A CONSTRUCTION FOR CERTAIN CLASSES OF SUPPLEMENTARY DIFFERENCE SETS

JOAN COOPER

(Received 1 December 1974)

Abstract

Let \( v = ef + 1 \) be a prime power, and consider \( G \) the cyclic group of order \( v - 1 \) with \( e \) cosets \( C_i \) of order \( f \) defined as \( C_i = \{x^j: 0 \leq j \leq f - 1\} \) and \( 0 \leq i \leq e - 1 \), where \( x \) is a primitive element of \( GF(p^e) \) and a generator of \( G \). By using these cosets we give a simple construction for certain classes of Supplementary Difference Sets, Difference Sets, and Szekeres Difference Sets. These classes are not new, but the simple method of construction is original.

By using cosets of the cyclic group \( G \) of order \( v - 1 \) \((v \) a prime power\) we give a simple construction for the following classes of Supplementary Difference Sets, Difference Sets, and Szekeres Difference Sets.

Supplementary Difference Sets
\[
\begin{align*}
\{v; f; f - 1\} & \quad v = ef + 1; \\
\{v; f + 1; f + 1\} & \quad v = ef + 1; \\
\frac{e}{2} - \left\{v; f; \frac{f - 1}{2}\right\} & \quad v = ef + 1, f \text{ odd}; \\
\frac{e}{2} - \left\{v; f + 1; \frac{f + 1}{2}\right\} & \quad v = ef + 1, f \text{ odd}.
\end{align*}
\]

Difference Sets
\[
\begin{align*}
\left(v, f, \frac{f - 1}{2}\right) & \quad v = 2f + 1, f \text{ odd}; \\
\left(v, f + 1, \frac{f + 1}{2}\right) & \quad v = 2f + 1, f \text{ odd}.
\end{align*}
\]

Szekeres Difference Sets
These classes are not new (see Sprott, (1956)), however, the simple method of construction is original.

A set of $k$ residues $D = \{a_1, a_2, \cdots, a_k\}$ modulo $v$ is called a $(v, k, \lambda)$-difference set if among the collection of elements $[a_i - a_j : i \neq j, 1 \leq i, j \leq k]$ each of the non-zero residues occurs precisely $\lambda$ times.

Let $S_1, S_2, \cdots, S_n$ be subsets of $V$, an additive abelian group, containing $c_1, c_2, \cdots, c_n$ 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 he $T_i$. If $T$ contains each non-zero element a fixed number of times, $\lambda$ say, then the sets $S_1, S_2, \cdots, S_n$ will be called $n - \{v; c_1, c_2, \cdots, c_n; \lambda\}$ supplementary difference sets, where $v$ is the order of $V$.

$2 - \{2m + 1; m; m - 1\}$ supplementary difference sets $M$ and $N \in G$, an additive abelian group, are called Szekeres difference sets if $a \in M \Rightarrow -a \notin M$.

We will be using the parameter $v = ef + 1 = p^a$ (a prime power) and the associated cyclic group $G$, of order $v - 1$, which is the multiplicative group of the field $GF(p^a)$. The cosets of $G$ will be defined as

$$C_i = \{x^{\alpha i^j} : 0 \leq j \leq f - 1\} \quad 0 \leq i \leq e - 1,$$

where $\alpha$ is a primitive element of $GF(p^a)$ and a generator of $G$.

The basic concepts of group theory and linear algebra have been assumed, for any reference to group theory see M. Hall Jr. (1959).

We shall be concerned with collections in which repeated elements are counted multiply rather than with sets. If $T_1$ and $T_2$ are two collections (or sets), then $T_1 \cup T_2$ will denote the adjunction of $T_1$ to $T_2$ with total multiplicities retained. We will use square brackets [ ] to denote collections and braces { } to denote sets.

**Example.** Let $S_1 = \{1, 2, x + 1, 2x + 2\}, \ S_2 = \{0, 1, 2, x + 1, 2x + 2\}$ be two sets. Then

$S_1 \cup S_2 = \{0, 1, 1, 2, 2, x + 1, 2x + 2, 2x + 2\}$.

