Combinatorics

29 oct 21

Lecture 9 — Symmetric Designs - 2

Symmetric design = 2-design with $b = v$.

→ Proj. plane = symm. design + $\lambda = 1$.

$2\text{-}(n^2+n+1, n+1, 1)$ design for some n. Order of proj. plane = n

Thm: If N is the incidence matrix of a symmetric design. Then so is N^T. In fact the parameters of this dual design are same.

pf:- Let $\mathcal{D}$ be the design whose incidence mx is N. Let $\mathcal{D}$ be $2\text{-}(v,k,\lambda)$ design.

Since $bk = vr$

We know that $k = r$ for $\mathcal{D}$.

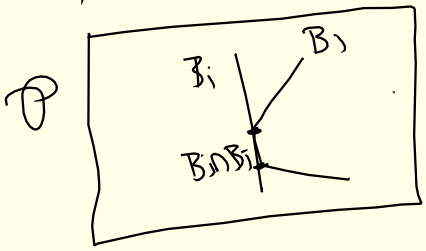
$\Rightarrow$ Every col^n of N^T has k non-zero entries.

$$N = \begin{matrix} \\ x \end{matrix}\overset{\overset{B}{\downarrow}}{\begin{bmatrix} \vdots \\ n_{ij} \\ \vdots \end{bmatrix}}, \quad N^T = \begin{bmatrix} \cdots & \cdots & \cdots \\ \vdots & m_{ij} = n_{ji} & \vdots \\ \cdots & \cdots & \cdots \end{bmatrix}$$

$\Rightarrow$ each "block" of incidence structure associated with N^T has size k.

$\therefore$ we only have to prove that any two points in the incidence structure asso with N^T must occur in λ blocks.

ie B_i, B_j are two blocks of $\mathcal{D}$, we will have to show that $|B_i \cap B_j| = \lambda$.



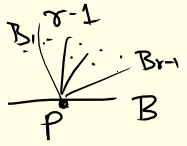
Fix a block B of $\mathcal{D}$ $\quad |B| = k$.

$\forall\ 0 \le i \le k$, let a_i denote the no. of blocks $\neq B$ of $\mathcal{D}$ having i points in common with B.

We need to show that $a_i = 0 \ \forall i \neq \lambda$.

$$\sum_{i=0}^{k} a_i = b - 1 \qquad (1)$$

Count pairs (p, B') with $p \in B \cap B'$.

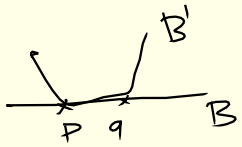


Fixing p-first we get $k(r-1) = k(k-1)$

Fixing B'-first we get $\sum_{i=0}^{k} i a_i$

$$\sum_{i=0}^{k} i a_i = k(k-1) \qquad (2)$$

Count tripleds $(\{p,q\}, B')$ s.t. $B' \neq B$ & $\{p,q\} \subseteq B \cap B'$.



Fixing $\{p,q\}$ first, we get $\binom{k}{2}(\lambda - 1)$

Fixing B' first, we get $\sum_{i=0}^{k} \binom{i}{2} a_i$.

$$\therefore \quad \sum_{i=0}^{k} \frac{i(i-1)}{2} \cdot a_i = \frac{k(k-1)}{2} \cdot (\lambda - 1) \qquad (3)$$

$$\sum_{i=0}^{k} (i-\lambda)^2 \cdot a_i \overset{?}{=} 0.$$

$$LHS = \sum_{i=0}^{k} (i^2 - 2\lambda i + \lambda^2) a_i = \sum i^2 a_i - 2\lambda \sum i a_i + \lambda^2 \sum a_i$$

$$= \sum (i^2 - i) a_i + \sum i a_i - 2\lambda \sum i a_i + \lambda^2 \sum a_i$$

$$= \not{2}\left(\frac{k(k-1)}{\not{2}}\right)(\lambda - 1) + k(k-1) - 2\lambda k(k-1) + \lambda^2 (v-1)$$

Note $\lambda(v-1) = r(k-1)$ any 2-design

symm $\Rightarrow r = k$. $\therefore \lambda(v-1) = k(k-1)$

$$LHS = \lambda k(k-1) - 2\lambda k(k-1) + \lambda k(k-1) = 0.$$

$$\therefore \sum (i-\lambda)^2 a_i = 0. \Rightarrow a_i = 0 \ \forall i \neq \lambda.$$

$\Rightarrow$ Any block intersects B in precisely λ points. But B was arbitrary. $\Rightarrow$ any two blocks

of B intersect in λ pts.

