RELATIVE DIFFERENCE SETS[1]

BY

J. E. H. ELLIOTT AND A. T. BUTSON

1. Introduction

DEFINITION 1.1. A set R of k elements in a group G of order mn is a *difference set of G relative to a normal subgroup H* of order $n \neq mn$ if the collection of differences $r - s$; $r, s \in R$, $r \neq s$ contains only the elements of G which are not in H, and contains every such element exactly d times.

This "relative difference set" will be denoted by $R(m, n, k, d)$. It is to be understood that $R(m, n, k, d)$ is in a group G of order mn relative to a normal subgroup H of order n unless the group and normal subgroup are specified explicitly.

If $n = 1$, R is an ordinary difference set with parameters (m, k, d), and this will be denoted by $D(m, k, d)$.

Difference sets in a cyclic group have been studied extensively by such authors as Marshall Hall [5], E. Lehmer [6], and H. B. Mann [7] to name only very few, and more recently this concept has been extended to an arbitrary group by R. H. Bruck [1], H. B. Mann [8], and P. Kesava Menon [10].

The concept of a relative difference set was introduced by A. T. Butson [2]. He considered the cyclic group, and obtained a class of cyclic relative difference sets. He also gave a necessary condition for the existence of cyclic $R(m, n, k, d)$.

In this paper, we consider relative difference sets in an arbitrary group. We first show that the existence of an $R(m, n, k\ d)$ implies the existence of a $D(m, k, \lambda)$ where $\lambda = nd$; and, in this case, the $R(m, n, k, d)$ will be called an extension of the $D(m, k, \lambda)$.

In Sections 3 and 4, $R(p^N, p, p^N, p^{N-1})$ and $R(p^{2N}, p^2, p^{2N}, p^{2N-2})$ are constructed in an elementary Abelian p-group, where p is an odd prime. In the elementary Abelian 2-group, two classes of $R(2^{2N}, 2, 2^{2N}, 2^{2N-1})$ are constructed. It will be shown in Section 6 that a relative difference set in an elementary Abelian 2-group is, necessarily, an $R(2^{2N}, 2^s, 2^{2N}, 2^{2N-s})$, (unless it is an $R(2^6, 2, 36, 10)$).

For cyclic groups, we are able to enlarge the class described in [2]. We also show, in direct contrast to the situation in elementary Abelian groups, that no cyclic $R(m, n, m, d)$, $nd = m$, $n > 1$, $m > 2$, exists.

In Section 7, we prove a "Multiplier Theorem" for relative difference sets. The proof generalizes H. B. Mann's proof of Marshall Hall's "Multiplier Theorem" for difference sets. In Section 8, further results for multipliers

---

Received June 3, 1965.

[1] This research was sponsored by a National Science Foundation grant.

are established; and, finally, in Section 9, it is shown that no

$$R(p^r = 4t - 1, t - 1, 2t - 1, 1),$$

extensions of the quadratic residue difference sets, can exist.

2. Preliminary results

THEOREM 2.1. *If R is an $R(m, n, k, d)$ and if σ is a homomorphism of G onto $\sigma(G)$ with kernel $K \subseteq H$, then $\sigma(R)$ is an $R(m, s, k, td)$ of $\sigma(G)$ relative to $\sigma(H)$, where $n = ts$, and t is the order of K.*

To see this, let $g \in G$ and $g \notin H$. Then there exist exactly td pairs $r, s \in R$ such that $\sigma(g) = \sigma(r) - \sigma(s)$; and, since $K \subseteq H$, $\sigma(r) \neq \sigma(s)$. If $g \in H$ and $\sigma(g) = \sigma(r) - \sigma(s)$ for some $r, s \in R$, then clearly $r = s$, and thus the theorem is proved.

COROLLARY 2.1.1. *If L is a normal subgroup of G of order t, and $L \subseteq H$, then the existence of an $R(m, n, k, d)$ implies the existence of an $R(m, s, k, td)$, where $ts = n$, in G/L relative to H/L.*

This is clear if we let the homomorphism of Theorem 2.1 be the natural map of G onto G/L.

Due to its importance, the special case in which $L = H$ is stated separately.

COROLLARY 2.1.2. *The existence of an $R(m, n, k, d)$ implies the existence of a $D(m, k, \lambda)$ in G/H, where $\lambda = nd$.*

Corollary 2.1.2 suggests the following definition.

DEFINITION 2.1. If an $R = R(m, n, k, d)$ maps onto a $D(m, k, \lambda)$ under the natural map of G onto G/H, and if $R \neq D$, then R *is called an extension of D.*

Thus, in the search for $R(m, n, k, d)$ and in attempting to prove their non-existence, particular attention is paid to those $R(m, n, k, d)$ which are extensions of well-known $D(m, k, \lambda)$.

It follows immediately from Corollary 2.1.2 that

$$k(k - 1) = (m - 1)nd, \tag{2.1}$$

$$k \leq m. \tag{2.2}$$

We may not, however, assume that $2k \leq m$; since, unlike a $D(m, k, \lambda)$, the complement of an $R(m, n, k, d)$ is not necessarily an $R(m', n', k', d')$. Indeed, we have the result below.

THEOREM 2.2. *The complement in G of an $R(m, n, k, d)$, $n > 1$, is an $R(m', n', k', d')$ if and only if $n = 2$ and $m = k$.*

To show this, let $R = R(m, n, k, d)$. If $g \in G$, and $g \notin H$, then, for exactly mn pairs of elements $g_1, g_2 \in G$, $g = g_1 - g_2$. For exactly k of these pairs

$g_1 \in R$, and for exactly d pairs $g_1 \in R$ and $g_2 \in R$. Thus, for exactly $k - d$ pairs $g_1 \in R$ and $g_2 \notin R$. Hence $g_1 \notin R$ and $g_2 \notin R$ for exactly $nm - 2k + d$ pairs.

