Combinatorics, 2017 Fall, USTC

Week 10 Note 1

2017.11.21, Tuesday

Difference Sets(DS)

Note: Recall that a (v, k, λ) design implies $r(k-1) = \lambda(v-1)$ and $bk = vr$. $\Longrightarrow \lambda(v-1) \equiv 0\ (k-1)$ and $\lambda v(v-1) \equiv 0\ (k(k-1))$.

Let $\mathbb{Z}_v = \{0, 1, 2, \ldots, v-1\}$.

Definition 1. *$2 \leq k < v$, $\lambda \geq 1$. A (v, k, λ) **difference set** is a k-subset $D = \{d_1, d_2, \ldots, d_k\} \subseteq \mathbb{Z}_v$ such that the collection of differences $d_i - d_j$ $(i \neq j)$ contains every element in $\mathbb{Z}_v \setminus \{0\}$ exactly λ times.*

Fact:

① $\lambda(v-1) = k(k-1)$.

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

Proof. 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.*

□

Theorem 1. *If D is a (v, k, λ) difference set, then $D, 1 + D, \ldots, (v-1) + D$ are blocks of a symmetric (v, k, λ) design.*

Proof. ① *v blocks, v points $\Longrightarrow$ symmetric.*

② *$|i + D| = k$, $\forall i$.*

③ *Show any pair of points is contained in exactly λ blocks. $\forall x \neq y \in \mathbb{Z}_v$, then $x, y \in a + D \iff \exists d_i \neq d_j$, s.t. $x = a + d_i, y = a + d_j \iff x - y = d_i - d_j \triangleq d$. 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. $s, y \in a + D$.* □

Theorem 2. *If v is a prime and $v \equiv 3\ (4)$, then all nonzero squares in $\mathbb{Z}_v$ form a (v, k, λ) DS with $k = \frac{v-1}{2}$ and $\lambda = \frac{v-3}{4}$.*

[The condition $v \equiv 3\ (4)$ is to ensure -1 is a nonsquare in $\mathbb{Z}_v$.]

Proof. *Since v is odd, then $a \neq -a$ in $\mathbb{Z}_v$ when $a \neq 0$. Therefore for $\forall a \in \mathbb{Z}_v \setminus \{0\}$, $x^2 = a^2$ has two different solutions $\pm a \in \mathbb{Z}_v$ and $\pm a$ gives one square $a^2 \in \mathbb{Z}_v$. We have $|D| = \frac{v-1}{2}$.*

Since $-1 \notin D$, then $-D$ is the set of all nonsquares. $\forall s \in D$, $\exists x, y \in D$ and $x - y = 1 \iff \exists sx, sy \in D$ and $sx - sy = s \iff \exists sx, sy \in D$ and $sy - sx = -s$. This means all nonzero squares and nonsquares have the same # of representatives as a difference of two elements in D.

Hence $\lambda = \frac{k(k-1)}{v-1} = \frac{\frac{v-1}{2}\frac{v-3}{2}}{v-1} = \frac{v-3}{4}$. □

Projective Planes(PG(q))

Consider a linear space $\mathcal{L} \subseteq 2^X$, $|L| = b$, $|X| = v$, then $b \geq v$.

We want $b = v$ and each line has $q + 1$ points, then any two lines share exactly one point. That is, all lines form a symmetric (v, k, λ) design with $\lambda = 1$, $k = q + 1$, then $b = v = q^2 + q + 1$. (Consider the dual design.)

Definition 2. *A **projective plane** of order q consists of a set X with $q^2 + q + 1$ points, and a family of lines satisfying*

① *each line has $q + 1$ points.*

② *any two points lie on a unique line.*

Note: A PG(q) is a $(q^2 + q + 1, q + 1, 1)$ design.

