2.2, Equal Intersection Size

$\mathcal{F}$: $\quad |X \cap Y| = k \quad$ for all $X \neq Y \in \mathcal{F}$

1940 Fisher

Thm (Nonuniform Fisher Inequality)

$k \geq 0$

$\mathcal{F}$: family of subsets of $\{1, 2, \dots, n\}$.

If $|X \cap Y| = k$ for all distinct $X, Y \in \mathcal{F}$

then $\quad |\mathcal{F}| \leq \boxed{n}$

Example : $\boxed{k=1}$ $\quad \left\{ \begin{array}{l} \{1\} \cup \{i\} \\ \{\{1\}\} \end{array} \right\} n$.

Proof. Let $m = |\mathcal{F}|$. $\quad \mathcal{F} = \{A_1, A_2, \dots, A_m\}$

If $|A_i| = k$, then

$$A_i \subseteq A_j \quad \text{for all } j$$

Assume $i = 1$.

$$\Rightarrow \underbrace{A_2 - A_1}_{\neq \emptyset},\ \underbrace{A_3 - A_1}_{\neq \emptyset}, \dots,\ \underbrace{A_m - A_1}_{\neq \emptyset}$$

is a partition of $\bigcup_{j=2}^{m} (A_j - A_1)$

$$\subseteq \{1, \dots, n\} - A_1$$

$$\Rightarrow |\mathcal{F}| \leq 1 + n - |A_1|$$

$$= 1 + n - k \leq n$$

Thus, we may assume $|A_i| \geq k+1$ for all i.

Let

$$M = \begin{array}{c|c} & 1 \sim m \\ \hline 1 \sim n & \begin{pmatrix} \\ m_{ij} \\ \\ \end{pmatrix} \end{array} \qquad m_{ij} = \begin{cases} 1 & \text{if } i \in A_j \\ 0 & \text{otherwise.} \end{cases}$$

Let $A = M^T M$

$$= \begin{array}{c} A_1 \\ \vdots \\ A_m \end{array} \; \overset{1\sim n}{\begin{pmatrix} \\ \boxed{0\,0\,1\,1\,0\cdots} \\ \\ \end{pmatrix}}_{1\sim m} \; {}_{1\sim n}\overset{1\sim m}{\begin{pmatrix} \boxed{\begin{matrix} 0 \\ 0 \\ 1 \\ 1 \\ \vdots \\ 0 \\ 0 \end{matrix}} \end{pmatrix}}$$

$$= \begin{pmatrix} |A_1| & & & k \\ & |A_2| & & \\ & & \ddots & \\ k & & & |A_m| \end{pmatrix} \qquad |A_i \cap A_j| = k$$

$$= kJ + C$$

J = all-1 $m \times m$ matrix

C = diagonal matrix whose diagonal entries are > 0.

$$rk(A) \leq rk(M) \leq n$$

Claim: A is nonsingular.

* An $m \times m$ matrix A is positive semidefinite if $x^T A x \geq 0$ for all $x \in \mathbb{R}^m$.

It is positive definite if in addition, $x^T A x = 0 \Leftrightarrow x = 0$.

Lemma: All positive definite matrices have the full rank.

(If not, then there is a non-trivial y such that $Ay=0 \Rightarrow y^T A y = 0$.)

Claim: $kJ + C$ is positive definite.

Suppose $x^T (kJ + C) x = 0$

$$k\, x^T J x + x^T C x = 0$$

$$k\, x^T \underbrace{\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \underbrace{(1 \cdots 1) x}}_{J} + x^T C x = 0$$

