On Some Theorems on Circulant Matrices

Paolo Zellini and Angela Mack
Istituto di Scienze dell'Informazione
Università di Pisa
Pisa, Italy

Submitted by David H. Carlson

ABSTRACT

In [2] some theorems on $n\times n$ circulant matrices were introduced under the hypothesis n a prime number. We extend these theorems to the case $n=2\cdot r$ where r is a prime greater then 2.

---

1. INTRODUCTION

In [2] the spaces Σ_g of $n\times n$ matrices $A(\mathrm{a})=\sum_{k=0}^{n-1}a_kJ_k$ were introduced, where a_k are complex and $J_0, J_1,\dots, J_{n-1}$ satisfy the following condition:

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

The following two theorems have been proved in [2] under the hypothesis n a prime number:

THEOREM 3.2. *If $\mathcal{J}$ satisfies $(*)$ and the J_k commute, then for P_n, the permutation matrix corresponding to the permutation $(1\,2\cdots n)$, the following holds:*

$(**)$ *For some permutation matrix P, and reindexing,*

$$J_k=P^TP_n^kP,\qquad k=0,1,\dots,n-1.$$

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

52 Vanderbilt Ave., New York, NY 10017 0024-3795/81/070137+13$02.50

An obvious consequence of Theorem 3.2 and Theorem 4.1 is stated in the following.

THEOREM 4.2 (see [2]). *The only* Σ_g *which constitute a commutative algebra are the spaces of* $n \times n$ *matrices* (n *prime*) *of the form* $P^T CP$, *where* C *is circulant, and* P, *which depends on the choice of the set* $\{J_k\}$, *is the permutation matrix or the identity.*

An alternative proof of Theorem 3.2 and Theorem 4.1 has been introduced in [1] by using the centralizers of a permutation group. In [1] Theorems 3.2 and 4.1 appear as corollaries of the following results:

THEOREM 1. *Let* n *be a positive integer. Let* $\mathcal{J}$ *satisfy* $(*)$ *and the* J_k *commute. Then for* P_n, *the permutation matrix corresponding to the permutation* $(0 1 2 \cdots n-1)$, $(**)$ *holds if and only if there exists a* J_q *in* $\mathcal{J}$ *which is an* n*-cycle.*

THEOREM 2. *Let* n *be a positive integer, and* $\mathcal{J}$ *satisfy* $(*)$ *and be closed under multiplication. Then* $(**)$ *holds if and only if there exists a* J_q *in* $\mathcal{J}$ *which is an* n*-cycle.*

In the present paper we find an extension of Theorem 3.2 and Theorem 4.1 to the case $n = 2 \cdot r$, where r is a prime >2. More precisely, Theorem 3.2 is still true in the case $n = 2 \cdot r$, while for the closure under multiplication some different spaces of matrices $A(\mathrm{a})$ are to be introduced beside the circulant. A new class of algebras of $n \times n$ matrices on the complex field is then introduced at the end of Section 3.

If $\mathcal{J}$ satisfies $(*)$, then we shall suppose, in the remainder of the paper, $J_0 = I$.

2. ON THE COMMUTATIVITY OF THE MATRICES OF THE SPACES Σ_g

The following Propositions are in some sense implicit in the results in [2] and in their proofs. In the following $j_{p,q}^{(k)}$ is the element (p,q) of the matrix J_k and $\Pi^{(k)}$ is the permutation mapping q to p in the case $j_{k,q}^{(p)} = 1$, i.e. $\Pi^{(k)}$ gives the exact disposition in the row k of $A(\mathrm{a})$ of the complex parameters $a_0, a_1, \dots, a_{n-1}$ (see [2, p. 37]). We suppose that $[a_0 a_1 \cdots a_{n-1}]$ is the first row of $A(\mathrm{a})$, i.e. $j_{0,k}^{(k)} = 1$.

