A Generalization of a Result of Newman on Multipliers of Difference Sets

R. L. McFarland

(June 17, 1965)

A theorem of M. Newman states that if \( v, k, \lambda, n \) are the parameters for a difference set \( D \), and \( k - \lambda = p \) or \( 2p \) (\( p \) a prime) then \( p \) is a multiplier of \( D \). This theorem is generalized to the case of an abelian difference set and several consequences are noted.

Key Words: Abelian, multipliers, block designs, difference sets.

1. Introduction

A difference set with parameters \((v, k, \lambda, n)\) is a subset

\[ D = \{d_1, \ldots, d_k\} \]

of \( k \) distinct elements of a (multiplicative) group \( G \) with finite order \( v \), such that every nonidentity element \( g \) in \( G \) can be expressed in exactly \( \lambda \) ways as

\[ d_i^{-1}d_j = g, \quad 1 \leq i, j \leq k. \]

The parameter \( n \) is defined by

\[ n = k - \lambda. \]

Counting the total number of nonidentity “differences,” \( d_i^{-1}d_j \), in two ways yields

\[ k(k - 1) = \lambda(v - 1). \quad (1) \]

The difference set \( D \) is said to be abelian (cyclic) in case the group \( G \) is abelian (cyclic). The exponent, \( v^* \), of the difference set \( D \) is the least common multiple of the orders of the elements of \( G \). An integer \( t \) is a multiplier of the difference set

\[ D = \{d_1, \ldots, d_k\} \]

in case the sets

\[ D(t) = \{d_t^1, \ldots, d_t^k\} \]

\[ gD = \{gd_1, \ldots, gd_k\} \]

are identical, apart from order, for some group element \( g \) in \( G \).

Newman [5] has proved the following result.

**Theorem 1.** Let \( D \) be a cyclic difference set with parameters \((v, k, \lambda, n)\). Suppose

\[ n = 2p, \quad (7p, v) = 1 \]

where \( p \) is a prime. Then \( p \) is a multiplier of \( D \).

Theorem 1 can be generalized in two ways. First of all, it can be generalized to abelian difference sets. Secondly, as H. B. Mann has pointed out, theorem 1 can be combined with the following multiplier theorem.

**Theorem 2.** Let \( D \) be an abelian difference set with parameters \((v, k, \lambda, n)\) and exponent \( v^* \). Suppose

\[ n_1 \mid n, \quad (n_1, v) = 1, \quad n_1 > \lambda, \quad n_1 = p_1^{f_1} \cdots p_s^{f_s} \]

where the \( p_i \) are distinct primes. If there exist integers \( f_1, \ldots, f_s \) such that

\[ t = p_1^{f_1} \cdots p_s^{f_s} \pmod{v^*} \]

then \( t \) is a multiplier of \( D \).

Theorem 2 was proven for cyclic difference sets by Hall [2]. It was generalized to abelian difference sets by Menon [4]. More recently, Mann [3] has given another proof of theorem 2.

These two generalizations of theorem 1 yield:

**Theorem 3.** Let \( D \) be an abelian difference set with parameters \((v, k, \lambda, n)\) and exponent \( v^* \). Suppose

\[ n = 2n_1, \quad (7n_1, v) = 1, \quad n_1 = p_1^{f_1} \cdots p_s^{f_s} \]

where the \( p_i \) are distinct primes. If there exist integers \( f_1, \ldots, f_s \) such that

\[ t = p_1^{f_1} \cdots p_s^{f_s} \pmod{v^*} \]

then \( t \) is a multiplier of \( D \).

---

1 Present address: 6970th Support Group, Fort George Meade, Maryland. 20755.
2 Figures in brackets indicate the literature references at the end of this paper.
A special case of theorem 3 is worthy of note.

**Corollary.** Let $D$ be an abelian difference set with parameters $(v, k, \lambda, n)$. If

$$n = 2p^e, \quad e \geq 1, \quad (7p, v) = 1$$

where $p$ is a prime, then $p$ is a multiplier of $D$.

This paper is devoted to the proof of theorem 3.

