MULTIPLIERS OF DIFFERENCE SETS

MORRIS NEWMAN

Introduction. Let λ, k, v be integers such that $0 < \lambda < k < v$. Then the set of integers

$$D = \{d_i\}, \qquad 1 \leqslant i \leqslant k$$

is a *difference set* with parameters v, k, λ if each non-zero residue modulo v occurs precisely λ times and zero occurs precisely k times among the k^2 numbers

$$d_i - d_j, \qquad 1 \leqslant i, j \leqslant k.$$

It is immediate that $\lambda(v - 1) = k(k - 1)$.

The integer t is a *multiplier* of D if there is an integer a such that the numbers $\{td_i\}$ coincide modulo v with the numbers $\{d_i + a\}$, apart from order. A well-known theorem of M. Hall and H. Ryser (see **2**, **3**) states that if q is a prime such that

$$q | k - \lambda, \qquad q > \lambda, \qquad (q, v) = 1$$

then q is a multiplier of D. The proof of this theorem is a complicated affair depending on polynomials in the indeterminates x, x^{-1}, and double modulus arguments. The purpose of this paper is to prove the Hall-Ryser theorem by arguments involving incidence matrices alone. One valuable feature of this approach is that the undesirable assumption $q > \lambda$ can be eliminated in some cases.

The referee points out that the authors' approach through circulant matrices that follows is closely related to the work of R. H. Bruck (**1**), which uses elements in the group ring of a cyclic group.

Let P be the $v \times v$ permutation matrix

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

and let C be the matrix

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

Received November 24, 1961. This paper was prepared while the author was a participant in the Combinatorial Mathematics Symposium sponsored by Rand during the summer of 1961.

Then P is the cycle of length v, and C satisfies

(1) $$CC' = C'C = nI + \lambda J, \qquad CJ = JC = kJ,$$

where J is the $v \times v$ matrix all of whose entries are 1, and

$$n = k - \lambda.$$

(Notice that $P^v = I, I + P + P^2 + \ldots + P^{v-1} = J$.)

Define

$$C_q = \sum_{i=1}^{k} P^{qd_i}.$$

Then the matrix C_q also satisfies (1) since $(q, v) = 1$ and $\{qd_i\}$ must also be a difference set. The matrices C and C_q commute (since they are each polynomials in P, or *circulants*) and in fact all matrices considered here will be circulants and so will commute.

The matrix C is non-singular since $k > \lambda > 0$ (CC' has the eigenvalue n $v - 1$ times and k^2 once since J has the eigenvalue 0 $v - 1$ times and v once) and so we can define

(2) $$M = C^{-1}C_q.$$

Then

$$MM' = M'M = I$$

since $CC' = C_qC_q'$. Multiplying in (1) by C^{-1} we find that

(3) $$C^{-1} = \frac{1}{n} C' - \frac{\lambda}{nk} J$$

and substituting (3) into (2) we find that

$$M = \frac{1}{n}\{C'C_q - \lambda J\}.$$

Put

(4) $$T = nM = C'C_q - \lambda J.$$

Then

(5) $$TT' = T'T = n^2 I, \qquad JT = TJ = nJ.$$

Since q is prime it is clear that

(6) $$C_q = C^q + qR,$$

where R is an integral circulant.

Substituting (6) into (4) and making use of (1) we find that

$$T = nC^{q-1} + \lambda(k^{q-1} - 1)J + qC'R.$$

Since $q|n$, $q|\lambda(k^{q-1} - 1)$, this implies that $T = qS$, where S is an integral circulant. By (5), S satisfies

$$SS' = S'S = \left(\frac{n}{q}\right)^2 I, \qquad SJ = JS = \frac{n}{q} J. \tag{7}$$

Furthermore by (4)

$$C'C_q = \lambda J + qS.$$

If we now assume that $q > \lambda$ then S can have no negative entries.