Proposition 2.1. *Let $\mathcal{J}=\{J_0, J_1,\dots, J_{n-1}\}$ satisfy $(*)$ and J_k commute. Then $\Pi^{(k)}$, for a $k\neq 0$, is an n-cycle if and only if J_k is an n-cycle. Also, if $\Pi^{(k)}$ or J_k is an n-cycle, then $\mathcal{J}$ satisfies $(**)$.*

Proof. Proposition 2.1 follows immediately from Lemma 3.4 in [2], which states that, if the commutativity of the J_k is assumed, then $j^{(p)}_{i,r}=j^{(q)}_{r,k}=j^{(q)}_{i,s}=1$ implies $j^{(p)}_{s,k}=1$. Hence, from $j^{(k)}_{0,k}=j^{(p)}_{k,r}=j^{(p)}_{0,p}=1$ we deduce $j^{(k)}_{p,r}=1$, and analogously, $j^{(p)}_{k,r}=1$ is a consequence of $j^{(p)}_{0,p}=j^{(k)}_{p,r}=j^{(k)}_{0,k}=1$, so we have the equivalence

$$j^{(p)}_{k,r}=1 \quad\Leftrightarrow\quad j^{(k)}_{p,r}=1. \tag{2.1}$$

Now it is easy to see that if the permutation $(h_0 h_1 \cdots h_{n-1})$ defines $\Pi^{(k)}$, then $(h_0 h_{n-1}\cdots h_1)$ defines J_k (and vice versa). The last part of Proposition 2.1 has been pointed out in [1]. It is also a direct consequence of the proof of Theorem 3.2 in [2]. ■

Proposition 2.2. *Let $\mathcal{J}=\{J_0, J_1,\dots, J_{n-1}\}$ satisfy $(*)$. Then the matrices J_k commute with each other only if $\Pi^{(k)}$, for every $k\neq 0$, is the product of disjoint cycles of the same length r where $r=n$ or r/n.*

Proof. Let the J_i commute, and let $\Pi^{(t)}$ be the product of cycles $\tau_1,\dots,\tau_m$ such that at least two of them have different lengths. Without loss of generality suppose that τ_1 and τ_l, for an index l, have lengths, respectively, r and s, with $r\neq s$. Then there are indices $p_0, p_1,\dots, p_r$ with $p_0=p_r=0$ and $p_{r-1}=t$ (we have $j^{(p_r)}_{t,p_{r-1}}\equiv j^{(0)}_{t,t}=1$) and $q_0, q_1,\dots, q_s$ $(q_0=q_s)$ such that

$$j^{(p_i)}_{t,p_{i-1}}=1,\quad j^{(q_m)}_{t,q_{m-1}}=1,\qquad i=1,\dots,r,\quad m=1,\dots,s.$$

Successive applications of (2.1) and Lemma 3.4 in [2] define the recurrent implications

$$j^{(q_{s-i+1})}_{p_i,q_1}=j^{(p_{i+2})}_{t,p_i}=j^{(q_{s-i+1})}_{t,q_{s-i}}=1 \quad\Rightarrow\quad j^{(p_{i+1})}_{q_{s-i},q_1}=j^{(q_{s-i})}_{p_{i+1},q_1}=1,$$
$$i=0,\dots,s-1; \tag{2.2}$$

$$j^{(p_{r-h})}_{q_{h+1},q_1}=j^{(q_{h+2})}_{t,q_{h+1}}=j^{(p_{r-h})}_{t,p_{r-h}}=1 \quad\Rightarrow\quad j^{(q_{h+2})}_{p_{r-h-1},q_1}=j^{(p_{r-h-1})}_{q_{h+2},q_1}=1,$$
$$h=0,\dots,r-1. \tag{2.3}$$

(2.2) and (2.3) correspond, respectively, to the recurrent relations (3.6) and (3.7) in [2]. They lead, for $r \neq s$, to a contradiction with ($*$). In fact, let $r > s$. Then we deduce, from (2.2), $j^{(p_{s-1})}_{q_2, q_1} = 1$. But we have also $j^{(t)}_{q_2, q_1} = 1$, because $j^{(q_2)}_{t, q_1} = 1$ and (2.1) holds; so, by the equality $t = p_{r-1}$, we have a contradiction. If $r < s$, then we have, from (2.3), $j^{(q_r)}_{p_1, q_1} = 1$. But this leads to a contradiction with the equality $j^{(q_s)}_{p_1, q_1} = 1$ that is deduced from (2.2). ■

Now we have the following.

