On Some Properties of Circulant Matrices

Paolo Zellini

Istituto di Scienze dell'Informazione
Università di Pisa
Pisa, Italy

Submitted by David H. Carlson

ABSTRACT

A class Σ of matrices is studied which contains, as special subclasses, p-circulant matrices (p > 1), Toeplitz symmetric matrices and the inverses of some special tridiagonal matrices. We give a necessary and sufficient condition in order that matrices of Σ commute with each other and are closed with respect to matrix product.

1. INTRODUCTION

A p-circulant matrix, as defined in [1], [4] and [6], is an n × n matrix over the complex field in which the 𝑖th row (𝑖 = 2, 3, ..., n) is obtained from the (𝑖−1)th row by shifting each element 𝑝 columns to the right. A p-circulant, for 𝑝 = 1, is a circulant matrix.

The following properties are verified: if 𝐴 is a p-circulant and 𝐵 is a q-circulant, then 𝐴𝐵 is a k-circulant, where 𝑘 ≡ 𝑝·𝑞 modulo n [1]; the inverse of a nonsingular p-circulant 𝐴 is a q-circulant 𝐵 where 𝑝·𝑞 ≡ 1 modulo n [4]. Also it is known that p-circulant n × n matrices can be simultaneously transformed to a direct sum of broken-diagonal matrices [1, 6]. Moreover a pseudocommutativity property is satisfied: p-circulant n × n matrices, with (𝑛, 𝑝) = 1, are k-commutative, where 𝑘 is the index to which 𝑝 belongs modulo n (see Theorem 3.1).

All these properties appear as a generalization of previously stated results about circulant matrices: the class of circulant matrices is a monoid. The inverse of a nonsingular circulant matrix is circulant. Circulant matrices can be simultaneously transformed by unitary transformations to an explicit canonical form. Finally, circulant matrices commute with each other. In this work we wish to explore the relationship between commutativity and...
$k$-commutativity and structural properties of $p$-circulant matrices. More precisely, we shall be considering in the next section a class $\Sigma$ of $n \times n$ matrices defined in terms of $n$ different parameters in the complex field, which contains, as a special subclass, $p$-circulant matrices. Subclasses $\Sigma_g \subset \Sigma$ are then defined in terms of different dispositions of these parameters in the matrices of $\Sigma$. If $n$ is a prime integer, then we prove, in Sec. 3, that the only $\Sigma_g$ whose matrices commute with each other are the spaces of matrices $A$ such that $A = P^{-1}CP$, where $C$ is circulant and $P$ is a permutation matrix, or the identity.

In the last section we prove also (if $n$ = prime integer) that matrices $P^{-1}CP$, where $C$ is $n \times n$ circulant and $P$ is a permutation matrix or the identity, are the unique $\Sigma$, which are closed with respect to matrix multiplication within a subclass $\Sigma'$ of $\Sigma$. Thus, in $\Sigma'$, the only subalgebra of dimension $n$ is the only class of matrices which commute with each other. In our opinion the proof of all these properties of circulant matrices may serve as an introduction to a deeper investigation of the existence of not accidental connections of commutativity and $k$-commutativity with structural properties of classes of matrices.

Also, not only commutativity (and $k$-commutativity), but also properties of special classes of $n \times n$ matrices which can be described as algebras of dimension $k < n^2$, are relevant to the solution of algebraic-complexity problems in which well-structured matrices are involved (see for instance [3] and [7]).

2. DEFINITION AND PROPERTIES OF THE CLASS $\Sigma$ AND $\Sigma'$

Let $\Sigma$ be the class of $n \times n$ matrices which is defined as follows: $A = (\alpha_{ij}) \in \Sigma$ if and only if there exist $n^2$ functions $f_{ij}$, $i, j = 0, 1, \ldots, n - 1$, of $n$ complex parameters $a_0, a_1, \ldots, a_n$, and choices $\tilde{a}_0, \tilde{a}_1, \ldots, \tilde{a}_{n-1}$ of the parameters such that

(i) $\forall i, j, f_{ij}(a) = a_k$ for some $k$;
(ii) $\forall k$ there is a pair of indices $i, j$ such that $f_{ij}(a) = a_k$;
(iii) $\alpha_{ij} = f_{ij}(\tilde{a}_0, \tilde{a}_1, \ldots, \tilde{a}_{n-1})$.

