Projective Planes of order n $\longleftrightarrow$ Affine Planes of Order n

$\updownarrow$

$OA(n, n+1)$

$OA(n,3) \longleftrightarrow$ Latin Square of order n.

Example: Construct an $OA(20,5)$.

Sol'n: There exist affine planes of order 4 and 5

Can construct $OA(4,5)$

Can construct $OA(5,6)$

Delete a column to get $OA(5,5)$

$\times$

Product Construction: $OA(20,5)$.

Mutually Orthogonal Latin Squares:

Two ~~orthogonal~~ Latin Squares $\circ$ and $\circ'$ are orthogonal if:

$(x \circ y, x \circ' y) \quad (x,y) \in [n]^2$

are the rows of an $OA(n,2)$

Example:

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

and

1	3	4	2
2	4	3	1
3	1	2	4
4	2	1	3

are orthogonal latin squares

We can check:

(1, 1), (2, 3), (3, 4), ... gives us all the possible pairs

col 1, row 1   col 2, row 1   col 3, row 2

We can also see that each of the 1's in the left are paired with a different # on the right

~~[illegible]~~

Note: The question for the first class is asking about ~~mutually~~ orthogonal LSs of order 6!

A set of Latin Squares is mutually orthogonal if every pair of LSs in the set is orthogonal

(In the defn before, 2 LSs are orthogonal iff $(x, y, x\circ y, x\circ' y)$ $(x,y)\in \mathbb{Z}_n^2$ are the rows of an $OA(n,4)$)

So, more generally, a set of k mutually orthogonal latin squares (MOLS) is equivalent to an $OA(n, k+2)$
(From the $OA(n, k+2)$, use cols $(1, 2, i)$ to get k MOLS).

From k MOLS, construct the $OA(n, k+2)$ with rows:
$(x, y, x \circ y, x \circ' y, x \circ'' y, \ldots)$ $(x,y) \in [n]^2$

Example (Continued)
Since we can construct an $OA(20, 5)$, we can find 3 MOLS of order 20.

Corollary:
If n is odd or $n \equiv 0 \pmod 4$, then there exist orthogonal Latin Squares of order n.
Proof:
We can write $n = q_1 q_2 \ldots q_s$, where $q_1 \ldots, q_s$ are prime powers and $q_i \geq 3$. There exist an affine plane of order q_i for each $i \Rightarrow$ there exist an $OA(q_i, q_i+1)$
$\Rightarrow OA(q_i, 4)$ since each $q_i \geq 3$.
By the product construction, $\exists\, OA(n, 4)$, which is equivalent to a pair of ~~mut~~ orthogonal Latin Squares $\square$.

Turns out that as $n \to \infty$, the maximum # of mutually orthogonal Latin Squares $\to \infty$
Proof: Uses Wilson's theorem

Cont

Existence of Designs:

Def'n Let v be a positive integer, $K \subseteq \mathbb{Z}_{\geq 2}$. A linear space $(V, \mathcal{B})$ is called a ~~[illegible]~~ $PBD(v,K)$ (a pairwise balanced design),

if $|V| = v$ and $|\alpha| \in K$

Example: A $(v,k,1)$-BIBD is a ~~[illegible]~~ $PBD(v, \{k\})$

Example: Starting from ~~a transversal design~~ an $OA(n,k)$, we get a transversal design in which the blocks have size k, and "groups" have size n. Any 2 points of a transversal design are in a common group and a ~~common~~ common block, but not both.