If $g \in H$, and $g \neq 0$, then for exactly mn pairs $g_1, g_2 \in G$, $g = g_1 - g_2$. For exactly k of these pairs $g_1 \in R$, which implies that $g_2 \notin R$; and, for exactly k pairs $g_2 \in R$, which similarly implies that $g_1 \notin R$. Thus $g \in H$, $g \neq 0$, can be expressed as a difference of two elements neither of which is in R, in exactly $mn - 2k$ ways.

For $m = k$, and $n = 2$, therefore, if $g \in H$, $g \neq 0$, g cannot be expressed as a difference of two elements of the complement of R; and if $g \notin H$, then g is expressed as such a difference in $mn - 2k + d$ ways.

Conversely, if the complement of R is an $R(m', n', k', d')$, it must necessarily be defined relative to the subgroup H, since $mn - 2k + d \neq mn - 2k$. Therefore, $mn = 2k$. By equation (2.2), $m \geq k$, and $n > 1$; and, thus, $n = 2$ and $m = k$, giving the required result.

If $G = \{g_1, g_2, \cdots, g_{mn}\}$, and if the elements are so arranged that

$$g_i + H = \{g_i, g_{i+m}, \cdots, g_{i+(n-1)m}\}$$

for $i = 1, 2, \cdots, m$, we may consider the $mn \times mn$ incidence matrix A of $R = R(m, n, k, d)$ defined by $a_{ij} = 1$, if $g_j \in g_i + R$, $a_{ij} = 0$ otherwise. Then

$$AA^T = A^TA = kI_{mn} + dJ_{mn} - d(I_m \otimes J_n),$$

where I_u is the $u \times u$ unit matrix, J_u the $u \times u$ matrix each of whose entries is one, and $\otimes$ denotes the left Kronecker product. Thus

$$(\det A)^2 = k^{m(n-1)+2}(k - nd)^{m-1}. \tag{2.3}$$

This proves the theorem below, which generalizes the known result for a $D(m, k, \lambda)$.

THEOREM 2.3. *If an $R(m, n, k, d)$ exists, then* (i) *if m is even, $k - nd$ is a square*; (ii) *if m is odd, and n is even, k is a square.*

3. Construction of relative difference sets in an elementary Abelian p-group, where p is an odd prime

The symbol $\oplus$ will be used to express the direct sum, A_p will denote the additive group of integers modulo p, and throughout this section, p will be an odd prime. We will denote by G_N the elementary Abelian p-group of order p^N, with identity $\mathbf{0}$, whose elements are expressed as N-tuples of elements of A_p.

THEOREM 3.1. *Let $G = A_p \oplus G_N$ and let $H = A_p \oplus \{\mathbf{0}\}$. If the rational integer $a_i \not\equiv 0 \pmod p$, for $i = 1, \cdots, N$, then*

$$R = \{(f(n), n); n = (n_1, n_2, \cdots, n_N) \in G_N\},$$

where $f(n) \equiv \sum_{i=1}^N a_i n_i^2 \pmod p$, is an $R(p^N, p, p^N, p^{N-1})$ of G relative to H.

To obtain this result, let $r(n) = (f(n), n)$, and

$$(a, g) = (a, g_1, \cdots, g_N) \in G,$$

where $(a, g) \notin H$. Then $(a, g) = r(n + g) - r(n)$ if and only if

$$a \equiv \sum_{i=1}^{N} \{2a_i n_i g_i + a_i^2 g_i^2\} \pmod p. \tag{3.1}$$

Now there exists $g_i \not\equiv 0 \pmod p$ for some i, $1 \leq i \leq N$. Therefore, choose n_j, $j = 1, \cdots, i-1, i+1, \cdots, N$ arbitrarily from A_p. Since $g_i \not\equiv 0 \pmod p$, for each such choice, there is a value of n_i in A_p satisfying equation (3.1).

Thus (a, g) can be expressed as a difference of two elements of R in exactly p^{N-1} ways.

Clearly, no element of H other than the identity can be expressed as such a difference.

COROLLARY 3.1.1. *Corresponding to each $R(p^N, p, p^N, p^{N-1})$ of the theorem, there exists an $R(p^N, p, p^N, p^{N-1})$ of G relative to any subgroup of order p.*

This result follows immediately from Theorem 2.1.

THEOREM 3.2. *Let $G = A_p \oplus A_p \oplus G_{2N}$, and $H = A_p \oplus A_p \oplus \{\mathbf{0}\}$. Let a_i be a quadratic residue modulo p for $i = 2, 4, \cdots, 2N$, and a quadratic non-residue modulo p for $i = 1, 3, \cdots, 2N - 1$. Then*

$$R = \{(f(n), h(n), n); n = (n_1, \cdots, n_{2N}) \in G_{2N}\},$$

where $f(n) \equiv \sum_{i=1}^{2N} a_i n_i^2 \pmod p$ and $h(n) \equiv \sum_{i=1}^{N} n_{2i-1} n_{2i} \pmod p$, is an $R(p^{2N}, p^2, p^{2N}, p^{2N-2})$ of G relative to H.

To obtain this result, let $r(n) = (f(n), h(n), n)$. If $(a, b, g) \in G$, and $(a, b, g) \notin H$, where $g = (g_1, \cdots, g_{2N}) \in G_{2N}$, then $(a, b, g) = r(n + g) - r(n)$ if and only if

$$a \equiv \sum_{i=1}^{2N} \{2a_i n_i g_i + a_i g_i^2\} \pmod p \tag{3.2}$$

and

$$b \equiv \sum_{i=1}^{N} \{g_{2i-1} n_{2i} + g_{2i} n_{2i-1} + g_{2i-1} g_{2i}\} \pmod p. \tag{3.3}$$

Some coordinate of g is non-zero, so suppose it is one of the pair g_{2i-1}, g_{2i}. Then choose n_j, $j = 1, 2, \cdots, 2i - 2, 2i + 1, \cdots, 2N$, arbitrarily in A_p. For each such choice, the conditions of the theorem ensure solutions for n_{2i-1} and n_{2i}, unique modulo p, satisfying (3.2) and (3.3). Hence $(a, b, g) \notin H$ can be expressed as a difference of two elements of R in p^{2N-2} ways, and $(a, b, \mathbf{0})$ clearly cannot be so expressed unless $a = b = 0$, completing the proof of this theorem.