$\Sigma$ may also be described as the class of $n \times n$ matrices which have the form

$$\sum_{k=0}^{n-1} a_k I_k.$$  (2.1)
for some complex $a_0, \ldots, a_{n-1}$, and some matrices $J_k = (j_{p,q}^{(k)})$ of zeros and ones which satisfy

(i') $\sum_{k=0}^{n-1} J_k = J$, where $J = (j_{p,q})$ is such that $j_{r,s} = 1$, $(r,s = 0,1,\ldots,n-1)$;
(ii') for every $k$, there exist indices $r,s$ for which $j_{r,s}^{(k)} = 1$;

The subclass $\Sigma \subset \Sigma$ is then defined as follows: a matrix $A$ of $\Sigma$ belongs to $\Sigma'$ if and only if

(iv) for every $i$ (or $j$) and for every $k$ there is an index $j$ (or $i$) such that

(v) $f_{ii}(a) = a_k$;

Thus $\Sigma'$ can be described by considering matrices (2.1) where each row and each column contains all parameters $a_k \ (k = 0,1,\ldots,n)$ and just one parameter is contained by the leading diagonal. This means that the $J_k$ must satisfy the following conditions:

(iii') Let $k$ be given; then for every $p$ (or $q$) there is only one $q$ (or $p$) such that $f_{p,q} = 1$;
(iv') $I_r = I$ for an index $r$.

Note that (i')-(iv') are equivalent to the following:

(*) $\mathcal{J} = \{J_0, J_1, \ldots, J_{n-1}\}$ is a set of $n \times n$ permutation matrices one of which is $I$ and such that $\sum_{k=0}^{n-1} I_k = J$.

Let $E_n = \{0,1,\ldots,n-1\}$, and let $g$ be a map of $E_n \times E_n$ onto $E_n$. This map defines a class $\Sigma_g \subset \Sigma$ whose matrices $A = (a_{ij})$ are such that $f_{ij}(a) = a_k$ with $k = g((i,j))$. Obviously, giving a map $g$ is the same as giving $n$ matrices $J_k$ which satisfy (i') and (ii'). Then these matrices $J_k$ form a base for the vector space $\Sigma_g$. In particular, if $g((i,j)) = n - ip + j \ (\text{mod} \ n)$ and $f_{ij} = a_{ij} \ (i,j = 0,1,\ldots,n-1)$, then $\Sigma_g$ is the space of $p$-circulant matrices.

Toeplitz symmetric matrices and the inverses of some special tridiagonal matrices (see [2]) give other examples of spaces $\Sigma_g$.

In the next section we shall prove (if $n = \text{prime integer}$) that the unique spaces $\Sigma_g$ whose matrices commute with each other are the spaces of matrices of the form $P^{T}CP$, where $C$ is circulant and $P$ is a permutation matrix or the identity.

In the last section we shall prove also (if $n = \text{prime integer}$) that matrices of the form $P^{T}CP$ are the unique $\Sigma_g \subset \Sigma'$ such that, if $A,B \in \Sigma_g$, then $A \cdot B \in \Sigma_g$. This means that if $n = \text{prime integer}$, then the space of $n \times n$ circulant matrices is the unique space $\Sigma_g$ which is an algebra of commutative matrices within the class $\Sigma$.
3. PROPERTY OF COMMUTATIVITY OF MATRICES OF $\Sigma$

In order to find spaces $\Sigma_g$ such that $A, B \in \Sigma_g$ implies $AB = BA$, we proceed as follows: at first, the commutativity property of matrices of a space $\Sigma_g$ is expressed in terms of commutativity of the matrices $J_k$ which are related to $g$ (Lemma 3.1).

Moreover, the matrices $J_k$ must satisfy the properties (iii') and (iv') (Lemma 3.2). A sufficient condition is then given in order that the matrices of a particular $\Sigma_g$ have the form $P^tCP$, where $C$ is circulant and $P$ is a permutation matrix or the identity (Lemma 3.3). Finally, this condition is shown to be verified by the spaces $\Sigma_g$ of $n \times n$ matrices (with $n =$ prime integer) which commute with each other (Theorem 3.2).

**Lemma 3.1.** Let $A(a) = \Sigma_{r=0}^{n-1} a_r J_r$ and $B(b) = \Sigma_{s=0}^{n-1} b_s J_s$. Then $A(a) \cdot B(b) = B(b)A(a)$ if and only if $I_j J_s = J_s I_j$ for every $r$ and $s$.

