Combinatorics 10 NOV 21

Lecture 11

Orthogonal Latin squares

R, C, S are three sets of cardinality n.

A latin square is a function $L : R \times C \to S$

s.t. $\forall r \in R$; $L|_{\{r\} \times C} \to S$ is iso.

$\forall c \in C$; $L|_{R \times \{c\}} \to S$ is iso.

(every symbol occurs in each row & in each column)

Orthogonal latin squares are two latin squares L_1 & L_2

$L_1 : R \times C \to S_1$
$L_2 : R \times C \to S_2$
such that $\forall s \in S_1, t \in S_2$ $\exists$ a $(r, c) \in R \times C$

$$(L_1(r,c), L_2(r,c)) = (s,t).$$

$$\underset{L_1}{\begin{bmatrix} & & \\ & \underset{(r,s)}{\overset{s}{*}} & \\ & & \end{bmatrix}_{n\times n}}, \quad \underset{L_2}{\begin{bmatrix} & & \\ & \underset{(r,s)}{\overset{t}{*}} & \\ & & \end{bmatrix}_{n \times n}} \qquad |S_1 \times S_2| = n^2$$

—x—x—x—

- Mutually orthogonal latin squares (MOLS) are latin squares $L_1, L_2, \dots, L_t$ of order n s.t. (L_i, L_j) are orthogonal $\forall i \neq j$.

- $\boxed{N(n) = \text{maximum number of MOLS of order } n.}$

Thm: If n is odd then $N(n) \geq 2$.

Pf: Let $G = \mathbb{Z}/n\mathbb{Z}$.

Let $R, C, S_1 \& S_2$ be all G.

$L_1(x,y) = x+y$ — multiplication table.

$L_2(x,y) = y-x$.

$$\begin{array}{c|cccc} & e & x_1 & \cdots & x_n \\ \hline e & e & x_1 & \cdots & x_n \\ x_1 & x_1 & 2x_1 & x_1+x_2 & \cdots \\ x_2 & & & & \\ x_n & x_n & & & \end{array}$$

For each x, $x+y = x+y \Leftrightarrow y = z$.

$\Rightarrow L_1$ is a latin square. | cancellation law of G.

$\|$ly L_2 is also latin square

Let $(g_1, g_2) \in G \times G$. To find $x \in G, y \in G$ s.t.

$L_1(x,y) = g_1$

$\& \; L_2(x,y) = g_2$.

ie $x+y = g_1$, $y-x = g_2$ we need a unique sol^n in x & y given g_1 & g_2.

$\Rightarrow 2y = g_1 + g_2 \Rightarrow \boxed{y = \frac{g_1+g_2}{2}}$

$\Rightarrow \boxed{x = \frac{g_1-g_2}{2}}$

QED.

Theorem:- If $q = p^r$ is a prime power, then $N(q) \geq q-1$.

Pf. Let $GF(q)$ be the field of order q.

$R, C, S_i \quad 1 \leq i \leq q-1$ equal to $GF(q)$.

$\forall a \in GF(q)^* = GF(q) \setminus \{0\}$ define

L_a by $\underline{L_a(x,y) = ax+y}$ (previous example $L_1 = L_1, L_2 = L_{-1}$)

$\forall y \in C$, $ax_0 + y = ax_1 + y \Leftrightarrow x_0 = x_1$ - since a is a unit

$\forall x \in R$, $ax + y_1 = ax + y_2 \Leftrightarrow y_1 = y_2$ - cancellation law.

$\Rightarrow L_a$ is a latin square $\forall a \in GF(q)^*$.

Given $s, t \in GF(q)$ & $a \neq b$ in $GF(q)^*$) we need to find $x, y \in GF(q)$ s.t. $L_a(x,y) = s$
$L_b(x,y) = t$.

$$\begin{aligned} ax + y &= s \\ bx + y &= t \end{aligned} \Rightarrow x = \frac{s-t}{(a-b)}. \qquad \text{unique sol}^n!$$

$$\& \ y = \frac{at - bs}{(a-b)}$$

$\Rightarrow N(q) \geq q-1.$ QED.

Thm: $N(n) \leq n-1$ for any n.

Pf. Note that if $L : R \times C \to S$ & $M : R \times S \to T$ are two latin squares, then L & $\sigma(M)$ are also orthogonal where $\sigma : T \to T$ is a permutation.

$$M = \begin{array}{c} \begin{array}{ccc} 1\,2 & 3 & \end{array} \\ \begin{bmatrix} m_{11} & \cdots & m_{1n} \\ & & \\ m_{n1} & & m_{nn} \end{bmatrix} \end{array} \qquad m_{ij} \in T.$$

$\{1, \cdots n-1, n\}$
$\downarrow \sigma$
$\{2, 3, \cdots, n, 1\}$

$$\sigma(M) = \begin{bmatrix} \sigma(m_{11}) & \cdots & \sigma(m_{1n}) \\ \sigma(m_{21}) & \cdots & \sigma(m_{2n}) \\ \sigma(m_{n1}) & \cdots & \sigma(m_{nn}) \end{bmatrix} \quad \text{is a latin square.}$$

$\forall (s,t) \in S \times T$. look at $(s, \sigma^{-1}(t)) \in S \times T$.
$\exists (x,y) \in R \times C$ s.t.
$\Rightarrow L(x,y) = s, \ M(x,y) = \sigma^{-1}(t)$

$\Rightarrow L(x,y) = s$ & $\sigma(M)((x,y)) = t$.