$$k \left(\sum_{i=1}^{n} x_i \right)^2 + \sum_{i=1}^{n} c_i x_i^2 = 0$$

$\Rightarrow$ $x_i = 0$ for all x

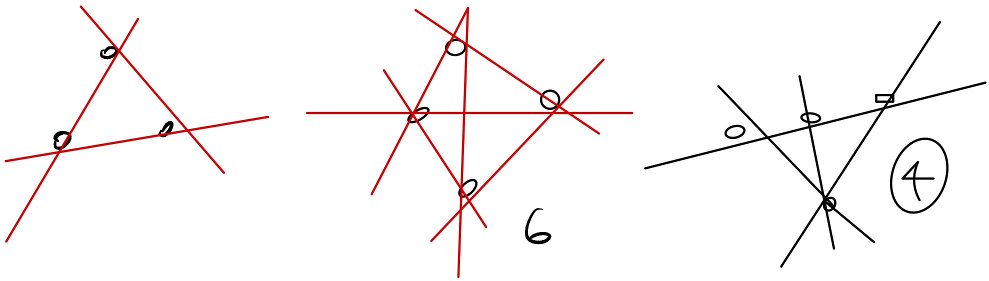
$x = 0$.

$\Rightarrow$ $kJ + C$ is nonsingular

$\text{rank}(kJ + C) = m$.

$m \leq n$. $\square$

<u>Corollary</u>: Suppose there are n distinct points on the plane such that not all of them are on one line. Then there are at least n distinct lines through at least 2 of the n points.



<u>Proof</u>. Let S be the set of lines through at least 2 of the n points.

For a point x, let A_x be the set of all lines through x.

$$|A_x \cap A_y| = 1 \quad \text{for all } x \neq y$$

$$A_{x_1} \quad A_{x_2} \quad \cdots \quad A_{x_n}$$

Since not all of them are in one line, $|A_x| \geq 2$ for all x.

By the non-uniform Fisher's inequality

$$n \leq |S| = m$$

↑ # lines

$\therefore$ # lines $\geq n$. $\square$

Alternative proof.

Let $p_1, p_2, \ldots, p_n$ be the points.

$L_1 \; L_2 \cdots L_m$ be the lines.

Suppose $m < n$.

Let $$g(x) = \sum_{k=1}^{m} \Big(\underline{\sum_{p_j \in L_k} x_j} \Big)^2$$

$x \in \mathbb{R}^n$.

Since $m < n$, there exists a nonzero $x^* = (x_1^*, \ldots, x_n^*)$ such that $g(x^*) = 0$

Expand g:

$$g(x) = 2 \sum_{i<j} x_i x_j + \sum_{i=1}^{n} \alpha_i \, x_i^2$$

$\alpha_i = \#$ lines through p_i

$\alpha_i \geq 2$

$$\geq 2 \sum x_i x_j + 2 \sum x_i^2$$

$$= \Big(\sum x_i\Big)^2 + \sum \big(x_i^2\big)$$

$g(x^*) \neq 0$ Contradiction $\square$

2.3. L-intersecting family

Let $L \subseteq \mathbb{Z}$.
We say a family $\mathcal{F}$ of sets is L-intersecting if for all $X, Y \in \mathcal{F}$, $X \neq Y$, $|X \cap Y| \in L$.

How large can $\mathcal{F}$ be, if it is L-intersecting, $|L| = s$?

Ex. $L = \{0, 1, 2, \ldots, s-1\}$
$\mathcal{F}$ = set of subsets of size $\leq s$
$$\Rightarrow \quad |\mathcal{F}| = \sum_{i=0}^{s} \binom{n}{i}$$

<u>Thm 1</u> (Frankl, Wilson 1981)
If $\mathcal{F}$ is an L-intersecting family of subsets of $\{1, 2, \cdots, n\}$, and $|L| = s$ then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$

What if $\mathcal{F}$ is uniform & L-intersecting? ---- $\binom{n}{s}$?

<u>Thm 2</u>. (Ray-Chaudhuri, Wilson 1975)
If $\mathcal{F}$ is an L-intersecting uniform family of subsets of $\{1, 2, \cdots, n\}$ and $|L| = s$, then
$$|\mathcal{F}| \leq \binom{n}{s}.$$

What if we ask
$$|X \cap Y| \in L \pmod{p}?$$
$$L + p\mathbb{Z} = \{a + p \cdot i : i \in \mathbb{Z}, a \in L\},$$

Thm 3. (Deza, Frankl, Singhi 1983)

Let p be a prime. Let $L \subseteq \{0, 1, \dots, p-1\}$, $|L| = s$

Let $\mathcal{F}$ be a family of subsets of $\{1, 2, \dots, n\}$.

