Combinatorics

12 NOV 21

Lecture 12   Euler's conjecture's disproof.

(Anupam Nayak)

1. ☺ $a^2 = 6x^2 - b^2$ has no non-zero integral sol^n

First assume that we have a non-zero sol^n with no common factor. Go mod 3. -1 is not a square mod 3.

- If $a \equiv 0 \pmod 3$ $\Rightarrow b \equiv 0 \pmod 3$
  $\Rightarrow a^2 \,\&\, b^2$ are divisible by 9.
  $\Rightarrow 6x^2$ is divisible by 9
  $\Rightarrow x$ is divisible by 3.
  contradicts that a, b, x has no common factor.
- if $a^2 \equiv 1 \pmod 3$, $\Rightarrow$ contradiction by going mod 3. as
  $LHS \equiv 1 \pmod 3$
  & $RHS \equiv -b^2 \pmod 3$
  $\equiv 0, -1 \pmod 3$.

- L, M Latin squares, on symbols S & T respectively, they are orthogonal iff the set $\{(L_{ij}, M_{ij})\}_{\substack{1 \le i \le n \\ 1 \le j \le n}}$ equals $S \times T$

- If $n \equiv 2 \pmod 4$ no obvious constructions for orthogonal Latin squares existed at the time of Euler.
  $n = 2, 6$ there are no pair of orthogonal Latin squares

Conjecture $\forall\, n \equiv 2 \pmod 4$ $N(n) = 1$.

(Recall $N(n) =$ max. no. of MOLS of order n).
$N(n) \le n-1$.

Today, we will construct pair of orthogonal Latin squares of order $\equiv 2 \pmod 4$.

Def^n :- 1. A Latin square whose rows, columns & symbols are indexed by same set is called a <u>quasigroup</u>.

(multiplication table of a finite gp is Latin square as above.)

$(x^2 = x \Leftrightarrow x$ is idempotent) in a group.

2. A quasigroup L is called <u>idempotent</u> if $L(x,x) = x \quad \forall x$.

Example $GF(q)$ - finite field of order q.

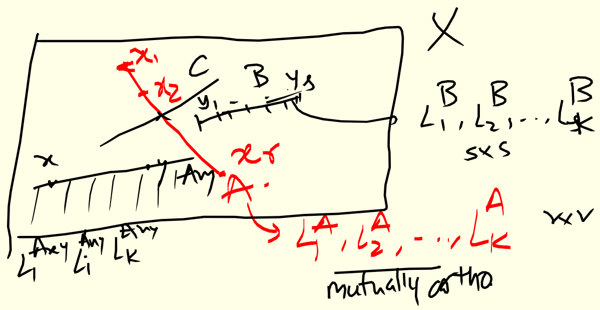
$$L_a(x,y) = ax + (1-a)y \qquad \boxed{a \neq 0,1}$$

Exercise L_a, L_b are orthogonal $\forall a \neq b$.

Note that $N(q) = q-1$ but here we have $q-2$ mutually orthogonal idempotent quasigroups.

Basic Construction

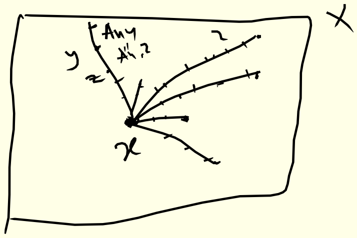
Recall that $(X, \mathcal{A})$ is called a linear space if every block has at least two pts & if any two points lie in a unique block. Let $(X, \mathcal{A})$ be a linear space. Assume that for each $A \in \mathcal{A}$, we have k idempotent quasigroups on A, that are mutually orthogonal. (i.e $|A|$ size latin square whose rows, col^{n}s, symbols are elements of A & $L(x,x) = x \ \forall x \in A$) denoted by $L_1^A, L_2^A, \dots, L_k^A$.



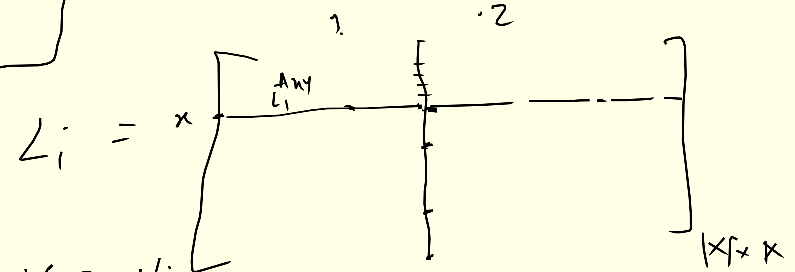
Given this, we now construct k - idempotent quasigroups that are mutually orthogonal on set X. $L_1, \dots, L_k$ of size $|X|$

Define: L_i by $L_i(x,x) = x \ \forall x \in X$

$L_i(x,y) = L_i^{A_{xy}}(x,y)$ if $x \neq y$ & A is the unique line joining x & y.



x^{th} row of L_i consists of x^{th} row of $L_i^{A_x}$ for various lines A_x passing through x.