**Proof.** The condition is known to be sufficient. The condition is also necessary because $AB - BA = \Sigma_{r,s} a_r b_s (J_r J_s - J_s J_r) \equiv 0$ in the $a_r$ and $b_s$ implies $I_r J_s - I_s J_r = 0$.

**Lemma 3.2.** Let $g$ be a map of $(E_n \times E_n)$ onto $E_n$. If $A, B \in \Sigma_g$ implies $AB = BA$, then $\Sigma_g \subset \Sigma'$.

**Proof.** Let $A(a) = \Sigma_{r=0}^{n-1} a_r J_r$, $B(b) = \Sigma_{s=0}^{n-1} b_s J_s$ and $A(a)B(b) - B(b)A(a) \equiv 0$. Suppose that condition (iii') is not verified; in particular, suppose that one of the following is satisfied:

1. There is a $k \in E_n$ such that, for an index $p \in E_n$, $i_{p,l}^{(k)} \neq 1$ for every $l \in E_n$.
2. There is a $k \in E_n$ such that, for an index $p \in E_n$, $i_{p,l}^{(k)} = i_{p,l'}^{(k)} = 1$ where $l \neq l'$.

Let (1) be satisfied; then there is a $q$ such that, for some $m \in E_n$, $i_{q,m}^{(k)} = 1$ [by (i')]; also, by (iii'), there is a $k' \in E_n$ such that $i_{p,q}^{(k')} = 1$. Thus we have $J_k J_k = J_{k'} J_{k'}$, but this is impossible by Lemma 3.1. If (2) is true, then also (1) is true [by (ii')]; this proves that condition (iii') must be verified. As regard as condition (iv'), suppose $i_{0,k}^{(k)} = 1$ for every $k$, and let $i_{p,q}^{(r,s)}$ be the element $(p,q)$ in the product $J_r J_s$. Now we have $i_{0,k}^{(0,k)} = 1$ for every $k$ and, as $J_0 J_k = J_k J_0$ for every $k$, we have also $i_{0,k}^{(k,0)} = 1$; then $i_{k,k}^{(0,0)} = 1$ for every $k$, i.e., $J_0 = 1$. 


COROLLARY 3.1. If \( g((i,j)) = n - ip + j, \ p > 1 \) (i.e., the matrices of \( \Sigma_g \) are \( p \)-circulant), then \( \Sigma_g \) is a space of matrices which commute with each other if and only if \( p = 1 \).

Proof. If \( p = 1 \), then the matrices of \( \Sigma_g \) are circulant and commute with each other. If the matrices of \( \Sigma_g \), where \( g((i,j)) = n - ip + j \), commute with each other, then, as we may suppose without loss of generality \( r_{0,k}^{(k)} = 1 \) \( \forall k \in \mathbb{E}_n \), we have \( g((i,i)) = 0, \ i = 0, \ldots, n - 1 \) (by the previous theorem). In the present case \( g((i,i)) = n - i(p - 1) \mod n \) implies \( g((i,i)) = 0 \) if and only if \( p = 1 \).

We recall that a set of matrices \( \{A_1, \ldots, A_n\} \) is said to be \( f \)-commutative if and only if \( f \) is the smallest integer such that all the products \( A_{p_1} A_{p_2} \ldots A_{p_f} \) commute with each other and some linear combination of \( A_1, \ldots, A_n \) is nonsingular.

If \( p > 1 \) and \( (n, p) = 1 \), then, by the results which are described in [1], it is easy to prove that \( n \times n \) \( p \)-circulant matrices are \( f \)-commutative for some integer \( f < \phi(n) \), where \( \phi(n) \) is the Euler function of \( n \).

THEOREM 3.1 (see [7]). Let \( (n, p) = 1 \), and let \( A_1, A_2, \ldots, A_k \) \( (k > 2) \) be \( p \)-circulant matrices of order \( n \). Then \( A_1, A_2, \ldots, A_k \) are \( f \)-commutative, where \( f \) is the index to which \( p \) belongs modulo \( n \).

Proof. If \( (n, p) = 1 \), then we have \( p^f \equiv 1 \) modulo \( n \), where \( f \) is the index to which \( p \) belongs modulo \( n \). Thus every product \( A_{q_1} A_{q_2} \ldots A_{q_f} \) is \( 1 \)-circulant (see [1], Theorem 3.1) and the \( A_i \) are \( f \)-commutative.

