PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 88, Number 1, May 1983

CIRCULANTS AND DIFFERENCE SETS[1]

MORRIS NEWMAN

For Ernst Straus, on his 60th birthday

ABSTRACT. Let F be any field, $f(x)$ a polynomial over F of degree $\leqslant v-1$, P the $v \times v$ full cycle, and C the $v \times v$ circulant $f(P)$. Assume that if F is of finite characteristic p, then $(p, v) = 1$. It is shown that the rank of C over F is $v - d$, where d is the degree of the greatest common divisor of $f(x)$ and $x^v - 1$. This result is used to determine the rank modulo a prime of the incidence matrix associated with a difference set. The notion of the *degree* of a difference set is introduced. Certain theorems connected with this notion are proved, and an open problem is stated. Some numerical results are appended.

Introduction. The subject matter of this note arose in connection with the isomorphism problem for incidence matrices. The general problem is to decide when two integral matrices A, B are permutation equivalent. A negative answer is furnished when A and B do not have the same Smith Normal Form, or when A and B do not have the same rank over GF(p), where p is a prime. Information concerning this rank is thus of interest. The special case when A and B are circulants is of particular interest, since it is directly linked to the isomorphism problem for (v, k, λ) difference sets. (See [3] for an exposition of this topic.)

We first prove a general theorem for the rank of a circulant, and then apply it to obtain results concerning difference sets. These lead to the interesting idea of the *degree* of a difference set, which in turn leads to a conjecture on the nonexistence of difference sets of a certain type. A partial solution is given, but the general problem remains open.

The rank of a circulant. Let F be a field, v a positive integer. If F is of finite characteristic p, assume that $(v, p) = 1$. Then the polynomial $p(x) = x^v - 1$ has distinct roots. Let F' be the splitting field of $p(x)$ over F. Then $F' = F(\theta)$, where $\theta^v = 1$, but $\theta^m \neq 1$ for $1 \leqslant m < v$.

Let P be the $v \times v$ full cycle

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

Received by the editors June 28, 1982 and, in revised form, August 22, 1982.
1980 *Mathematics Subject Classification.* Primary 05B10; Secondary 15A36.
[1]The preparation of this paper was supported by the National Science Foundation.

0002-9939/82/0000-1072/$02.25

Let $f(x)$ be the polynomial

$$f(x) = \sum_{k=0}^{v-1} a_k x^k, \qquad a_k \in F.$$

The circulant C associated with $f(x)$ is the $v \times v$ matrix

$$C = f(P) = \sum_{k=0}^{v-1} a_k P^k.$$

We are interested in $r(C)$, the rank of C over F. We will prove the following:

THEOREM 1. *The rank of C is given by the formula*

$$r(C) = v - d, \tag{1}$$

where d is the degree of the greatest common divisor of $f(x)$ *and* $p(x)$, *considered as polynomials over F.*

PROOF. The rank of C over F is the same as the rank of C over F'. Define the $v \times v$ Schur matrix S by $S = [\theta^{-ij}]$. Then S is a nonsingular matrix over F', because of the Vandermonde formula for the determinant of S, and the fact that θ is a primitive vth root of unity. Furthermore

$$SPS^{-1} = D = \operatorname{diag}(\theta, \theta^2, \ldots, \theta^v).$$

It follows that

$$SCS^{-1} = f(D) = \operatorname{diag}(f(\theta), f(\theta^2), \ldots, f(\theta^v)).$$

Thus the rank of C, which is the same as the rank of $f(D)$, equals the number of nonzero eigenvalues of C.

Suppose now that over F, $(f(x), p(x)) = d(x)$. Write

$$f(x) = d(x)f_1(x), \qquad p(x) = d(x)p_1(x),$$

where $(f_1(x), p_1(x)) = 1$. It follows that polynomials $g(x)$, $h(x)$ over F exist such that

$$g(x)f_1(x) + h(x)p_1(x) = 1. \tag{2}$$

Let r be any root of $p(x)$ (thus $r = \theta^t, 0 \leq t \leq v - 1$). If r is a root of $d(x)$, then $f(r) = 0$; while if r is a root of $p_1(x)$, $f_1(r) \neq 0$ (because of (2)) and so $f(r) \neq 0$. It follows that the number of zero eigenvalues of C is just d, the degree of $d(x)$. Thus the number of nonzero eigenvalues of C is $v - d$, and the proof is completed.

An immediate consequence of Theorem 1 is

THEOREM 2. *Let*

$$C = f(P) = \sum_{k=0}^{v-1} a_k P^k$$

be an integral $v \times v$ *circulant. Let p be a prime which does not divide v. Then* $r_p(C)$, *the rank of C over* GF(p), *is given by the formula* $r_p(C) = v - d$, *where d is the degree of* $(f(x), x^v - 1)$ *over* GF(p).