$\Rightarrow$ any two pts of structure asso. with N^T are in exactly λ-blocks.

QED.

Ryser's theorem :- Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ be an incidence structure. Assume $|\mathcal{P}| = |\mathcal{B}|$ and $|B| = k$ $\forall B \in \mathcal{B}$. If any two blocks have exactly λ points in common, then $\mathcal{D}$ is a (symmetric) 2-design.

pf. By previous theorem, it is enough to prove that the inci. structure given by the N^T is a 2-design where N is the incidence mx. of $\mathcal{D}$.

(1) $N^T N = (k-\lambda) I + \lambda J$ (any blocks have λ pts in common & block size is k)

$$\begin{bmatrix} k & \lambda \\ \lambda & k \end{bmatrix}$$

(2) $JN = kJ$ ($\because$ block size is k)

$$\begin{bmatrix} 1 & \cdots & 1 \\ 1 & \cdots & 1 \\ 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} n_{ij} \end{bmatrix} = \begin{bmatrix} k & \cdots & k \\ k & \cdots & k \end{bmatrix}$$

All we need to prove that the structure asso. with N^T has same block size.

ie we need to prove that $NJ = \ell J$ for some ℓ.

Using (1) we see that zero is not an eigen value of $N^T N$ (check the proof of Fisher's inequality)

$\Rightarrow \det N^T N = v^2 \neq 0 \Rightarrow N$ is invertible.

$JN = kJ \Rightarrow \underline{J = kJN^{-1}}$

$\therefore J(N^T N) = J((k-\lambda) I + \lambda J)$

$= (k-\lambda) J + \lambda J^2$

$= (k-\lambda + \lambda v) J$

$$\begin{bmatrix} 1 & \cdots & 1 \\ 1 & \cdots & 1 \end{bmatrix}^2_{v \times v} = \begin{bmatrix} v & \cdots & v \\ v & \cdots & v \end{bmatrix} = vJ$$

$$\therefore \quad JN^T = (k+\lambda(v-1))JN^{-1}$$
$$= \underbrace{(k+\lambda(v-1)\cdot k^{-1}}_{\ell}\cdot(kJN^{-1})$$
$$= J.$$

$$\Rightarrow \quad JN^T = \underbrace{((k+\lambda(v-1))k^{-1})}_{\ell} J.$$

$$\{n_{ij}\}\begin{bmatrix}1 & \cdots & 1\\ 1 & \cdots & 1\\ 1 & \cdots & 1\end{bmatrix} \Rightarrow NJ = \ell J.$$

QED.

Remark: Having proved that the structure given by above theorem is a 2-design we get that

$$(k+\lambda(v-1))k^{-1} = k.$$

But $\lambda(v-1) = r(k-1)$ & $r = k \Rightarrow k+\lambda(v-1)$
$= k + k(k-1) = k^2.$

$\therefore (k+\lambda(v-1))k^{-1} = k.$

(1950)

(Bruck-Ryser-Chowla) Theorem.

If v, k, λ are integers such that $\lambda(v-1) = k(k-1)$, then for the existence of a symmetric $2-(v,k,\lambda)$ design, we must have:

(1) If v is even then $k-\lambda$ is a perfect square.

(2) If v is odd, then the equation

$$z^2 = (k-\lambda)x^2 + (-1)^{\frac{v-1}{2}}\lambda y^2$$ has a non-zero integral solution.

Ingredients: (1) Euler's four square formula.

→ product of two integers which are sum of four squares is also a sum of four squares.