If (1) $|A| \notin L + p\mathbb{Z}$ for all $A \in \mathcal{F}$

(2) $|A \cap B| \in L + p\mathbb{Z}$ for all distinct $A, B \in \mathcal{F}$

then

$$|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$$

Thm 4. (Alon, Babai, Suzuki 1991)

Let p be a prime.

Let $L \subseteq \{0, 1, \dots, p-1\}$, $|L| = s$

Assume $s + k \leq n$.

Let $\mathcal{F}$ be a family of subsets of $\{1, 2, \dots, n\}$.

If

(1) $|A| \equiv k \pmod{p}$ for all $A \in \mathcal{F}$

(2) $k \notin L + p\mathbb{Z}$

(3) $|A \cap B| \in L + p\mathbb{Z}$ for all distinct $A, B \in \mathcal{F}$.

then

$$|\mathcal{F}| \leq \binom{n}{s}.$$

Proof of Thm 3:

Let $\mathcal{F} = \{A_1, A_2, \dots, A_m\}$

Let $a_i = \begin{pmatrix} a_{i1} \\ a_{i2} \\ \vdots \\ a_{in} \end{pmatrix} \in \mathbb{F}_p^n$ $\qquad \mathbb{F}_p = \{0, 1, \dots, p-1\}$

where $a_{ij} = \begin{cases} 1 & \text{if } j \in A_i \\ 0 & \text{otherwise} \end{cases}$.

characteristic vector of A_i

Let $L = \{l_1, l_2, \dots, l_s\}$

For $i \in \{1, \dots, m\}$ let

$$f_i(x) = \prod_{j=1}^{s} \left(\underbrace{x \cdot a_i}_{\left(\sum_{p=1}^{n} x_p \cdot a_{jp}\right)} - l_j \right) \quad \text{for } x \in \mathbb{F}_p^n.$$

$$f_i(a_i) = \prod_{j=1}^{s} (|A_i| - l_j) \not\equiv 0 \pmod p$$

$$i \neq j \quad f_i(a_j) = \prod_{p=1}^{s} (|A_i \cap A_j| - l_p) \equiv 0 \pmod p$$

$\Rightarrow f_1, f_2, \dots, f_m$ are linearly independent

$(\Rightarrow m \leq \dim (\;?\; \to \deg \leq s \text{ poly}))$

Trick:

We obtain $\tilde{f}_i$ from f_i by replacing x_j^2 to x_j after expanding it.

$$\Rightarrow \tilde{f}_i(a_i) = f_i(a_i) \not\equiv 0 \pmod p$$

$$i \neq j \quad \tilde{f}_i(a_j) = f_i(a_j) \equiv 0 \pmod p$$

$\Rightarrow \tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_m$ are linearly independent.

if not, $\sum c_i \tilde{f}_i(x) \equiv 0 \pmod p$

$$\sum c_i f_i(a_j) \equiv 0 \pmod p$$

$$\Rightarrow c_j \underline{f_j(a_j)} \equiv 0 \pmod p$$

$$\Rightarrow c_j \equiv 0 \pmod p$$

$c_j = 0.$

all $\tilde{f}_i$ are contained in the span of multilinear polynomials of degree $\le s$ with n variables $x_1, \dots x_n$

$$\langle x_{i_1} x_{i_2} x_{i_3} \cdots x_{i_\ell} \mid 1 \le i_1 < i_2 < \cdots < i_\ell \le s \rangle$$

# of these $= \sum_{i=0}^{s} \binom{n}{i}$

$$\therefore \quad m \le \sum_{i=0}^{s} \binom{n}{i} \qquad \square$$

Proof of Thm 1. $\mathcal{F} = \{A_1, A_2, \dots, A_m\}$

$L = \{l_1, l_2, \dots, l_s\}$

Let $a_i \in \mathbb{R}^n$ be the characteristic vector of A_i

We assume $|A_1| \le |A_2| \le \cdots \le |A_m|$.

