PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 68, Number 3, March 1978

TRANSLATES AND MULTIPLIERS OF ABELIAN DIFFERENCE SETS

ROBERT L. MCFARLAND AND BART F. RICE

ABSTRACT. It is shown that every abelian difference set has a translate which is fixed by all numerical multipliers. If an abelian difference set in a group of order v has numerical multipliers $t_1, \ldots, t_m$ which satisfy $\gcd(t_1 - 1, \ldots, t_m - 1, v) = 1$, then there is a unique translate which is fixed by all multipliers.

1. Introduction. Let G be a multiplicative group of finite order v. A subset $D := \{d_1, \ldots, d_k\}$ of G is a *difference set* in G with parameters (v, k, λ) in case the aggregate of "differences", $d_i^{-1}d_j$ $(i, j = 1, \ldots, k, i \neq j)$, replicates each nonidentity element of G exactly λ times. We assume $0 < \lambda < k < v - 1$ to avoid the trivial difference sets which have $k = 0$, 1, $v - 1$ or v. The difference set is *cyclic*, *abelian* or *nonabelian* if the group G is cyclic, abelian or nonabelian, respectively. For additional information on difference sets see Baumert [1], Hall [3, Chapter 11] or Mann [4, Chapters 6, 7, 8].

For any g in G we call $Dg := \{d_1 g, \ldots, d_k g\}$ a *translate* of D. Note that Dg is also a difference set. Furthermore, $Dg = D$ if and only if $g = 1$, for otherwise there would be k $(> \lambda)$ replications of g among the "differences" $d_i^{-1}d_j$.

If $\sigma\colon g \mapsto g^\sigma$ is an automorphism of G, define $D(\sigma) := \{d_1^\sigma, \ldots, d_k^\sigma\}$. If $D(\sigma)$ is a translate of D, then σ is called a *multiplier* of D. The multiplier σ *fixes* the translate Dg in case $(Dg)(\sigma) = Dg$. If there is an integer t such that the action of the multiplier σ on G is $\sigma\colon g \mapsto g^t$, then we identify t and σ and call t a *numerical multiplier*; otherwise σ is a *nonnumerical multiplier*. The multipliers of D constitute a subgroup of the automorphism group of G, called the *multiplier group* of D. The numerical multipliers are a subgroup of the center of the multiplier group.

In this paper we consider the question: Must an abelian difference set have a translate which is fixed by all of its multipliers? The answer is known to be yes if the parameters v and k of the difference set are relatively prime or if there is a numerical multiplier t such that $t - 1$ is prime to v. A difference set in an elementary abelian group of order 16 shows that the answer is not always yes.

We prove that such a fixed translate exists for all *numerical* multipliers.

Received by the editors May 30, 1975 and, in revised form, April 7, 1977.
AMS (MOS) subject classifications (1970). Primary 05B10.
Key words and phrases. Difference set, multiplier.

Thus, in particular, a cyclic difference set always has a translate which is fixed by all multipliers. We also give a new condition for an abelian difference set to have a translate which is fixed by all multipliers.

2. Fixed translates. It is well known, Mann and McFarland [5], that a multiplier of a difference set must fix at least one translate. Indeed, a multiplier of a difference set D in a group G induces the same orbit structure on the translates of D as it induces on the elements of G, cf. Parker [6]. The number of translates fixed by a multiplier σ is the order of the subgroup $\{g \in G: g^\sigma = g\}$.

J. Jans (see Hall [3, p. 140]) has noted that if the parameters of an abelian difference set D satisfy $\gcd(v, k) = 1$, then there is a unique translate Dg for which the product of the elements of Dg is 1, and this translate is fixed by all multipliers. In this situation there can be other translates which are also fixed by all multipliers. For example, the cyclic difference set with parameters $(v, k, \lambda) = (57, 8, 1)$ has exactly three translates which are fixed by the multiplier 7 which is a generator of the multiplier group.

The case $m = 1$ of the following theorem is proved in [5] and in [4, p. 81].

THEOREM 1. *Suppose a difference set D in an abelian group G of order v has (some) numerical multipliers $t_1, \ldots, t_m$ which satisfy*

$$\gcd(t_1 - 1, \ldots, t_m - 1, v) = 1.$$

Then D has a unique translate which is fixed by every multiplier.