Suppose that

$$S = \sum_{i=0}^{v-1} c_i P^i, \qquad c_i \geqslant 0.$$

Then

$$\sum_{i=0}^{v-1} c_i^2 = \frac{n^2}{q^2}, \qquad \sum_{i=0}^{v-1} c_i = \frac{n}{q}.$$

Since $c_i \geqslant 0$ this is only possible if

$$S = \frac{n}{q} P^a$$

where a is an integer such that $0 \leqslant a \leqslant v - 1$. But then

$$M = \frac{1}{n} T = \frac{q}{n} S = P^a$$

and the conclusion follows from the relationship

$$C_q = P^a C.$$

We now drop the assumption that $q > \lambda$. We can prove:

THEOREM. *If $n = q$ then q is always a multiplier of D. If $n = 2q$ and $(v, 7) = 1$ then q is always multiplier of D.*

Proof. We must show that $S = (n/q)P^a$, for some integer a satisfying $0 \leqslant a \leqslant v - 1$. Suppose that $n = q$. Then (7) becomes

$$SS' = S'S = I, \qquad SJ = JS = J,$$

the solutions of which are clearly $S = P^a$, $0 \leqslant a \leqslant v - 1$. Now suppose that $n = 2q$. Then (7) becomes

$$SS' = S'S = 4I, \qquad SJ = JS = 2J,$$

the solutions of which are $S = 2P^a$, $0 \leqslant a \leqslant v - 1$ and possibly

$$S = P^a(P^{a_1} + P^{a_2} + P^{a_3} - I), \quad 0 \leqslant a \leqslant v - 1, \quad v > a_1 > a_2 > a_3 > 0. \tag{8}$$

We shall show that (8) is a solution only if $v \equiv 0 \pmod 7$, when S (or S') becomes

$$P^a(P^{4v/7} + P^{2v/7} + P^{v/7} - I).$$

We notice first that v is odd. For if v is even, then $n = 2q$ is a square (see

https://doi.org/10.4153/CJM-1963-014-7 Published online by Cambridge University Press

3), which implies that $q = 2$ since q is prime. But then $(q, v) = 2$, a contradiction. Next a necessary and sufficient condition that S given by (8) satisfy

$$SS' = S'S = 4I$$

is that the sets

$$\{a_1, a_2, a_3, v - a_1, v - a_2, v - a_3\}$$

and

$$\{a_1 - a_2, a_1 - a_3, a_2 - a_3, v - a_1 + a_2, v - a_1 + a_3, v - a_2 + a_3\}$$

coincide, apart from order. Comparing a_3 with each element of the latter set we find three possibilities:

(i) $$a_1 = a_2 + a_3,$$

(ii) $$a_1 = 2a_3,$$

(iii) $$a_2 = 2a_3.$$

Condition (i) implies immediately that v is even, which cannot happen. Condition (ii) implies that

$$a_1 = 6v/7, \qquad a_2 = 5v/7, \qquad a_3 = 3v/7;$$

and Condition (iii) implies that

$$a_1 = 4v/7, \qquad a_2 = 2v/7, \qquad a_3 = v/7.$$

Since

$$\frac{6v}{7} = v - \frac{v}{7}, \qquad \frac{5v}{7} = v - \frac{2v}{7}, \qquad \frac{3v}{7} = v - \frac{4v}{7},$$

these results are the desired ones and the theorem is proved.

It is clear that further progress depends on a study of the solutions of (7) in integral circulants S.

References

1. R. H. Bruck, *Difference sets in a finite group*, Trans. Amer. Math. Soc., *78* (1955), 464–481.
2. M. Hall, Jr., *Cyclic projective planes*, Duke Math. J., *14* (1947), 1079–1090.
3. M. Hall, Jr. and H. J. Ryser, *Cyclic incidence matrices*, Can. J. Math., *3* (1951), 495–502.

National Bureau of Standards
and
Rand Corporation