Let $f_i(x) = \prod_{\substack{j : j \in \{1, \dots, s\} \\ l_j < |A_i|}} (x \cdot a_i - l_j)$

Let $\tilde{f}_i(x)$ be the multilinear polynomial Obtained from $f_i(x)$ by reducing x_j^2 to x_j repeatedly

So that $\tilde{f}_i(x) = f_i(x)$ for all $x \in \{0,1\}^n$.

Now $\tilde{f}_i(a_i) = f_i(a_i) = \prod_{l_j < |A_i|} (|A_i| - l_j) \neq 0$

$\tilde{f}_i(a_j) = f_i(a_j) = \prod_{k : l_k < |A_i|} (|A_i \cap A_j| - l_k) = 0$ $\boxed{\text{for } i > j}$

$\tilde{f}_1, \tilde{f}_2 \ldots \tilde{f}_m$ are linearly independent

The dimension of the subspace of multilinear polynomials of degree $\leq s$ is $\leq \sum_{i=0}^{s} \binom{n}{i}$

$\Rightarrow m \leq \sum_{i=0}^{s} \binom{n}{i}$. $\square$

What if $|A_i \cap A_j| = |A_i| = l_j$

$(A_i \subsetneq A_j)$

$\Rightarrow |A_j| > |A_i|$

$\Rightarrow j > i$

Still, $\tilde{f}_1, \tilde{f}_2, \ldots, \tilde{f}_m$ are linearly independent.

Suppose $\sum_{i=1}^{n} c_i \tilde{f}_i(x) = 0$

$x = a_1$: $c_1 \tilde{f}_1(a_1) = 0$

$x = a_2$: $c_1 \tilde{f}_1(a_2) + c_2 \tilde{f}_2(a_2) = 0$

$x = a_3$: $c_1 \tilde{f}_1(a_3) + c_2 \tilde{f}_2(a_3) + c_3 \tilde{f}_3(a_3) = 0$

$\vdots$

$x = a_m$: $\sum c_i \tilde{f}_i(a_m) = 0$

If $c_1 = c_2 = c_3 = \cdots = c_{k-1} = 0$

then $\sum c_i \tilde{f}_i(a_k) = 0$

$\Rightarrow c_k \tilde{f}_k(a_k) = 0$

$c_k = 0$.

Proof of Thm 2.

Let $\mathcal{F} = \{A_1, A_2, \dots, A_m\}$ $\quad k = |A_1| = \dots = |A_m|$.

Let $a_i \in \mathbb{R}^n$ characteristic vector of A_i

$L = \{l_1, \dots, l_s\}$

We may assume $l_i < k$.

Let $$f_i(x) = \prod_{j=1}^{s} (x \cdot a_i - l_j) \quad \text{for } x \in \mathbb{R}^n.$$

Let $\tilde{f}_i$ be the multilinear polynomial obtained from f_i by reducing x_j^2 to x_j repeatedly.

Then $\tilde{f}_i(x) = f_i(x)$ for $x \in \{0,1\}^n$.

$$\left\{ \begin{array}{l} \tilde{f}_i(a_i) \neq 0 \\ \tilde{f}_i(a_j) = 0 \quad \text{for } i \neq j \end{array} \right) \quad \tilde{f}_1, \dots, \tilde{f}_m \text{ are linearly indep.}$$

For each subset I of $\{1, 2, \dots, n\}$ with $|I| < s$ let
$$g_I(x) = \left(\sum_{i=1}^{n} x_i - k\right) \prod_{i \in I} x_i$$

$($ $x \in \{0,1\}^n$ with $x \cdot x = k$ then $g_I(x) = 0$ $)$

Let $\tilde{g}_I(x)$ = multilinear polynomial obtained from g_I by reducing x_j^2 to x_j repeatedly

Claim: $\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_m$, $\tilde{g}_I$ for all $I \subseteq \{1, \dots, n\}$, $|I| < s$ are linearly independent.

