JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematics and Mathematical Physics
Vol. 69B, Nos. 1 and 2, January–June 1965

A Note on Multipliers of Difference Sets

R. A. Brualdi

(October 29, 1964)

Let v, k, λ be integers with $0<\lambda<k<v-1$. A set $D=\{d_1, d_2, \ldots, d_k\}$ of k integers distinct modulo v is a *difference set* with parameters v, k, and λ provided every nonzero residue c modulo v can be written in precisely λ ways in the form $d_i-d_j\equiv c \pmod{v}$. An integer t is a *multiplier* of D provided there exists an integer s such that the sets of numbers $\{td_1, \ldots, td_k\}$ and $\{d_1+s, \ldots, d_k+s\}$ coincide modulo v. It is shown that -1 cannot be a multiplier of the difference set D. A consequence is that a Hadamard matrix of order v cannot be a symmetric circulant for $v>4$.

Introduction

In a recent paper [1] [1] Gordon, Mills, and Welch state that it is known that -1 cannot be a multiplier of a nontrivial difference set. No proof of this fact appears ever to have been published. The purpose of this note is to give an elementary matrix-theoretic proof of this assertion using the approach of M. Newman in [2]. Some implications are also noted.

Let v, k, λ be integers with $0<\lambda<k<v-1$. A set $D=\{d_1, d_2, \ldots, d_k\}$ of k integers distinct modulo v is a *difference set* with parameters v, k, and λ provided every nonzero residue c modulo v can be written in precisely λ ways in the form

$$d_i-d_j\equiv c \pmod{v},$$

with d_i and d_j in D. A simple count yields

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

An integer t is a *multiplier* of D provided there exists an integer s such that the sets of numbers $\{td_1, td_2, \ldots, td_k\}$ and $\{d_1+s, d_2+s, \ldots, d_k+s\}$ coincide modulo v.

Let P be the v-square permutation matrix

$$P=\begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ . & . & . & \ldots & . \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix}$$

and C the circulant matrix

$$C=\sum_{i=1}^{k} P^{d_i} \tag{2}$$

We have $P^v=I$, and the properties of the difference set D imply that

$$CC^T=C^TC=(k-\lambda)I+\lambda J, \qquad CJ=JC=kJ \tag{3}$$

where J is the v-square matrix of all 1's. For t an integer let

$$C_t=\sum_{i=1}^{k} P^{td_i}.$$

Then t is a multiplier of the difference set D if and only if there exists an integer s where $0\leqq s\leqq v-1$ such that

$$C_t=P^sC. \tag{4}$$

THEOREM: *Let* $\mathrm{D}=\{\mathrm{d}_1, \mathrm{d}_2, \ldots, \mathrm{d}_\mathrm{k}\}$ *be a difference set with parameters* v, k, *and* λ *where* $0<\lambda<\mathrm{k}<\mathrm{v}-1$. *Then* -1 *is not a multiplier of* D.

PROOF: Suppose -1 is a multiplier. Then

$$C_{-1}=\sum_{i=1}^{k} P^{-d_i}=C^T,$$

and thus

$$C^T=P^sC \tag{5}$$

for some integer s, $0\leqq s\leqq v-1$. If s is even, say $s=2r$, then (5) can be written as $(P^rC)^T=P^rC$ where P^rC also satisfies (3). If s is odd and v is odd, then since $P^{v+s}=P^v\cdot P^s=P^s$ a similar remark holds. In case s is odd, say $s=2r+1$, and v is even then (5) can be written as $(P^rC)^T=P(P^rC)$ where P^rC again satisfies (3). Hence we may assume that either

$$C^T=C, v \text{ odd or even}, \tag{6}$$

or

$$C^T=PC, v \text{ even}. \tag{7}$$

We proceed to show that a circulant matrix C of 0's and 1's which satisfies (3) with $0<\lambda<k<v-1$ and either (6) or (7) does not exist. Let

$$c_0, c_1, c_2, \ldots, c_{v-1}$$

denote the first row of C, so that

$$c_0, c_{v-1}, c_{v-2}, \ldots, c_1$$

is the first row of C^T.