Theorem 2.1 immediately implies the following corollaries.

COROLLARY 3.2.1. *The set*

$$R' = \{(h(n), n); n \in G_{2N}\}$$

is an $R(p^{2N}, p, p^{2N}, p^{2N-1})$ in $A_p \oplus G_{2N}$ relative to $A_p \oplus \{\mathbf{0}\}$.

COROLLARY 3.2.2. *There exist* $R(p^{2N}, p^2, p^{2N}, p^{2N-2})$ *in* $A_p \oplus A_p \oplus G_{2N}$ *relative to any subgroup of order* p^2, *and there exist* $R(p^{2N}, p, p^{2N}, p^{2N-1})$ *in* $A_p \oplus G_{2N}$ *relative to any subgroup of order* p.

Relative difference sets similar to those of Corollary 3.2.1 may be constructed in $A_p \oplus G_{2N+1}$. This result is stated in the theorem below, the proof of which is entirely similar to that of Theorem 3.1.

THEOREM 3.3. *Let* $G = A_p \oplus G_{2N+1}$, *and let* $H = A_p \oplus \{\mathbf{0}\}$; *then*

$$R = \{(f(n), n); n = (n_1, \cdots, n_{2N+1}) \in G_{2N+1}\},$$

where

$$f(n) \equiv \textstyle\sum_{i=1}^{N} (n_{2i-1} n_{2i} + n_{2N+1}^2) \pmod p,$$

is an $R(p^{2N+1}, p, p^{2N+1}, p^{2N})$ *of* G *relative to* H.

Again, appropriate isomorphisms give $R(p^{2N+1}, p, p^{2N+1}, p^{2N})$ *of* G *relative to any subgroup of order* p.

4. Construction of relative difference sets in an elementary Abelian 2-group

In this section, K_N will denote the elementary Abelian 2-group of order 2^N whose elements are N-tuples of elements of A_2, the additive group of integers modulo 2. The identity of K_N will be denoted by $\mathbf{0}$.

THEOREM 4.1. *Let* $G = A_2 \oplus K_{2N}$, $H = A_2 \oplus \{\mathbf{0}\}$, *and*

$$M = \{g = (g_1, \cdots, g_{2N}) \in K_{2N}; \quad \textstyle\sum_{i=1}^{2N} g_i \equiv 0 \quad or \quad 1 \pmod 4\}.$$

Then

$$R = \{(0, g); g \in M\} \cup \{(1, g); g \in K_{2N}, g \notin M\}$$

is an $R(2^{2N}, 2, 2^{2N}, 2^{2N-1})$ *of* G *relative to* H.

To prove this, it is first noted that M is a Menon

$$D(2^{2N}, 2^{2N-1} \pm 2^{N-1}, 2^{2N-2} \pm 2^{N-1}),$$

[10]. The complement of M in K_{2N} is, therefore, a

$$D(2^{2N}, 2^{2N-1} \mp 2^{N-1}, 2^{2N-2} \mp 2^{N-1}).$$

Thus, if $(0, g) \in G, g \neq \mathbf{0}$, then $(0, g) = (0, a) - (0, b)$, for exactly $2^{2N} \pm 2^{N-1}$ pairs of elements $a \in M$, $b \in M$; and $(0, g) = (1, a) - (1, b)$ for exactly $2^{2N-2} \mp 2^{N-1}$ pairs $a \notin M$, $b \notin M$. Hence $(0, g)$, where $g \neq \mathbf{0}$, can be expressed as a difference of two elements of R in exactly 2^{2N-1} ways.

However, $g = a - b$ for exactly $2^{2N-1} \pm 2^{N-1}$ pairs a, b where $a \in M$ and $b \in K_{2N}$, and for exactly $2^{2N-2} \pm 2^{N-1}$ of these pairs, $b \in M$; thus, for exactly 2^{2N-2} pairs $a \in M$, $b \notin M$. Similarly, for exactly 2^{2N-2} pairs $a \notin M$, $b \in M$. Hence $(1, g)$, $g \neq \mathbf{0}$, is expressed as a difference of two elements of R in 2^{2N-1} ways.

Clearly, $(1, \mathbf{0})$ cannot be so expressed, and thus the proof of Theorem 4.1 is completed.

We have also the following $R(2^{2N}, 2, 2^{2N}, 2^{2N-1})$.

THEOREM 4.2. *If* $G = A_2 \oplus K_{2N}$, *and* $H = A_2 \oplus \{\mathbf{0}\}$, *then*

$$R = \{(h(n), n) \in G; n = (n_1, \cdots, n_{2N}) \in K_{2N}\}$$

where $h(n) \equiv \sum_{i=1}^{N} n_{2i-1} n_{2i} \pmod 2$, *is an* $R(2^{2N}, 2, 2^{2N}, 2^{2N-1})$ *of* G *relative to* H.

To see this, let $r(n) = (h(n), n)$, and choose $(a, g) \in G$, $g \neq \mathbf{0}$. Then $(a, g) = r(n + g) - r(n)$ if and only if

$$a \equiv \sum_{i=1}^{N} \{g_{2i-1} n_{2i} + g_{2i} n_{2i-1} + g_{2i-1} g_{2i}\} \pmod 2.$$

The proof then proceeds similarly to the proof of Theorem 3.1.