LEMMA 2.1. *Let $\mathcal{J} = \{J_0, J_1, \ldots, J_{n-1}\}$ satisfy ($*$), and J_i commute. Let $\Pi^{(t)}$, for some t, be the product of l_t disjoint cycles of the same length r. Then there exist indices $p_0, p_1, \ldots, p_r$, with $p_0 = p_r = 0$, $p_{r-1} = t$, such that $J_{p_1}, \ldots, J_{p_{r-1}}$ are completely defined by, and correspond to, $r - l$ permutations σ_{p_k} $(k = 1, \ldots, r-1)$ which are the product of n/r disjoint cycles of length r. Analogously all permutations $\Pi^{(p_k)}$ are defined and are the product of l_t cycles of length r. In particular if $l_t = 1$ and $r = n$, then any J_i is an n-cycle and ($**$) holds.*

Proof. Suppose, without loss of generality, $t = 1$. As $\Pi^{(1)}$ is the product of r-cycles, there are indices $p_0, p_1, \ldots, p_r$ with $p_0 = p_r = 0$, $p_{r-1} = 1$ such that

$$j^{(p_k)}_{1, p_{k-1}} = 1, \qquad k = 1, 2, \ldots, r. \tag{2.4}$$

By successive applications of Lemma 3.4 in [2] and (2.1) we have (the indices are all taken modulo r)

$$j^{(p_1)}_{1, p_0} = j^{(p_{k+1})}_{0, p_{k-1}} = j^{(p_{k+1})}_{1, p_k} = 1 \quad \Rightarrow \quad j^{(p_1)}_{p_k, p_{k-1}} = j^{(p_k)}_{p_1, p_{k-1}} = 1, \tag{2.5}$$

i.e., $\Pi^{(p_1)}$, as well as J_{p_1}, contains an r-cycle. If $r = n$, then we obtain the Lemma and the result of Theorem 3.2 in [2] (see the second part of the proof of Theorem 3.2 in [2, pp. 38–39]). If $r \backslash n$, then consider another r-cycle of $\Pi^{(1)}$:

$$j^{(q_k)}_{1, q_{k-1}} = 1, \qquad k = 1, 2, \ldots, r, \tag{2.6}$$

where $q_0 = q_r$. Successive applications of Lemma 3.4 in [2] give the following implications:

$$
\begin{aligned}
j^{(q_k)}_{1,q_{k-1}} = j^{(1)}_{q_{k-1},q_{k-2}} = j^{(1)}_{1,p_{r-2}} = 1 \quad &\Rightarrow \quad j^{(q_k)}_{p_{r-2},q_{k-2}} = j^{(p_{r-2})}_{q_k,q_{k-2}} = 1,\\
j^{(q_k)}_{1,q_{k-1}} = j^{(p_{r-2})}_{q_{k-1},q_{k-3}} = j^{(p_{r-2})}_{1,p_{r-3}} = 1 \quad &\Rightarrow \quad j^{(q_k)}_{p_{r-3},q_{k-3}} = j^{(p_{r-3})}_{q_k,q_{k-3}} = 1,\\
&\ \vdots\\
j^{(q_k)}_{1,q_{k-1}} = j^{(p_{r-s})}_{q_{k-1},q_{k-s-1}} = j^{(p_{r-s})}_{1,p_{r-s-1}} = 1 \quad &\Rightarrow \quad j^{(q_k)}_{p_{r-s-1},q_{k-s-1}} = j^{(p_{r-s-1})}_{q_k,q_{k-s-1}} = 1,
\end{aligned}
\tag{2.7}
$$

where $s=1,2,\dots,r-2$ and $k=1,2,\dots,r$. The following recurrent relations are also deduced from Lemma 3.4 in [2]:

$$
j^{(p_k)}_{1,p_{k-1}} = j^{(p_s)}_{p_{k-1},p_{s+k-1}} = j^{(p_s)}_{1,p_{s-1}} = 1 \quad \Rightarrow \quad j^{(p_k)}_{p_{s-1},p_{s+k-1}} = j^{(p_{s-1})}_{p_k,p_{s+k-1}} = 1,
$$

$$
s=2,3,\dots,r-1. \tag{2.8}
$$

Now let $q_0, q_1, \dots, q_{r-1}$ run over the set of disjoint subcycles of $\Pi^{(1)}$ which do not involve 0 or 1. Then Lemma 2.1 follows from (2.7) and (2.8). Also, observe that $J^{(i)}_{p_k} \in \mathcal{J}$, where $i=1,2,\dots,r-1$. ■

EXAMPLE 2.1. Let $n=6$ and let $[a_4\ a_0\ a_5\ a_2\ a_1\ a_3]$ be the second row of the matrix $A(\mathrm{a})=\sum_{k=0}^{n-1} a_k J_k$, corresponding to the permutation $\sigma=(0\,4\,1)(2\,5\,3)$:

$$
A(\mathrm{a}) = \begin{bmatrix}
a_0 & a_1 & a_2 & a_3 & a_4 & a_5\\
a_4 & a_0 & a_5 & a_2 & a_1 & a_3\\
\cdot & \cdot & a_0 & a_1 & \cdot & a_4\\
\cdot & \cdot & a_4 & a_0 & \cdot & a_1\\
a_1 & a_4 & a_3 & a_5 & a_0 & a_2\\
\cdot & \cdot & a_1 & a_4 & \cdot & a_0
\end{bmatrix}. \tag{2.9}
$$