[1] Figures in brackets indicate the literature references at the end of this paper.

Case 1. $C^T = C$; v even, say $v = 2r$.

Comparing the first rows of C^T and C we find that $c_j = c_{v-j}$, $j = 1, 2, \ldots, v-1$. Thus the matrix C assumes the form

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \ldots & c_{r-1} & c_r & c_{r-1} & \ldots & c_2 & c_1 \\ c_1 & c_0 & c_1 & \ldots & c_{r-2} & c_{r-1} & c_r & \ldots & c_3 & c_2 \\ c_2 & c_1 & c_0 & \ldots & c_{r-3} & c_{r-2} & c_{r-1} & \ldots & c_4 & c_3 \\ . & . & . & . & . & . & . & . & . & . \end{bmatrix}$$

By (3) the inner product of any two distinct rows of C is equal to λ. The inner product of row 1 and row 2 shows that λ is even. The inner product of row 1 and row 3 is congruent to $c_1^2 + c_{r-1}^2 = c_1 + c_{r-1}$ modulo 2. Since λ is even, $c_1 = c_{r-1}$. The inner product of row 1 and row 5 gives $c_2 = c_{r-2}$. Continuing in this way we conclude that the first row of C has the form

$$c_0, c_1, c_2, \ldots, c_2, c_1, c_r, c_1, c_2, \ldots, c_2, c_1.$$

The inner product of row 1 and row $(r+1)$ then yields

$$\lambda = c_1^2 + c_2^2 + \ldots + c_2^2 + c_1^2 + 2c_0c_r + c_1^2 + c_2^2 + \ldots + c_2^2 + c_1^2$$

or since the c's are either 0 or 1,

$$\lambda = c_1 + c_2 + \ldots + c_2 + c_1 + 2c_0c_r + c_1 + c_2 + \ldots + c_2 + c_1.$$

Since the sum of the entries in the first row of C is equal to k, we then have $\lambda - k = 2c_0c_r - c_0 - c_r$. Because c_0 and c_r are either 0 or 1, this implies $\lambda = k$ or $\lambda = k-1$. Since $\lambda = k-1$ implies by (1) that $k = v-1$, we have a contradiction.

Case 2. $C^T = C$; v odd, say $v = 2r+1$.

In this case the matrix C has the form

$$\begin{bmatrix} c_0 & c_1 & c_2 & \ldots & c_{r-1} & c_r & c_r & c_{r-1} & \ldots & c_2 & c_1 \\ c_1 & c_0 & c_1 & \ldots & c_{r-2} & c_{r-1} & c_r & c_r & \ldots & c_3 & c_2 \\ c_2 & c_1 & c_0 & \ldots & c_{r-3} & c_{r-2} & c_{r-1} & c_r & \ldots & c_4 & c_3 \\ . & . & . & . & . & . & . & . & . & . & . \end{bmatrix}$$

The inner product of row 1 and row 2 shows that $\lambda \equiv c_r \pmod 2$.

The inner product of row 1 and row 3 shows that $\lambda \equiv c_1 \pmod 2$. Continuing in this way we see that

$$\lambda \equiv c_j \pmod 2, \qquad j = 1, 2, \ldots, r.$$

Since the c's are either 0 or 1, we conclude that $c_1 = c_2 = \ldots = c_r$. Since by (3) $k = c_0 + 2(c_1 + \ldots + c_r)$ and $k \geqq 2$, this common value must be 1. But then $k = v$ or $k = v-1$ and we have a contradiction.

Case 3. $C^T = PC$, v even, $v = 2r$.

