathbb{F}_2^n$ as before. So we have $n+1$ vectors in an n-dimension space. Thus, they must be linearly dependent, i.e. $\exists \alpha_A \in \{0,1\}$ (not all zeros), s.t. $\sum_{A\in\mathscr{F}} \alpha_A \mathbf{1}_A = \mathbf{0}$. We also have

$$\begin{cases} \mathbf{1}_A \cdot \mathbf{1}_A = 0, & \forall A \in \mathscr{F} \\ \mathbf{1}_A \cdot \mathbf{1}_B = 1, & \forall A \neq B \in \mathscr{F}. \end{cases} \tag{2}$$

Then for each $B \in \mathscr{F}$,

$$0 = \mathbf{0} \cdot \mathbf{1}_B = \left(\sum_A \alpha_A \mathbf{1}_A \right) \cdot \mathbf{1}_B = \sum_{A \neq B} \alpha_A.$$

This shows that all α_B's are equal. Because not all α_B's are zeros, we have $\alpha_B = 1$ for each $B \in \mathscr{F}$.

$$\Rightarrow \sum_{A\in\mathscr{F}} \mathbf{1}_A = \mathbf{0}. \tag{3}$$

$\Rightarrow n = \sum_{A\neq B} \alpha_A = 0 \Rightarrow n$ is even.

Consider $\mathscr{F}^c = \{A^c : A \in \mathscr{F}\}$ we will see that $\mathscr{F}^c$ also has Even/Odd condition.

- $|A^c| = n - |A|$ is even, for all $A \in \mathscr{F}$.

- $|A^c \cap B^c| = n - ||A \cup B| = n - (|A| + |B| - |A \cap B|)$ is odd, for all $A \neq B \in \mathscr{F}$.

Repeating the previous proof, we can get

$$\sum_{A \in \mathscr{F}} \mathbf{1}_{A^c} = \mathbf{0}. \tag{4}$$

Now (3)+(4) we get $\mathbf{0} = \sum_{A \in \mathscr{F}} (\mathbf{1}_A + \mathbf{1}_{A^c}) = (n+1)\mathbf{1} = \mathbf{1}$ as n is even, a contradiction. ∎

Even/Even-town

Let $\mathscr{F} \subset 2^{[n]}$ be s.t.:

(i) $|A|$ =even, for all $A \in \mathscr{F}$,

(ii) $|A \cap B|$ =even, for all $A \neq B \in \mathscr{F}$.

Then $|\mathscr{F}| \leq 2^{n/2}$.

Fisher's Inequality

Theorem 3 (Fisher's Inequality)**.** *Let $\mathscr{F} \subseteq 2^{[n]}$ be s.t. for some fixed k, $|A \cap B| = k$, for all $A \neq B \in \mathscr{F}$. Then, $|\mathscr{F}| \leq n$.*

Proof. For each $A \in \mathscr{F}$, define $\mathbf{1}_A$ as before (over $\mathbb{R}$). $\Rightarrow \forall A, B \in \mathscr{F}$, $\mathbf{1}_A \cdot \mathbf{1}_b = k$. Again, we want to show $\mathbf{1}_A$'s are linearly independent over $\mathbb{R}^n$. Let $\sum_{A \in \mathscr{F}} \alpha_A \mathbf{1}_A = \mathbf{0}$, where $\alpha_A \in \mathbb{R}$. Then

$$0 = \left(\sum_{A \in \mathscr{F}} \alpha_A \mathbf{1}_A \right) \cdot \left(\sum_{A \in \mathscr{F}} \alpha_A \mathbf{1}_A \right) = \sum_{A \in \mathscr{F}} \alpha_A^2 \mathbf{1}_A \cdot \mathbf{1}_A + \sum_{A \neq B} \alpha_A \alpha_B \mathbf{1}_A \cdot \mathbf{1}_B$$

$$= \sum_{A\in\mathscr{F}} \alpha_A^2|A| + k\cdot\sum_{A\neq B}\alpha_A\alpha_B = k\left(\sum_{A\in\mathscr{F}}\alpha_A\right)^2 + \sum_{A\in\mathscr{F}}\alpha_A^2(|A|-k) \geq 0,$$

where the last inequality holds because each A is of size at least k. Moreover, we know there is at most one set A of size exactly k.

