g-CIRCULANT MATRICES OVER A FIELD OF PRIME CHARACTERISTIC[1]

BY

J. L. BRENNER

1. Introduction

This article is concerned with circulant matrices (and certain generalizations of them) over a field of prime characteristic.

In previous papers, the roots, vectors, and determinants of circulant matrices and g-circulant matrices have been found [1], [2]. A circulant matrix $A = (a_{ij})$ is one in which each row (except the first) is obtained from the preceding row by a cyclic shift:

$$a_{i+1,j} = a_{i,j-g} .$$

When g is 1, A is a classical (1-) circulant. When g is prime to the order n of the matrix, the theory is a generalization of the classical one. When g, n have common factors, complications can occur.

Let $P = P_n$ be the permutation matrix corresponding to the cyclic permutation $(123\cdots n)$:

$$P = P_n = \begin{bmatrix} 0 & I_{n-1} \\ 1 & 0 \end{bmatrix},$$

where I_{n-1} is the identity matrix of dimension $n - 1$. A classical (1-) circulant is a matrix A of the form $a_{11} I_n + a_{12} P + \cdots + a_{1n} P^{n-1}$. The following lemma is an easy consequence of this definition.

LEMMA 1. *A is a 1-circulant if and only if the relation $AP_n = P_n A$ holds.*

First proof. For any matrix, $P_n A$ is the matrix obtained by raising the rows of A, and AP_n is the matrix obtained by circulating the columns of A. A necessary and sufficient condition that A be a 1-circulant is that these be equal.

Second proof. If A is a polynomial in P_n, clearly $AP_n = P_n A$. Conversely, if $AP_n = P_n A$, then A is a polynomial in P_n, since the eigenvalues w_i of P_n satisfy $\det [w_i^j]_1^n \neq 0$.

LEMMA 2. *A necessary and sufficient condition that A be a g-circulant is is that the relation $P_n A = AP_n^g$ hold.*

The proof of Lemma 2 is the same as the first proof of Lemma 1. A g-circulant is not necessarily a polynomial in P_n.

If A_1 is an invertible g-circulant, and A is an arbitrary g-circulant, the

Received November 4, 1961.

[1] Sponsored by the Mathematics Research Center, U. S. Army, Madison, Wisconsin.

matrix AA_1^{-1} is a 1-circulant. When $(g, n) > 1$, this statement is vacuous, since there is no invertible g-circulant in this case.

If the underlying field has prime characteristic p and the dimension n is divisible by p, the theory is different from the classical one. The first proof of Lemma 1 remains valid, but the second proof requires modification; it is necessary to exhibit the vectors of the matrix P_n itself.

In this article, the structure of P_n is found, and the eigenvalues, vectors, and determinant of A are obtained as a corollary. This recaptures results of Silva [4]. The (more complicated) structure of a g-circulant matrix A over a field of prime characteristic can also be found from the structure of P_n. The intricacies of the calculation do not seem worth expounding in all detail; representative results and corollaries are given (Theorems 2, 3).

The methods of this article apply also to composite matrices (Kronecker products); this has been pointed out by B. Friedman [3].

2. Circulant matrices over a field of prime characteristic. 1-circulants

When the underlying field K has prime characteristic p, new phenomena arise if the characteristic divides the order of the matrices.

Suppose $n = p^t m$, $(m, p) = 1$, $q = p^t$. Let the field K be extended (if necessary) so that 1 has m distinct m^{th} roots $r, r^2, \cdots, r^m = 1$. The solution of an $n \times n$ matrix $A = (a_{ij})$ for which

$$P_n A = AP_n$$

is obtained as follows.

Let N be the $n \times n$ matrix $[N_1, N_2, \cdots, N_m]$, where N_h is the $n \times q$ matrix

$$N_h = \begin{bmatrix} 1 & & & \\ r^h & 1 & & \\ r^{2h} & 2r^h & 1 & \\ r^{3h} & 3r^{2h} & 3r^h & 1 \\ & \cdots & & \\ r^{(n-1)h} & \cdots & & \end{bmatrix},$$

the coefficients of the powers of r being the binomial coefficients, and write $D_h = r^h I_q + H_q$, where

$$H_q = \begin{bmatrix} 0 & I_{q-1} \\ 0 & 0 \end{bmatrix}.$$

LEMMA 3. *Suppose $n = p^t m = qm$, $(m, p) = 1$. Then for $1 \leqq k < q$, the binomial coefficient C_k^n is divisible by p.*

Proof. From elementary number theory, C_k^n is divisible by p exactly

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^t}\right]+\left[\frac{n}{p^{t+1}}\right]+\cdots-\left[\frac{n-k}{p}\right]-\left[\frac{n-k}{p^2}\right]$$
$$-\cdots-\left[\frac{k}{p}\right]-\left[\frac{k}{p^2}\right]-\cdots-\left[\frac{k}{p^{t-1}}\right]$$

times. Since $\left[\frac{n-k}{p^t}\right] < \left[\frac{n}{p^t}\right]$, the lemma follows.