## 2. Preparatory Lemmas

Let $R_G$ denote the group ring of the finite multiplicative abelian group $G$ over the rational integers. The elements of $R_G$ are of the form

$$\sum_{g \in G} a_g g$$

where the coefficients $a_g$ are integral. Addition in $R_G$ is component addition of the coefficients

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g.$$

Multiplication in $R_G$ is the usual multiplication in an associative algebra with basis consisting of the elements of $G$

$$\left( \sum_{g \in G} a_g g \right) \left( \sum_{g \in G} b_g g \right) = \sum_{h \in G} \sum_{g \in G} a_g b_h g.$$

No confusion will result if we let $G$ denote the element

$$G = \sum_{g \in G} g$$

in $R_G$, that has every coefficient equal to one. Similarly, if the difference set $D$ in $G$ consists of the $k$ elements $d_1, \ldots, d_k$ we shall write $D$ to denote the element

$$D = d_1 + \cdots + d_k$$

in $R_G$. For any integer $t$ and any group element $g$ we define

$$D(t) = d_1 t + \cdots + d_k t$$

$$tD = td_1 + \cdots + td_k$$

$$gD = gd_1 + \cdots + gd_k.$$

The definition of a difference set implies that

$$D(-1)D = n + \lambda G$$

(2)

where we have suppressed the identity element of $G$ on $n$. Also

$$DG = kG.$$  

(3)

The integer $t$ is a multiplier of the difference set $D$ if and only if

$$D(t) = gD$$

(4)

for some $g$ in $G$.

**Lemma 1.** Let $D$ and $D^*$ be difference sets with parameters $(v, k, \lambda, n)$ in the same group $G$. Let

$$F = D(-1)D^* - \lambda G.$$

Then

(i) $FG = nG$

(ii) $F(-1)F = n^2$

(iii) $FD = nD^*$.

If $F$ has nonnegative coefficients, then

$$gD = D^*$$

as desired.

**Proof.** Parts (i), (ii), and (iii) can be verified by straightforward computations using eqs (1), (2), and (3). If $F$ has nonnegative coefficients, then part (ii) implies that $F$ has exactly one nonzero coefficient, say

$$F = ng, \quad g \in G.$$

Then part (iii) implies that

$$gD = D^*$$

as desired.

**Lemma 2.** Let $G$ be a finite abelian group with order $v$ prime to 2 and 7. Let $E$ be an element in the group ring $R_G$ such that

(i) $EG = 2G$

(ii) $E(-1)E = 4$.

Then $E$ has nonnegative coefficients.

**Proof.** Let

$$E = \sum_{g \in G} a_g g$$

with $a_g$ integral. Hypothesis (i) implies

$$\sum_{g \in G} a_g = 2$$

(5)

while hypothesis (ii) implies

$$\sum_{g \in G} a_g^2 = 4$$

(6)

and

$$\sum_{g \in G} a_g a_{g^{-1}} = 0, \quad h \neq 1.$$  

(7)
Assume that \( E \) has a negative coefficient. Then eqs (5) and (6) imply that \( E \) has one coefficient equal to minus one, three coefficients equal to plus one, and the remaining coefficients zero. Thus

\[
E = -w + x + y + z
\]  

(8)

for distinct group elements \( w, x, y, z \) in \( G \). Letting \( h = w^{-1}x, w^{-1}y, w^{-1}z \) in eq (7) we obtain either two or four nonzero terms in the left-hand sum. Suppose four nonzero terms occur for \( h = w^{-1}x \). Then there are exactly three possibilities, namely

\[
h = w^{-1}x = x^{-1}w = y^{-1}z = z^{-1}y \\
h = w^{-1}x = x^{-1}y = y^{-1}z = z^{-1}w \\
h = w^{-1}x = x^{-1}z = y^{-1}w = z^{-1}y.
\]

In each of these three possibilities, \( h^4 = 1 \). Thus \( h = 1 \), since \( v \) is odd; a contradiction. Therefore, by symmetry among \( x, y, z \), we conclude that exactly two nonzero terms occur in eq (7) for \( h = w^{-1}x, w^{-1}y, w^{-1}z \). Now eq (7) implies that there are four possible values for each of \( w^{-1}x, w^{-1}y, w^{-1}z \).

\[
\begin{align*}
& w^{-1}x = x^{-1}y, x^{-1}z, y^{-1}z, z^{-1}y \\
& w^{-1}y = x^{-1}z, y^{-1}x, y^{-1}z, z^{-1}x \\
& w^{-1}z = x^{-1}y, y^{-1}x, z^{-1}x, z^{-1}y.
\end{align*}
\]

We shall use the symbol "\( \Leftrightarrow \)" to indicate that a contradiction has been obtained.

**Case 1:** \( w^{-1}x = x^{-1}y \).

**Case 1a:** \( w^{-1}x = x^{-1}y, w^{-1}z = x^{-1}y \).

Then \( x^2 = wy = xz \Rightarrow x = z \Leftrightarrow \).

**Case 1b:** \( w^{-1}x = x^{-1}y, w^{-1}z = y^{-1}x \).

Then \( w^{-1}x = x^{-1}y = z^{-1}w \) so eq (7) contains more than two nonzero terms \( \Leftrightarrow \). 