Combining groups and blocks, we get a $PBD(nk, \{k,n\})$

(Necessary Conditions)

Proposition:

If $PBD(v,K)$ exists, then

$v-1 \equiv 0 \pmod{l}$, and

$v(v-1) \equiv 0 \pmod{m}$

where $l = \gcd\{k-1 \mid k \in K\}$ and $m = \gcd\{k(k-1) \mid k \in K\}$

Note: If K is a single element, then we just get the previous conditions for a BIBD! i.e. $v-1 \equiv 0 \pmod{k-1}$ and $v(v-1) \equiv 0 \pmod{k(k-1)}$)

Scanned with CamScanner

Proof:

This follows from:

$$v-1 = \sum_{\substack{\alpha\in\mathcal{B} \\ x\in\alpha}} (|\alpha|-1) \quad \text{for } x\in V$$

as above.

$$v(v-1) = \sum_{\alpha\in\mathcal{B}} |\alpha|(|\alpha|-1)$$

and $\sum_{\substack{\alpha\in\mathcal{B} \\ x\in\alpha}}(|\alpha|-1)$ is divisible by l, since by defn, l is a gcd of #'s of this form, and likewise with $\sum_{\alpha\in\mathcal{B}}|\alpha|(|\alpha|-1)$

□

Write $B(K) = \{v\in\mathbb{Z}_{\geq 2} \mid \text{a PBD}(v,K) \text{ exists}\}$

$K_{l,m} = \{v\in\mathbb{Z}_{\geq 2} \mid v-1\equiv 0 \pmod{l} \text{ and } v(v-1)\equiv 0 \pmod{m}\}$

Defn: A set K is called PBD-closed if $B(K)=K$.

Example:

- $B(K)$ is PBD-closed $(B(B(K)) = B(K))$

  Proof:

  First, for all $k\in K$, a PBD(k,k) exists. (Trivial Construction, one block with all the points inside it).

  So, $B(B(K)) \supseteq B(K)$.

  Suppose we have $v\in B(B(K))$. There exists a PBD$(v, B(K))$, say $(V,\mathcal{B})$. Moreover, for each block $\alpha\in\mathcal{B}$, there exists a PBD$(|\alpha|, K)$ since $|\alpha|\in B(K)$, say $(\alpha, \mathcal{C}_\alpha)$.

  Let $\mathcal{C} = \bigcup_{\alpha\in\mathcal{B}} \mathcal{C}_\alpha$. Check that $(V,\mathcal{C})$ is a PBD(v,K).

  □

• $K_{e,m}$ is PBD-closed:
Follows from the necessary conditions
(If a PBD$(v, K_{e,m})$ exists $\Rightarrow v \in K_{e,m}$).
Exercise: Work through details.

• For any k, λ
$\{v \mid \text{a } (v,k,\lambda)\text{-BIBD exists}\}$
is PBD-closed
(Note: case where $\lambda = 1$ is a special case of $B(B(K)) = B(K)$,
i.e. the case $K = \{k\}$)

• For fixed k,
$\{r \mid \text{a } (v,b,r,k,1)\text{-BIBD exists}\}$
is PBD-closed
Proof: See text

• For fixed s, the set of v s.t. $\exists$ s idempotent
MOLS is PBD-closed (on HW)

Mar 4th

Wilson's Existence Theorem:
Every PBD-closed set K is of the form
$K = K_{l,m} \setminus (\text{finite set})$.
where
$l = \gcd\{k-1 \mid k \in K\}$ and $m = \gcd\{k(k-1) \mid k \in K\}$
In particular, the necessary conditions for the existence of a PBD(v, K) are sufficient with finitely many exceptions.

Example: For which values of v does a $(v,4,2)$-BIBD exist?
Sol'n:
~~[illegible]~~
Let K be the set of all such v. K is PBD-closed, and moreover since a $\underbrace{(4,4,2)}_{\text{trivial design}}$-BIBD exists and a $\underbrace{(7,4,2)}_{\text{complement of Fano plane}}$-BIBD exists,
so $4, 7 \in K$ and we can see that
$K = K_{3,6} \setminus (\text{finite set})$ as $K_{3,6} = \{v \mid v \equiv 1 \pmod 3\}$ and there is no other $K_{l,m}$ such that $K_{l,m} \supsetneq K_{3,6}$