JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematics and Mathematical Physics
Vol. 69B, No. 4, October–December 1965

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

R. L. McFarland [1]

(June 17, 1965)

A theorem of M. Newman states that if v, k, λ, 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, λ, 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 λ ways as

$$d_i^{-1}d_j=g, \qquad 1 \leqq i, j \leqq k.$$

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

$$k(k-1)=\lambda(v-1). \tag{1}$$

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

$$D(t)=\{d_1^t, \ldots, d_k^t\}$$

$$gD=\{gd_1, \ldots, gd_k\}$$

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

Newman [5][2] has proved the following result.

THEOREM 1. *Let* D *be a cyclic difference set with parameters* (v, k, λ, n). *Suppose*

$$n=2p, \ (7p, v)=1$$

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, λ, n) *and exponent* v*. *Suppose*

$$n_1|n, \qquad (n_1, v)=1, \qquad n_1>\lambda, \qquad n_1=p_1^{e_1}\cdots p_s^{e_s}$$

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

$$t \equiv p_1^{f_1} \equiv \cdots \equiv p_s^{f_s} (\mathrm{mod}\ v^*)$$

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, λ, n) *and exponent* v*. *Suppose*

$$n=2n_1, \qquad (7n_1, v)=1, \qquad n_1=p_1^{e_1}\ldots p_s^{e_s}$$

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

$$t \equiv p_1^{f_1} \equiv \cdots \equiv p_s^{f_s} \ (\mathrm{mod}\ v^*)$$

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, λ, n). *If*

$$n=2p^e, \qquad e \geqq 1, \qquad (7p, v)=1$$

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

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

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

$$\sum_g a_g g + \sum_g b_g g = \sum_g (a_g+b_g)g.$$

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

$$\left(\sum_g a_g g\right)\left(\sum_{\bar{g}} b_{\bar{g}}\bar{g}\right)=\sum_h h \sum_{g\bar{g}=h} a_g b_{\bar{g}}.$$

No confusion will result if we let G denote the element

$$G=\sum_g g$$

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

$$D(-1)D=n+\lambda G \tag{2}$$

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

$$DG=kG. \tag{3}$$

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

$$D(t)=gD \tag{4}$$

for some g in G.

LEMMA 1. *Let* D *and* D* *be difference sets with parameters* (v, k, λ, 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*

$$gD=D^*$$

for some g *in* G.

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

$$F=ng, \qquad g\epsilon G.$$

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

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

with a_g integral. Hypothesis (i) implies

$$\sum_g a_g=2 \tag{5}$$

while hypothesis (ii) implies

$$\sum_g a_g^2=4 \tag{6}$$

and

$$\sum_{g^{-1}\bar{g}=h} a_g a_{\bar{g}}=0, \qquad h\neq 1. \tag{7}$$

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

$$E=-w+x+y+z \tag{8}$$

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 $w^{-1}x$, $w^{-1}y$, $w^{-1}z$.

$$w^{-1}x=x^{-1}y,\ x^{-1}z,\ y^{-1}z,\ z^{-1}y$$
$$w^{-1}y=x^{-1}z,\ y^{-1}x,\ y^{-1}z,\ z^{-1}x$$
$$w^{-1}z=x^{-1}y,\ y^{-1}x,\ z^{-1}x,\ z^{-1}y$$

We shall use the symbol "$\nLeftrightarrow$" to indicate that a contradiction has been obtained.

Case I: $w^{-1}x=x^{-1}y$.

Case $\mathrm{I_A}$: $w^{-1}x=x^{-1}y$, $w^{-1}z=x^{-1}y$.

Then $x^2=wy=xz \Rightarrow x=z \nLeftrightarrow$.

Case $\mathrm{I_B}$: $w^{-1}x=x^{-1}y$, $w^{-1}z=y^{-1}x$.

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

Case $\mathrm{I_C}$: $w^{-1}x=x^{-1}y, w^{-1}z=z^{-1}y$.

Then $x^2=wy=z^2 \Rightarrow x=z \nLeftrightarrow$.

Case $\mathrm{I_D}$: $w^{-1}x=x^{-1}y$, $w^{-1}z=z^{-1}x$.

Applying the permutation $x\rightarrow z$, $y\rightarrow x$, $z\rightarrow y$ to Cases $\mathrm{I_A}$, $\mathrm{I_B}$, $\mathrm{I_C}$ 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 $w^{-1}z=z^{-1}x$ and $w^{-1}y=y^{-1}z$. Eliminating w^{-1} among these three equations yields $x^{-2}y=y^{-2}z=z^{-2}x$. Now eliminating an appropriate power of x yields $y^7=z^7$. Thus $y=z$, since $(v, 7)=1$; a contradiction.

Therefore Case I is impossible. By the symmetry among x, y, z we have

$$w^{-1}x\neq x^{-1}y,\ x^{-1}z$$
$$w^{-1}y\neq y^{-1}z,\ y^{-1}x$$
$$w^{-1}z\neq z^{-1}x,\ z^{-1}y.$$

Thus there are eight possibilities remaining, namely

$$w^{-1}x=y^{-1}z,\ z^{-1}y$$
$$w^{-1}y=x^{-1}z,\ z^{-1}x$$
$$w^{-1}z=x^{-1}y,\ y^{-1}x.$$

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

$$w^{-1}x=y^{-1}z=wx^{-1} \Rightarrow w^2=x^2 \Rightarrow \mathrm{w}=x \nLeftrightarrow,$$

while in the second case

$$w^{-1}y=x^{-1}z=wy^{-1} \Rightarrow w^2=y^2 \rightarrow w=y \nLeftrightarrow.$$

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, λ, n) *in the group* G. *Let* p *be a prime such that*

$$\mathrm{p^e}|\mathrm{n}, \qquad (\mathrm{p}, \mathrm{v})=1.$$

Then for every integer f, *the coefficients of*

$$\mathrm{F}=\mathrm{D}(-1)\mathrm{D}(\mathrm{p^f})-\lambda\,\mathrm{G}$$

are divisible by $\mathrm{p^e}$.

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, λ, n) *and exponent* v*. *Suppose*

$$\mathrm{n}=2\mathrm{n}_1, \qquad (7\mathrm{n}_1, \mathrm{v})=1, \qquad \mathrm{n}_1=\mathrm{p}_1^{\mathrm{e}_1}\cdots \mathrm{p}_s^{\mathrm{e}_s}$$

where the $\mathrm{p_i}$ *are distinct primes. If there exist integers* $\mathrm{f}_1, \ldots, \mathrm{f_s}$ *such that*

$$\mathrm{t}\equiv \mathrm{p}_1^{\mathrm{f}_1}\equiv\cdots\equiv \mathrm{p}_s^{\mathrm{f}_s}\ (\mathrm{mod}\ \mathrm{v}^*)$$

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

$$D(p_i^{f_i}) = D(t), \qquad (i = 1, \ldots, s),$$

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

[1] S. Chowla and H. J. Ryser, Combinatorial problems, Can. J. Math. **2,** 93–99 (1950).

[2] Marshall Hall, Jr., A survey of difference sets, Proc. Amer. Math. Soc. **7,** 975–986 (1956).

[3] H. B. Mann, Balanced incomplete block designs and abelian difference sets, Ill. J. Math. **8,** 252–261 (1964).

[4] P. Kesava Menon, Difference sets in abelian groups, Proc. Amer. Math. Soc. **11,** 368–376 (1960).

[5] Morris Newman, Multipliers of difference sets, Can. J. Math. **15,** 121–124 (1963).

(Paper 69B4–161)