From this, we see it must be an equality, i.e. $\sum_{A\in\mathscr{F}}\alpha_A = 0$ and $\alpha_A^2(|A|-k) = 0$ for all $A \in \mathscr{F}$. Let A^* be the unique set (if exist) of size k. So for each $A \in \mathscr{F}\setminus\{A^*\}$, $\alpha_A = 0$. But $\sum_{A\in\mathscr{F}}\alpha_A = 0$. This shows $\alpha_{A^*} = 0$. so all α_A's are 0. $\Rightarrow |\mathscr{F}| \leq \#$ dimension $= n$. ∎

Lemma 4. *Suppose P is a set of n points in $\mathbb{R}^2$. Then either they are in a line, or they define at least n lines.*

Proof. Let L be the family of all lines defined by P. For each point $x_i \in P$, define $L_i = \{l \in L : l \text{ passes through } x_i\} \subseteq L$. Observe that for all i, j, $|L_i \cap L_j| = 1$. So this satisfies Fisher's by viewing $[N] = L$. In case the points of P are not in a line, for all $i \neq j$, $L_i \neq L_j$. By Fisher's,

$$n = |P| = \#L_i's \leq N = |L|.$$

∎

Lemma 5. *Let G be a graph whose vertices are triples in $\binom{[k]}{3}$ and $\forall A, B \in \binom{[k]}{3}, A \sim B$ iff $|A\cap B| = 1$. Then G doesn't have any clique or independent set of size k+1.*

Corollary 6. $R(k+1,k+1) > \binom{k}{3}$

Remark. This gives us an explicit construction for R(k+1,k+1).

This bound is much weaker than previous $R(k+1,k+1) > c\cdot k2^{\frac{k}{2}}$.

Proof. Consider the maximum clique of G, say $A_1, A_2, ..., A_m \in \binom{[k]}{3}$ with $|A_i \cap A_j| = 1, \forall 1 \leq i < j \leq m$. By Fisher's inequality, $m \leq k$.

Consider the maximum independent set of G, say $B_1, B_2, ..., B_t$,

$$\Longrightarrow \begin{cases} |B_i| = 3 \quad is \quad odd \\ |B_i \cap B_j| = 0 \quad or \quad 2 \quad is \quad even \end{cases}$$

By Odd/Even-town, we have #maximum independent set= $t \leq k$. ∎

1-Distance Problems

Problem. Given n points in $\mathbb{R}^2$, how many pairs of distance 1 can we have?

Theorem 7. *There are at most $O(n^{\frac{3}{2}})$ pairs at distance 1.*

Proof. Define a graph on n points as following: for points a,b, $a \sim b$ iff d(a,b)=1.

Claim: G is $K_{2,3}$-free.

Proof. The neighbors of the point a must lie on the circle with center a and with radius 1. But any such 2 circles can intersect at most 2 points. This shows that G is $K_{2,3}$-free. ∎

#pairs at distance 1=$e(G) \leq ex(n, K_{2,3}) = O(n^{\frac{3}{2}})$. ∎

Problem (Erdős)**.** Can one find an example of n point in $\mathbb{R}^2$ with n^{1+c} pairs at distance 1 for c>0?

Problem. How many points in $\mathbb{R}^n$ s.t. the distance between any 2 points is 1?

Theorem 8. *There are at most n+1 such points in* $\mathbb{R}^n$.

Proof. Assume we have m such points in $\mathbb{R}^n$. We assume one of them is $\mathbf{0}$ and let others be $\boldsymbol{v_1}, \boldsymbol{v_2}, ..., \boldsymbol{v_{m-1}} \in \mathbb{R}^n$.

$$\Longrightarrow \begin{cases} \boldsymbol{v_i} \cdot \boldsymbol{v_i} = ||\boldsymbol{v_i} - \mathbf{0}||^2 = 1 \\ \boldsymbol{v_i} \cdot \boldsymbol{v_j} = \dfrac{1}{2}, i \neq j \end{cases}$$

because $1 = ||\boldsymbol{v_i} - \boldsymbol{v_j}||^2 = ||\boldsymbol{v_i}||^2 + ||\boldsymbol{v_j}||^2 - 2\boldsymbol{v_i} \cdot \boldsymbol{v_j} = 1 + 1 - 2\boldsymbol{v_i} \cdot \boldsymbol{v_j}$

$$\Longrightarrow \boldsymbol{v_i} \cdot \boldsymbol{v_j} = \frac{1}{2}.$$

Consider

$$A = \begin{pmatrix} \boldsymbol{v_1} \\ \boldsymbol{v_2} \\ \vdots \\ \boldsymbol{v_{m-1}} \end{pmatrix}_{(m-1)\times n}$$

So

$$A \cdot A^T = \begin{pmatrix} 1 & \frac{1}{2} & \cdots & \frac{1}{2} \\ \frac{1}{2} & 1 & \cdots & \frac{1}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2} & \frac{1}{2} & \cdots & 1 \end{pmatrix}_{(m-1)\times(m-1)}$$

Since $det(A \cdot A^T) \neq 0, \Rightarrow rank(A \cdot A^T) = m - 1$.

$$\Longrightarrow n \geq rankA \geq rank(A \cdot A^T) = m - 1$$

$$\Longrightarrow m \leq n + 1.$$

2-Distance Problems

Definition 9. A 2-distance set is a set of points in $\mathbb{R}^n$ whose pairwise distance is either c or d for some c,d>0.

