Combinatorics, 2017 Fall, USTC

Week 10 Note 2

2017.11.24, Friday

Resolvable Designs

Definition 1. *D is a (v, k, λ) design over X. A **parallel** class in D is a subset of disjoint blocks from D whose union is X. Each parallel class has $\frac{v}{k}$ blocks. So we have $\frac{|D|}{\frac{v}{k}} = \frac{\lambda v(v-1)}{k(k-1)} \cdot \frac{k}{v} = \frac{\lambda(v-1)}{k-1}$ such classes, which equals the replication number. A partition of D into r parallel classes is called a **resolution**, and a design is said to be **resolvable** if it has at least one resolution.*

Problem: A football league of $2n$ teams,each team plays exactly once against every other team. Is it possible to arrange a schedule so that all matches are played in $2n-1$ days, and on each day every team plays one match?

The answer is a resolvable $(2n, 2, 1)$ design, $r = \frac{1\times(2n-1)}{2-1} = 2n-1$.

Let our ground set be $X\{*, 1, \ldots, 2n-1\}$, $D = \binom{X}{2}$. Define $D_1, \ldots, D_{2n-1}$, for $i \in [2n-1]$ as follows:

$$D_i = \{\{i, *\}\} \cup \{\{a, b\} : \ a + b \equiv 2i \ mod \ 2n-1\}.$$

① $\forall a \neq b \in X \setminus \{*\}$, $\exists!\ i \in [2n-1]$ s.t. $a + b \equiv 2i \ mod \ (2n-1)$. Then $\exists!\ D_i$ s.t. $\{a, b\} \subset D_i$. $\Longrightarrow D = D_1 \cup D_2 \cup \cdots \cup D_{2n-1}$ is a partition.

② $\forall i \in [2n-1]$, show D_i is a parallel class. If $a \notin \{i, *\}$, the unique block in D_i containing a is $\{a, b\}$ with $b \equiv 2i - a (mod\ 2n-1)$.

Definition 2 (**Affine Plane**). *An affine plane $AG(q)$ is a $(q^2+q, q, 1)$ design.*

For $AG(q)$, we have $r = \frac{q^2-1}{q-1} = q+1$, $b = \frac{vr}{k} = q^2+q$.
Parallel lines: lines that don't meet each other.

Construction 1: Let $(X, \mathcal{L})$ be a $PG(q)$. Fix one line $L_0 \in \mathcal{L}$. Let $X' = X \setminus \{L_0\}$, $\mathcal{L}' = \{L \setminus L_0 : \ L \in \mathcal{L}, L \neq L_0\}$. Then $(X', \mathcal{L}')$ is an $AG(q)$. Further, $(X', \mathcal{L}')$ is a resolvable $(q^2, q, 1)$ design.

Proof. *$|X'| = q^2$, $b = |\mathcal{L}'| = q^2 + q$, $k = |L \setminus L_0| = q$. By definition of $PG(q)$, any two points lies on a unique line. So it is an $AG(q)$. Next, show resolvability.*

$\forall x \in L_0$, *let* $L_x = \{L \setminus \{x\} : \ L \in \mathcal{L}, L \neq L_0, x \in L\} \subset \mathcal{L}'$. *Then* L_x *is a partition of* X', *i.e. a parallel class. Since in* $PG(q)$, *every line intersects* L_0 *in exactly one point, we have* $L_x(x \in L_0)$ *is a partition of* $\mathcal{L}'$. □

Construction 2: q prime, $\mathbb{Z}_q$ is a cyclic additive group and $\mathbb{Z}_q^*$ is a cyclic multiplicative group.($\mathbb{F}_q$ is a finite field.)

Let $X = \mathbb{Z}_q \times \mathbb{Z}_q$. Let $\mathcal{L}$ be the set of all lines of the form

$$L(a,b) = \{(x,y) \in X : \ y = ax + b\}, \ a, b \in \mathbb{Z}_q,$$

and

$$L(c) = \{(c,y) \in y \in \mathbb{Z}_q\}, \ c \in \mathbb{Z}_q.$$

Then $(X, \mathcal{L})$ is an $AG(q)$, and further resolvable.