$L_i^{A_{xz}}(x,x) = x \ \forall z . \forall i$

Clearly L_i $1 \le i \le k$ are idempotent $n \times n$ arrays $n = |X|$

Fixing x look at the x^{th} row of L_i.

let $y \in X$. to show that y occurs as $L_i(x,z)$ for some z.

$\overset{A}{x}$

let A be the line joining x & y & look at $L_i^A(x,-)$.

$\exists z$ s.t. $y = L_i^A(x,z)$ since L_i^A is a latin square on A.

$\therefore L_i(x,z) = L_i^A(x,z) = y$.

||ly for columns.

Further, L_i, L_j are orthogonal too.

ie given $s,t \in X$, we need to find $x,y \in X$ s.t. $(L_i(x,y), L_j(x,y)) = (s,t)$

(1) if $s=t$ then take $x=y=s$.

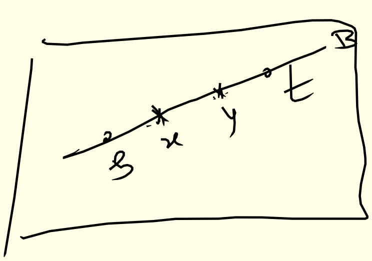
$(L_i(s,s), L_j(s,s)) = (s,s)$!

(2) $s \ne t$. $\exists!$ line joining s & t say B.

L_i^B & L_j^B are orthogonal on B.

$\Rightarrow \exists x,y \in B$ s.t. $(L_i^B(x,y), L_j^B(x,y)) = (s,t)$.

$x \ne y$ as $s \ne t$.



$\therefore$ B is the unique line joining x & y.

$\Rightarrow L_i(x,y) = L_i^B(x,y) = s$

& $L_j(x,y) = L_j^B(x,y) = t$ QED.

$\Rightarrow \exists$ k idempotent quasigroups of order $|X|$.

Theorem :- Given $k+1$ mutually ortho. quasigroups on a set S, there exists k idempotent quasigroups on S that are mutually ortho.

proof. Let $H_1, \dots, H_{k+1}$ be mutually orthogonal quasigroups on S.

Pick any $s \in S$. Then in each row of H_{k+1} s occurs exactly once.

$$H_{k+1} = \begin{bmatrix} s & & & \\ & s & & s \\ & & s & \\ s & & & \end{bmatrix}_{|S|\times|S|}$$

Claim: $\sigma \in Sym(|S|)$ such that applying that σ on the columns of H_{k+1} we get a new Latin square $\tilde{H}_{k+1}$ s.t. $\tilde{H}_{k+1}(x,x) = s \;\forall x$.

$$\tilde{H}_{k+1} = \begin{bmatrix} s & & * \\ & \ddots & \\ * & & s \end{bmatrix}$$

~~proof~~ — Exercise.

Apply same σ to all $H_1, \dots, H_k$ to get $\tilde{H}_1, \tilde{H}_2, \dots, \tilde{H}_k, \tilde{H}_{k+1}$ that are still mutually orthogonal. since s occurs on diagonal of $\tilde{H}_{k+1}$ & since H_i & $\tilde{H}_{k+1}$ are orthogonal $\forall\, 1 \le i \le k$ we must have $\{H_i(x,x) \mid x \in S\} = S$. since given any $y \in S$ the pair (y, s) must occur as $(\tilde{H}_i(x,y), \tilde{H}_{k+1}(x,y))$.

$$\tilde{H}_{k+1} \begin{bmatrix} s & & \\ & \ddots & \\ & & s \end{bmatrix} \qquad \tilde{H}_i = \begin{bmatrix} \overset{x,s}{h_{11}} & & * \\ & \ddots & \\ * & & h_{nn} \end{bmatrix}$$

permute the entries of S for each $\tilde{H}_i$'s so that $\hat{H}_i(x,x) = x$. To get $\hat{H}_i$ $1 \le i \le k$ that are idempotent mutually orthogonal quasigroups.

QED.

Thm: For any linear space $(X, \mathcal{A})$ with $|X| = n$, we have $N(n) \geq \min_{A \in \mathcal{A}} (N(|A|) - 1)$.

proof. Using above theorem, we get k idempotent mutually orthogonal quasigroups on A $\forall A \in \mathcal{A}$, where $k = \min_{A \in \mathcal{A}} (N(|A|) - 1)$

Using construction given before the theorem, we get k idempotent mutually ortho-quasigroups of size n.

QED.

Application :- • Proj-plane of order 4 - $\mathbb{P}^2(4)$

$\exists \ \frac{4^3 - 1}{4 - 1}$ points. $= 21$.

$\frac{4^3-1}{4-1} = 4^2 + 4 + 1$ 21 lines.

