MA 437 LESSON 29

CONSTRUCTING Block Designs

Constructing Block Designs

Def. Let G be an abelian group of order v and identity element 0. Let D be a subset of G of order k. If every element* in G can be expressed as the difference of two elements from D in exactly $\lambda < k$ ways, the D is called a diffenence set in G. We denote the set of parameters as (v, k, λ)

* Every element except 0

Ex. Let $G = Z_7$ $D = \{1, 2, 4\}$. This is a $(7, 3, 1)$ difference set:

$1 = 2 - 1$
$2 = 4 - 2$
$3 = 4 - 1$

$4 = 1 - 4 \bmod 7 = -3 \bmod 7 = 4$
$5 = 2 - 4 \bmod 7 = -2 \bmod 7 = 5$
$6 = 1 - 2 \bmod 7 = -1 \bmod 7 = 6$

These are all possible differences, $\lambda = 1$

Our interest in difference sets results from the fact that they can be used to construct block designs as follows

Let D be the diffence set in G

Form $g + D$ for all $g \in G$

These are the blocks.

Ex $D = \{1, 2, 4\}$ in $G = \mathbb{Z}_7$

$0 + D = \{1, 2, 4\}$

$1 + D = \{2, 3, 5\}$

$2 + D = \{3, 4, 6\}$

$3 + D = \{4, 5, 0\}$

$4 + D = \{5, 6, 1\}$

$5 + D = \{6, 0, 2\}$

$6 + D = \{0, 1, 3\}$

Thm. A (v, k, λ) diffence set D is used to construct a (v, v, k, k, λ) block design where the blocks are all

$$g + D, \quad g \in G$$

Proof. There are v elements ($|G| = v$) and v blocks ($|D| = k$) so there are k elements in each block. Add $d \in D$ to each $a \in G$. The result is G again. So each element in G appears k times among all the $g_i + d_j$, $i = 1, \dots v$, $j = 1, \dots k$. Thus each $g \in G$ is in k blocks.

We need to show each pair of elements in G appear together in λ blocks.

Let $x, y \in G$, $x \neq y$. If x, y are in some block, $g + D$, then

$$x = g + d_i \qquad y = g + d_j$$

$\rightarrow$ $x - y = d_i - d_j$ so $x - y$ is the difference of those 2 elements in D. This can happen in λ ways. So x & y can not appear in more than λ blocks

Conversely, suppose $x-y = d_i - d_j$

Then $x = g + d_i$

$$y = x - (d_i - d_j) = (x - d_i) + d_j$$
$$= g + d_j$$

$\Rightarrow x, y \in D_b$ So x, y must appear together in at least λ blocks. Thus

x, y appear together in exactly λ blocks. This allows us to again construct symmetric block designs.

Generalization.

Let G be a group of order v and $D_0, \ldots, D_{t-1}$ be subsets of G of order k. each. If every non zero element in G can be written as the difference of 2 elements <u>from the same D_i</u> in exactly λ ways, then $D_0, \ldots D_{t-1}$ are the initial blocks in a generalized difference set.

Thm. Let $D_0, \cdots D_{t-1}$ be the initial blocks in a generalized diffence set in G, $|G| = v$

$|D| = k$ for each D.

(A (v, k, λ) generalized difference set with t blocks)

Then $g_i + D_j$, $i = 1, \cdots v$, $j = 1, \cdots t-1$

are the blocks in a

(v, vt, kt, k, λ) block design

Ex $G = Z_{19}$ $D_0 = \{1, 7, 11\}$

$D_1 = \{2, 3, 14\}$ $D_2 = \{4, 6, 9\}$

These are the initial blocks in a generalized difference set

$(v, k, \lambda) = (19, 3, 1)$ $t = 3$

Then $g_i + D_0$, $g_i + D_1$, $g_i + D_2$

are blocks in a $(19, 57, 9, 3, 1)$ block design.

6 Constructing the $g_i + D_j$ is easy. What needs to be checked is that the difference of elements from D_0, D_1, D_2 are ~~in some~~ give the elements of g once each ($\lambda = 1$) Check:

$1 = 3 - 2$
$2 = 6 - 4$
$3 = 9 - 6$
$4 = 11 - 7$
$5 = 9 - 4$
$6 = 7 - 1$
$7 = 2 - 14 = -12 = 7$
$8 = 3 - 14 = -11 = 8$
$9 = 1 - 10 = -10 = 9$
$10 = 11 - 1$
$11 = 14 - 3$

$12 = 14 - 2 = 12$
$13 = 1 - 7 = -6 = 13$
$14 = 4 - 8 = -5 = 14$
$15 = 7 - 11 = -4 = 15$
$16 = 6 - 9 = -3 = 16$
$17 = 4 - 6 = -2 = 17$
$18 = 2 - 3 = -1 = 18$

To construct the block design $g + D$

D_0	D_1	D_2
$0 + D_0 = \{1, 7, 11\}$	$0 + D_1 = \{2, 3, 14\}$	$0 + D_2 = \{4, 6, 9\}$
$1 + D_0 = \{2, 8, 12\}$	$1 + D_1 = \{3, 4, 15\}$	$1 + D_2 = \{5, 7, 10\}$
$2 + D_0 = \{3, 9, 13\}$	$2 + D_1 = \{4, 5, 16\}$	$2 + D_2 = \{6, 8, 11\}$
$\vdots$		

2.