From now on we shall suppose, for all \( \Sigma_g \subset \Sigma' \), that \( r_{0,k}^{(k)} = 1, \ k = 0, 1, \ldots, n - 1 \).

LEMMA 3.3. Let \( J_0, J_1, \ldots, J_{n-1} \) be \( n \) matrices which satisfy (i'), (ii'), (iii'), (iv'), and let \( (h_0 h_1 \cdots h_{n-1}) (h_0 = 0) \) be a permutation of \( E_n \) such that \( r_{0,k}^{(k)} = 1 \) implies

\[
h_k + h_q = n \mod n. \tag{3.1}
\]

then \( P J_k P = C_k, \ k = 0, 1, \ldots, n - 1 \), where \( C_k \) is circulant and \( P \) is the permutation matrix whose \( i \)th row is the \( h_i \)th row of the identity.

Proof. Let \( C_k = P J_k P \) with \( p_{i,i} = \delta_{i,k} \). Then one easily calculates that \( r_{0,k}^{(k)} = 1 \) implies \( h_k + p = q \mod n \). Thus \( C_k \) is circulant with \( c_{0,k}^{(k)} = 1 \).
Example 3.1. Let $n=5$, and let $\Sigma_g$ be the space of matrices $A(a) = \Sigma_{a=0}^{n-1} a_k I_k$ which have the following form:

$$A(a) = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ a_2 & a_0 & a_3 & a_4 & a_1 \\ a_1 & a_4 & a_0 & a_2 & a_3 \\ a_4 & a_3 & a_1 & a_0 & a_2 \\ a_3 & a_2 & a_4 & a_1 & a_0 \end{bmatrix}.$$

The permutation $(h_0 h_1 h_2 h_3 h_4) = (01432)$ satisfies (3.1). (For instance $i^{(1)}_1 = 1$, i.e., $a_1$ is in the 2nd row and in the 5th column, corresponds to the identity $h_1 + h_1 = h_4$ modulo 5, i.e., $1 + 1 = 2$.) If instead it is not possible to find a permutation $(h_0 h_1 h_2 h_3 h_4)$ which satisfies the condition (3.1). In fact we cannot find a permutation matrix $P$ such that $P^T A(a) P$ is circulant.

Let us observe that the position $h_0=0$ is related to the fact that $J_0 = I$.

Lemma 3.4. Let $J_0, J_1, \ldots, J_{n-1}$ be $n$ matrices which satisfy (i'), (ii'), (iii'), (iv'), and let $j^{(p)}_{i,k} = j^{(q)}_{i,k} = j^{(r)}_{i,k} = 1$ for some $p$, $q$, $i$ and $k$. If $J_r J_s = J_s J_r$ ($r,s = 0,1,\ldots,n-1$), then $j^{(p)}_{i,k} = 1$.

Proof. By multiplying $J^p$ by $J^q$ we find $j^{(p,q)}_{i,k} = 1$ (i.e., the element in the $i$th row and $k$th column of $J^p J^q$ is 1). By the hypothesis $J_r J_q = J_q J_r$; then we must have $j^{(p,q)}_{i,k} = 1$, that is, $j^{(p)}_{i,k} = 1$.

Theorem 3.2. Let $n$ be prime. If $J$ satisfies (*), and the $J_i$ commute, then for $P_n$, the permutation matrix corresponding to the permutation $(12\ldots n)$, the following holds:

$$(**) \text{ For some permutation matrix } P, \text{ and reindexing, } \quad J_k = P_i^T P_n^{k+i} \quad k = 0,1,\ldots,n-1.$$
Proof. Let the matrices of \( \Sigma_k \) be commutative. Then we have \( I, I, = I J, \)
\((r, s=0,1, \ldots, n-1)\). By Lemma 3.2 the \( J_k \) must satisfy (iii') and (iv'). For every element \( j_{p, q}^{(k)} \) which is different from zero in the matrix \( J_k \) we can define the congruence \( h_k + h_q = h_q \mod n \), where \( h_k, h_p, \) and \( h_q \) are unknowns. Then we associate to the set of all matrices \( J_r \) the set \( S \) of congruences defined below:

\[
h_r + h_p = h_q \mod n, \quad r=0,1, \ldots, n-1, \tag{3.2}
\]

where \( p, q, r \in \mathbb{Z}_n, h_0=0 \) and \( h_1, h_2, \ldots, h_{n-1} \) are unknowns. It is clear that \((p, q) \neq (p', q') \) for \( r \neq r' \).