If the J_k commute, then the rows and the columns of $A(\mathrm{a})$ corresponding, respectively, to the indices $p_0=0$, $p_1=4$, $p_2=1$ and $q_0=2$, $q_1=5$, $q_2=3$ are defined as in (2.9). Observe that $J_{p_1}=J_4$ and $J_{p_2}=J_1$ correspond, respectively, to the permutations σ and σ^2, i.e. $J_1=J_4^2$.

LEMMA 2.2. *Let $n=2\cdot r$ where r is a prime >2. Let $J_0, J_1, \ldots, J_{n-1}$ commute and satisfy* $(*)$. *Then $\Pi^{(k)}$ cannot be, for every k, the product of 2-cycles.*

Proof. Consider $\Pi^{(1)}$ and $\Pi^{(2)}$, and suppose they are the product of 2-cycles. Then for some indices $q_1^{(1)}, q_2^{(1)}, \ldots, q_{n-1}^{(1)}$ and $q_1^{(2)}, q_2^{(2)}, \ldots, q_{n-1}^{(2)}$ with $q_1^{(1)}=1$, $q_2^{(2)}=q_2^{(1)}$, $q_1^{(2)}=2$, $q_j^{(2)} \neq q_j^{(1)}$ for $j>2$ we have

$$\begin{Bmatrix} j_{1,0}^{(q_1^{(1)})}=1 \\ j_{1,q_1^{(1)}}^{(0)}=1 \end{Bmatrix}, \quad \begin{Bmatrix} j_{1,2}^{(q_2^{(1)})}=1 \\ j_{1,q_2^{(1)}}^{(2)}=1 \end{Bmatrix}, \ldots, \quad \begin{Bmatrix} j_{1,n-1}^{(q_{n-1}^{(1)})}=1 \\ j_{1,q_{n-1}^{(1)}}^{(n-1)}=1 \end{Bmatrix}; \tag{2.10}$$

$$\begin{Bmatrix} j_{2,0}^{(q_1^{(2)})}=1 \\ j_{2,q_1^{(2)}}^{(0)}=1 \end{Bmatrix}, \quad \begin{Bmatrix} j_{2,1}^{(q_2^{(2)})}=1 \\ j_{2,q_2^{(2)}}^{(1)}=1 \end{Bmatrix}, \ldots, \quad \begin{Bmatrix} j_{2,n-1}^{(q_{n-1}^{(2)})}=1 \\ j_{2,q_{n-1}^{(2)}}^{(n-1)}=1 \end{Bmatrix}. \tag{2.11}$$

Also we have for some $r_3, \ldots, r_{n-1}$ and $s_3, \ldots, s_{n-1}$, with $s_j \neq j$ and $r_j \neq j$,

$$\begin{Bmatrix} j_{1,s_3}^{(q_3^{(2)})}=1 \\ j_{1,q_3^{(2)}}^{(s_3)}=1 \end{Bmatrix}, \ldots, \quad \begin{Bmatrix} j_{1,s_{n-1}}^{(q_{n-1}^{(2)})}=1 \\ j_{1,q_{n-1}^{(2)}}^{(s_{n-1})}=1 \end{Bmatrix}; \tag{2.12}$$

$$\begin{Bmatrix} j_{2,r_3}^{(q_3^{(1)})}=1 \\ j_{2,q_3^{(1)}}^{(r_3)}=1 \end{Bmatrix}, \ldots, \quad \begin{Bmatrix} j_{2,r_{n-1}}^{(q_{n-1}^{(1)})}=1 \\ j_{2,q_{n-1}^{(1)}}^{(r_{n-1})}=1 \end{Bmatrix}. \tag{2.13}$$

Let us observe that, if the J_k commute and $\Pi^{(k)}$ has subcycles of length 2 for every k, then each J_k is symmetric. In fact we have the following obvious implications:

$$j_{p,q}^{(k)}=1 \;\Rightarrow\; j_{k,q}^{(p)}=1 \;\Rightarrow\; j_{k,p}^{(q)}=1 \;\Rightarrow\; j_{q,p}^{(k)}=1. \tag{2.14}$$

