Combinatorics

Lecture 6. Examples of Steiner Systems.

We gave nec. conditions on the parameters of a t-design.

① $b = \dfrac{\lambda\binom{v}{t}}{\binom{k}{t}}$ b = # blocks in a design.

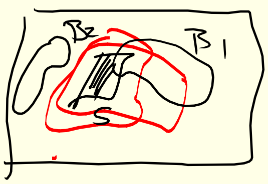
② $b_i = \dfrac{\lambda\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$ b_i = # blocks containing a fixed set of size i.

$b_0 = b$.

Corollary:- If $\mathcal{D}$ is a t-design and $S \subseteq \mathcal{P}$ with $|S| \le t$ (i), then the triple $(\mathcal{P}\setminus S, \mathcal{B}\setminus S, I)$ is an $S_\lambda(t-i, k-i, v-i)$ design where

$$\mathcal{B}\setminus S := \left\{ B\setminus S \;\middle|\; \begin{matrix} S\subseteq B \\ B\in\mathcal{B} \end{matrix} \right\}$$

consists of only those blocks that contain S & remove S from each one of them.



proof:- Exercise.

→ This design is denoted by $\mathcal{D}_S$ & is called the derived design of $\mathcal{D}$ at S.

Theorem Let $0 \le j \le t$. The number of blocks of an $S_\lambda(t,k,v)$ design that "miss" a subset J of size j of $\mathcal{P}$ is

$b^2 \ne b$ squared !) = # blocks avoiding a set of size 2 $\Leftarrow$ $b^j := \dfrac{\lambda\binom{v-j}{k}}{\binom{v-t}{k-t}}$

proof:- ① $S_3 = \left\{ (J,B) \;\middle|\; \begin{matrix} J\subseteq\mathcal{P};\ |J|=j \\ B\in\mathcal{B},\ J\cap B=\emptyset \end{matrix} \right\}$

② Fixing J first, we get $\binom{v}{j} b^j = |S_3|$

③ Fixing B first, we get $b\binom{v-k}{j}$

$$\Rightarrow \quad b^j = \frac{b\binom{v-k}{j}}{\binom{v}{j}} \quad \text{\& we know } b = \frac{\lambda\binom{v}{t}}{\binom{k}{t}}$$

$$= \frac{\lambda\binom{v}{t}\binom{v-k}{j}}{\binom{k}{t}\binom{v}{j}} = \lambda\frac{\cancel{v!}}{\cancel{t!}(v-t)!}\cdot\frac{\cancel{t!}(k-t)!}{k!}\cdot\frac{(v-k)!\,\cancel{j!}\,(v-j)!}{\cancel{j!}(v-k-j)!\;\cancel{v!}}$$

$$= \lambda\frac{\overset{((v-t)-(k-t))!}{\overset{\shortparallel}{}}\ (k-t)!\,(v-k)!\,(v-j)!}{(v-t)!\,k!\,(v-k-j)!}$$

$$= \frac{\lambda\binom{v-j}{k}}{\binom{v-t}{k-t}}.$$

This proof "assumes" that # blocks missing a set of size j is independent of a particular set of size j. Why is it true?
Unless we prove it, this proof is incomplete!

$\therefore$ We now prove that $\underset{\substack{\shortparallel \\ \#B \text{ s.t.} \\ B\cap J=\phi.}}{b^J} = b^{J_1} \quad \forall\ |J|=j,\ |J_1|=j.$

But $b^J = b - \left(\text{blocks that intersect } J \text{ non-trivially}\right)$

$$= b - \Big(\underbrace{\tbinom{j}{1}b_1}_{\substack{\#\text{ blocks} \\ \text{containing} \\ \text{at least one pt} \\ \text{of } J}} - \underbrace{\tbinom{j}{2}b_2}_{\substack{\#\text{ blocks} \\ \text{containing} \\ \text{at least} \\ 2 \text{ pts of } J}} + \underbrace{\tbinom{j}{3}b_3}_{\substack{\text{containing} \\ \geq 3 \text{ pts of } J}} - \cdots\Big) \quad \cdots$$

$$\Rightarrow \quad b^J = b^{J_1} \quad \forall\ |J| = |J_1|$$

Now the proof is complete! **QED.**

Examples :- (1) $GF(2)^4 = V$ $\quad \mathcal{P} = V - \{0\}$

$\boxed{v = 15}$

blocks are triples $\{x, y, z\}$ s.t. $x+y+z=0$.
↳ subsets of size 3.