Proof. $|X| = q^2$, $k = |L| = q$. $\forall (x_1, y_1) \neq (x_2, y_2) \in X$,

① *if* $x_1 = x_2$, *then the unique line containing them is* $L(x_1)$.

② *if* $x_1 \neq x_2$, *then*

$$\begin{cases} y_1 = ax_1 + b \\ y_2 = ax_2 + b \end{cases}$$

has a unique solution (a, b). *Then the unique line is* $L(a, b)$.

$\{L(a,b) : \ b \in \mathbb{Z}_q\}(a \in \mathbb{Z}_q)$, $\{L(c) : \ c \in \mathbb{Z}_q\}$ *is a resolution.* □

Homework: Any $AG(q)$ is resolvable.

Definition 3 (Hadamard Matrices). *A Hadamard matrix is a square* $n \times n$ *matrix* H *with entries* ± 1, *such that* $HH^{\mathrm{T}} = nI$.

E.g.

$$H_1 = [1], \ H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \ H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Fact:

① H is invertible.

② All rows(columns) are mutually orthogonal.

③ If H is a Hadamard matrix, then exchanging two rows(or columns), multiplying (-1) to any row(columns) also gives a Hadamard matrix.

If a Hadamard matrix(H-matrix) has all 1's in the first row and the first column, we say it is **normalized**.

Fact: An $n \times n$ H-matrix exists $\Longleftrightarrow$ an $n \times n$ normalized H-matrix exists.

Theorem 1. *If H is an $n \times n$ normalized H-matrix, then every except the first row has $\frac{n}{2}$ positive and $\frac{n}{2}$ negative entries. If $n > 2$, then any two rows other than the first row have exactly $\frac{n}{4}$ 1's in common. (Same for columns.)*

Proof. *The first statement is clear.*

Let u, v be any two rows other than the first row. Let a(resp. b) be the number of places where they both have 1's(resp. -1's). Since v has $\frac{n}{2}$ positives and $\frac{n}{2}$ negatives, then $(\frac{n}{2} - a) + b = \frac{n}{2}$. Hence $a = b$. Since $(u, v) = 0$, we have $a + b - (\frac{n}{2} - a + \frac{n}{2} - b) = 0 \Longrightarrow a = \frac{n}{4}$. □

Definition 4 (**Hadamard Code** C_n)**.** *H is an $n \times n$ H-matrix, take all rows of H and $-H$, and change -1 to 0. Let C_n be the set of all the resulting $1 \times n$ vectors, then C_n is the set of $2n$ binary vectors. $\forall x, y \in C_n$, the* ***Hamming distance*** *of x, y, $d_H(x, y)$ is the number of positions they differ.*

Theorem 2. $\forall x \neq y \in C_n$, $d_H(x, y) \geq \frac{n}{2}$.

Proof. ① *If x is obtained from the i^{th} row of H, y is obtained from the i^{th} row of $-H$, then $d_H(x, y) = n$.*

② *Otherwise, $\exists$ two rows u, v of H, such that x is obtained from u or $-u$, and y is obtained from v or $-v$. In any case, $d_H(x, y) = \frac{n}{2}$.* □

Theorem 3. *Every H-matrix of size $4n \times 4n$ gives an symmetric $(4n - 1, 2n - 1, n - 1)$ design.(This design is called Hadamard Design.)*

Proof. *Let H be a normalized H-matrix of size $4n \times 4n$. After deleting the first row and the first column, we have a $(4n-1) \times (4n-1)$ matrix. Then change -1 to 0. Denote it by M. Then each row of M has $(2n - 1)$ 1's, which corresponds to a block of size $2n - 1$. Every two columns have $(n - 1)$ 1's in common.* □

Hadamard Conjecture: Hadamard matrix exists for all orders divisible by 4.

Theorem 4. *If H is an $n \times n$ H-matrix, then $\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$ is also an H-matrix of order $2n$.*