By Lemma 3.4, if \( j_{p, r}^{(k)} = j_{r, q}^{(k)} = j_{r, s}^{(k)} = 1 \), then the congruence \( h_1 + h_s = h_q \) belongs to \( S \), that is,

\[
\{h_1 + h_p = h_q \in S, \quad h_1 + h_r = h_q \in S, \quad h_1 + h_r = h_s = h_q \in S\} \Rightarrow h_1 + h_r = h_s = h_q \in S.
\]

where we understand modulo \( n \). Let us observe that the congruence on the right is an implication of the three congruences on the left (in fact, it is obtained from the second one by substituting \( h_1 + h_p \) for \( h_1 \), and then \( h_1 \) for \( h_1 + h_r \)). Moreover, if we choose \( \mu = s, \rho = \lambda \), and \( p = 0 \) in (3.3), we have that if \( h_1 + h_r = h_q \in S \), then \( h_1 + h_r = h_q \in S \).

Now, consider the \( n-1 \) permutations \( \Pi^{(p)} \) \((p=1,2, \ldots, n-1) \) of \( \mathbb{Z}_n \)
which are defined as follows: if \( j_{p, r}^{(k)} = 1 \), then \( \Pi^{(p)} = r \). It is clear that \( \Pi^{(p)} \) gives the exact disposition in the \( p \)th row of the parameters \( a_0, a_1, \ldots, a_{n-1} \).

Every permutation \( \Pi^{(p)} \) can be written as a product of \( l_p \) disjoint cycles whose degrees are, respectively, \( r_1^{(p)}, r_2^{(p)}, \ldots, r_{l_p}^{(p)} \). Also, \( \sum_{p=1}^{l_p} r_p^{(p)} = n \), and by (i')-(iv'), \( r_{l_p}^{(p)} > 2 \).

Consider the permutation \( \Pi^{(k)}, k \neq 0 \). We want to prove that \( l_k = 1 \). Let \( l_k > 1 \); then, as \( n \) is prime, there exist indices \( p_1, p_2, \ldots, p_r \) and \( q_1, q_2, \ldots, q_s \) with \( r \neq s, r + s < n \) and \( p_1 = 0, p_r = k \) such that the following congruences belong to \( S \):

\[
h_{p_i} + h_k = h_{p_{i-1}}, \quad i=2, \ldots, r, r+1, \tag{3.4}
\]

\[
h_{q_j} + h_k = h_{q_{j-1}}, \quad j=2, \ldots, s, s+1, \tag{3.5}
\]
where we have put $h_{p_{i+1}} = h_0$ and $h_{q_{i+1}} = h_{q_1}$ (we also have $h_{p_k} = h_k$). Let $s < r$; then by Lemma 3.4, (3.3), (3.4) and (3.5) we have the following recurrent relations:

$$\{ h_{q_{i+1}} + h_{p_{i+1}} = h_{q_1} \in S, \quad h_{q_{i+1}} + h_k = h_{p_{i+1}} \in S, \quad h_{q_{i+1}} + h_k = h_{q_{i-1}} \in S \}$$

$$\Rightarrow \quad h_{q_{i+2}} + h_{q_{i-1}} = h_{q_1} \in S, \quad i = 0, 1, \ldots, s - 2. \quad (3.6)$$

The top congruence in (3.6) is trivial for $i = 0$, and for $i > 1$ is obtained from the last congruence $h_{q_{i+2}} + h_{q_{i-1}} = h_{q_1}$ and from the fact that $h_k + h_p = h_q \in S$ implies $h_k + h_r - h_q \in S$. From (3.6) we infer that both congruences $h_{q_1} + h_{p_k} = h_{q_1}$ and $h_{q_1} + h_{q_1} = h_{q_1}$ must belong to the system (3.2). But this is impossible, because $r \neq s$.

An analogous result is obtained in the case $s > r$. By Lemma 3.4, (3.3), (3.4) and (3.5) we can deduce the following recurrence relations:

$$\{ h_{p_{i+1}} + h_{q_{i+1}} = h_{q_1} \in S, \quad h_{q_{i+1}} + h_k = h_{q_{i+1}} \in S, \quad h_{q_{i+1}} + h_k = h_{p_{i+1}} \in S \}$$

$$\Rightarrow \quad h_{q_{i+2}} + h_{p_{i-1}} = h_{q_1} \in S, \quad j = 0, 1, \ldots, r - 2. \quad (3.7)$$

This implies $h_{q_1} + h_{p_k} = h_{q_1} \in S$ and $h_{q_1} + h_{p_k} - h_{q_1} \in S$, which is obviously impossible.