In fact: $(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2) = y_1^2+y_2^2+y_3^2+y_4^2$

with
$$y_1 = a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4$$
$$y_2 = a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3$$
$$y_3 = a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2$$
$$y_4 = a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1$$

Note that:
$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & -a_4 & a_3 \\ a_3 & a_4 & a_1 & -a_2 \\ a_4 & -a_3 & a_2 & a_1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}$$
$$= A.$$

$AA^T = (\Sigma a_i^2)\cdot Id. \Rightarrow A$ is invertible

& hence b_i's are linear combinations of y_j's,

since $\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} = A^{-1}\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix}$.

Lagrange – Every prime is a sum of 4 squares.
$\Rightarrow$ every natural no is a sum of 4-squares

(2) Third isomorphism theorem of ring theory!

Proof of the BRC theorem.

(1) Note that if v is even, then the result follows by the proof of Fisher's inequality (i.e. compute $\det(NN^T)$)

(2) Assume v is odd. Assume that $\exists$ a symmetric $2\text{-}(v,k,\lambda)$ design with $\lambda(v-1) = k(k-1)$.

since $v > k$, we must have $\lambda < k$.

$\longrightarrow$ Let $n = (k-\lambda) > 0$ & hence is a sum of 4-squares.

$\longrightarrow$ All our calculations are in $\mathbb{Z}[x_1, x_2, \ldots, x_v]$.

Look at N = incidence mx of $\mathcal{D}$. N is a $v \times b$ mx.

Let $N \begin{bmatrix} x_1 \\ \vdots \\ x_v \end{bmatrix} = \begin{bmatrix} L_1 \\ L_i \\ L_v \end{bmatrix}$ where L_i's are linear poly. in x_j's

$L_i = n_{i1}x_1 + n_{i2}x_2 + \cdots n_{iv}x_v$

$$[x_1 \cdots x_v] N^T N \begin{bmatrix} x_1 \\ \vdots \\ x_v \end{bmatrix} = ?$$

$N \begin{bmatrix} x_1 \\ \vdots \\ x_v \end{bmatrix} = \begin{bmatrix} L_1 \\ \vdots \\ L_v \end{bmatrix}$ $\Rightarrow$ LHS $= \sum_{i=1}^{v} L_i^2$

On the other hand $N^T N = (k-\lambda)I + \lambda J$

$$\therefore \quad LHS = [x_1 \cdots x_v]\left((k-\lambda)I + \lambda J\right)\begin{bmatrix} x_1 \\ \vdots \\ x_v \end{bmatrix}$$

$$= \underbrace{(k-\lambda)}_{n}\sum_{i=1}^{v} x_i^2 + \lambda\left(\sum x_i\right)^2$$

since

$[x_1 \cdots x_v]\, \lambda J \begin{bmatrix} x_1 \\ \vdots \\ x_v \end{bmatrix} = X \cdot \lambda \begin{bmatrix} \sum x_i \\ \sum x_i \\ \sum x_i \end{bmatrix} = \lambda\left(\sum x_i\right)^2.$ Note that $n = k - \lambda$.

$$(*) \quad L_1^2 + L_2^2 + \cdots + L_v^2 = n(x_1^2 + \cdots x_v^2) + \lambda w^2$$

inside $\mathbb{Z}[x_1, \cdots x_v]$.

where $w = \sum_{i=1}^{v} x_i$

($\mathbb{Z}[x_1, \cdots x_v] \xrightarrow{\theta} R$ $\quad\theta$ ring homo. this eq^n is preserved.)