Example:

(1) $q = 1$:

(2) $q = 2$, Fano plane:

Propositon 3. *In a projective plane of order q*

① *Any point lies in $q+1$ lines.*

② *There are q^2+q+1 lines.*

③ *Any two lines meet in a unique point.*

Proof. ① *$\forall x \in X$, there are q^2+q points different from it. Each line containing x contains q further points, and no other overlaps between them. So there must be $q+1$ lines through x.*

② *Double count (x, L), $x \in L$, $L \in \mathcal{L}$.*

$$(q^2+q+1)(q+1) = |\mathcal{L}|(q+1) \Longrightarrow |\mathcal{L}| = q^2+q+1.$$

③ *If $L_1 \cap L_2 = \emptyset$, $x \in L_1$, then the $q+1$ points of L_2 gives $q+1$ different lines containing x. Thus we get $q+2$ different lines through x, contradiction.* □

Construction of PG(q), $q \geq 2$ prime

Recall $\mathbb{Z}_q$ and $\mathbb{Z}_q^* = \mathbb{Z}_q \setminus \{0\}$ are cyclic groups.

$V\{(x_0, x_1, x_2) \in \mathbb{Z}_q^* : \ (x_0, x_1, x_2) \neq (0,0,0)\}$, $|V| = q^3 - 1$.
points: $[x_0, x_1, x_2] = \{(cx_0, cx_1, cx_2) : \ c \in \mathbb{Z}_q^*\}$. So there are $\frac{q^3-1}{q-1} = q^2+q+1$ points.
lines: $L(a_0, a_1, a_2)$ ($(a_0, a_1, a_2) \in V$) is defined to be the set of points $[x_0, x_1, x_2]$ for which $a_0x_0 + a_1x_1 + a_2x_2 = 0$. There are $q^2 - 1$ solutions to this equation, thus there are $\frac{q^2-1}{q-1}$ points in line $L(a_0, a_1, a_2)$.
check any two points lie on a unique line: i.e. $\forall [x_0, x_1, x_2] \neq [y_0, y_1, y_2]$, $\exists!$ $L(a_0, a_1, a_2)$, s.t.

$$\begin{cases} a_0x_0 + a_1x_1 + a_2x_2 = 0 \\ a_0y_0 + a_1y_1 + a_2y_2 = 0 \end{cases}.$$

Since $\begin{bmatrix} x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \end{bmatrix}$ has rank 2, the solution space has dimension 1, i.e. $\exists!$ line $L(a_0, a_1, a_2)$ contains both $[x_0, x_1, x_2], [y_0, y_1, y_2]$.

Bruen's Theorem

A blocking set in a PG(q) is a set of points which intersects with every line. E.g. the lines. A blocking set containing a line is called **trivial**.
Homework: the smallest blocking sets are just lines.

Question: what can be said about the size of non-trivial blocking sets?

Theorem 4 (Bruen's Theorem)**.** *Let B be a non-trivial blocking set in a PG(q). Then $|B| \geq q + \sqrt{q} + 1$.*

[**Note:** Bruen's theorem means that any set of at most $q + \sqrt{q}$ points either contains a line or avoids a line.]

Proof. *If $q = 1$, the claim is true. Let $q \geq 2$. Let $|B| = q + m$, $m < \sqrt{q} + 1$, and B is a blocking set.*

*Let l_i=#{lines containing exactly i points in$B$}.(**Homework:** check when $i > m$, $l_i = 0$.)*

Double count lines, $L \cap V \neq \emptyset$, point-line (x, L), $x \in L \cap B$, and triples (x, y, L) with $x \neq y$ in $B \cap L$, then

$$\sum_{i=1}^{m} l_i = q^2 + q + 1,$$

$$\sum_{i=1}^{m} i l_i = |B|(q+1), \text{ every point lies on } q+1 \text{ lines},$$

$$\sum_{i=1}^{m} i(i-1) l_i = |B|(|B|-1), \text{ two points lie on exactly one line.}$$

Since $m < \sqrt{q} + 1$, $i - \sqrt{q} - 1 < 0, i \in [m]$, so

$$\begin{aligned} 0 &\geq \textstyle\sum_{i=1}^{m} (i-1)(i-\sqrt{q}-1) l_i \\ &= \textstyle\sum_{i=1}^{m} i(i-1) l_i - (\sqrt{q}+1) \sum_{i=1}^{m} i l_i + (\sqrt{q}+1) \sum_{i=1}^{m} l_i \\ &= |B|(|B|-1) - (\sqrt{q}+1)|B|(q+1) + (\sqrt{q}+1)(q^2+q+1) \\ &= [|B| - (q + \sqrt{q} + 1)][|B| - (q\sqrt{q} + 1)] > 0. \end{aligned}$$

Contradiction. □