COROLLARY 4.2.1. *The complements of the relative difference sets of Theorems* 4.1 *and* 4.2 *are relative difference sets.*

5. Construction of cyclic relative difference sets

In [2] a class of cyclic relative difference sets was constructed with parameters $((p^N - 1)/(p - 1), (p - 1), p^{N-1}, p^{N-2})$, where p is a prime. This result generalizes to a power of a prime. These relative difference sets are constructed from maximal length linearly recurring sequences [11].

THEOREM 5.1. *For each m-sequence over a field of* $q = p^s$ *elements, there exists a cyclic*

$$R((q^N - 1)/(q - 1), q - 1, q^{N-1}, q^{N-2}),$$

where $q^N - 1$ *is the period of the m- sequence.*

The proof proceeds exactly as for [2]. *If* $\{a_i; i = 0, 1, \cdots\}$ *is the given m-sequence, then* $\{i; 0 \leq i < q^N - 1, a_i = 1\}$ *is the derived difference set in the group of additive integers modulo* $(q^N - 1)$.

COROLLARY 5.1.1. *There exist cyclic* $R((q^N - 1)/(q - 1), n, q^{N-1}, q^{N-2} d)$, *where* $nd = q - 1$.

This follows from Theorem 2.1.

6. Non-existence

Any relative difference set in an elementary Abelian 2-group is obviously an extension of a difference set also in an elementary Abelian 2-group. It has been shown by H. B. Mann [9, Theorem 7.1] that such difference sets have either the parameters of the Menon difference sets, or else they are trivial difference sets: that is, the $D(m, k, \lambda)$ in an elementary Abelian 2-group are

(a) $D(2^{2N}, 2^{2N-1} \pm 2^{N-1}, 2^{2N-2} \pm 2^{N-1})$,
(b) $D(2^N, 2^N - 1, 2^N - 2)$,
or (c) $D(2^N, 2^N, 2^N)$.

We now show that the Menon difference sets have no extensions in an elementary Abelian 2-group, with the possible exception of $D(2^6, 36, 20)$; and, further, if any relative difference set does exist in an elementary Abelian 2-group, it is necessarily an $R(2^{2N}, 2^s, 2^{2N}, 2^{2N-s})$, (again with the possible exception of $R(2^6, 2, 36, 10)$). This result is stated in the theorem below, which is proved in several lemmas.

THEOREM 6.1. *In an elementary Abelian 2-group no $R(m, n, k, d)$ can exist other than an $R(2^{2N}, 2^s, 2^{2N}, 2^{2N-s})$, except possibly an $R(2^6, 2, 36, 10)$.*

LEMMA 6.1.1. *The $D(2^{2N}, 2^{2N-1} \pm 2^{N-1}, 2^{2N-2} \pm 2^{N-1})$ have no extensions in an elementary Abelian 2-group, unless that extension is an $R(2^6, 2, 36, 10)$.*

To prove Lemma 6.1.1, suppose that such an extension does exist. Theorem 2.1 then implies the existence of an extension

$$R = R(2^{2N}, 2, 2^{2N-1} \pm 2^{N-1}, 2^{2N-3} \pm 2^{N-2})$$

in an elementary Abelian 2-group, G. The elements of G may be expressed as $(2N + 1)$-tuples of ones and zeros; and, since any subgroup of order 2 may be mapped isomorphically onto $\{(i, 0, \cdots, 0) \in G; i = 0, 1\}$, it may be assumed that this set is H.

Let t be the number of elements of R with first coordinate one. Counting the number of differences of elements of R of the form $(1, g_2, \cdots, g_{2N+1})$ yields the equation

$$2t(2^{2N-1} \pm 2^{N-1} - t) = (2^{2N} - 1)(2^{2N-3} \pm 2^{N-2}).$$

Solving for t we obtain

$$2t = 2^{2N-1} \pm 2^{N-1} \pm \sqrt{(2^{2N-1} \pm 2^{N-1})}.$$

Therefore $(2^N \pm 1) = x^2$, where x is a rational integer. Since $N \geq 3$, $2^N - 1 = x^2$ yields an impossibility for $x^2 \not\equiv -1 \pmod 4$.

Now consider $2^N + 1 = x^2$. Then $x + 1$ and $x - 1$ are two positive integers differing by 2, and are both powers of 2. This is possible only if $x = 3$ and $N = 3$. Thus no extension of a $D(2^{2N}, 2^{2N-1} \pm 2^{N-1}, 2^{2N-2} \pm 2^{N-1})$ other than a $D(2^6, 36, 20)$ exists in an elementary Abelian 2-group.

To complete the proof of the lemma, we note that if an $R(m, n, k, d)$ exists in an elementary Abelian 2-group, then n must be a power of two. Since $g = r - r'$ implies that $g = r' - r$, d must necessarily be even. This shows that the only possible extension of a $D(2^6, 36, 20)$ is an $R(2^6, 2, 36, 10)$, completing the proof of Lemma 6.1.1. It also proves the following lemma.

LEMMA 6.1.2. *In an elementary Abelian 2-group, no extension of a $D(2^N, 2^N - 1, 2^N - 2)$ can exist.*

To complete the proof of Theorem 6.1, we need only to prove the following lemma.

LEMMA 6.1.3. *If an extension R of a $D(2^N, 2^N, 2^N)$ exists in an elementary Abelian 2-group G, then N is even.*

To see this, it is first noted that the existence of R implies, by Theorem 2.1, the existence also of an $R(2^N, 2, 2^N, 2^{N-1})$ in an elementary Abelian 2-group. We may, therefore, assume that this is R. Expressing the elements of G as $(N+1)$-tuples of ones and zeros, it may be assumed, again by Theorem 2.1, that $H = \{(i, 0, 0, \cdots, 0); i = 0, 1\}$. Let t be the number of elements of R with first coordinate 1. Counting the number of ways in which elements of G with first coordinate 1 can be expressed as a difference of two elements of R yields the equation $2t(2^N - t) = (2^N - 1)2^{N-1}$. Therefore, N must be even, and the proofs of Lemma 6.1.3 and, consequently, Theorem 6.1 are complete.