Instead of considering vectors, one also can define certain polynomials, as polynomials of certain degree also form a vector space.

Lemma 10. *Let $f_i : \Omega \to \mathscr{F}$ be polynomials for i=1,2,...,n. If $\exists v_i \in \Omega$ for i=1,2,...,n s.t.*

$$\begin{cases} f_i(v_i) \neq 0, & \forall i \\ f_i(v_j) = 0, & \forall j < i \end{cases}$$

then $f_1, f_2, ..., f_n$ are linear independent over $\mathbb{F}^\Omega$.

Theorem 11. *Any 2-distance set in $\mathbb{R}^n$ has at most $\frac{1}{2}(n+1)(n+4)$ points.*

Proof. Let $A \subset \mathbb{R}^n$ be such a set with distances $c > 0$, $d > 0$. Let $A = \{\boldsymbol{a_1}, \boldsymbol{a_2}, ..., \boldsymbol{a_m}\}$. For $\forall i \in [m]$, let $f_i(\boldsymbol{x}) = (||\boldsymbol{x} - \boldsymbol{a_i}||^2 - c^2)(||\boldsymbol{x} - \boldsymbol{a_i}||^2 - d^2)$

$$\Rightarrow \begin{cases} f_i(\boldsymbol{a_i}) = c^2 d^2 \neq 0 \\ f_i(\boldsymbol{a_j}) = (||\boldsymbol{a_j} - \boldsymbol{a_i}||^2 - c^2)(||\boldsymbol{a_j} - \boldsymbol{a_i}||^2 - d^2) = 0, & \forall j \neq i \end{cases}$$

By lemma, we see $f_1, f_2, ..., f_m$ are linearly independent. We want to bound the dimension of "some vector space" which contains all polynomials $f_1, f_2, ..., f_m$.

Note that

$$f_i(\boldsymbol{x}) = (\sum_i (x_i - a_i)^2 - c^2)(\sum_i (x_i - a_i)^2 - d^2)$$
$$= (\sum_i x_i^2 - 2\sum_i x_i a_i + \sum_i a_i^2 - c^2)(\sum_i x_i^2 - 2\sum_i x_i a_i + \sum_i a_i^2 - d^2)$$

can be expressed as the linear combination of the following:

$$B = \{(\sum_i x_i^2)^2, x_j(\sum_i x_i^2), x_i x_j, x_i, 1\}$$

$$|B| = 1 + n + \binom{n}{2} + n + n + 1 = \frac{n(n-1)}{2} + 3n + 2 = \frac{(n+1)(n+4)}{2}$$

So $f_1, f_2, ..., f_m$ are in the space V spanned by B.

$$\Longrightarrow |A| = m \leq dim(V) = |B| = \frac{(n+1)(n+4)}{2}.$$

∎

Remark. This can be extended to 3-distance Problem, even t-distance problem.

Next, we consider a generalization of Fisher's inequality.

Definition 12. Let $L \subset \{0, 1, 2, ..., n\}$. We say a family $\mathscr{F} \subset 2^{[n]}$ is L-intersecting, if $|A \cap B| \in L$ for $\forall A \neq B \in L$.

Theorem 13 (Frankl-Wilson, 1981)**.** *If $\mathscr{F}$ is an L-intersecting family in $2^{[n]}$, then $|\mathscr{F}| \leq \sum_{k=0}^{|L|} \binom{n}{k}$.*

Proof. Let $\mathscr{F} = \{A_1, A_2, ..., A_m\}$ where $|A_1| \leq |A_2| \leq \cdots \leq |A_m|$. For

$i \in [m]$, let $f_i(\boldsymbol{x})$ in $\mathbb{R}^n$ by

$$f_i(\boldsymbol{x}) = \prod_{l \in L, l < |A_i|} (\boldsymbol{x} \cdot \mathbf{1}_{\boldsymbol{A_i}} - l).$$

So $f_i(\boldsymbol{x})$ is a polynomial with n variables and with degree$\leq |L|$.

Note that $f_i(\mathbf{1}_{\boldsymbol{A_i}}) = \prod_{l \in L, l < |A_i|}(|A_i| - l) \neq 0$.

Claim: For j<i,

$$f_i(\mathbf{1}_{\boldsymbol{A_j}}) = \prod_{l \in L, l < |A_i|} (|A_i \cap A_j| - l) = 0.$$

Since $\mathscr{F}$ is L-intersecting and $|A_j| \leq |A_i|$. $l = |A_j \cap A_i| < |A_i|$.

(To be continued.)