$\therefore$ L & $\sigma(M)$ are also ortho.

Let $L_1, L_2, \ldots L_k$ be k MOLS of order n. WLOG assume that all symbols are $\{1, \ldots, n\}$
Now For each L_i, permute the symbols so that the first row of each L_i is $[1\ 2 \cdots n]$

$$L_1 = \begin{bmatrix} 1 & 2 & \cdots & n \\ * & * & & \\ \vdots & & & \\ \end{bmatrix}, \quad L_2 = \begin{bmatrix} 1 & 2 & \cdots & n \\ * & & & \\ & * & & \\ \end{bmatrix}, \cdots L_k = \begin{bmatrix} 1 & \cdots & n \\ * & * & \end{bmatrix}.$$

{ Remark: This operation is NOT permuting columns, because

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \text{ - MOLS.}$$

$$\Downarrow$$

$$\begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \text{ NOT MOLS.} \}$$

Since L_i's are mutually orthogonal & since (a,a) occurs in $L_i(1,a), L_j(1,a)$ $\forall i \neq j$

we see that $L_i(2,1) \neq L_j(2,1)$ $\forall i \neq j$.

Also 1 occurs in $(1,1)^{th}$ place $\forall L_i$.

$\therefore$ $L_i(2,1) \neq 1$ $\forall i$.

$\Rightarrow$ $L_1(2,1) \in \{2, \ldots n-1\}$, $L_2(2,1) \in \{2, \ldots n-1\} \setminus L_1(2,1)$

$\therefore$ $\exists$ at most $n-1$ choices for the $(2,1)^{st}$ entry for L_i $1 \leq i \leq k$, & no entry is repeated.

$\Rightarrow$ pigeon hole principle $\Rightarrow$ $k \leq n-1$.

QED.

Cor $N(q) = q-1$, if $q = p^r$ is a prime power.

—x—x—

Thm: ① $N(nm) \geq \min\{N(n), N(m)\}$

② $N(n) \geq \min_{1 \leq i \leq t} (p_i^{e_i} - 1)$ if $n = \prod_{i=1}^{t} p_i^{e_i}$

Remark :- ② follows from ① & previous thm & ind. on t

Pf. ① If A & B are latin squares of order n & m respectively, construct $A \otimes B$

a latin square of order nm by

rows of $A\otimes B$ are idexed by $R_A \times R_B$

col'ns ———— " ———— $C_A \times C_B$

symbols ———— " ———— $S_A \times S_B$

Define $\quad A\otimes B\,((i,k),(l,m)) = (\underbrace{A(i,l)}_{R_A\times C_A},\ \underbrace{B(k,m)}_{R_B\times C_B})$

$\uparrow$

$S_A \times S_B$

Check that it is a latin square.

Fixing $(i,k)\in R_A\times R_B$ & $(s,t)\in S_A\times S_B$ we need $(l,m)\in C_A\times C_B$ s.t. $A(i,l)=s$, $B(k,m)=t$.

such l & m obviously exist because A & B are latin squares themselves! Illy columns have all entries of $S_A\times S_B$.

<u>Exercise</u> :- If $\{A_i\}_{1\le i\le k}$ & $\{B_j\}_{1\le j\le l}$ are MOLS of order n & m respectively, then $\{A_s\otimes B_s\}_{1\le s\le \min\{k,l\}}$ are MOLS of order nm.

This "proves" ① ~~of~~ the theorem.

<u>Cor</u>: $\quad N(n)\ge 2\ \forall$ odd n & all multiples of 4.

<u>pf</u> $\quad$ use part ②!

<u>Q</u>. what happens for $n\equiv 2 \pmod 4$?

<u>Euler's Conjecture</u>: $\quad N(n)=1\ \forall\ n\equiv 2 \pmod 4$.

$\rightarrow\ n=2,\ \colon= \begin{bmatrix}1&2\\2&1\end{bmatrix}$ & $\begin{bmatrix}2&1\\1&2\end{bmatrix}$. only latin squares. not MOLS!

$\rightarrow n = 6 \qquad N(6) = 1$. ✓

<u>Bose-Shrikhande-Parker</u> :- $N(n) = 1$ only for $n = 2, 6$. !!!

i.e. $N(n) \geq 2$ $\forall n$ except 2 & 6.