$17 + D_0 = \{18, 5, 9\}$

$18 + D_0 = \{0, 6, 10\}$

$17 + D_1 = \{0, 1, 12\}$

$18 + D_1 = \{1, 2, 13\}$

$17 + D_2 = \{2, 4, 7\}$

$18 + D_2 = \{3, 5, 8\}$.

So we can construct a (v, vt, kt, k, λ) block design if we can find a (v, k, λ) difference set with t initial blocks. We present several methods for finding them. Today the groups will all have p = prime number of elements. We will generalize this to p^n elements next time. In fact the group $G = \mathbb{Z}_p$ today

8. Thm A. Suppose $v = 6t+1 = p$ where p is a prime and t is a positive integer let G = the group of non zero elements in Z_p. and multiplication. This group is always cyclic so there is a cyclic generator a. The sets

$$D_i = \{a^i, a^{2t+i}, a^{4t+i}\} \quad i=0,\ldots t-1$$

are initial blocks for a $(6t+1, 3, 1)$ generalized difference set

Thm B. Suppose $v = 4t+1 = p$ where p is a prime and t is a positive integer. Let G be the group of non zero elements in Z_p and a be a cyclic generator Then the sets

$$D_i = \{a^i, a^{t+i}, a^{2t+i}, a^{3t+i}\} \quad i=0,\ldots t-1$$

are the initial blocks for a $(4t+1, 4, 3)$ generalized difference set

9. The proofs are similar. Let's look at Theorem B

Proof $|a| = p-1 = 4t$. Thus

$a^{4t} = 1$, $a^{2t} \neq 1$. But

$0 = a^{4t} - 1 = (a^{2t}-1)(a^{2t}+1)$, so $a^{2t} = -1$

Also $a^t - 1 \neq 0$. Hence $a^t - 1 = a^s$ for some $1 \leq s \leq 4t$. Form differences

1. $\pm a^l(a^t - 1) = \pm a^l a^s = a^{l+s}, a^{l+s+2t}$
2. $\pm a^l(a^{2t}-1) = \pm a^l(2a^{2t}) = 2a^l, 2a^{l+2t}$
3. $\pm a^l(a^{2t} - a^t) = \pm a^l a^t(a^t - 1) = a^{l+t+s}, a^{l+3t+s}$
4. $\pm a^l(a^{3t}-1) = \pm a^l a^{3t}(1-a^t) = a^{l+t+s}, a^{l+3t+s}$
5. $\pm a^l(a^{3t} - a^t) = \pm a^l a^t(2a^{2t}) = 2a^{l+3t}, 2a^{l+t}$
6. $\pm a^l(a^{3t} - a^{2t}) = \pm a^l a^{2t} a^s = a^{l+2t+s}, a^{l+s}$

Multiplication by 2 or a^s are bijections so can be cancelled. This leaves

$a^l, a^{t+l}, a^{2t+l}, a^{3t+l}$ repeated 3 times each. Hence $\lambda = 3$

Ex $13 = 4t+1 \quad t=3$

The non zero elements of Z_{13} have $a=2$ as a cyclic generator under multiplication: multiply by 2 to get next:

2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1

$D_0 = \{a^0, a^3, a^6, a^9\}$
$= \{1, 8, 12, 5\}$

$D_1 = \{a^1, a^4, a^7, a^{10}\}$
$= \{2, 3, 11, 10\}$

$D_2 = \{4, 6, 9, 7\}$

are the initial sets. To get the block design, compute $g+D_0$, $g+D_1$, $g+D_2$ where $g \in Z_{13}$

$0+D_0 = \{1, 8, 12, 5\}$
$1+D_0 = \{2, 9, 0, 6\}$
$2+D_0 = \{3, 10, 1, 7\}$
$\vdots$

$0+D_1 = \{2, 3, 11, 10\}$
$1+D_1 = \{3, 4, 12, 11\}$
$2+D_1 = \{4, 5, 0, 12\}$
$\vdots$

$0+D_2 = \{4, 6, 9, 7\}$
$1+D_2 = \{5, 7, 10, 8\}$
$2+D_2 = \{6, 8, 11, 9\}$
$\vdots$