COROLLARY. *The matrix equation $PN_h = N_h D_h$ holds.*

(This is checked by direct computation, with Lemma 3 providing support for the equality of the last rows of the matrix products PN_h, $N_h D_h$.)

Thus the matrix N transforms P into the classical canonical form

$$N^{-1}PN = D = D_1 \oplus \cdots \oplus D_m .$$

Therefore $N^{-1}AN$ must have the form

$$N^{-1}AN = A^{(1)} \oplus \cdots \oplus A^{(m)},$$

where

$$A^{(h)} = w_1(h, A)\, I_q + w_2(h, A)\, H_q + w_3(h, A)\, H_q^2 + \cdots ,$$

and

$$w_k(h, A) = \sum_{j=0}^{n-k} a_{1,k+j}\, r^{jh}\, C_j^{k+j}, \qquad 1 \leqq k \leqq q. \tag{1}$$

These facts are summarized in the following theorem.

THEOREM 1. *Let $A = (a_{ij})$ be an $n \times n$ circulant matrix, $P_n A = AP_n$, over a field K of prime characteristic p, $n = p^t m$, $(m, p) = 1$, $p^t = q$. Let r be a primitive m^{th} root of 1 in a suitable extension field of K.*

1. *The roots of A are $w_1(h, A)$ as given by (1) $(h = 1, 2, \cdots, m)$. Each has algebraic multiplicity $q = p^t$.*

2. *The geometric multiplicity corresponding to the root $w_1(h, A)$ is l, where $l = l(h) \leqq q$ is defined by the requirements*

$$w_2(h, A) = \cdots = 0, \qquad w_{l+1}(h, A) \neq 0.$$

In particular, $l = 1$ if $w_2(h, A) \neq 0$, and $l = q$ if

$$w_2(h, A) = \cdots = w_q(h, A) = 0.$$

The vectors which correspond to these roots are obtainable by inspection of the canonical form for A. The results of [4] are clearly corollary to Part 1 of Theorem 1, since

$$\det A = \textstyle\prod_h \det F_h = [\prod_h w_1(h, A)]^q.$$

The following examples are of interest. The matrix

$$\begin{bmatrix} 1 & -1 & 1 & -1 & 0 \\ 0 & 1 & -1 & 1 & -1 \\ -1 & 0 & 1 & -1 & 1 \\ 1 & -1 & 0 & 1 & -1 \\ -1 & 1 & -1 & 0 & 1 \end{bmatrix}$$

has determinant 0, and over a ground field of characteristic 5 has the elementary divisors λ^3, λ^2.

If all the zeros in this matrix are replaced by units, the new matrix has the elementary divisor $(\lambda - 1)^5$ over the same ground field.

3. Circulant matrices over a field of prime characteristic. g-circulants

Let $A = (a_{ij})$ be an $n \times n$ matrix over the field K of characteristic p, $n = p^t m$, $(m, n) = 1$, $q = p^t$. Suppose A is a g-circulant, i.e.,

$$P_n A = A P_n^g, \qquad (g, m) = 1.$$

By using the equivalence relation "$\sim$" among the residue classes mod m:

$$h_1 \sim h_2 \quad \Leftrightarrow \quad \exists x,\ g^x h_1 \equiv h_2 \pmod{m},$$

we separate these residue classes mod m into k equivalence classes C_i, with $f_1, f_2, \cdots, f_k$ elements

$$C_i \equiv \{g h_i, g^2 h_i, \cdots, g^{f_i} h_i \mod m\}, \qquad i = 1, 2, \cdots, k.$$

If D_h is the matrix $r^h I_q + H_q$, there is a matrix N which transforms P_n into the canonical form

$$\tilde{P} = N^{-1} P_n N = D^{(1)} \oplus \cdots \oplus D^{(k)}, \tag{2}$$

where

$$D^{(i)} = D_{gh_i} \oplus D_{g^2 h_i} \oplus \cdots \oplus D_J, \qquad \text{where } J = g^{f_i} h_i. \tag{3}$$

Let $\tilde{A}$ be the matrix $N^{-1} A N$. Then the relation

$$\tilde{P} \tilde{A} = \tilde{A} \tilde{P}^g$$

holds. We now use the following lemma.

LEMMA 4. *If G, K are square matrices, the matrix equation*

$$GX = XK$$

has only the trivial solution $X = 0$ unless G, K have a common eigenvalue.