Difference sets and circulants. Let v, k, λ be integers such that $0 < \lambda < k < v - 1$, and let $D = \{d_1, d_2, \ldots, d_k\}$ be a (v, k, λ) difference set. This means that every nonzero residue modulo v occurs exactly λ times among the k^2 differences $d_i - d_j$, $1 \leqslant i, j \leqslant k$, while the residue 0 occurs exactly k times. Then $\lambda(v - 1) = k(k - 1)$. As usual, put $n = k - \lambda$.

We say that the difference set D is of *order* n. If $\lambda = 1$, we say that D is *planar*. In this case $k = n + 1$, $v = n^2 + n + 1$.

With the difference set D we associate the circulant C, given by

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

Then C satisfies the usual incidence equations

$$CC^T = C^TC = nI + \lambda J, \qquad CJ = JC = kJ,$$

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

Let a, b be integers, $(a, v) = 1$, and define

$$D' = aD + b = \{ad_1 + b, ad_2 + b, \ldots, ad_k + b\}.$$

It is readily verified that D' is also a difference set. We say that D and D' are *equivalent*. We require the follcwing elementary result:

LEMMA 1. *If D and D' are equivalent, then C_D and $C_{D'}$ are permutation equivalent.*

The proof (which we omit) is an immediate consequence of the fact that P^a is also a full cycle, since $(a, v) = 1$, and so a permutation matrix Q exists such that $P^a = Q^TPQ$.

We now introduce the notion of the *degree* of the difference set D. Clearly, we may assume that $0 \leqslant d_1 < d_2 < \cdots < d_k \leqslant v - 1$, and replacing D by the equivalent difference set $D - d_1$, we may also assume that $d_1 = 0$. If D satisfies $0 = d_1 < d_2 < \cdots < d_k \leqslant v - 1$, we say that D is *normalized*.

Let $D' = \{d_1', d_2', \ldots, d_k'\}$ be any normalized difference set equivalent to D. Define $\delta = \min d_k'$, where D' runs over all normalized difference sets equivalent to D. Then δ will be called the *degree* of D.

It is of interest to bound this number. We prove

THEOREM 3. *The degree δ of D satisfies $\delta \geqslant (v - 1)/2$. If $\lambda > 1$, then the inequality is strict.*

PROOF. The numbers $d_k - d_{k-1}$, $d_{k-1} - d_{k-2}, \ldots, d_2 - d_1$ consist of k positive integers with the property that no integer appears among them more than λ times. Write

$$k - 1 = q\lambda + r, \quad q = [(k - 1)/\lambda], \qquad 0 \leqslant r \leqslant \lambda - 1. \tag{3}$$

Then

$$\sum_{i=2}^{k} (d_i - d_{i-1}) \geqslant \lambda(1 + 2 + \cdots + q) + r(q + 1),$$

which implies that

$$d_k \geqslant (q+1)(\tfrac{1}{2}\lambda q + r) = (q+1)((k-1+r)/2).$$

Suppose first that λ does not divide $k-1$. Then $r \geqslant 1$, $q+1 > (k-1)/\lambda$, and (3) implies that

$$d_k > \left(\frac{k-1}{\lambda}\right)\left(\frac{k}{2}\right) = \frac{v-1}{2}.$$

(Notice that $\lambda > 1$ in this case.) Now suppose that λ does divide $k-1$. Then $r = 0$, $q = (k-1)/\lambda$, and (3) implies that

$$d_k \geqslant \left(\frac{k-1}{\lambda} + 1\right)\left(\frac{k-1}{2}\right).$$

Thus if $\lambda > 1$,

$$d_k > \left(\frac{k}{\lambda}\right)\left(\frac{k-1}{2}\right) = \frac{v-1}{2};$$

and if $\lambda = 1$,

$$d_k \geqslant k\left(\frac{k-1}{2}\right) = \frac{v-1}{2}.$$

This completes the proof.