Comparing the first rows of C^T and PC, we see that $c_j = c_{v-1-j}$, $j = 0, 1, \ldots, v-1$. The matrix C then has the form

$$\begin{bmatrix} c_0 & c_1 & c_2 & \ldots & c_{r-1} & c_{r-1} & \ldots & c_2 & c_1 & c_0 \\ c_0 & c_0 & c_1 & \ldots & c_{r-2} & c_{r-1} & \ldots & c_3 & c_2 & c_1 \\ c_1 & c_0 & c_0 & \ldots & c_{r-3} & c_{r-2} & \ldots & c_4 & c_3 & c_2 \\ . & . & . & . & . & . & . & . & . & . \end{bmatrix}$$

The inner product of row 1 and row 3 shows λ must be even. The inner product of row 1 and row 2 implies $\lambda \equiv c_0 + c_{r-1} \pmod 2$. Hence $c_0 = c_{r-1}$. The inner product of row 1 and row 4 yields $c_1 = c_{r-2}$. In general, $c_j = c_{r-1-j}$, $j = 0, 1, \ldots, r-1$. Hence the first row of C has the form

$$c_0, c_1, \ldots, c_1, c_0, c_0, c_1, \ldots, c_1, c_0.$$

The inner product of row 1 and row $(r+1)$ then gives

$$\lambda = c_0 + c_1 + \ldots + c_1 + c_0 + c_0 + c_1 + \ldots + c_1 + c_0 = k.$$

But $\lambda = k$ is a contradiction. This completes the proof of the theorem.

If t is a multiplier of a difference set D with parameters v, k, and λ, then $(t, v) = 1$. Moreover it is easily verified that the set of multipliers modulo v form a multiplicative group M which is a subgroup of the multiplicative group G of all integers modulo v which are prime to v. Let $|M|$ denote the order of M and $\varphi(v)$ the Euler function of v, that is the number of positive integers not greater than and prime to v. Then

COROLLARY 1: M *is a proper subgroup of* G *and hence* $|\mathrm{M}| \leqq \frac{\varphi(\mathrm{v})}{2}$.

PROOF: -1 is an element of G but by the theorem not of M.

A $(v, k, \lambda)-$*matrix* is a v-square matrix of 0's and 1's which satisfies

$$AA^T = (k-\lambda)I + \lambda J,$$

where $0 < \lambda < k < v-1$. In the proof of the theorem we have shown that there do not exist $(v, k, \lambda)-$matrices A which are circulants and satisfy $A^T = P^sA$ where $0 \leqq s \leqq v-1$. In particular there do not exist symmetric circulant $(v, k, \lambda)-$matrices.

We are indebted to Morris Newman for pointing out to us the following consequence. A *Hadamard matrix H* is a v-square matrix of $+1$'s and -1's such that $HH^T = vI$. It has been conjectured [3] that a Hadamard matrix cannot be a circulant for $v > 4$. In this regard we have

COROLLARY 2: *A Hadamard matrix cannot be a symmetric circulant for* $\mathrm{v} > 4$.

PROOF: For, if H is a symmetric Hadamard circulant, then

$$K = \frac{1}{2}(H + J)$$

is a symmetric circulant (v, k, λ)-matrix with $k = \frac{v \pm \sqrt{v}}{2}$ and $\lambda = \frac{v \pm 2\sqrt{v}}{4}$, unless $k=0, 1, v-1, v$.

But it is easily checked that these requirements cannot be satisfied for $v > 4$. This proves the corollary.

Part of the work for this paper was done while the author was a National Research Council—National Bureau of Standards Postdoctoral Research Associate, 1964-1965. The author wishes to thank Morris Newman for helpful comments concerning the exposition of this paper.

Note added in proof: In the Canadian Journal of Mathematics (Vol. **16,** 1964) E. C. Johnsen in his paper "The Inverse Multiplier For Abelian Group Difference Sets" investigates a problem similar to ours for the more general abelian group difference sets. In the then special case of our circumstances he obtains by nonelementary means a proof of the theorem in our paper.

References

[1] B. Gordon, W. H. Mills, and L. R. Welch, Some new difference sets, Can. J. Math. **14,** 614-625 (1962).

[2] M. Newman, Multipliers of difference sets, Can. J. Math. **15,** 121-124 (1963).

[3] H. J. Ryser, Combinatorial Mathematics, Carus Math. Monograph, No. 14, (John Wiley & Sons, Inc., New York, N.Y., 1963).

(Paper 69B1–138)