CO 434

Jan 20th

Note:

Other ways to express Fisher's inequality:

$b \geq v \iff r \geq k \iff v \geq 1 + \frac{k(k-1)}{\lambda}$.

Counting vector spaces over finite fields:

Let V be a d-dimensional vector space over $GF(q)$.

How many m-dimensional linear subspaces?

$$\frac{(q^d-1)(q^d-q)(q^d-q^2)\cdots(q^d-q^{m-1})}{(q^m-1)(q^m-q)(q^m-q^2)\cdots(q^m-q^{m-1})} = \binom{d}{m}_q$$

# of different bases of size m (list of m linearly independent vectors)

# of lists that gives a basis for any particular m-dimensional subspace

$q^d - 1$ ← The first vector cannot be zero! : First vector

↳ any $q^d \in V = GF(q)^d$

$q^d - q$: 2nd vector

↳ multiples of the first vector

etc.

→ The numerator gives us a list of l.i. vectors (out of a basis of size d).

(and similarly for the denominator).

A construction:

Let q be a prime power and $\mathbb{F} = GF(q)$.

Let W be a finite dimensional vector space over $\mathbb{F}$ of dimension d (Ex. $W = \mathbb{F}^d$).

Let $\mathcal{L} = \{$1-dim'l linear subspaces of $W\}$ (i.e. The set of lines)

Let $\mathcal{H} = \{(d-1)$-dim'l —— " —— $\}$ (i.e hyperplanes)

$(\mathcal{L}, \mathcal{H})$ is an incidence structure under the relation $\subseteq$ (i.e. For $l \in \mathcal{L}$, $h \in \mathcal{H}$, either $l \subseteq h$ or $l \not\subseteq h$).

Theorem: $(\mathcal{L}, \mathcal{H})$ is the incidence structure of a symmetric design with parameters

$$v = \frac{q^d - 1}{q-1}, \quad k = \frac{q^{d-1}-1}{q-1}, \quad \lambda = \frac{q^{d-2}-1}{q-1}.$$

Proof:

$v = |\mathcal{L}| =$ # of 1-dim'l linear subspaces of W

$= \frac{q^d - 1}{q^1 - 1}$.

(d-1)-dim'l. vector space

$k =$ # of 1-dim'l linear subspaces of $h \in \mathcal{H}$.

$= \frac{q^{d-1}-1}{q-1}$. (so, same formula, but with $d-1$ vs. d.)

(Note: Does not depend on choice of h).

Proof: (Con't)

Finally, if $l_1, l_2 \in \mathcal{L}$, ~~[illegible]~~ l_1, l_2 distinct. A hyperplane contains both iff it contains $l_1 + l_2$ ← The 2-dim'l vector space containing lin. combs of the lines.

Such hyperplanes are in bijection with $(d-3)$-dim'l subspaces of $W/(l_1+l_2)$ (mod).

~~[illegible]~~

Since $\dim(W/(l_1+l_2)) = d-2$, there are:

$$\lambda = \frac{(q^{d-2}-1)(q^{d-2}-q)\cdots\cdots(q^{d-2}-q^{d-4})}{(q^{d-3}-1)(q^{d-3}-q)\cdots\cdots(q^{d-3}-q^{d-4})}$$

$$= \frac{\cancel{1\cdot q\cdot q^2\cdots q^{d-4}}\,(q^{d-2}-1)\cancel{(q^{d-3}-1)}\cancel{(q^{d-4}-1)}\cdots\cancel{(q^{2}-1)}}{\cancel{1\cdot q\, q^2\cdots q^{d-4}}\,\cancel{(q^{d-3}-1)}\cancel{(q^{d-4}-1)}\cdots\cdots(q-1)}$$

$$= \frac{q^{d-2}-1}{q-1}.$$

such hyperplanes.

(Exercise: Check that this design is symmetric) ☒

<u>Def'n</u>

A symmetric design with $\lambda = 1$ is called a <u>projective plane</u>.

<u>Corollary</u>: If q is a prime power, there exists a projective plane of order q. (i.e. $k = q+1$).

