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 \( k_1 = k_2 = \ldots = k_n \), \( k_{i+1} = k_{i+2} = \ldots = k_{i+j} \), \( i = \ldots = k_n \), 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 \( v = 4r (2\lambda + 1) + 1 = p^7 \), 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

\[
L = H_{2i_0} \cup H_{2i_2} \cup \cdots \cup H_{2i_m}
\]

for some \( m, 0 < m < 2r \), where the \( i_j \) are distinct integers. Now we consider the differences between elements of \( H_{2i_0} \), that is, the collection

\[
\begin{align*}
\{ x^{4rj+2l} - x^{4rl+2l} : j \neq l, 0 \leq j, l \leq 2\lambda \} \\
\{ x^{4rj+2l} : 0 \leq j \leq 2\lambda \} \text{ times } [1 - x^{4rt-j}] : l \neq j, 0 \leq l \leq 2\lambda \\
= H_{2i_0} \text{ times } [1 - x^{4rt-j}] : l \neq j, 0 \leq l \leq 2\lambda 
\end{align*}
\]

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

\[
= \bigcup_{k=0}^{4r-1} b_k H_k,
\]

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 $-1 \in H_{2\lambda}$. 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 $y \in H_\zeta \Rightarrow -y \in H_{\zeta + 2r}$. Thus $b_k = b_{k + 2r}$.

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

$$[x^{4rj + 2l} - x^{4rl + 2k}; 0 \leq j, l \leq 2\lambda]$$

$$= \{x^{4rj + 2l}; 0 \leq j \leq 2\lambda\} \text{ times } \left[1 - x^{4r(\zeta - j) + 2(\zeta - k)}; 0 \leq l \leq 2\lambda\right]$$

$$= H_{2l} \text{ times } \left[1 - x^{4r(\zeta - j) + 2(\zeta - k)}; 0 \leq l \leq 2\lambda\right]$$

$$= \sum_{n=0}^{4r-1} c_n H_\zeta$$

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

$$\text{[differences from } H_{2l}; j = 1, 2, \ldots, m\}$$

$$\& \text{[differences from } H_{2k}; i_j \neq i_k, 0 \leq i_j, i_k \leq m\}$$

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

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 $\nu=4r(2\lambda+1)+1=p^r$, 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

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

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

$$r(s + t) - \{4r(2\lambda+1) + 1\}; \text{rt}: m(2\lambda+1) + 1; \text{rs}: m(2\lambda+1);$$

$$\varphi \left\lceil \frac{m^2(2\lambda+1)(t+s)+m(t-s)}{2} \right\rceil$$

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

$$L_j = H_{2l_i + 2j} \cup H_{2l_i + 2j} \cup \cdots \cup H_{2l_i + 2j}$$

is $x^{2j}$ times the totality of differences from $L_0$ or

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

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

$$X = \sum_{l=0}^{2r-1} \left\lceil \frac{m^2(2\lambda+1)(t+s)+m(t-s)}{2} \right\rceil$$

$$= \sum_{l=0}^{2r-1} (xH_{2l} \cup \beta H_{2l+1}).$$

The totality of differences, then, from the sets

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

is

$$Z = \sum_{l=0}^{2r-1} (\beta H_{2l} \cup (x + m) H_{2l+1}).$$

There are four cases to consider:

(i) $x \geq \beta$ and $\beta \geq x + m$, which is impossible;

(ii) $x \leq \beta$ and $\beta \leq x + m$. Here $w = x - \beta$ is negative and $m > \beta - x = -w$. 


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

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

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

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

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

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

$$((\beta^2 - z^2 - zm)/z) G$$

and

$$((x^2 + zm - \beta^2)/z) G$$

respectively.

Then, noting that by summing the elements of $X$ in two ways we find $x + \beta = \frac{1}{2}m [m(2r + 1) - 1]$, 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,$$M_j = H_{2j_1 + 2} \cup H_{2j_1 + 2} \cup \cdots \cup H_{2j_m + 2} \quad j = 0, 1, \ldots, r - 1$$

where all the $j_k$ 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