If $n$ is prime, then we must have $l_k = 1$ for every $k$, $k = 1, 2, \ldots, n - 1$. This implies the existence of $n$ indices $p_1, p_2, \ldots, p_n$ with $p_1 = 0$ and $p_n = k$ such that the following congruences belong to $S$:

$$h_{p_k} + h_k = h_{p_{i-1}} \quad i = 2, \ldots, n, n + 1. \quad (3.8)$$
where we put $h_{p_i \pm 1} = h_{p_i} = h_0$. By Lemma 3.4, (3.3) and (3.8) we have

$$\{ h_{p_{j-1}} + h_{p_{j+1}} = h_{p_j} \in \mathcal{S}, $$

$$h_{p_{j+2}} + h_k = h_{p_{j+1}} \in \mathcal{S}, $$

$$h_{p_{j-1}} + h_k = h_{p_j} \in \mathcal{S} \}$$

$$\Rightarrow h_{p_{j+2}} + h_{p_{j-1}} = h_{p_j} \in \mathcal{S},$$

$$2 < j < n, \quad l = 0, 1, \ldots \left[ \frac{i-3}{2} \right]; \quad (3.9)$$

$$\{ h_{p_{j-t+1}} + h_{p_{j+1}} = h_{p_j} \in \mathcal{S}, $$

$$h_{p_{j+t+1}} + h_k = h_{p_{j+t}} \in \mathcal{S}, $$

$$h_{p_{j-t+1}} + h_k = h_{p_{j-t}} \in \mathcal{S} \}$$

$$\Rightarrow h_{p_{j+t+1}} + h_{p_{j-t}} = h_{p_j} \in \mathcal{S},$$

$$1 < j < n-1, \quad l = 0, 1, \ldots \left[ \frac{n-j-1}{2} \right]. \quad (3.10)$$

From (3.9) and (3.10) we deduce that, if commutativity is satisfied, then all matrices $J_r$, $r = 0, 1, \ldots, n-1$, are completely defined through the congruences (3.8), i.e., through the choice of the $k$th row of each matrix $J_r$ for a single $k$. As any $J_k$ corresponds to a cyclic permutation, it is non-derogatory, and commutes only with polynomials $p(J_k)$. Thus the only permutation matrices commuting with $J_k$ are the monomials $J_k^t$, $t = 0, 1, \ldots, n-1$; so the set $\{ J_k^t \}_{t=0,1,\ldots,n-1}$ is the same set $\{ J_0, J_1, \ldots, J_{n-1} \}$, and the proof is completed.

We note that sets $\mathcal{J}$ satisfying (*) do not necessarily satisfy (**): take for instance $n = 5$ and $\mathcal{J}$ formed by the permutation matrices corresponding to the permutations 1, (12)(345), (13)(524), (14)(235), (15)(423) (see Example 3.1).
Example 3.2. Let \( n = 7 \), and let the permutation \( \Pi^{(3)} \) be written as the product of two cycles of degrees, respectively, 4 and 3:

\[
A(a) = \begin{bmatrix}
    a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\
    \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
    a_1 & a_2 & a_3 & a_0 & a_6 & a_4 & a_5 \\
    \vdots & \vdots & \vdots & a_0 & \vdots & \vdots & \vdots \\
    \vdots & \vdots & \vdots & \vdots & a_1 & \vdots & \vdots \\
    \vdots & \vdots & \vdots & \vdots & \vdots & a_2 & \vdots 
\end{bmatrix}
\]

If the 4th row of \( A(a) \) is \([a_1 a_2 a_3 a_0 a_6 a_4 a_5] \), then we have \( p_1 = 0, p_2 = 1, p_3 = 2, p_4 = 3, p_5 = 0 \) and \( q_1 = 4, q_2 = 6, q_3 = 5 \) (with \( r = 4 \) and \( s = 3 \)), so that (3.4) and (3.5) are, respectively, the following:

\[
\begin{align*}
    h_1 + h_3 &= h_0, & h_6 + h_3 &= h_4, \\
    h_2 + h_3 &= h_1, & h_5 + h_3 &= h_6, \\
    h_3 + h_3 &= h_2, & h_3 + h_3 &= h_5, \\
    h_0 + h_3 &= h_3; 
\end{align*}
\]

(3.11)

Then, repeated applications of (3.6), for \( i = 0, 1 \), lead to \( f^{(3)}_{i_0 i_1} = 1 \); but from (3.11) we infer that \( f^{(3)}_{i_0 i_1} = 1 \), which is impossible.