Since characteristic is 2, $\forall\ x \neq y$, $x+y \neq x$ or y.
$\in \mathcal{P}$. & $(x+y)+(x+y)=0$.

$\therefore$ $\forall \{x,y\}$ $\exists!$ block $\{x, y, x+y\}$ containg x & y

$\therefore$ $\boxed{t=2 \ \& \ \lambda=1}$; $\boxed{\text{clearly } k=3}$

(2) $\mathcal{P} = GF(2)^4$ $\quad \boxed{v=16}$ $\quad$ blocks are 4-subsets

$\{x, y, z, w\}$ s.t. $x+y+z+w=0$. (x, y, z, w distinct)

Given 3 distinct elements of $\mathcal{P}$ say x, y & z ; w is uniquely determined as $x+y+z$.

we need to prove that $x+y+z \neq x$ $\forall$ distinct x, y, z.

$x+y+z = x$ then $(x+y+z)+x=0$.
$\Rightarrow y+z=0$.
$\Rightarrow y=-z \Rightarrow y=z$ $\Rightarrow\!\Leftarrow$!!

$\therefore$ $\{x, y, z, x+y+z\}$ is a 4-subset !!

$\therefore$ $\boxed{t=3,\ \lambda=1,\ k=4,\ v=16.}$

Remark :- Ex. (1) is derived from Ex. (2) at the pt. $\underline{0}$.

Ex. (3) Steiner triple systems

Recall that for $\lambda=1$ we denote design by $S(t,k,v)$ & called it a Steiner design.

simplest possible 2-design is when $t=2$,
$\lambda=1$
& $k=3$.

Such a design is called a Steiner triple system.

History: In 1850 the following question was asked

"Fifteen young ladies in a school walk three abreast for seven days in succession. It is required to arrange them daily so that no two should walk twice abreast"

This was generalised for $v = 6m+3$ (instead of 15) & $3m+1$ (for 7) by

Dijen Ray-Chaudhary in 1969 together with R.M. Wilson (his student)

End of part 1.

For any 2-design we have

$$\left.\begin{array}{l}\lambda(v-1) = r(k-1) \\ \& \quad bk = v.r.\end{array}\right\} \quad (r = b_1 \text{ - blocks containing a pt.})$$

Since $k=3$ & $\lambda=1$, we get $v-1 = 2r \Rightarrow \boxed{v = 2r+1}$ - odd no.

$$3b = r(2r+1). \Rightarrow 3 \mid r(2r+1)$$

if $3 \mid r$ then $v \equiv 1 \pmod 6$. ---- ①

if $3 \mid 2r+1$ then $3 \mid 2r+4 = (2r+1)+3$

$\& \; 2 \mid 2r+4$

$\Rightarrow 6 \mid 2r+4 \Rightarrow 6 \mid v+3$

$v \equiv 3 \pmod 6$ ---- ②

$\therefore$ For a Steiner triple system to exist, we must have $v \equiv 1 \text{ or } 3 \pmod 6$.

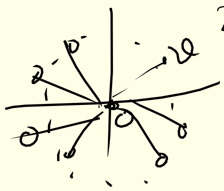
Interestingly for each $v \equiv 1 \text{ or } 3 \pmod 6$, $\exists$ Steiner triple systems on v-points.

① $v=3$ (then $v=k$) $\Rightarrow$ Design is just a single block of size 3.