{ Principle of permance of identity

$$R \xrightarrow{\theta} S$$

$E_1 \longrightarrow \theta(E_1)$ will also be true. }

$\det(AB) = \det A \cdot \det B$.

case 1 $v \equiv 1 \pmod 4$

Write n as sum of four squares & choosing $x_i, x_{i+1}, x_{i+2}, x_{i+3}$ at a time we write

$$n(x_i^2 + x_{i+1}^2 + x_{i+2}^2 + x_{i+3}^2) = y_i^2 + y_{i+1}^2 + y_{i+2}^2 + y_{i+3}^2$$

$\in \mathbb{Z}[x_i, x_{i+1}, x_{i+2}, x_{i+3}]$ $\quad$ $\in \mathbb{Z}[x_i, x_{i+1}, x_{i+2}, x_{i+3}]$

$= \mathbb{Z}[y_i, y_{i+1}, y_{i+2}, y_{i+3}]$

$\therefore$ (*) can be rewritten as

$$L_1^2 + L_2^2 + \cdots + L_v^2 = y_1^2 + y_2^2 + \cdots + y_{v-1}^2 + n x_v^2 + \lambda W^2$$

$$\mathbb{Z}[X_1 \cdots X_v] \xrightarrow{\pi} \frac{\mathbb{Z}[X_1 \cdots X_v]}{\langle L_1 - y_1 \rangle}$$

$\cong$

$\mathbb{Z}[y_1 \cdots y_{v-1}, x_v]$ $\nearrow$

Note that $x_1 \cdots x_{v-1}$ can be written as a linear comb. of $y_1 \cdots y_{v-1}$.

$\therefore W$ also is a linear comb. of $y_1 \cdots y_{v-1}, x_v$.

so are L_i's

L_1 is a linear comb of $y_1, \cdots, y_{v-1}, x_v$.

case a coeff y_1 is L_1 is not equal to 1. $\Rightarrow L_1 - y_1$ has non-zero coeff of y_1

$\therefore$ in $\dfrac{\mathbb{Z}[y_1 \cdots y_{v-1}, x_v]}{(L_1 - y_1)} = S$ $\quad L_1 - y_1 = d y_1 + \sum_{i=2}^{v-1} a_i y_i + e_v x_v$

$\Rightarrow y_1$ can be expressed in S. as a rational linear expression in $y_2, \cdots y_{v-1}, x_v$.

$\therefore$ In $\mathbb{Q}[y_1 \cdots y_{v-1}, x_v]$ (*) becomes :

$$L_2^2 + \cdots L_v^2 = y_2^2 + y_3^2 + \cdots + y_{v-1}^2 + n x_v^2 + \lambda W^2$$

where each L_i's & W are lin. expressions of $y_2, \cdots y_{v-1}, x_v$.

$\therefore$ This equation is true in $\mathbb{Q}[y_2, \cdots y_{v-1}, x_v]$.

→ Same thing works by looking at $\frac{\mathbb{Z}[y_1 \cdots y_{v-1}, x_v]}{\langle L_1 + y_1 \rangle}$ if coeff of y_1 in L_1 is 1. ←

we get eqn $L_2^2 + \cdots L_{v-1}^2 + L_v^2 = y_2^2 + \cdots y_{v-1}^2 + n x_v^2 + \lambda w^2$

in $\mathbb{Q}[y_2, \cdots y_{v-1}, x_v]$.

Repeat for $L_2, L_3, \ldots, L_{v-1}$!!!

finally we get ⊛ becomes in $\mathbb{Q}[x_v]$

$L_v^2 = n x_v^2 + \lambda w^2$. Removing the denominations, we get $z^2 = n x^2 + \lambda y^2$ in $\mathbb{Z}[x]$.

Choosing appropriate: $\mathbb{Z}[x] \to \mathbb{Z}$. $x \to \alpha$. we get a non-zero soln. of the required Diophantine eqn!!

Case 2 $v \equiv 3 \pmod 4$

Add a variable $n x_{v+1}^2$ to ⊛ to get

$L_1^2 + \cdots + L_v^2 + n x_{v+1}^2 = n \sum_{i=1}^{v+1} x_i^2 + \lambda \left(\sum_{i=1}^{v} x_i \right)^2$

w

we get $n x_{v+1}^2 = y_{v+1}^2 + \lambda w^2$

where y_{v+1} & w are rational multiples of x_{v+1}

$\therefore$ $n x_{v+1}^2 - \lambda w^2 = y_{v+1}^2$ This completes the proof.

$(-1)^{\frac{v-1}{2}}$

QED.