In an elementary Abelian p-group, $R(m, n, m, d)$, where $nd = m$, have been constructed. In a cyclic group, the situation is entirely different, as the following theorem shows.

THEOREM 6.2. *In a cyclic group, there exist no $R(m, n, m, d)$, where $nd = m$, if $n > 1$ and $m > 2$.*

To prove this theorem, it is sufficient to consider the group G of additive integers modulo mn. We suppose that $R = R(m, n, m, d)$, $nd = m$, $n > 1$, does exist, and $H = \{im; i = 0, 1, \cdots, m-1\}$. Since no two distinct elements of R are congruent modulo m, and since R contains m elements, there must exist an $r(i) \in R$ such that $r(i) \equiv i \pmod{m}$ for each $i = 0, 1, \cdots, m-1$; that is, $R = \{r(i) = i + a(i)m; i = 0, 1, \cdots, m-1\}$. For each b, $1 \leq b < m - 1$,

$$r(i+b) - r(i) \equiv b + [a(i+b) - a(i)]m \pmod{mn}$$

for $i = 0, 1, \cdots, m-1-b$,

$$r(i+b-m) - r(i) \equiv b + [a(i+b-m) - a(i) - 1]m \pmod{mn}$$

for $i = m-b, m-b+1, \cdots, m-1$.

Thus the collection of integers $a(i+b) - a(i); i = 0, 1, \cdots, m-1-b$, and $a(i+b-m) - a(i) - 1; i = m-b, \cdots, m-1$ together forms a complete set of residues modulo n replicated d times. Adding the elements in this collection gives

$$(6.1) \qquad (-1)b \equiv d\{1 + 2 + \cdots + (n-1)\} \pmod{n} \quad \text{for each} \quad b, 1 \leq b < m-1.$$

Since $n > 1$, for $m > 2$, letting $b = 1$ and $b = 2$ in equation (6.1) gives a contradiction, proving the theorem.

It is noted that cyclic $R(2, 2, 2, 1)$ do exist.

7. The multiplier theorem

Throughout the remainder of this paper all groups considered will be Abelian; and v^* will denote the L.C.M. of the orders of the elements of the group G.

DEFINITION 7.1. Let R be an $R(m, n, k, d)$, and let t be a rational integer such that

$$\{tr; r \in R\} = \{r + g; r \in R\}$$

for some $g \in G$, then *t is called a multiplier of R*. If $g = 0$, *R is said to be fixed by t.*

Multipliers of relative difference sets play a part in the study of $R(m, n, k, d)$ comparable to that of multipliers in the study of $D(m, k, \lambda)$. In this section a "Multiplier Theorem", Theorem 7.1, is proved. The proof parallels the proof of the "Multiplier Theorem" for difference sets as proved by H. B. Mann [9, Theorem 7.3].

THEOREM 7.1. *If t is a multiplier of a $D = D(m, k, \lambda)$, where $\lambda = nd$, $k \equiv 0 \pmod{k'}$, $k' > d$, $k' = p_1^{e_1} \cdots p_s^{e_s}$, where the p_i are distinct primes, and if there exist f_i, $i = 1, \cdots, s$ such that $p_i^{f_i} \equiv t \pmod{v^*}$, then t is a multiplier of every $R(m, n, k, d)$ which is an extension of D.*

To prove Theorem 7.1, we consider the group ring A of G over the rational integers I, and following the notation in [9] express the elements of A as polynomials, $F(x) = \sum_{g \in G} f_g x^g$, where $f_g \in I$. In particular, if S is a set of elements of G, then $S(x)$ denotes the element of A defined by $S(x) = \sum_{g \in S} x^g$. The mn characters of G will be denoted by χ_i, $i = 1, \cdots, mn$, where χ_1 is the principal character, and χ_i, for $i = 1, 2, \cdots, m$, is the identity on the subgroup H.

If $F(x) \in A$, where $F(x) = \sum_{g \in G} f_g x^g$ and $f_g \in I$, then we define

$$\chi_i(F(x)) = \sum_{g \in G} f_g \chi_i(g) \qquad \text{for} \quad i = 1, \cdots, mn.$$

The proof of Theorem 7.1 will be given in several lemmas.

LEMMA 7.1.1. *If $C(x) \in A$, a is a rational integer such that $(a, mn) = 1$,*

$$\chi_1(C(x)) \equiv (m-1)nd \pmod{a},$$
$$\chi_i(D(x)) \equiv -nd \pmod{a} \qquad \textit{for} \quad i = 2, 3, \cdots, m,$$

and

$$\chi_i(C(x)) \equiv 0 \pmod{a} \qquad \textit{for} \quad i = m+1, \cdots, mn,$$

then

$$C(x) = d[G(x) - H(x)] + aF(x), \qquad \textit{where} \quad F(x) \in A.$$

Letting $C(x) = \sum_{g \in G} c_g x^g$, where $c_g \in I$, then the inversion formula [9, 7.6] states that $mnc_g = \sum_{i=1}^{mn} \chi_i(C(x))\chi_i(x^{-g})$, for each $g \in G$. Hence

$$mnc_g \equiv (m-1)n\, d - n\, d \sum_{i=2}^{m} \chi_i(x^{-g}) \pmod{a}.$$

Therefore, if $g \in H$, then $c_g \equiv 0 \pmod a$; and, if $g \notin H$, since the χ_i, $i = 1, \cdots, m$, may be regarded as characters on the factor group G/H, then $c_g \equiv d \pmod a$. Hence $C(x) = d[G(x) - H(x)] + aF(x)$, where $F(x) \in A$.