Suppose that $\sum_{i=1}^{m} \alpha_i \tilde{f}_i(x) + \sum_I \beta_I \tilde{g}_I(x) = 0$

By taking $x = a_j$: $0 = \sum \alpha_i \tilde{f}_i(a_j) = \alpha_j f_j(a_j)$

$$\Rightarrow \alpha_j = 0$$

$$\Rightarrow \alpha_1 = \alpha_2 = \dots = \alpha_m = 0$$

If there is I such that $\beta_I \neq 0$
then choose I_0 that is minimal among them

Let x^* be the characteristic vector of I_0.

$$\tilde{g}_I(x^*) = g_I(x^*) = (|I_0| - k) \prod_{i \in I} x_i$$

$$= 0 \text{ if } I - I_0 \neq \phi$$

$$\therefore \beta_{I_0} \tilde{g}_{I_0}(x^*) = 0 \quad \Rightarrow \beta_{I_0} = 0.$$

Contradiction.

$$m + \sum_{i=0}^{s-1} \binom{n}{i} \leq \dim (\dots) = \sum_{i=0}^{s} \binom{n}{i}$$

$$\therefore m \leq \binom{n}{s} \qquad \square$$

2.4 Möbius inversion in a partially ordered set

$$g(n)=\sum_{d|n} f(d) \Rightarrow f(n)=\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

Möbius inversion formula

$P=(X,\leq)$ is a partial order if

(1) $x\leq x$ for all $x\in X$

(2) $x\leq y,\ y\leq x \Rightarrow x=y$

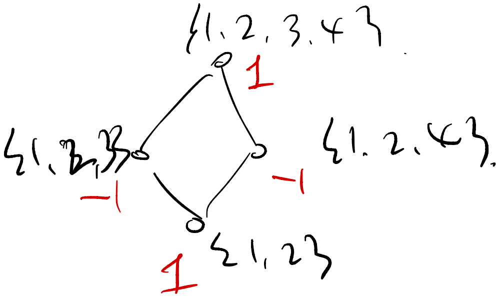
(3) $x\leq y,\ y\leq z \Rightarrow x\leq z$

$(\{\text{subsets of } \mathcal{U}\},\ \subseteq)$

We define $\mu(s,t)$ for $s,t\in P$

$$\mu(s,t)=\begin{cases} 1 & \text{if } s=t \\ 0 & \text{if } s\not\leq t \\ -\sum_{s\leq u<t} \mu(s,u) & \text{otherwise} \end{cases}$$

$$\Leftrightarrow \quad \sum_{s\leq u\leq t} \mu(s,u)=\begin{cases} 1 & \text{if } s=t \\ 0 & \text{if } s<t \end{cases}$$



$\mu(\{1,2\},\{1,2,3,4\})$
$=1$

Claim: $\sum_{u \le s \le t} \mu(\boxed{s}, t) = \begin{cases} 1 & \text{if } u = t \\ 0 & \text{otherwise.} \end{cases}$ for u, t

$\Uparrow$

Def: $\sum_{s \le \boxed{u} \le t} \mu(s, \boxed{u}) = \begin{cases} 1 & \text{if } s = t \\ 0 & \text{otherwise} \end{cases}$ for s, t

Proof of the claim:

Induction on $|\{ s : u \le s \le t \}|$.

If $u = t$, then it is trivial.