② $v=7$ ($\mathbb{P}^2(GF(2))$ has 7 elements.

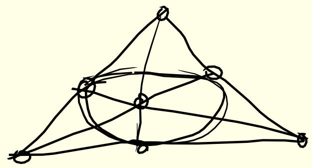
$\qquad \qquad \qquad \qquad ||$

$(GF(2)^3)\setminus\{0\}$ & Any 2-dim'l subspace will contain 3 elts of $(GF(2))^{3*}$



$\therefore$ $\mathbb{P}^2(GF(2))$ is required Steiner triple system on 7 points.

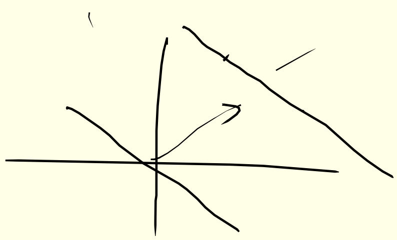
//



③ $v=9$ then $(GF(3))^2$ & lines is a sol^n.

$\mathcal{P}=(GF(3))^2$

Blocks are 1-dim'l subspaces & their cosets.



Example :- $v \equiv 3 \pmod 6$ Let $v=6t+3$

Let $n=2t+1$ Define $\mathcal{P}=\mathbb{Z}_n\times\mathbb{Z}_3$.

$|\mathcal{P}|=v$. Blocks are of two types :

(I) $\{(x,0),(x,1),(x,2)\}$ $x\in\mathbb{Z}_n$

(II) $\{(x,i),(y,i),(\frac{1}{2}(x+y),\ i+1)\}$ $x\neq y$ in $\mathbb{Z}_n$, $i\in\mathbb{Z}_3$

Since $n=2t+1$ is odd, $\frac{1}{2}\in\mathbb{Z}/n\mathbb{Z}$.

Claim :- ① Every pair of the type $(x,i),(x,j)$ occurs uniquely in a block of type I.

② Every pair of type $(x,i)(y,i)$ & $(x,i),(y,j)$, $x\neq y$ occurs uniquely in blocks of type (II).

Pf. ① is obvious

② $(x,i),(y,i)$ ✓

③ $(x,i),(y,j)$? $i \neq j$.

$\{(x,i),(y,i),(\frac{1}{2}(x+y),i+1)\}$

$\{0,1,2\}$

then $|i-j| = 1 \pmod 3$

i.e. one can always write $j = i+1$ or $i = j+1$

$\therefore$ WLOG can assume the pair is of the type $(x,i),(y,i+1)$

to find z s.t. $\frac{1}{2}(x+z) = y \iff z = 2y - x$. which is unique in $\mathbb{Z}_n$

then we have unique block

$$\{(x,i),(2y-x,i),(y,i+1)\}$$

$$\because y = \frac{1}{2}(x+(2y-x))$$

Hence we got our required example!

—x—x—

Example :- Let $v = 6t+1$.

$$P = \mathbb{Z}_{2t} \times \mathbb{Z}_3 \sqcup \{\infty\}$$

Define usual addition on elts of $\mathbb{Z}_{2t} \times \mathbb{Z}_3$ (coordinate wise)

& $\infty + (x,i) = \infty \quad \forall (x,i) \in \mathbb{Z}_{2t} \times \mathbb{Z}_3$

We write (x,i) by x_i i.e. $(x,0) = x_0$, $(x,1) = x_1$, $(x,2) = x_2$ $\forall x \in \mathbb{Z}_{2t}$

i.e. $x_0 + x_2 = (2x)_2$

$x_1 + y_2 = (x+y)_0$

Four types of base blocks

1 (I) $\{0_0, 0_1, 0_2\}$

3 (II) $\{\infty, 0_0, t_1\}, \{\infty, 0_1, t_2\}, \{\infty, 0_2, t_0\}$

3(t-1) (III) $\{0_0, i_1, (-i)_1\}, \{0_1, i_2, (-i)_2\}, \{0_2, i_0, (-i)_0\}$ $1 \le i \le t-1$

$3t$ IV $\{t_0, i_1, (1-i)_1\}, \{t_1, i_2, (1-i)_2\}, \{t_2, i_0, (1-i)_0\}$

$i = 1, \dots, t$

$\exists$ $1 + 3 + 3t + 3(t-1) = 6t + 1$ base blocks.