Each line has $\frac{4^2 - 1}{4 - 1} = 5$ points.

$\Rightarrow N(5) = 4 \Rightarrow \exists$ 3 idempotent quasigroups of size $|A|$ $\forall A \in \mathcal{B}$.

$\Rightarrow \boxed{N(21) \geq 3}$ note: $21 = 3 \cdot 7$.

Thm: $N(n) \geq \min_{p^e \| n} (p^e - 1)$ p prime

OR $n = \prod_{i=1}^{r} p_i^{e_i}$

then $N(n) \geq \min_{1 \leq i \leq r} p_i^{e_i} - 1$

MacNeish's conjecture (1922) $N(n) = \min_{p^e \| n} (p^e - 1)$.

$\boxed{\text{Disproves this conjecture}}$.

Thm. Let $(X, \mathcal{A})$ be linear space $n = |X|$ & $\mathcal{B} \subset \mathcal{A}$ be a set of pairwise disjoint lines. Then

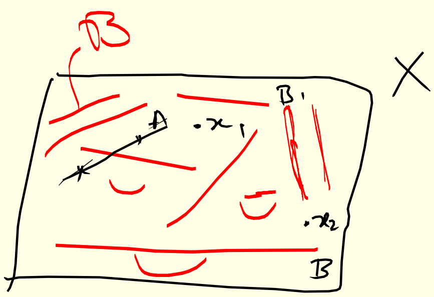
$$N(n) \geq \min\left(\{N(|A|)-1 \mid A \in \mathcal{A} \setminus \mathcal{B}\} \cup \{N(B) \mid B \in \mathcal{B}\}\right)$$

Remark :- This is an improvement over the previous thm.

Proof :- Let k be the above minimum.

Then $\exists$ k - idempotent mutuall ortho. quasigroups ~~on~~ on A for ever $A \in \mathcal{A} \setminus \mathcal{B}$

& k - quasigroups (not nec. idempotent) on B for all $B \in \mathcal{B}$.



if $\bigsqcup_{B \in \mathcal{B}} B \neq X$ then we add singleton sets $\{x\}$ $\forall x \in X \setminus \bigsqcup_{B \in \mathcal{B}} B$

to get $\tilde{\mathcal{B}} = \underbrace{\mathcal{B}}_{B_1 \ldots B_l} \cup \underbrace{\{x\}}_{\vec{B}_{l+1} \cdot B_q} \mid x \notin \bigsqcup B\}$.

$\to$ $[x]$ & $[x]$ is orthogonal!

$\therefore$ $\exists$ k mutually orthogonal quasigroups for each is B in $\tilde{\mathcal{B}}$ & $\bigsqcup_{B \in \tilde{\mathcal{B}}} B = X$

Construction :- k idempotent mutually ortho. quasigroups of size $n = |X|$.

$$L_i(x, x) = x \quad \forall x \in X.$$

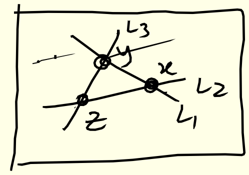
& $L_i(x, y) = L_i^C(x, y)$ $\forall x \neq y$ & C is the unique line joining x & y irr. of $C \in \mathcal{B}$ or not

Exercise $L_1, \ldots, L_k$ are MOLS (idempotent quasigroups)

QED.

Application

① $\mathbb{P}^2(4)-\{x,y,z\}=X$



x,y,z non-collinear.

Lines are lines of $\mathbb{P}^2(4)$ intersecting with X.

line sizes are $5,4,3 \to$ only L_1,L_2,L_3.

L_1,L_2,L_3 are mutually disjoint in X $\quad \mathcal{B}=\{L_1,L_2,L_3\}$

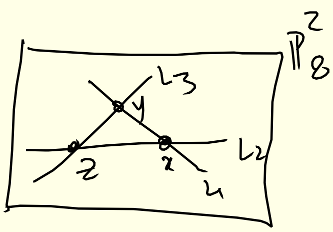
$$\Rightarrow \quad N(18) \geq \min\{4,3,2\}$$

$$\geq 2. \quad \text{but } 18 \equiv 2 \pmod 4 \,!$$

$\therefore$ Euler's conjecture is false!

② $\mathbb{P}^2(8)$ has $8^2+8+1=73$ points.

delete three non-collinear points to get induced linear space X on 70 points.



Line sizes of X are $9,8,7 \to$ only L_1,L_2,L_3.

take $\mathcal{B}=\{L_1,L_2,L_3\}$ & apply the theorem.

$$N(70) \geq \min\{\underset{N(9)-1}{7},\ \underset{N(8)-1}{6},\ \underbrace{6}_{N(7)}\}$$

$$\geq 6. \qquad \boxed{N(70)\geq 6} \ !!$$

<u>Next:</u> We will connect existence of MOLS with existence of projec. planes.