This property of symmetry and successive applications of Lemma 3.4 in [2] give rise to

$$j_{2,i}^{(q_i^{(2)})}=j_{i,1}^{(q_i^{(1)})}=j_{2,r_i}^{(q_i^{(1)})}=1 \quad\Rightarrow\quad j_{r_i,1}^{(q_i^{(2)})}=j_{1,r_i}^{(q_i^{(2)})}=1,$$

$$i=3,\ldots,n-1. \tag{2.15}$$

From (2.12) and (2.15) we have

$$r_i = s_i, \qquad i=3,\dots,n-1. \tag{2.16}$$

This means that the third row of $A(\mathbf{a})=\sum_{k=0}^{n-1} a_k J_k$ is a permutation Π of the second row such that Π is the product of 2-cycles.

Now if $j_{2,l}^{(k)}=1$ and $j_{1,l}^{(k')}=1$ for some k and k' then we have, as a consequence of (2.10)–(2.11) and (2.16), the following configuration for the matrix $A(\mathbf{a})$ (we suppose, without loss of generality, $l<l'<k<k'$):

$$\begin{array}{lccccccccc} \text{first row:} & \cdots & a_l & \cdots & a_{l'} & \cdots & a_k & \cdots & a_{k'} & \cdots \\ \text{second row:} & \cdots & a_{k'} & \cdots & a_k & \cdots & a_{l'} & \cdots & a_l & \cdots \\ \text{third row:} & \cdots & a_k & \cdots & a_{k'} & \cdots & a_l & \cdots & a_{l'} & \cdots \end{array} \tag{2.17}$$

i.e. we deduce, for some l', $j_{1,l'}^{(k)}=j_{2,l'}^{(k')}=j_{1,k'}^{(l)}=j_{2,k}^{(l)}=j_{1,k}^{(l')}=j_{2,k'}^{(l')}=1$. Now (2.17) is consistent only with the case $4|n$; in fact if $4\nmid n$, then we obtain, for some r and s, $j_{2,r}^{(r)}=1$, or simultaneously $j_{2,r}^{(s)}=1$ and $j_{1,r}^{(s)}=1$, i.e. a contradiction. ∎

THEOREM 2.1. *Let $n=2\cdot r$ where r is a prime >2. Let the J_k commute and satisfy* $(*)$. *Then* $(**)$ *holds.*

Proof. Consider the following four cases for $k=1,2,\dots,n-1$:

(α) every $\Pi^{(k)}$ is the product of two cycles of length r;
(β) every $\Pi^{(k)}$ is the product of r cycles of length 2;
(γ) every $\Pi^{(k)}$ can be the product of 2-cycles or the product of r-cycles;
(δ) there exists a k such that $\Pi^{(k)}$ is an n-cycle.

These cases exhaust all the different possibilities of choice of the matrices J_k. Clearly (β) is impossible by Lemma 2.2. We claim that (α) and (γ) are also impossible, so (δ) holds and the Theorem 2.1 follows from Proposition 2.1 (or from Theorem 1 in [1]).

Let condition (α) be verified and let $\Pi^{(1)}$ be the product of two r-cycles:

$$j_{1,p_{k-1}}^{(p_k)}=1, \qquad j_{1,q_{k-1}}^{(q_k)}=1,$$

$$k=0,1,\dots,r, \quad q_j\neq p_i \ \ \forall i,j, \quad p_0=p_r=0, \quad p_{r-1}=1, \quad q_0=q_r. \tag{2.18}$$

Consider a row q_k of the matrices J_i. From (2.7)–(2.8) we have that $J_{q_k,0}^{(1)}=1$ implies $l\neq p_i$ for every i [this follows immediately from the equalities $0=p_0$

and $j^{(p_{r-s-1})}_{q_k,q_{k-s-1}}=1$, i.e., every matrix J_{p_i} is defined and cannot have 1 in the position $(q_k,0)$]. Also, by (2.7), $j^{(l)}_{q_k,q_s}=1$ implies $l\neq q_t$ for every t, so $l=p_i$ for some i. Analogously, $j^{(l)}_{q_k,p_s}=1$, with $p_s\neq 0$, implies $l=q_i$ for some i; otherwise we have a contradiction with the last equality of (2.7). From $j^{(0)}_{q_k,q_k}=1$ we deduce that $\Pi^{(q_k)}$ has a subcycle defined by some indices $p_{t(i)}$ and $q_{t(i)}$ such that

$$j^{(q_{t(1)})}_{q_k,0}=j^{(p_{t(2)})}_{q_k,q_{t(1)}}=j^{(q_{t(3)})}_{q_k,p_{t(2)}}=\cdots=j^{(0)}_{q_k,q_k}=1,$$

so $\Pi^{(q_k)}$ has a subcycle of length m where m is even, which is impossible.

