Combinatorics 2018 Fall

Taught by: Professor Xiande Zhang

2018.11.26

Key words: Difference Set, Finite Linear Space

Recall:
A (v, k, λ) design (X, D), $|X| = v$, $|D| = b$, r replicaiton number satisfies each pair $\{x, y\} \subset X$ appears in exactly λ blocks.

- $b \geq v$, if $b = v$, called symmetric design
- $r(k-1) = \lambda(v-1)$ & $bk = rv$

G is an Abelian group of size v
Def: $2 \leq k < v$, $\lambda \geq 1$, A (v, k, λ) **difference set** (D, S) is a k-subset $D = \{d_1, d_2, \cdots, d_k\} \subseteq G$, s.t. the collection of differences $d_i - d_j$ $(i \neq j)$ contains every element in $G \setminus \{0\}$ exactly λ times.
Note: If $G = \mathbb{Z}_v$, call D is cyclic DS
E.g. $G = \mathbb{Z}_7$, (7,3,1)-DS, $D = \{0, 1, 3\}$

此处 $r = k$.
$b = v$.

Fact:

① $\lambda(v-1) = k(k-1) \implies \lambda < k$.

② A **translate** of D is $a + D = \{a + d_1, a + d_2, \ldots, a + d_k\}$ for some $a \in G$. Then $a + D \neq D$ if $a \neq 0$.

proof:. k-1个 translations.

① Count # of differences in D.

② If $a + D = D$ for some $a \neq 0$, then $\exists$ a permutation π of $[k]$ satisfies that $\pi(i) \neq i$ and $d_i + a = d_{\pi(i)}$ for all $i \in [k]$. Then a is expressed as a difference $d_{\pi(i)} - d_i$ in k ways. But $k > \lambda$, contradiction.

$\square$

Theorem 1. *If D is a (v,k,λ) difference set, then $\{a+D:\ a\in G\}$ are blocks of a symmetric (v,k,λ) design.*

proof:.

1. $b=v=|G| \Longrightarrow$ symmetric.
2. $|i+D|=k$, $\forall i$.
3. Show any pair of points is contained in exactly λ blocks. $\forall x\neq y\in G$, assume $x-y=d\neq 0$, then $\{x,y\}\subset a+D \Longleftrightarrow x=a+d_i, y=a+d_j$ for some $i\neq j \Longleftrightarrow x-y=d_i-d_j=d\neq 0$. Since there are exactly λ pairs d_i,d_j s.t. $d_i-d_j=d$, and for each such pair, there are exactly one $a=x-d_i=y-d_j$ s.t. $\{x,y\}\subset a+D$.

$\square$

Theorem 2. *If q is a prime power, $q\equiv 3\ (4)$, then nonzero squares in F_q form a $(q,\frac{q-1}{2},\frac{q-3}{4})$ DS.*

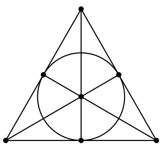
proof:.
$G=F_q=\{0,\alpha^0,\alpha^1,\cdots,\alpha^{q-2}\},\ D=\{\alpha^0,\alpha^2,\cdots,\alpha^{q-3}\}$,then
$k=\dfrac{q-1}{2}$
$\because q\equiv 3\ (4),\ \therefore -1=\alpha^{\frac{q-1}{2}}\notin D \Longrightarrow$ if $s\in D$, then $-s\notin D$
$\forall s\in D$, $\exists x,y\in D$ and $x-y=1 \Longleftrightarrow \exists sx,sy\in D$ and $sx-sy=s$ $\Longleftrightarrow \exists sx,sy\in D$ and $sy-sx=-s$. This means all nonzero space and nonsquares have the same # of representatives as a difference of two elements in D.

$$\Longrightarrow \lambda=\frac{k(k-1)}{q-1}=\frac{\frac{q-1}{2}\frac{q-3}{2}}{q-1}=\frac{q-3}{4}$$

$\square$

Def: Finite linear space over a finite set X is a family α of subsets of X called lines such that:

- every line contains at least 2 points
- any 2 points are on exactly one line

E.g. 

Theorem 3. *If α is a finite linear space over X with $|\alpha| \geq 2$, then $|\alpha| \geq |X|$ with equality holds iff any two lines share exactly one point.*

proof:(Conway).
Let $b = |\alpha| \geq 2,\ v = |X|$. $\forall x \in X$, let r_x be the replication number, i.e. $\#$ lines through x
Choose a line $L \in \alpha$ and a point $x \notin L$. $\because \forall a \neq b \in L, \{x, a\} and \{x, b\}$ are on different lines, $\therefore r_x \geq |L|$
Assume $b \leq v$, then $b(v - |L|) = bv - b|L| \geq bv - vr_x = v(b - r_x)$
$\Longrightarrow$

$$\frac{1}{v - |L|} \leq \frac{b}{v(b - r_x)}$$

$$\begin{aligned} b = \sum_{L \in \alpha} 1 &= \sum_{L \in \alpha} \sum_{x \in X : x \notin L} \frac{1}{v - |L|} \leq \frac{b}{v} \sum_{L \in \alpha} \sum_{x \in X : x \notin L} \frac{1}{b - r_x} \\ &= \frac{b}{v} \sum_{x \in X} \sum_{L \in \alpha : x \notin L} \frac{1}{b - r_x} = \frac{b}{v} \sum_{x \in X} 1 = b \end{aligned}$$

This implies all inequalities are equalities so that $b = v$ and $r_x = |L|$ whenever $x \notin L$, i.e. any line containing x share one point with L.
$\therefore b \geq v$ with equality holds iff any two lines share exactly one point.
$\square$

如果 $b \leq v \Rightarrow b = v$.

从而 $b \geq v$.