A note on supplementary difference sets

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au
A note on supplementary difference sets

Abstract
Let $S_1, S_2, \ldots, S_n$ be subsets of $G$, a finite abelian group of order $v$, containing $k_1, k_2, \ldots, k_n$ elements respectively. Write $T_i$ for the totality of all differences between elements of $S_i$ (with repetitions), and $T$ for the totality of elements of all the $T_i$. We will denote this by $T = T_1 \& T_2 \& \ldots \& T_n$. If $T$ contains each non-zero element of $G$ a fixed number of times, lambda say, then the sets $S_1, S_2, \ldots, S_n$ will be called $n$-{v; $k_1, k_2, \ldots, k_n$; lambda} supplementary difference sets.

Disciplines
Physical Sciences and Mathematics

Publication Details

This journal article is available at Research Online: https://ro.uow.edu.au/infopapers/957
A Note on Supplementary Difference Sets

JENNIFER WALLIS (Newcastle, New South Wales, Australia)

Let $S_1, S_2, \ldots, S_n$ be subsets of $G$, a finite abelian group of order $v$, containing $k_1, k_2, \ldots, k_n$ elements respectively. Write $T_i$ for the totality of all differences between elements of $S_i$ (with repetitions), and $T$ for the totality of elements of all the $T_i$. We will denote this by $T = T_1 \& T_2 \& \ldots \& T_n$. If $T$ contains each non-zero element of $G$ a fixed number of times, $\lambda$ say, then the sets $S_1, S_2, \ldots, S_n$ will be called $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ supplementary difference sets.

If $k_1 = k_2 = \ldots = k_n = k$ we will write $n - \{v; k; \lambda\}$ to denote the supplementary difference sets. If $k_1 = k_2 = \ldots = k_n$, $k_{i+1} = \ldots = k_n$, then sometimes we write $n - \{v; i; k_1, j; k_{i+1}, \ldots, \lambda\}$. It can be easily seen by counting the differences that the parameters of $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ supplementary difference sets satisfy

$$\lambda(v - 1) = \sum_{j=1}^{n} k_j(k_j - 1).$$

We use braces, $\{\}$, to denote sets and square brackets, $[\ ]$, to denote collections where repetitions may remain.

We now let $v = 4r(2\lambda + 1) + 1 = p^r$, where $p$ is a prime and further let

$$H_i = \{x^{4rj+i} : 0 \leq j \leq 2\lambda\}, \quad i = 0, 1, \ldots, 4r - 1$$

with $x$ a primitive element of $GF(v)$. Write

$$L = H_{2i_1} \cup H_{2i_2} \cup \ldots \cup H_{2i_m}$$

for some $m, 0 < m < 2r$, where the $i_j$ are distinct integers. Now we consider the differences between elements of $H_{2i}$, that is, the collection

$$[x^{4rj+2l} - x^{4r(2\lambda + 1) + 2l} : j \neq l, 0 \leq j, l \leq 2\lambda] = \{x^{4rj + 2l} : 0 \leq j \leq 2\lambda\} \text{ times } [1 - x^{4r(i - j)} : l \neq j, 0 \leq l \leq 2\lambda]$$

and, since any element of a group multiplied onto a coset gives a coset, this expression must represent cosets with certain multiplicities, say $b_k$, write

$$= \sum_{k=0}^{4r-1} b_k H_k,$$

Received December 9, 1971 and in revised form July 13, 1972
where, since \( H_{2l} \) has \( 2\lambda + 1 \) elements, the number of elements in (1) is \( 2\lambda (2\lambda + 1) \) and the number of elements in (2) is \( \sum_{k=0}^{4r-1} b_k (2\lambda + 1) \). So

\[
\sum_{k=0}^{4r-1} b_k = 2\lambda.
\]

Now \( 2\lambda + 1 \) is odd, so \( -1 \in H_{2r} \). Then if \( x^a - x^b \) appears in (1) so does \( x^b - x^a \). Thus whenever an element \( y \) occurs so does \( -y \) and \( y \in H_c \Rightarrow -y \in H_{c+2r} \). Thus \( b_k = b_{k+2r} \).

The differences between elements of \( H_{2l} \) and \( H_{2k} \) are given by the collection

\[
[x^{4rj+2i} - x^{4rl+2k}: 0 \leq j, l \leq 2\lambda] = \{x^{4r(j-i)}: 0 \leq j \leq 2\lambda\} \times \{1 - x^{4r(l-i)}: 0 \leq l \leq 2\lambda\}
\]

\[
= \times \sum_{n=0}^{4r-1} c_n H_n
\]

where \( c_n \) give the multiplicities. By the same reasoning as before,

\[
\sum_{n=0}^{4r-1} c_n = 2\lambda + 1.
\]

Now consider the differences from \( L \), that is

\[
[\text{differences from } H_{2l}; j = 1, 2, \ldots, m] \times \{1 - x^{4r(l-i)}: 0 \leq l \leq 2\lambda\}
\]

and \( [\text{differences from } H_{2l} - H_{2k}; i, j \neq i, k, 0 \leq i, j, k \leq m] \)

\[
= \sum_{k=0}^{4r-1} a_k H_k \quad \text{using (2) and (4).}
\]

Counting elements we see (5) and (6) have \( m(2\lambda + 1) (m(2\lambda + 1) - 1) \) and (7) has \( (2\lambda + 1) \sum_{k=0}^{4r-1} a_k \) elements. Hence

\[
\sum_{k=0}^{4r-1} a_k = m (m(2\lambda + 1) - 1).
\]

Finally, we note that in (6) if \( H_a - H_b \) occurs so does \( H_b - H_a \) so if \( y \) occurs so does \( -y \) and as before we see that

\[
a_k = a_{k+2r}.
\]

Write

\[
w = \sum_{k=0}^{r-1} a_{2k} - \sum_{k=0}^{r-1} a_{2k+1}
\]

\[
z = (w, w + m), \quad s = |w + m|/z, \quad t = |w|/z.
\]
We now show, using \( L \) to construct sets of size \( m(2\lambda + 1) \) and \( m(2\lambda + 1) + 1 \), how to find some supplementary difference sets.