PROOF. Let $D(t_i) = Dg_i$ $(i = 1, \ldots, m)$. Then $D(t_i t_j) = D(t_j t_i)$ implies that

$$g_i^{t_j - 1} = g_j^{t_i - 1} \qquad (i, j = 1, \ldots, m).$$

There are integers $a_1, \ldots, a_m$ such that

$$a_1(t_1 - 1) + \cdots + a_m(t_m - 1) \equiv 1 (\mathrm{mod}\ v).$$

Let $g = g_1^{a_1} \cdots g_m^{a_m}$. Then

$$g^{t_j - 1} = \prod_{i=1}^{m} g_i^{a_i(t_j - 1)} = \prod_{i=1}^{m} g_j^{a_i(t_i - 1)} = g_j.$$

Therefore, the translate $D_1 := Dg^{-1}$ is fixed by each of $t_1, \ldots, t_m$. Suppose $D_1 h$ is also fixed by $t_1, \ldots, t_m$. Then $(D_1 h)(t_i) = D_1 h$ implies that $h^{t_i - 1} = 1$ $(i = 1, \ldots, m)$. Thus

$$h = h^{a_1(t_1 - 1) + \cdots + a_m(t_m - 1)} = 1.$$

Hence D_1 is the only translate which is fixed by each of $t_1, \ldots, t_m$. Let σ be any multiplier and suppose $D_1(\sigma) = D_1 h$. Then $D_1(\sigma t_i) = D(t_i \sigma)$ implies that $h^{t_i - 1} = 1$. Hence $h = 1$ as above, so D_1 is fixed by every multiplier.

Dembowski [2, p. 85] notes that in general an abelian difference set need not have a translate which is fixed by all its multipliers. For example, let G be an elementary abelian group of order 16 with generators a, b, c, d. Then $D = \{1, a, b, c, d, abcd\}$ is a difference set in G with parameters $(v, k, \lambda) = (16, 6, 2)$. The automorphism α defined by α: $a \mapsto b \mapsto c \mapsto d \mapsto a$ is a

multiplier which fixes D. The automorphism β defined by β: ($a \mapsto abcd$, $b \mapsto bcd$, $c \mapsto acd$, $d \mapsto abd$) is a multiplier since $D(\beta) = Dabcd$. The automorphism group generated by α and β is transitive on the nonidentity elements of G, so no translate of D can be fixed by both α and β.

To prove the next theorem we introduce the group ring $\mathbf{Z}G$ of the finite multiplicative abelian group G over the ring $\mathbf{Z}$ of integers. We identify any subset S of G with its characteristic function in $\mathbf{Z}G$, i.e., $S = \sum_{g \in G} a_g g$, where the coefficients $a_g = 1$ or 0 according to whether $g \in S$ or $g \notin S$. In particular, a difference set D in G, an element $g \in G$ or G itself can be considered elements of $\mathbf{Z}G$. However, we write $G(1)$ to denote the characteristic function of G. For any element $A \in \mathbf{Z}G$,

$$A := \sum_{g \in G} a_g g, \qquad a_g \in \mathbf{Z},$$

and any integer t we define

$$A(t) := \sum_{g \in G} a_g g^t.$$

Thus in the group ring notation, an integer t is a multiplier of the difference set D in case $D(t) = Dg$ for some group element g. The difference set property implies that

$$D(-1)D = (k - \lambda)1_G + \lambda G(1),$$

where k, λ are those parameters of D and 1_G is the identity of G.

We also utilize the concept of characters of G acting on $\mathbf{Z}G$ and the inversion formula which expresses the coefficients of an element $A \in \mathbf{Z}G$ in terms of the values the characters take on A. In particular, if A, B are two elements of $\mathbf{Z}G$ such that $\chi(A) = \chi(B)$ for all characters χ, then $A = B$. For details see Mann [**4**, pp. 73–75].

THEOREM 2. *Every abelian difference set has a translate which is fixed by all of its numerical multipliers.*

PROOF. Let D be a difference set in the finite abelian group G. Express G as the direct product $G = G_1 \times \cdots \times G_m$, where each G_i is a cyclic group of prime power order. Let D_i be the image of D under the natural group ring epimorphism $\mathbf{Z}G \to \mathbf{Z}G_i$ induced by the canonical group epimorphism α_i: $G \to G_i$. We assert that each G_i contains an element g_i such that the translate $D_i g_i$ is fixed by every numerical multiplier of D. Let T be the group of numerical multipliers of D and let T_i be the multiplier group for D_i obtained by reducing the elements of T modulo the order of G_i. First suppose T_i is cyclic. Let $t \in T$ be a generator of T_i and let Dg be a translate fixed by t. Let α_i: $g \mapsto g_i$. Then $D_i g_i$ is fixed by t. Hence $D_i g_i$ is fixed by every element of T_i and thus also fixed by every element of T.