LEMMA 7.1.2. *Let R and R^* be two $R(m, n, k, d)$ both in G, and both relative to H such that*

$$R(x^{-1})R^*(x) = d[G(x) - x^gH(x)] + k'F(x), \quad \text{where } k' > d,\ F(x) \in A, \tag{7.1}$$

and

$$R^*(x)H(x) = R(x)H(x). \tag{7.2}$$

Then $R^*(x) = x^aR(x)$, where $a \in g + H$.

To prove this, it is first noted that

$$R(x)R(x^{-1}) = R^*(x)R^*(x^{-1}) = d[G(x) - H(x)] + k. \tag{7.3}$$

Multiplying (7.1) by $H(x)$, and using (7.2) yields, upon simplification,

$$k'F(x)H(x) = kx^gH(x). \tag{7.4}$$

The principal character applied to (7.4) gives

$$k'\chi_1(F(x)) = k. \tag{7.5}$$

Applying the automorphism $x \to x^{-1}$ to equations (7.1) and (7.4) yields

$$R(x)R^*(x^{-1}) = d[G(x) - x^{-g}H(x)] + k'F(x^{-1}), \tag{7.6}$$

and

$$k'F(x^{-1})H(x) = kx^{-g}H(x). \tag{7.7}$$

Then multiplying equation (7.1) by (7.6) and simplifying gives

$$k'^2F(x)F(x^{-1}) = k^2. \tag{7.8}$$

As in the proof for difference sets, since $k' > d$, it is clear from equation (7.1) that the coefficients of $F(x)$ are non-negative. Thus, (7.8) implies that $F(x)$ contains one term only; that is, $k'F(x) = kx^a$, for some $a \in G$. Equation (7.4) yields the fact that $a \in g + H$, and multiplying (7.6) by $R^*(x)$ and simplifying we have $R^*(x) = x^aR(x)$.

LEMMA 7.1.3. *Let R and R^* be two $R(m, n, k, d)$ of G relative to H, where $k \equiv 0 \pmod{p^j}$, $j > 0$, and $(p, mn) = 1$. If*

$$(\chi_i(R(x)), p^j) = (\chi_i(R^*(x)), p^j) \quad \text{for } i = m + 1, \cdots, mn, \tag{7.9}$$

and

$$R^*(x)H(x) = x^gR(x)H(x) \quad \text{for some } g \in G, \tag{7.10}$$

then

$$R(x^{-1})R^*(x) = d[G(x) - x^g H(x)] + p^j F(x), \qquad \textit{where} \quad F(x) \in A.$$

In order to obtain this result, we note that (7.3) holds and, therefore,

$$(7.11) \qquad \chi_i(R(x^{-1}))\chi_i(R(x)) \equiv \chi_i(R^*(x))\chi_i(R^*(x^{-1})) \pmod{p^j}$$

for $i = m + 1, \cdots, mn$.

From equations (7.9) and (7.11), we thus have that

$$(7.12) \quad \chi_i(R(x^{-1}))\chi_i(R^*(x)) \equiv 0 \pmod{p^j} \quad \text{for} \quad i = m + 1, \cdots, mn;$$

and, since the characters χ_i, $i = 1, \cdots, m$, may be regarded as the m characters of the group G/H, equations (7.10) and (7.3) imply that

$$(7.13) \quad \chi_i(R(x^{-1}))\chi_i(R^*(x)) \equiv -\chi_i(x^g)nd \pmod{p^j} \quad \text{for} \quad i = 2, \cdots, m,$$

and

$$(7.14) \qquad \chi_1(R(x^{-1}))\chi_1(R^*(x)) \equiv 0 \pmod{p^j}.$$

We now infer from Lemma 7.1.1 that

$$x^{-g}R(x^{-1})R^*(x) = d[G(x) - H(x)] + p^j F(x), \qquad \text{where} \quad F(x) \in A.$$

Multiplication by x^g, completes the proof of this lemma.

To prove Theorem 7.1, it is first observed that since t is a multiplier of the difference set induced in G/H, then $R(x^t)H(x) = x^g R(x)H(x)$, for some $g \in G$. The proof of the theorem now follows exactly as for difference sets, [9, Theorem 7.3].

8. Further theorems concerning multipliers

In this section, we include some useful results concerning multipliers. Theorems 8.1, 8.2 and 8.5 are generalizations of theorems of H. B. Mann, [9, Theorem 7.2, Corollaries 7.4.1, 7.7.1], and Theorem 8.6 extends a result of Marshall Hall, Jr., [4, Theorem 4.6].

THEOREM 8.1. *Let t be a multiplier of an $R(m, n, k, d)$, where $mn \equiv 0 \pmod{v'}$, and $m \not\equiv 0 \pmod{v'}$, and let p be a prime divisor of k. If there exists an f such that $tp^f \equiv -1 \pmod{v'}$, then k is exactly divisible by an even power of p.*

The hypothesis of the above theorem ensures that there exists a character χ of G which maps the elements of G into v'^{th} roots of unity, and which is not the identity on H.

Then $\chi(R(x)R(x^{-1})) = k \equiv 0 \pmod{p^j}$, where p^j divides k. The proof then follows as for a difference set. We refer the reader to [9, Page 76].

We note that if R is any $R(m, n, k, d)$ such that $k \neq m$, then from equations (2.1) and (2.2), $k - nd > 0$; thus, by equation (2.3), the incidence matrix of

R is non-singular. We therefore have the further analogue of a result for difference sets.