**Case 1c:** \( w^{-1}x = x^{-1}y, w^{-1}z = z^{-1}y \).

Then \( x^2 = wy = z^2 \Rightarrow x = z \Leftrightarrow \).

**Case 1d:** \( w^{-1}x = x^{-1}y, w^{-1}z = z^{-1}x \).

Applying the permutation \( x \rightarrow z, y \rightarrow x, z \rightarrow y \) to Cases 1a, 1b, 1c we see that \( w^{-1}z = z^{-1}x \) implies \( w^{-1}y \neq z^{-1}x, x^{-1}z, y^{-1}x \). Therefore \( w^{-1}x = x^{-1}y \) implies that \( w^{-1}z = x^{-1}x \) and \( w^{-1}y = y^{-1}z \). Eliminating \( w^{-1} \) among these three equations yields \( x^{2}y = y^{2}z = z^{-1}x \). Now eliminating an appropriate power of \( x \) yields \( y^2 = z^2 \). Thus \( y = z \), since \( (v, 7) = 1 \); a contradiction. Therefore Case 1 is impossible. By the symmetry among \( x, y, z \) we have

\[
\begin{align*}
w^{-1}x & \neq x^{-1}y, x^{-1}z \\
w^{-1}y & \neq y^{-1}z, y^{-1}x \\
w^{-1}z & \neq z^{-1}x, z^{-1}y.
\end{align*}
\]

Thus there are eight possibilities remaining, namely

\[
\begin{align*}
w^{-1}x &= y^{-1}z, z^{-1}y \\
w^{-1}y &= x^{-1}z, z^{-1}x \\
w^{-1}z &= x^{-1}y, y^{-1}x.
\end{align*}
\]

By the symmetry between \( y \) and \( z \) we can assume

\[
w^{-1}x = y^{-1}z.
\]

Either \( w^{-1}z = x^{-1}y \), or else \( w^{-1}z = y^{-1}x \). In the first case

\[
w^{-1}x = y^{-1}z = x^{-1}z = w^{-1}x \Rightarrow w^2 = x^2 \Rightarrow w = x \Leftrightarrow,
\]

while in the second case

\[
w^{-1}y = x^{-1}z = w^{-1}y \Rightarrow w^2 = y^2 \Rightarrow w = y \Leftrightarrow.
\]

We have now exhausted all possibilities. Therefore \( E \) cannot have a negative coefficient, and the proof is complete.

**Lemma 3.** Let \( D \) be an abelian difference set with parameters \( (v, k, \lambda, n) \) in the group \( G \). Let \( p \) be a prime such that

\[
p \mid n, \quad (p, v) = 1.
\]

Then for every integer \( f \), the coefficients of

\[
F = D(-1)D(p^f) - \lambda G
\]

are divisible by \( p^f \).

**Proof.** Lemma 3 appears as a part of the proof of corollary 4.1 of Mann [3]. Alternatively, lemma 3 is a special case of eq (3.9) of Menon [4].

### 3. Theorem

**Theorem 3.** Let \( D \) be an abelian difference set with parameters \( (v, k, \lambda, n) \) and exponent \( v^k \). Suppose

\[
n = 2n_1, \quad (7n_1, v) = 1, \quad n_1 = p_1^{f_1} \cdots p_k^{f_k}
\]

where the \( p_i \) are distinct primes. If there exist integers \( f_1, \ldots, f_k \) such that

\[
t = p_1^{f_1} = \cdots = p_k^{f_k} \pmod{v^k}
\]

then \( t \) is a multiplier of \( D \).

**Proof.** If \( D \) is a difference set in the group \( G \), then \( G - D \) is also a difference set. Clearly any multiplier of \( D \) is also a multiplier of \( G - D \). Furthermore, one of these difference sets has \( \lambda > n \). Consequently, if \( n_1 \) is even, then theorem 3 is a special case of theorem 2. Now assume \( n_1 \) is odd. Then \( n = 2n_1 \) is not a square. In this case it is well known (e.g. theorem 3 of Chowla and Ryser [1]) that \( v \) is odd.
Let

\[ F = D(-1)D(t) - \lambda G. \]

Since

\[ D(p^i) = D(t), \quad (i = 1, \ldots, s), \]

lemma 3 implies that the coefficients of \( F \) are divisible by \( n_1 \). Let

\[ E = n_1^{-1}F. \]

Parts (i) and (ii) of lemma 1 imply that \( E \) satisfies the hypotheses (i) and (ii) of lemma 2. Therefore \( E \), and consequently \( F \), has nonnegative coefficients. Then by lemma 1,

\[ gD = D(t) \]

for some group element \( g \). Thus \( t \) is a multiplier of \( D \).

4. References