Let \( n = 5 \), and let the 3rd row of \( A(a) \) be \([a_3 a_2 a_0 a_4 a_1] \) (i.e., the permutation \( \Pi^{(2)} \) is a single cycle). The congruences (3.8) are then the following:

\[
\begin{align*}
    h_3 + h_2 &= 0, \\
    h_4 + h_3 &= h_3, \\
    h_1 + h_2 &= h_4, \\
    h_2 + h_2 &= h_1, \\
    h_0 + h_2 &= h_2, 
\end{align*}
\]

(3.12)

with \( p_1 = 0, p_2 = 3, p_3 = 4, p_4 = 1, p_5 = 2 \).

If commutativity is assumed, then through some repeated applications of (3.9) and (3.10) we can fill in the blanks exactly as shown in the matrix \( A(a) \).
written below:

\[
A(a) = \begin{bmatrix}
  a_0 & a_1 & a_2 & a_3 & a_4 \\
  a_4 & a_0 & a_3 & a_1 & a_2 \\
  a_3 & a_2 & a_0 & a_4 & a_1 \\
  a_2 & a_4 & a_1 & a_0 & a_3 \\
  a_1 & a_3 & a_4 & a_2 & a_0
\end{bmatrix}
\]

4. CLOSURE WITH RESPECT TO PRODUCT OF THE MATRICES OF \( \Sigma' \)

In the present section we are going to find the spaces \( \Sigma_g \subset \Sigma' \) which are closed with respect to matrix product. Lemma 4.1 gives a necessary condition which must be satisfied by the matrices \( I_r \) in order that \( AB \in \Sigma_g \) for any \( A \) and \( B \) which belong to \( \Sigma_g \). If \( n \) is prime, then the previous condition is proved to be a sufficient condition for the commutativity of the matrices \( I_r \). The conclusion then follows from Theorem 3.2: the only \( \Sigma_g \subset \Sigma' \) which is an algebra, apart from transformations through permutation matrices, is the space of circulant matrices. Then commutativity and closure with respect to matrix product are the same concept within all \( \Sigma_g \) which are subclasses of \( \Sigma' \).

**Lemma 4.1.** Let \( \Sigma_g \) (\( \Sigma_g \subset \Sigma' \)) be closed with respect to matrix product. Then for every \( p \) and \( q \) \((p,q \in E_n)\) there is a \( k \in E_n \) such that \( I_p I_q = I_k \).