THEOREM 8.2. *If t is a multiplier of $R(m, n, k, d)$, where $m \neq k$, then some translate $g + R$, $g \in G$, is fixed by t.*

If, further, $(t - 1, mn) = 1$, then this translate is fixed by all multipliers.

The following theorem concerns relative difference sets fixed by a multiplier, and this theorem is used in the proof of Theorem 9.1.

THEOREM 8.3. *Let t be a multiplier of an $R(m, n, k, d) = R$, where $(km, n) = 1$ and $(t - 1, n) = n$. If R is an extension of a $D(m, k, nd) = D$, and if D is fixed by t, then R is fixed by t.*

To prove this let $tR = \{tr;\, r \in R\} = \{r + a;\, r \in R\}$ where $a \in G$. Consideration of the difference set, D, at once shows that $a \in H$, and, consequently, $na = 0$. However, for each $r \in R$, there exists $r' \in R$ such that $tr = r' + a$. Therefore, $(t - 1)\pi = ka$, where $\pi = \sum_{r \in R} r$; and, since n divides $t - 1$, ka has order a divisor of m. Now $na = 0$ and $(km, n) = 1$, hence $a = 0$, proving the theorem.

THEOREM 8.4. *If t is a multiplier of an $R(m, n, k, d)$, and if $t^e \equiv 1 \pmod{m^*}$, where m^* is the L.C.M. of the orders of the elements of G/H, then $t^e \equiv 1 \pmod{v^*}$.*

To obtain this result, we may, by Theorem 8.2, assume that $R = R(m, n, k, d)$ is fixed by the multiplier t^e. Since it is assumed that $m > 1$, it is first noted that there exists $g \in G$ of order v^* such that $g \notin H$. For each $r \in R$, there exists $r' \in R$ such that $t^e r = r'$. Consideration of the factor group G/H then reveals that $r \in r' + H$; and, by the definition of a relative difference set, therefore, $r = r'$. Thus, for every $r \in R$, $(t^e - 1)r = 0$. However, there exists $g \in G$, $g \notin H$, g of order v^*, and $g = r - r'$, for some $r, r' \in R$. Thus $(t^e - 1)g = 0$, giving the above result.

For the special case in which $d = 1$ we have two further results.

THEOREM 8.5. *Let t_1, t_2, t_3 and t_4 be multipliers of an $R(m, n, k, 1)$ which is fixed by all multipliers. If $t_1 + t_2 \equiv t_3 \pmod{v^*}$ and $t_2 \not\equiv t_4 \pmod{v^*}$, then $t_1 + t_4$ is not a multiplier of R.*

To prove this, it is again remarked that there exists $g \in G$, $g \notin H$, and g of order v^*. The proof is now an exact analogue of that for difference sets [9, Corollary 7.7.1].

THEOREM 8.6. *Let t be a multiplier of an $R = R(m, n, k, d)$, and let R be fixed by t. Let $G' = \{g \in G;\, tg = g\}$, $H' = H \cap G'$ and $R' = R \cap G'$. Then, if $H' \neq G'$, R' is an $R(m', n', k', 1)$ of G' relative to H' such that every multiplier of R is a multiplier of R'.*

If, further, R is cyclic, then $(t - 1, mn) = m'n'$ and $(t - 1, n) = n'$.

9. Further non-existence theorems

In the additive group of a Galois field K of p^N elements, where p is a prime such that $p^N \equiv 3 \pmod 4$, the quadratic residues of K form a

$$D = D(p^N = 4t - 1, 2t - 1, t - 1)$$

[8, Theorem 2]. Since the product of two quadratic residues is a quadratic residue, if t is any quadratic residue of K, then t is a multiplier of D and D is fixed by t. In particular, identifying the rational integers with the elements of the prime field of K, a rational integer t is a multiplier of D if t is a quadratic residue modulo p, and then, also, D is fixed by t.

We now examine relative difference sets which are extensions of quadratic residue difference sets, and are able to state the following theorem.

THEOREM 9.1. *There do not exist any $R(p^N = 4t - 1, t - 1, 2t - 1, d = 1)$, where $p \neq 3$ is a prime, which are extensions of a quadratic residue*

$$D(4t - 1, 2t - 1, t - 1).$$

To prove this, suppose that R does exist and that K is the field of p^N elements in which D is defined. Now G has order $p^N(t - 1)$; and, since $p \neq 3$, $(p^N, t - 1) = 1$. Therefore, $G = A \oplus H$, where A is a Sylow p-subgroup of G. Thus, $A \cong G/H$, the additive group of K.

It is noted that if $g \in G$, then $g \in A$ if and only if $(4t - 1)g = 0$, and that $g \in H$ if and only if $(t - 1)g = 0$.

The case in which t is odd is considered first. Then, by Theorem 2.3, $2t - 1$ is a square and is a multiplier of D. Theorem 7.2 then implies that $2t - 1$ is a multiplier of R.

Now $(2t - 1)^2 \equiv t \pmod{p^N(t - 1)}$; and, thus, t also is a multiplier of R. Since some translate of R is fixed by $2t - 1$, it may be assumed that this translate is R. Then, clearly, R is fixed by t also.

Choosing $r \in R$, $r \notin H$, then $(2t - 1)r - tr = tr - r$; but $d = 1$ and $r, tr, (2t - 1)r \in R$. Hence $(t - 1)r = 0$, which implies that $r \in H$, yielding a contradiction.

Now suppose that t is even. If q is any prime divisor of $(2t - 1)$, then q^2 is a multiplier of D. Also, $(2t - 1)^2 \equiv t \pmod{p^N(t - 1)}$ and, hence, t is a multiplier of R by Theorem 7.2. By Theorem 8.3, R is fixed by t and, consequently, by t^2 which is also a multiplier.