The class product of two collections (or sets) $T_1$ and $T_2$ will be denoted by $T_1 \wedge T_2$ which is defined as

$$T_1 \wedge T_2 = \{x_1 + x_2 : x_1 \in T_1, x_2 \in T_2\}.$$

The transpose of a coset, $C_i^T$, will be defined as $-C_i$ where

$$-C = -\{x^{\alpha i^j} : 0 \leq j \leq f - 1\} = \{-x^{\alpha i^j} : 0 \leq j \leq f - 1\}.$$
In Storer (1967) p. 24 it is shown that

\[ -1 = x^{eq+k} \text{ where } 0 \leq q \leq k - 1 \]

(1)

and \( k = \begin{cases} 
\frac{e}{2} & f \text{ odd} \\
0 & f \text{ even} 
\end{cases} \)

Thus

\[ C_i^T = \{ x^{e(q+j)+i+k} : 0 \leq j \leq f - 1 \}. \]

For proofs of the following four lemmas see Cooper (1972).

**Lemma 1.** If \( C_i \) is a coset of the cyclic group \( G \) then

\[ C_i \wedge C_i^T = \{ x^{e(j+i)+i+k} : 0 \leq j, i \leq f - 1 \} = f\{0\} \wedge \sum_{t=0}^{e-1} a_t C_s \quad a_s \text{ are integer} \]

and

\[ \sum_{t=0}^{e-1} a_t = f - 1. \]

**Lemma 2.** If \( C_i \) and \( C_j \) are cosets of the cyclic group \( G \) then

\[ C_i \wedge C_j = \sum_{t=0}^{e-1} a_t C_s \quad (C_i \neq C_j^T) \]

and

\[ \sum_{t=0}^{e-1} a_t = f. \]

**Lemma 3.** If \( C_i \wedge C_j = \sum_{t=0}^{e-1} a_t C_s \)

then

\[ C_{i+1} \wedge C_{j+1} = \sum_{t=0}^{e-1} a_{s+1} C_s. \]

**Lemma 4.** If \( C_i \) is a coset of \( G \) then

(i) \( C_i^T = C_i \) if \( f \) is even

(ii) \( C_i^T = C_{i+\xi} \) if \( f \) is odd.
[Note: $\epsilon^{-1}_{s=0} C_i = G$.]

We will start by considering the collection of differences between the elements of $C_i$. This collection is given by

\[
\begin{align*}
\{x^{q^s+j} - x^{q^s+t} : 0 \leq j, t \leq f-1, j \neq t \} \\
= \{x^{q^s+j} + (-1)x^{q^s+t} : 0 \leq j, t \leq f-1, j \neq t \} \\
= \{x^{q^s+j} + x^{q^s+k}(x^{q^s+t}) : 0 \leq j, t \leq f-1, j \neq t \} \text{ (from (1))} \\
= \{x^{q^s+j} + x^{q^{(q^s+j)}} + k : 0 \leq j, t \leq f-1, j \neq t \}.
\end{align*}
\]

Now equation (3) corresponds to $C_i \land C_i^T$ (see lemma 1) with the terms that add to zero excluded. Thus the collection of differences between the elements of any coset $C_i$ will be given by

\[
\begin{align*}
\& \in \epsilon^{-1}_{s=0} a, C_i \text{ (where } \sum_{s=0}^{\epsilon^{-1}} a_s = f - 1) \\
(\text{see Lemma 1}).
\end{align*}
\]

We will talk about the collection of differences between elements of any coset $C_i$ in terms of

\[
C_i \land C_i^T = \epsilon^{-1}_{s=0} a, C_i \text{ (terms adding to zero excluded).}
\]

**Theorem 5.** Let $v = ef + 1 = p^\alpha$ (a prime power) and $G$ the associated cyclic group of order $v - 1$. The set of $e$-disjoint cosets from the cyclic group $G$ form $e - \{v; f; f - 1\}$ supplementary difference sets.

**Proof.** The collection of differences from any coset is given by

\[
C_i \land C_i^T = \epsilon^{-1}_{s=0} a, C_i \text{ (terms adding to zero excluded).}
\]

Now the totality of differences from all cosets will be

\[
\begin{align*}
\epsilon^{-1}_{s=0} a, C_i + C_i^T = \epsilon^{-1}_{s=0} \left( \epsilon^{-1}_{s=0} a, C_i \right) \text{ (see Lemma 3)} \\
= \epsilon^{-1}_{s=0} a, C_i + C_i^T \\
= \epsilon^{-1}_{s=0} a, G \\
= (f - 1)G \text{ (see Lemma 1).}
\end{align*}
\]
Thus in the totality of differences from the cosets every non-zero elements occur \((f - 1)\) times and the \(e\) cosets \(C_i\) of order \(f\) form

\[ e - \{v; f; f - 1\} \] supplementary difference sets.