For each $a \in \{0, 1, \dots, t-1\}$ we add elt. a_0 (ie $(a, 0)$) to each of these $6t+1$ blocks; to get a total of $t(6t+1)$ blocks.

(If this were to be design $b = \frac{1\binom{v}{2}}{\binom{3}{2}} = \frac{v(v-1)}{6}$
$= t(6t+1)$
if $t = 6t+1$.)

Claim :- Any pair of elts occurs in exactly one block.

Exercise! ① prove that any pair occurs at least once.

② count the no. of pairs of pts & show that it equals the no. of pairs that can occur in blocks.

① & ② $\Rightarrow \lambda = 1$.

(R.C. Bose) Let $q = 6t+1$ be a prime power.

(Difference sets technique) $\langle \alpha \rangle = GF(q)^*$.

Define $B_{i,\xi} = \{\alpha^i + \xi, \alpha^{2t+i} + \xi, \alpha^{4t+i} + \xi\}$ $0 \le i \lneq t$, $\xi \in GF(q)$

$\# B_{i,\xi}$'s $= t(6t+1)$

Claim $\left(GF(q), \left\{B_{i,\xi} \,\middle|\, \begin{matrix} 0 \le i < t \\ \xi \in GF(q) \end{matrix}\right\}, \text{inclusion}\right)$ is a Steiner triple system.

$\alpha^{6t} = 1. \Rightarrow \alpha^{3t} = -1$ Define s by $\alpha^s = \alpha^{2t} - 1$

look at $B_{0,0} = \{1, \alpha^{2t}, \alpha^{4t}\}$ the six differences of elts of $B_{0,0}$ are

1. $\alpha^{2t}-1=\boxed{\alpha^{s}}$; $-(\alpha^{2t}-1)=\alpha^{3t}\alpha^{s}=\boxed{\alpha^{s+3t}}$

2. $\alpha^{4t}-\alpha^{2t}=\alpha^{2t}(\alpha^{2t}-1)=\boxed{\alpha^{s+2t}}$, $-\alpha^{s+2t}=\boxed{\alpha^{s+5t}}$

3. $\alpha^{6t}-\alpha^{4t}=\alpha^{4t}\cdot\alpha^{s}=\boxed{\alpha^{s+4t}}$, $-\alpha^{s+4t}=\boxed{\alpha^{s+t}}$

These are all distinct! Thus for any $\eta\neq 0$ in $GF(q)$,

$\exists\ i$ $0\leq i<t$ s.t. η occurs as difference of two elts of $B_{i,0}$.

$\therefore$ $\forall\ x\neq y$ in $GF(q)$. let $\eta=x-y$. Let $\exists!\ i$ s.t. $B_{i,0}=\{\alpha^{i},\alpha^{2t+i},\alpha^{4t+i}\}$ contains η as a difference. Take ξ s.t. one of $\alpha^{i},\alpha^{2t+i},\alpha^{4t+i}$ equals x.

Since $x-y=\eta$ occurs as a diff. in $B_{i,\xi}$

y must occur in $B_{i,\xi}$!!

QED !!

Remark :- let $\eta=\alpha^{\beta}-\alpha^{\gamma}$ where $\{\beta,\gamma\}\subseteq\{i,2t+i,4t+i\}$

then choose ξ s.t. $\alpha^{\beta}+\xi=x$.

then $\alpha^{\gamma}+\xi$ must be y as their diff is still $x-y$!

QED-2 !!