**THEOREM 1.** Let \( v = 4r(2\lambda + 1) + 1 = p^i \), where \( p \) is a prime and \( r = 2^k \). Then \( s \) copies of each of

\[
L_j = x^{2j}L, \quad j = 0, 1, \ldots, r - 1,
\]

and \( t \) copies of each of

\[
K_j = 0 \cup x^{2j+1}L, \quad j = 0, 1, \ldots, r - 1,
\]

where \( s, t \) and \( w \) are given by (9), \( i = 0 \) if \( w \) is negative and \( m > -w \), \( i = 1 \) otherwise, are

\[
rs: \{4r(2\lambda + 1) + 1; \, m(2\lambda + 1) + 1; \, rs: m(2\lambda + 1); \}
\]

supplementary difference sets.

**Proof.** Since \( 2\lambda + 1 \) is always odd, \( -1 \in H_{2r} \), we have from (8) \( a_k = a_{k+2r} \). The totality of differences from

\[
L_j = H_{2l+2j} \cup H_{2l+2j+1} \cup \cdots \cup H_{2lm+2j},
\]

is \( x^{2j} \) times the totality of differences from \( L_0 \) or

\[
\sum_{k=0}^{2r-1} a_{4r-2j+k}H_k = \sum_{k=0}^{2r-1} a_{2r-2j+k}(H_k \cup H_{k+2r}).
\]

So by taking all the differences from \( L_j, j = 0, 1, \ldots, r - 1 \) we have

\[
X = \sum_{i=0}^{2r-1} \left\{ \left( \sum_{k=0}^{r-1} a_{2k} \right) H_{2l+i} \cup \left( \sum_{k=0}^{r-1} a_{2k+1} \right) H_{2l+i+1} \right\}
\]  

\[
= \sum_{i=0}^{2r-1} (\alpha H_{2i} \cup \beta H_{2i+1}).
\]

The totality of differences, then, from the sets

\[
K_j = 0 \cup H_{2l+2j+1} \cup H_{2l+2j+1} \cup \cdots \cup H_{2lm+2j+1}, \quad j = 0, 1, \ldots, r - 1,
\]

is

\[
Z = \sum_{i=0}^{2r-1} (\beta H_{2i} \cup (\alpha + m) H_{2i+1}).
\]

There are four cases to consider:

(i) \( \alpha > \beta \) and \( \beta > \alpha + m \), which is impossible;

(ii) \( \alpha \leq \beta \) and \( \beta \leq \alpha + m \). Here \( w = \alpha - \beta \) is negative and \( m > \beta - \alpha = -w \).
So, if instead of the sets $K_j$ we use the totality of differences from the sets $0 \cup L_j$, then we have the differences

$$Y = \sum_{i=0}^{2r-1} ((x + m) H_{2i} \& \beta H_{2i+1}).$$

Now $s$ times $X$ plus $t$ times $Y$ (where $s$ and $t$ are defined in (9)) gives $(\beta m/z) G$;

(iii) $\alpha < \beta$ and $\beta \geq \alpha + m$; and

(iv) $\alpha > \beta$ and $\beta \leq \alpha + m$.

In these last two cases $s$ times $X$ and $t$ times $Z$ gives

$$(m^2 - \alpha^2 - \alpha m)/z) G \quad \text{and} \quad (\alpha^2 + \alpha m - \beta^2)/z) G$$

respectively.

Then, noting that by summing the elements of $X$ in two ways we find $\alpha + \beta = \frac{1}{2}M(I\lambda + 1) - 1$, we have the result of the theorem.

**EXAMPLE.** With $v=41$, $r=2$, $\lambda=2$, and $m=3$, $w=1$, $s=2$, $t=1$ we find $6 - \{41; 2; 16, 4; 15; 33\}$ supplementary difference sets.

In the theorem the initial set $L$ has been left reasonable undecided but if we choose another initial set.

$$M_j = H_{2j}, H_{2j+1} \cup H_{2j+2} \cup \cdots \cup H_{2j_m+2j} \quad j = 0, 1, \ldots, r - 1$$

where all the $j_a$ are distinct, we may get a different set of supplementary difference sets.

For example: with $v=41$, $r=2$, $\lambda=2$, with $m=2$ and the initial set $H_0 \cup H_2$ we get $w=1$, $s=3$, $t=1$ and hence $8 - \{41; 2; 11, 6; 10; 19\}$ supplementary difference sets, while with the initial set $H_0 \cup H_4$ we get $w=-3$, $s=1$, $t=3$ and hence $8 - \{41; 6; 11, 2; 10; 21\}$ supplementary difference sets.

Finally we note that balanced incomplete block designs may be obtained from supplementary difference sets with two $k$ values by using the results of Jennifer Wallis [2].

**REFERENCES**


University of Newcastle