**Lemma 6.** If \(f\) is odd the first \(\frac{1}{2}e\) cosets \(C_0, C_1, \cdots, C_{\frac{1}{2}e - 1}\) form

\[ \frac{e}{2} - \{v; f; \frac{f - 1}{2}\} \] supplementary difference sets.

**Proof.** From the definition of \(C_i^T\) the collection of differences from \(C_i^T\) will be the same as that of \(C_i\).

If \(f\) is odd \(C_i^T = C_{i+\frac{1}{2}}\) (Lemma 4) and

\[ \bigwedge_{i=0}^{\frac{f-1}{2}} C_{i+1} \land C_{i+1}^T = \bigwedge_{i=0}^{\frac{e-1}{2}} C_{i+1} \land C_{i+1}^T. \]

From Theorem 5, \(\bigwedge_{i=0}^{\frac{f-1}{2}} C_{i+1} \land C_{i+1}^T = (f - 1)G\); thus for \(f\) odd

\[ \bigwedge_{i=0}^{\frac{f-1}{2}} C_{i+1} \land C_{i+1}^T = \frac{f - 1}{2} G. \]

**Lemma 7.** If \(v = 2f + 1\) and \(f\) is odd, then \(C_0\) and \(C_1\) form

(a) \(\left(v, f, \frac{f - 1}{2}\right)\) difference sets, and

(b) \(2 - \{v; f; f - 1\}\) Szekeres difference sets.

**Proof.** (a) Immediate from Lemma 6.

(b) As \(f\) is odd, \(C_i^T = C_{i+\frac{1}{2}}\) and \(C_0^T = C_1^T\).

Now if \(a \in C_0\), \(-a \in C_1\), from the definition of Szekeres difference sets, \(C_0\) and \(C_1\) form

\[ 2 - \{v; f; f - 1\} \] Szekeres difference sets.

**Theorem 8.** Let \(v = ef + 1 = p^n\) (a prime power) and \(G\) the associated cyclic group of order \(v - 1\). The \(e\)-sets \(\{0\} \cup C_{i}\)

\[ i = 0, 1, \cdots, e - 1, \] where \(C_i\) are the cosets of \(G_i\), form

\[ e - \{ef + 1; f + 1; f + 1\} \] supplementary difference sets.

**Proof.** From Theorem 5 the collection of differences for any coset is expressed as

\[ \bigwedge_{s=0}^{\frac{e-1}{2}} a_i C_s. \]
It can easily be seen that the differences between the elements of \( C_i \) and \( \{0\} \) will give \( C_i \) and \(-C_i = C_i^T\).

Thus the collection of differences of \( \{0\} \cup C_i \) will be given by

\[
\begin{align*}
&\bigcup_{s=0}^{r-1} a_s C_i \cup C_i \cup C_i^T, \\
&\quad \text{and}
\end{align*}
\]

Now the totality of differences from the set of cosets will be

\[
\begin{align*}
&\bigcup_{s=0}^{r-1} \bigcup_{t=0}^{r-1} \bigcup_{\lambda=0}^{r-1} a_s C_{i+t} \cup C_{i+t} \cup C_{i+t}^T, \\
&\quad \text{and}
\end{align*}
\]

\[
(f-1)G \cup G \cup G = (f+1)G.
\]

As every non-zero element occurs \((f+1)\) times, we have

\[
e - \{v; f+1; f+1\} \text{ supplementary difference sets.}
\]

**Lemma 9.** Let \( v = ef + 1 \) and \( f \) odd, then the sets \( \{0\} \cup C_i, i = 0, 1, \ldots, \frac{f}{2} - 1 \) form

\[
\frac{1}{2}e - \left\{ef + 1; f + 1; \frac{f+1}{2}\right\} \text{ supplementary difference sets.}
\]

The proof is similar to that for Lemma 6 and Theorem 8.

**Lemma 10.** If \( v = 2f + 1 \) and \( f \) is odd then \( \{0\} \cup C_0 \) and \( \{0\} \cup C_1 \) form \( \{v; f+1; (f+1)/(2)\} \) difference sets.

The proof follows from Lemma 9.

**Bibliography**


D. A. Sprott (1956), 'Some series of balanced incomplete block designs', *Sankhya* Ser. A17, 185–192.