This lemma is usually derived as a corollary to a longer theorem. A simple direct inductive proof can be given, the induction being on the dimension of G. Without loss of generality, assume G, K to be in Jordan form (otherwise consider $SGS^{-1}(SXT) = (SXT)T^{-1}KT$). If no eigenvalue of K is equal to the last eigenvalue of G, the last row of X is zero in the first, second, $\cdots$, every column. This reduces the dimension of the assertion by one unit, and the induction is complete.

From Lemma 3 it follows that $\tilde{A}$ has the form $\tilde{A} = A^{(1)} \oplus \cdots \oplus A^{(k)}$, conformal with (2), and the form of $A^{(i)}$ will be obtained from the determining condition

$$D^{(i)}A^{(i)} = A^{(i)}\,[D^{(i)}]^{g},$$

where $D^{(i)}$ is given by (3). A second application of Lemma 4 shows that $A^{(i)}$ must have the form

$$A^{(i)} = \begin{bmatrix} 0 & 0 & \cdots & A_1^{(i)} \\ A_2^{(i)} & 0 & \cdots & 0 \\ 0 & A_3^{(i)} & \cdots & 0 \\ & \cdots & & \\ 0 & 0 & \cdots & A_{f_i}^{(i)} \end{bmatrix},$$

conformal with $D^{(i)}$, each square submatrix $A_j^{(i)}$ being of dimension q. Moreover, these submatrices must satisfy the equations (indices i omitted)

$$D_{gh}\,A_1 = A_1[D_{g^fh}]^g,$$
$$D_{g^2h}\,A_2 = A_2[D_{gh}]^g,$$
$$\vdots$$
$$D_{g^fh}\,A_f = A_f[D_{g^{f-1}h}]^g\,.$$

The most general solution of these equations can be found by use of the binomial formula

$$[D_h]^g = r^{gh}I_q + gr^{h(g-1)}H_q + \tfrac{1}{2}g(g-1)r^{h(g-2)}H_q^2 + \cdots .$$

(Note that H_q^α has a line of 1's in the α^{th} superdiagonal and 0's elsewhere.)

We shall not carry out the details, except to note the interesting fact that each $A_s^{(i)}$ is upper triangular, and the (u, u) element of $A_s^{(i)}$ is $g^{u-1}r^{e(s)}$ times as great $[e(s) = (u-1)g^{s-1}h(g-1)]$ as the $(1, 1)$ element $a_{11}^{(is)}$ of $A_s^{(i)}$ $(u = 2, \cdots, f)$.

THEOREM 2. *If $(g, p) = 1$, the matrix $A^{(i)}$ is either invertible or nilpotent.*

Proof. It is obvious that $[A^{(i)}]^{f_i}$ is (upper triangular, and) either invertible or nilpotent. Theorem 2 follows.

This theorem has interesting corollaries. We mention only

COROLLARY 1. *If $p = 5$, a 3-circulant of dimension $4\cdot 5^t$ is either invertible or nilpotent.*

For 3 is a primitive root mod 4. More generally, we have

COROLLARY 2. *If g is a primitive root* mod p_1^α [mod $2p_1^\alpha$], *a g-circulant of dimension $p_1^\alpha p_2^\beta$ [dimension $2p_1^\alpha p_2^\beta$] is either invertible or nilpotent, provided* $(g, p_1 p_2) = 1$ $[(g, 2p_1 p_2) = 1]$ *($p_1 \neq p_2$ odd primes).*

THEOREM 3. *The eigenvalues of $A^{(i)}$ are precisely the numbers*

$$\rho\, g^{u-1} a^{(i)} \qquad (u = 1, \cdots, q, \quad g^0 = 1),$$

where $a^{(i)}$ is an f_i^{th} root of $\prod_{s=1}^{f_i} a_{11}^{(is)}$, and ρ runs through the f_i^{th} roots of 1.

COROLLARY. *If $(g, p) = 1$, and if all $f_i < p$ (in particular, if $m < p$), the elementary divisors of A are all simple if A is invertible.*

In the contrary case, this need not be true.

The eigenvectors of A can be given explicitly. Since the results are not startling, the work is straightforward, and the details are tedious, they are omitted.

REFERENCES

1. C. M. ABLOW AND J. L. BRENNER, *Circulant and composite circulant matrices*, Trans. Amer. Math. Soc., to appear.
2. J. L. BRENNER, *Mahler matrices and the equation $QA = AQ^m$*, Duke Math. J., vol. 29 (1962), pp. 13–28.
3. B. FRIEDMAN, *Eigenvalues of composite matrices*, Proc. Cambridge Philos. Soc., vol. 57 (1961), pp. 37–49.
4. JOSEPH A. SILVA, *A theorem on cyclic matrices*, Duke Math. J., vol. 18 (1951), pp. 821–825.

UNIVERSITY OF WISCONSIN
MADISON, WISCONSIN
STANFORD RESEARCH INSTITUTE
MENLO PARK, CALIFORNIA