Proof:
~~If~~ $d=3$ in the construction just given, we get:

$$v = \frac{q^3-1}{q-1} = q^2+q+1$$

$$k = \frac{q^2-1}{q-1} = q+1$$

$$\lambda = \frac{q-1}{q-1} = 1.$$

$\square$

Open Problem: Is there a projective plane of order n, n is not a prime power.

Derived and Residual Designs:
Given any symmetric design $(V, \mathcal{B})$, we can construct 2 new ~~designs~~ (non-symmetric) BIBDs:
Let $\alpha \in \mathcal{B}$:

$$\mathrm{Der}(V, \mathcal{B}, \alpha) = (\alpha, \{\beta \cap \alpha \mid \beta \in \mathcal{B}, \beta \neq \alpha\})$$

$$\mathrm{Res}(V, \mathcal{B}, \alpha) = (V \setminus \alpha, \{\beta \setminus \alpha \mid \beta \in \mathcal{B}, \beta \neq \alpha\})$$

Exercise: Check that these are BIBDs and work out the parameters.
Exercise 2: What is the precise relation b/w these constructions? (Hint: Something to do with complements, can go from Der $\rightarrow$ Res)

Jan 28th

Congruence of matrices:

Def'n Let $\mathbb{F}$ be a field (we will usually take $\mathbb{F}=\mathbb{Q}$ here) Let $A, B \in M_{n\times n}(\mathbb{F})$. We say that A is congruent to B over $\mathbb{F}$ if there exists an invertible $P \in M_{n\times n}(\mathbb{F})$ such that:

$$P^T A P = B$$

and we write $A \approx_{\mathbb{F}} B$ or $A \approx B$ (if $\mathbb{F}$ is understood from context)

Note: This is different from similar matrices, where A is similar to B iff $P^{-1}AP = B$.

Unlike similarity, congruence of matrices is very sensitive to the field. (i.e. ~~Similarity~~ If similarity is achieved in a field extension, it can be achieved in the original field)

Example

Over $\mathbb{R}$,

$$\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \approx_{\mathbb{R}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \approx_{\mathbb{R}} \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$$

Take $P = \begin{pmatrix} \sqrt{3} & 0 \\ 0 & \sqrt{3} \end{pmatrix}$ Take $P = \begin{pmatrix} \sqrt{5} & 0 \\ 0 & \sqrt{5} \end{pmatrix}$

But, over $\mathbb{Q}$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \approx_{\mathbb{Q}} \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$, but $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \not\approx_{\mathbb{Q}} \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$

Why?: 5 can be written as the sum of 2 squares, but 3 cannot

Moral: Congruence over $\mathbb{Q}$ is a non-trivial number theory problem.

What does this have to do with designs?

Prop: If a symmetric (v,k,λ)-design exists, then $I_v \equiv_{\mathbb{Q}} nI_v + \lambda \mathbb{J}_v$ $(n=k-\lambda)$.

Proof: The incidence matrix $N \in M_{v\times v}(\mathbb{Q})$ is invertible and $N^T I_v N = N^T N = nI_v + \lambda J_v$ ◻ (3)

So, $5 = 2^2 + 1^2$

Let $P = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$ ← Note that this is almost orthogonal.

Then, ~~...~~

$$P^T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} P = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$$

Now, suppose that we had

$$P^T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} P = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}.$$

Let's write $P = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, then: $(a,b,c,d \in \mathbb{Q})$

$$P^T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} P = \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}.$$

In particular, we need:

$a^2+b^2 = 3$, where $a,b \in \mathbb{Q}$.

But (we claim) this equation has no rational sol'ns.

To continue, we need:

Theorem (Fermat Sum of Squares Theorem)

Let n be a positive integer. Then, $x^2+y^2=n$ has an integer solution with $x,y \in \mathbb{Z}$ if and only if $n = m^2 p_1 p_2 \dots p_\ell$, where $m \in \mathbb{Z}$, and $p_1, \dots, p_\ell$ are distinct primes where $p_i \not\equiv 3 \pmod 4$ $\forall 1 \le i \le \ell$.

So, write $a = x/m$, $b = y/m$, $x,y,m \in \mathbb{Z}$.

Then, $a^2+b^2=3$ iff $x^2+y^2 = 3m^2$

and $3m^2$ is not of the required form, since $3 \not\equiv 1 \pmod 4$

$\therefore P$ does not exist. (Back, ... see top of page)