For s and t, $(s \neq t)$

$$\sum_{s \le u_1 \le u_2 \le t} \mu(u_1, u_2) = \sum_{s \le u_1 \le t} \underbrace{\sum_{u_1 \le u_2 \le t} \mu(u_1, u_2)}_{\neq 0 \text{ iff } \boxed{u_1 = t}}$$

$$= 1$$

$$\|$$

$$\sum_{s \le u_2 \le t} \sum_{s \le u_1 \le u_2} \mu(u_1, u_2)$$

$$= \sum_{s \le u_2 < t} \underbrace{\left(\sum_{s \le u_1 \le u_2} \mu(u_1, u_2) \right)}_{\neq 0 \iff s = u_2} + \sum_{s \le u_1 \le t} \mu(u_1, t)$$

$$= 1 + \sum_{s \le u_1 \le t} \mu(u_1, t)$$

$$\therefore \sum_{s \le u_1 \le t} \mu(u_1, t) = 0$$

$\square$

If $P = (2^X, \subseteq)$ then

$$\mu(A,B) = (-1)^{|B|-|A|} \quad \text{if } A \subseteq B.$$

$$\left(\sum_{A \subseteq U \subseteq B} (-1)^{|U|-|A|} = \sum_{k=0}^{|B|-|A|} (-1)^k \binom{|B|-|A|}{k} \right.$$

$k = |U| - |A|$

$$= \begin{cases} 1 & \text{if } |B| = |A| \\ 0 & \text{otherwise} \end{cases}$$

μ is called the Möbius function for P.

Thm Let P be a partially ordered set.

Let f, g be functions defined on P.

Then $g(t) = \sum_{s \leq t} f(s)$ for all $t \in P$

$$\iff f(t) = \sum_{s \leq t} \mu(s,t)\, g(s) \quad \text{for all } t \in P.$$

Proof. ($\Rightarrow$)

$$\sum_{s \leq t} \mu(s,t)\, g(s) = \sum_{s \leq t} \mu(s,t) \left(\sum_{u \leq s} f(u) \right)$$

$$= \sum_{u \leq s \leq t} \mu(s,t) f(u)$$

$$= \sum_{u \le t} \left(\sum_{u \le s \le t} \mu(s,t) \right) f(u)$$

$\boxed{u=t}$

$$= f(t).$$

$(\Leftarrow)$

$$f(t) = \sum_{s \le t} \mu(s,t)\, g(s)$$

$$\sum_{s \le t} f(s) = \sum_{s \le t} \left(\sum_{u \le s} \mu(u,s)\, g(u) \right)$$

$$= \sum_{u \le s \le t} \mu(u,s)\, g(u)$$

$$= \sum_{u \le t} \left(\sum_{u \le s \le t} \mu(u,s) \right) g(u)$$

$u=t$

$$= g(u). \qquad \square$$

$$\left(\begin{array}{lll} g(x) = \int f(x)\,dx & \Rightarrow & f(x) = g'(x) \\ g(t) = \sum_{s \le t} f(s) & \Rightarrow & f(t) = \sum_{s \le t} \mu(s,t)\, g(s) \end{array} \right)$$

<u>Lemma</u>. Let P, Q be partially ordered sets. Let $f : P \times Q \to \mathbb{F}$, $g : P \times Q \to \mathbb{F}$ such that

$$g(t_1, t_2) = \sum_{s_1 \le t_1} \sum_{s_2 \le t_2} f(s_1, s_2).$$

Then

$$\boxed{\sum_{s_2 \le t_2} \mu(s_2, t_2)\, g(t_1, s_2) = \sum_{s_1 \le t_1} f(s_1, t_2)}$$

Proof

$$\sum_{s_2 \le t_2} \mu(s_2, t_2)\, g(t_1, s_2)$$

$$= \sum_{s_2 \le t_2} \mu(s_2, t_2) \sum_{u_1 \le t_1} \sum_{u_2 \le s_2} f(u_1, u_2)$$

$$= \sum_{u_1 \le t_1} \sum_{u_2 \le t_2} \underbrace{\left(\sum_{u_2 \le s_2 \le t_2} \mu(s_2, t_2) \right)}_{} f(u_1, u_2)$$

$\boxed{u_2 = t_2}$

$$= \sum_{u_1 \le t_1} f(u_1, t_2)$$

$\square$