Last time:

- rank(AA^t) = rank(A) (Theorem from linear algebra)

"If A is a real $k \times l$ matrix, then A and AA^T have the same column space

$\Rightarrow$ rank(A) = dim Col(A) = dim Col(AA^T) = rank(AA^T)."

(analogous thm for $\mathbb{C}$: rank(AA^*) = rank(A), and thm is false for finite fields).

(Takeaway: For this course, the field we work over will make a difference)

- $(r-\lambda)I_v + \lambda J_v$ invertible:

Proof #1:

First, let's figure out the eigenvalues of J_v:

rank(J_v) = 1. So, the eigenvalues are: $\underbrace{0,\dots,0}_{v-1}, \theta$.

Now, $tr(J_v)$ = sum of eigenvalues = $v = \theta$

Then, for the matrix we care about, the eigenvalues are:

$f(J_v)$, where $f(x) = \lambda x + (r-\lambda)$

This has eigenvalues

$f(0), \dots, f(0), f(v)$

None of which are $0 \Rightarrow$ Invertible

Proof ~~#2~~:

Thm If A is an invertible matrix. Then, there is a poly $p(x)$ s.t. $A^{-1} = p(A)$.

What do the powers of $(r-\lambda)I_v + \lambda J_v$ look like?:

Answer: They are all of the form: $sI + tJ$

$\therefore$ If $(r-\lambda)I + \lambda J$ is invertible, then its inverse must be of same form:

$$((r-\lambda)I_v + \lambda J_v)^{-1} = sI + tJ.$$

So:

Try to solve:

$$(sI + tJ)((r-\lambda)I_v + \lambda J_v) = I.$$

$\square$

Fisher's Inequality: $b \geq v$.

Proof:

$b = \#$ of cols N

$\geq \text{rank}(N) = v$. :)

$\square$.

— (End of first "section": Intro to design!) —

Jan 15th

Next: We'll look at the extreme situation where Fisher's inequality is an equality.

Symmetric Designs:

Def'n: A BIBD is symmetric if $v=b$.

Example.
(i) The Fano plane is symmetric.
(ii) Any design from a difference set construction is symmetric

Basic Facts:
- $v=b$ iff $r=k$.
- The incidence matrix of a symmetric design is invertible. (Since rows are l.i., and the matrix is square)
- All symmetric designs are simple (Since, if not, then the incidence matrix has 2 identical columns corresponding to the identical blocks. But, the matrix is invertible so this cannot happen).
- $\frac{v(v-1)}{k(k-1)} = \frac{b}{\lambda}$ and $v=b$
  $\Rightarrow v = 1 + \frac{k(k-1)}{\lambda}$.   * Does taking the complement give you the other value of k?

In particular $k(k-1) \equiv 0 \pmod{\lambda}$.

Lemma: The incidence matrix of a symmetric design is normal. (i.e. $NN^T = N^T N$)

Proof:

We have $NJ = N\mathbb{1}\mathbb{1}^T = (r\mathbb{1})\mathbb{1}^T = kJ$, and

$JN = \mathbb{1}\mathbb{1}^T N = \mathbb{1}(k\mathbb{1}^T) = kJ$.

So, $NJ = JN$.

Then,

$$\begin{aligned} NNN^T &= N((r-\lambda)I + \lambda J) \quad (N \text{ commutes w/ } J \text{ and } I) \\ &= ((r-\lambda)I + \lambda J)N \\ &= NN^T N \end{aligned}$$

And since N invertible $N^{-1}NNN^T = N^{-1}NN^T N \Rightarrow NN^T = N^T N$ □.

Def'n (Order)

The order of a symmetric design is $n = k - \lambda = r - \lambda$.

Thus: $NN^T = N^T N = nI + \lambda J$.

Theorem: Let $(V, \mathcal{B})$ be a symmetric design with params (v, k, λ). For any 2 blocks, $\alpha, \beta \in \mathcal{B}$, $\alpha \neq \beta$, we have $|\alpha \cap \beta| = \lambda$.

Proof:

Since $N^tN = nI + \lambda J$.

$$\lambda = (N^tN)_{ij} = \sum_{l=1}^{v} N^t_{il} N_{lj}$$

$$= \sum_{l=1}^{v} N_{li} N_{lj}$$

$$= |\alpha_i \cap \alpha_j|$$

Def'n (Dual Design)

Let (V, B) be a design. The dual design is $(B, \tilde{V})$ where:

$$\tilde{V} = \{\{\alpha \in B \mid v \in \alpha\} \mid v \in V\}.$$

If N is the incidence matrix of (V, B), then N^T ——— " ——— $(B, \tilde{V})$.

Notes:

- If (V, B) is a symmetric design, then the dual is also a symmetric design with the same parameters.
(In general, the dual of a BIBD is not a BIBD)
- "Symmetric" refers to this very superficial parameter symmetry.

It is NOT necessarily true that a symmetric design and its dual are isomorphic.

Finite Fields Primer:

- Existence: $\exists$ a finite field $GF(q)$ with q elements (order q) iff $q = p^d$ (p prime).
  (p is called the "characteristic")
- Uniqueness: Any 2 fields with the same # of elements are isomorphic.
- Construction: $GF(q) = \mathbb{Z}_p[x]/\langle f(x) \rangle$, where $f(x) \in \mathbb{Z}_p[x]$ is irreducible of degree d.

Example:

To construct $GF(4)$, we need $f(x) \in \mathbb{Z}_2[x]$ irreducible of degree 2:

$$\underbrace{x^2, \quad \underset{(x+1)^2}{\underset{\shortparallel}{x^2+1}}, \quad \underset{x(x+1)}{\underset{\shortparallel}{x^2+x}}}_{\text{So, All these factor}}, \quad \underset{\text{We can only use this one}}{\underset{\downarrow}{x^2+x+1}}$$

So: $GF(4) = \mathbb{Z}_2[x]/\langle x^2+x+1 \rangle$

Elements of $GF(4)$: $0, 1, x, x+1$.

Mult table:

	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

- Additive Group Structure:

$$(GF(q), +) \cong (\mathbb{Z}_p^d, +)$$

In particular: for $a \in GF(q)$

$$pa = \underbrace{a + \dots + a}_{p \text{ times}} = 0$$

- Subfields:

$GF(q_1)$ is a subfield of $GF(q_2)$ iff $q_2 = q_1^{l}$.
In which case, $GF(q_2)$ is an l-dimensional vector space over $GF(q_1)$.

- Linear Algebra:
  - Most of linear algebra works the same way regardless of the field.

Next time: Counting vector spaces.

- If $V = GF(q)^d$, how many linear subspaces of V (of dim k).