The next theorem we wish to prove is as follows:

THEOREM 4. *Let D be a difference set of degree δ. Let p be a prime dividing n which does not divide v. Then*

$$v - \delta \leqslant r_p(C_D) \leqslant 1 + \delta. \tag{4}$$

PROOF. Because of Lemma 1, we may assume that $0 = d_1 < d_2 < \cdots < d_k = \delta$. Then (as in [**2** or **5**]), the polynomial $f(x) = \sum_{i=1}^{k} x^{d_i}$ satisfies

$$x^{\delta} \cdot f(x) f\left(\frac{1}{x}\right) \equiv nx^{\delta} + \lambda \frac{x^v - 1}{x - 1} \mod x^v - 1.$$

Thus over GF(p), since p divides n, we have

$$x^{\delta} f(x) f\left(\frac{1}{x}\right) = g(x)\frac{x^v - 1}{x - 1},$$

where $\deg g(x) = 2\delta - v + 1$, since $\deg x^{\delta} f(x) f(1/x) = 2\delta$. Put

$$d = \deg(f(x), x^v - 1).$$

Then certainly $d \leqslant \deg f(x) = \delta$, so that $v - d \geqslant v - \delta$. Furthermore, if $h(x) = (f(x), g(x))$, then $f(x)/h(x)$ divides $x^v - 1$, so that

$$d \geqslant \deg \frac{f(x)}{h(x)} \geqslant \delta - (2\delta - v + 1) = v - 1 - \delta.$$

Thus $v - d \geqslant 1 + \delta$, and the proof is completed.

Notice that if $\delta = (v-1)/2$, then $v - \delta = 1 + \delta = (v+1)/2$, so that $r_p(C_D) = (v+1)/2$ in this case.

A similar argument shows that the inequality

$$r_p(C_D) \leqslant (v+1)/2 \tag{5}$$

is always valid.

It was shown in [2] that if n is square-free and $(n, \lambda) = 1$, then the Smith Normal Form of C_D is

$$I_{v+1}/2 \dot{+} n(I_{v-3}/2) \dot{+} nkI_1.$$

Thus $r_p(C_D)$ is also equal to $(v+1)/2$ in this case, where p is any prime dividing n.

By Theorem 3, a difference set of degree $(v-1)/2$ must be planar. G. Wilson has shown that there are just two such planar difference sets, namely

$$\{0,1,3\} \quad (n=2, v=7, k=3, \lambda=1),$$
$$\{0,2,5,6\} \quad (n=3, v=13, k=4, \lambda=1).$$

Some numerical results, and an open problem. A program which computes the greatest common divisor of two polynomials over GF(p) was prepared, and the rank modulo p of numerous incidence matrices was computed, together with the degrees of the associated difference sets. We give below the results of the computation for the planar difference sets given by H. J. Ryser in [3], and for two other difference sets (with $\lambda = 7, 10$, respectively) given by M. Hall in [1]. The results for the rank when n is prime were predictable by virtue of the fact that the rank modulo n must then be $(v+1)/2$.

An open question is to determine the rank modulo p as a function of v, k, λ, n, p (if indeed such a formula exists) even for the case when n is a power of p.

The inequality $v - \delta \leqslant r_p$ of (4) becomes an equality in cases 1, 2, 3, 6, 9 below. All instances of $p = 2$ occur among these. The inequality $r_p \leqslant \delta + 1$ of (4) becomes an equality only for cases 1, 2 below. This prompts the (somewhat dubious) conjecture that if n is even and v is odd, then $r_2 + \delta = v$. The inequality $r_p \leqslant (v+1)/2$ given in (5) becomes an equality when n is square-free and $(n, \lambda) = 1$, as was already mentioned. Quite possibly these are the only cases of equality.

v	k	λ	n	p	D	r_p	δ
7	3	1	2	2	0, 1, 3	4	3
13	4	1	3	3	0, 2, 5, 6	7	6
21	5	1	4	2	0, 1, 4, 14, 16	10	11
31	6	1	5	5	0, 1, 3, 8, 12, 18	16	17
57	8	1	7	7	0, 1, 3, 13, 32, 36, 43, 52	29	35
73	9	1	8	2	0, 1, 3, 7, 15, 31, 36, 54, 63	28	45
91	10	1	9	3	0, 1, 3, 9, 27, 49, 56, 61, 77, 81	37	55
133	12	1	11	11	0, 1, 3, 12, 20, 34, 38, 81, 88, 94, 104, 109	67	85
31	15	7	8	2	0, 1, 2, 3, 5, 7, 11, 14, 15, 16, 22, 23, 26, 28, 29	6	25
43	21	10	11	11	0, 1, 2, 3, 4, 7, 10, 11, 15, 18, 19, 20, 21, 26, 31, 32, 34, 36, 38, 40, 41	22	37

References

1. M. Hall, Jr., *A survey of difference sets*, Proc. Amer. Math. Soc. **7** (1956), 975–986.

2. M. Newman, *Invariant factors of combinatorial matrices*, Israel J. Math. **10** (1971), 126–130.

3. H. J. Ryser, *Combinatorial mathematics*, Carus Math. Monographs, no. 14, Math. Assoc. Amer., distributed by Wiley, New York, 1963.

Department of Mathematics, University of California, Santa Barbara, California 93106