**Proof.** As we have \( \Sigma_g \subset \Sigma' \) the matrices \( I_r I_s \) satisfy the following conditions: for every \( r \) and \( s \) we can find \( p \) and \( q \) such that \( i_{p,q}^{(r,s)} = 1 \), for every \( p \) (or \( q \)) there is a unique \( q \) (or \( p \)) such that \( i_{p,q}^{(r,s)} = 1 \). Also, if \( i_{p,q}^{(r,s)} = i_{p,q}^{(r',s')} \) and there are not other indices \( t, h \) such that \( i_{p,q}^{(t,h)} = 1 \), then we must have \( I_r I_{r'} I_s I_{s'} = \cdots = I_{s'} I_s I_{r'} I_r \). In fact a proof of the impossibility of the existence of indices \( i \) and \( j \), \( i \neq j \), such that \( I_r I_{r'} I_s I_{s'} \) can be sketched as follows: Let \( I_r I_{r'} I_s I_{s'} \) \((i \neq j)\); then \( i_{p,q}^{(r,s)} \neq i_{p',q'}^{(r,s)} \) for some indices \( p, q, p' \neq p \) and \( q' \neq q \) (we may suppose \( i_{p',q'}^{(r,s)} = 1 \) and \( i_{p,q}^{(r,s)} = 0 \)). In order that \( AB \in \Sigma_g \) for every choice of \( A \) and \( B \) in \( \Sigma_g \), we must have \( A(a) B(b) = \Sigma_{r=0}^{n-1} Y_r I_r \), where the \( Y_r \) are polynomials in the \( a \) and \( b \). Now it is clear that there must be an index \( m \) such that \( Y_m = \sum_{i=1}^{k} a_i b_i \) and \( i_{p,q}^{(m,s)} = 1 \). Also, we cannot find an index \( q_2 \neq q_1 \) such that \( i_{p,q_2}^{(r,s)} = 1 \); thus there is no index \( r \) such that \( i_{p,r}^{(r,s)} = i_{p,r}^{(r,s')} = \cdots = i_{p,r}^{(r,s''')} = 1 \); this means that \( i_{p,s}^{(m)} = 0 \) for every \( s \), which is an absurdity.
Now suppose $J_1J_2 = J_2J_1 = \cdots = J_nJ_1 = J^* \neq I$ for every $t$ ($l > 1$). Let $j^{(a)}_{l,r,s} = 1$. We can find a $J_k$ with $j^{(a)}_{l,r,s} = 1$, and then, from $A(a) = B(b) = \sum_{r,s=0}^{n} b_{r,s} J_{r,s}$, we have $\gamma_k = \sum_{r,s=0}^{n} a_{r,s} b_{r,s}$: in fact we cannot find another product of matrices $J$, which is different from $J^*$ and has 1 in the position $(r,s)$ (this product would bring, eventually, some other $a$ and $b$ into the expression of $\gamma_k$). As $J^* \neq I$, there are indices $t_1, t_2$ with $j^{(a)}_{t_1,t_2} \neq j^{(a)}_{t_1,t_2}$. We may suppose without loss of generality that $j^{(*)}_{t_1,t_2} = 1$ and $j^{(*)}_{t_1,t_2} = 0$. Now there is a $k' \neq k$ such that $j^{(*)}_{t_1,t_2} = j^{(*)}_{t_1,t_2} = 1$, and then $\gamma_{k'} = \sum_{r,s=0}^{n} a_{r,s} b_{r,s} = \gamma_k$, which is impossible.

**Theorem 4.1.** Let $n$ be prime. If $\mathcal{J} = \{J_0, J_1, \ldots, J_{n-1}\}$ satisfies (*) and is closed under multiplication, then (**) holds.

**Proof.** Fix $J_k \neq I$, and consider the disjoint-cycle decomposition of the permutation $\sigma$ corresponding to $J_k$. Let $\tau$ be a cycle of minimal length $t > 1$ in $\sigma$. Then $\tau = 1$ and, as $J_k \in \mathcal{J}$, we have $J_k^t = I$. As $t$ is the minimal length of cycles of $\sigma$, all cycles of $\sigma$ have length $t$, and $t$ divides $n$, a contradiction if $t \neq n$.

Let us observe that Theorem 3.2 and Theorem 4.1 are false for $n$ not prime. For instance, let

$$n = 4 \quad \text{and} \quad P_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

then the matrices

$$I \otimes I, \quad I \otimes P_2, \quad P_2 \otimes I, \quad P_2 \otimes P_2$$

commute with each other and form a set which is closed under multiplication. Obviously they are not similar to a circulant through the same permutation matrix.

We can summarize some of the results we have obtained up to this point in the following

**Theorem 4.2.** The only $\Sigma_n \subset \Sigma$ which constitute a commutative algebra are the spaces of $n \times n$ matrices ($n = \text{prime integer}$) of the form $P^T \mathcal{C} P$, where $\mathcal{C}$ is circulant and $P$, which depends on $g$, is a permutation matrix or the identity.
5. CONCLUDING REMARKS

The previous results give some suggestions for a generalization, which has not yet been proved, to the case where \( n \) is any integer, not necessarily prime. The following points may be further investigated: Structural properties of \( p \)-circulant matrices appear as a generalization of the well-known "stronger" properties which are verified by circulant matrices. In addition, the \( k \)-commutativity of \( p \)-circulant matrices appears as a generalization of the commutativity of circulant matrices. Thus we may look for a proof of the analogues of Theorem 3.2 and Theorem 4.1 where we substitute "\( p \)-circulant matrices" and "\( f \)-commutative matrices" respectively for "circulant matrices" and "commutative matrices," and eventually introduce a notion of "\( k \)-closure" with respect to matrix product. Studying these problems may be useful for a deeper understanding of interesting relationships among some different properties of matrices: that is, \( k \)-commutativity \( (k \geq 1) \) and properties of spaces of matrices which form an algebra.

REFERENCES


Received 17 October 1977; revised 16 July 1978