Now suppose T_i is not cyclic. The automorphism group $\mathfrak{A}_i$ of G_i is noncyclic only if the order of G_i is 2^e for some $e \geqslant 3$, and then $\mathfrak{A}_i$ is isomorphic to the direct product of a group of order 2 with a cyclic group of

order 2^{e-2}. Any noncyclic subgroup of $\mathcal{Q}_i$ must contain all three elements of $\mathcal{Q}_i$ which have order 2. In particular, T_i contains -1. Thus T contains an element $t \equiv -1 \pmod{2^e}$. Let Dg be a translate fixed by this t. Let α_i: $g \mapsto g_i$ and let $E_i := D_i g_i$. Then $E_i(-1) = E_i$. Hence

$$E_i^2 = E_i(-1)E_i = (k - \lambda)1_i + \lambda[G: G_i]G_i(1),$$

where k, λ are those parameters of D, 1_i is the identity of G_i and $[G: G_i]$ is the index of G_i in G. Each character χ of G_i can be extended linearly to yield a homomorphism from $\mathbf{Z}G_i$ into the order $\mathbf{Z}[\zeta]$ generated by a primitive 2^eth root of unity ζ. If χ_0 is the principal character, then $\chi_0(E_i) = k$. If χ is a nonprincipal character of G_i, then $\chi(G_i(1)) = 0$, so

$$\chi(E_i)^2 = \chi(E_i^2) = k - \lambda.$$

Since the order of G is even, the well-known Bruck-Ryser-Chowla conditions imply that $k - \lambda$ is a square. Hence $\chi(E_i) \in \mathbf{Z}$ for every character χ. For every odd integer s let σ_s be the automorphism of $\mathbf{Z}[\zeta]$ defined by σ_s: $\zeta \mapsto \zeta^s$. Then

$$\chi(E_i(s)) = \sigma_s\chi(E_i) = \chi(E_i)$$

for every character χ of G_i. Hence by the inversion formula for $\mathbf{Z}G_i$, $E_i(s) = E_i$. That is, every odd integer s is a multiplier which fixes E_i. Since the order of G is even, T contains no even integers. Thus $E_i = D_i g_i$ is fixed by every element of T.

Use the values of g_i specified above to define $g := (g_1, \ldots, g_m) \in G_1 \times \cdots \times G_m$. Let $t \in T$ and suppose $(Dg)(t) = Dh$, where $h =: (h_1, \ldots, h_m)$. Apply the group ring epimorphism induced by α_i to obtain $(D_i g_i)(t) = D_i h_i$. But t fixes $D_i g_i$, so $D_i g_i = D_i h_i$. Multiply this equation by $D_i(-1)$ to see that $g_i = h_i$. Thus $g = h$ so the translate Dg is fixed by every numerical multiplier.

Note that the proof of Theorem 2 is not valid for nonnumerical multipliers, since nonnumerical multipliers will not necessarily commute with the epimorphisms α_i.

Since a cyclic group has only "numerical automorphisms", we have

COROLLARY. *Every cyclic difference set has a translate which is fixed by all of its multipliers.*

The authors wish to thank John F. Dillon for pointing out to them their common interest in the problems considered in this paper.

REFERENCES

1. L. D. Baumert, *Cyclic difference sets*, Lecture Notes in Math., vol. 182, Springer-Verlag, New York, 1971.
2. P. Dembowski, *Finite geometries*, Springer-Verlag, New York, 1968.
3. M. Hall, Jr., *Combinatorial theory*, Blaisdell, Waltham, Massachusetts, 1967.
4. H. B. Mann, *Addition theorems*, Wiley, New York, 1965.

5. H. B. Mann and R. L. McFarland, *On multipliers of difference sets*, Canad. J. Math. **17** (1965), 541–542.

6. E. T. Parker, *On collineations of symmetric designs*, Proc. Amer. Math. Soc. **8** (1957), 305–351.

Department of Mathematics, Wright State University, Dayton, Ohio 45435

Department of Defense, Fort George G. Meade, Maryland 20755