It is noted that $0 \notin D$ so that $R \cap H = \emptyset$. Consider

$$S_1 = \{(t - 1)r;\ r \in R\}.$$

We now show that S_1 consists of $2t - 1$ distinct non-zero elements of A. For, if $s \in S_1$, then $(4t - 1)s = 0$ and so $s \in A$. If $(t - 1)r = (t - 1)r'$ for $r, r' \in R$, then $(t - 1)(r - r') = 0$, $r - r' \in H$, and thus $r = r'$. If $s = (t - 1)r = 0$, then $r \in H$, which contradicts the statement above that $R \cap H = \emptyset$.

Hence S_1 does consist of $(2t - 1)$ distinct non-zero elements of A. Now consider

$$S_2 = \{(t^2 - 1)r;\, r \in R\}.$$

It is noted that $(t + 1, 4t - 1) = 1$. Hence, if $(t^2 - 1)r = 0$, then $(t - 1)r = 0$. However, the elements of S_1 are non-zero and thus the elements of S_2 are non-zero. The elements of S_2 are also contained in A, and they are distinct; for, if $(t^2 - 1)r = (t^2 - 1)r'$, for $r, r' \in R$, then, since $(t + 1, 4t - 1) = 1$, $(t - 1)(r - r') = 0$. The elements of S_1 are distinct and thus it follows that the elements of S_2 are distinct. Therefore, S_1 and S_2 each contain $2t - 1$ non-zero elements of A.

We now show that $S_1 \cap S_2 = \emptyset$. Deny this; then $tr - r = t^2r'$ for $r, r' \in R$; but $d = 1$, and $r, tr, r', t^2r' \in R$, and $(t - 1)r \neq 0$. Therefore, $r = r'$ and $tr = t^2r'$, yielding a contradiction.

Hence $S_1 \cap S_2 = \emptyset$, and S_1 and S_2 together consist of the $4t - 2$ non-zero elements of A. Now consider $a = (t^3 - 1)r$, for arbitrary $r \in R$. Then $a \in A$, and, if $a \in S_1$, then $(t^3 - 1)r = (t - 1)r' \neq 0$, for $r' \in R$. Since $d = 1$, and $r, r', tr', t^3r \in R$, then $r = r'$ and $t^3r = tr'$. This implies that $(t^2 - 1)r = 0$, which is a contradiction. Therefore $a \notin S_1$. Similarly it may be shown that $a \notin S_2$. Therefore, $a = (t^3 - 1)r = 0$; but r was chosen arbitrarily, and, hence, $(t^3 - 1)r = 0$ for all $r \in R$. There exists $g \in A$ of order p, and $g = r - r'$, for $r, r' \in R$. Hence, $(t^3 - 1)g = 0$, and so p divides $t^3 - 1$, and, consequently, $t^2 + t + 1$. Since p also divides $4t - 1$, it may be concluded that $p = 7$. If $p = 7$, then 3 divides k, and Theorem 7.1 then implies that 9 is a multiplier of R. Applying Theorem 8.4 gives $9^3 \equiv 1 \pmod{v^*}$. Since $H \neq \{0\}$, there exists $h \in H$ of prime order q, where q divides $(t - 1)$, $q \neq 7$; and, therefore, $9^3 \equiv 1 \pmod{7q}$. This, then, yields that $q = 13$, and $4t - 1 = 7^N \equiv 3 \pmod{13}$.

Now N is necessarily odd, 7 is a quadratic non-residue modulo 13, giving a final contradiction, which proves the theorem.

Summary

In view of Theorem 2.1, in the search for relative difference sets and in proving their non-existence, particular attention has been paid to extensions of well-known difference sets.

Simple difference sets have obviously no extensions, and their complements, $D((r^3 - 1)/(r - 1), r^2, r)$, are, for $r \leq 1600$, a special case of the difference sets in [3], which have been shown to extend in Section 5.

The Menon difference sets have no extensions in the elementary Abelian 2-group, (with one possible exception); and, in these groups, it has been shown that only the $D(m, k, \lambda)$ with $m = k = \lambda$, may extend, (again, with one possible exception).

Trivial $D(m, m, m)$, while extending in elementary p-groups, have been shown to have no extensions in the cyclic group.

Of the quadratic residue difference sets, there can be no extensions of the form $R(p^N = 4t - 1, t - 1, 2t - 1, 1)$, when $p \neq 3$.

BIBLIOGRAPHY

1. R. H. BRUCK, *Difference sets in a finite group*, Trans. Amer. Math. Soc., vol. 78 (1955), pp. 464–481.
2. A. T. BUTSON, *Relations among generalized Hadamard matrices*, Canad. J. Math., vol. 15 (1963), pp. 42–48.
3. B. GORDON, W. H. MILLS, AND L. R. WELCH, *Some new difference sets*, Canad. J. Math., vol. 14 (1962), pp. 614–625.
4. MARSHALL HALL, JR., *Cyclic projective planes*, Duke Math. J., vol. 14 (1947), pp. 1079–1090.
5. ———, *A survey of difference sets*, Proc. Amer. Math. Soc., vol. 7 (1956), pp. 975–986.
6. E. LEHMER, *On residue difference sets*, Canad. J. Math., vol. 5 (1953), pp. 425–432.
7. H. B. MANN, *Some theorems on difference sets*, Canad. J. Math., vol. 4 (1952), pp. 222–226.
8. ———, *Difference sets in elementary abelian groups*, M. R. C. Tech. Summary Report No. 422, September 1963.
9. ———, *Addition theorems*, New York, John Wiley and Sons, 1965.
10. P. KESAVA MENON, *Difference sets in abelian groups*, Proc. Amer. Math. Soc., vol. 11 (1960), pp. 368–376.
11. N. ZIERLER, *Linear recurring sequences*, J. Soc. Indust. Appl. Math., vol. 7 (1959), pp. 31–48.

UNIVERSITY OF MIAMI
CORAL GABLES, FLORIDA