Let condition (γ) be verified. Suppose that $\Pi^{(1)}$ is the product of two r-cycles [i.e. (2.18) holds]. Then $\Pi^{(q_k)}$, for every k, is an n-cycle [i.e. (δ) is verified] or is the product of 2-cycles. Let this last condition hold. Fix a q_k and let $j^{(1)}_{q_k,q_s}=1$ [we cannot have $j^{(1)}_{q_k,p_s}=1$ for some p_s; in fact $1=p_{r-1}$ in (2.18) and (2.7) holds]; this implies $j^{q_s}_{q_k,1}=1$. From $j^{(q_{k+1})}_{1,q_k}=1$ we obtain, by the commutativity, $j^{(1)}_{q_{k+1},q_k}=1$ and then, as $\Pi^{(q_{k+1})}$ has subcycles of length 2, $j^{(q_k)}_{q_{k+1},1}=1$. By the commutativity $j^{(q_{k+1})}_{q_k,1}=1$, so we obtain $q_s=q_{k+1}$, $j^{(1)}_{q_k,q_{k+1}}=1$, and $j^{(q_k)}_{1,q_{k+1}}=1$. This last equality and $j^{(q_{k+1})}_{1,q_k}=1$ imply that $\Pi^{(1)}$ has a subcycle of length 2, i.e. a contradiction. ∎

EXAMPLE 2.2. The following matrix $A(\mathbf{a})$ $(n=10)$ shows that if the commutativity is not assumed, then condition (β) does not contradict $(*)$. Observe that all J_k are symmetric:

$$A(\mathbf{a})=\begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \\ a_1 & a_0 & a_4 & a_6 & a_2 & a_8 & a_3 & a_9 & a_5 & a_7 \\ a_2 & a_4 & a_0 & a_7 & a_1 & a_9 & a_8 & a_3 & a_6 & a_5 \\ a_3 & a_6 & a_7 & a_0 & a_5 & a_4 & a_1 & a_2 & a_9 & a_8 \\ a_4 & a_2 & a_1 & a_5 & a_0 & a_3 & a_9 & a_8 & a_7 & a_6 \\ a_5 & a_8 & a_9 & a_4 & a_3 & a_0 & a_7 & a_6 & a_1 & a_2 \\ a_6 & a_3 & a_8 & a_1 & a_9 & a_7 & a_0 & a_5 & a_2 & a_4 \\ a_7 & a_9 & a_3 & a_2 & a_8 & a_6 & a_5 & a_0 & a_4 & a_1 \\ a_8 & a_5 & a_6 & a_9 & a_7 & a_1 & a_2 & a_4 & a_0 & a_3 \\ a_9 & a_7 & a_5 & a_8 & a_6 & a_2 & a_4 & a_1 & a_3 & a_0 \end{bmatrix}. \tag{2.19}$$

If the commutativity is assumed, then the impossibility of (β) (Lemma 2.2) is shown in the following case $(n=10)$: take for instance the second row of $A(\mathbf{a})$ in (2.19). As $j^{(2)}_{2,0}=1$, we have, according to (2.17), $j^{(1)}_{2,4}=j^{(4)}_{2,1}=1$ and, obviously, $j^{(0)}_{2,2}=1$. Now let for instance $j^{(5)}_{2,3}=1$. This implies $j^{(6)}_{2,8}=j^{(8)}_{2,6}=j^{(3)}_{2,5}=1$

and leads to the contradiction $J_{2,7}^{(7)}=1$ or $j_{2,7}^{(9)}=1$:

$$A(\mathbf{a})=\begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \\ a_1 & a_0 & a_4 & a_6 & a_2 & a_8 & a_3 & a_9 & a_5 & a_7 \\ a_2 & a_4 & a_0 & a_5 & a_1 & a_3 & a_8 & \cdot & a_6 & \cdot \\ a_3 & a_6 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_4 & a_2 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_5 & a_8 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_6 & a_3 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_7 & a_9 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_8 & a_5 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_9 & a_7 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}.$$

3. CLOSURE UNDER MULTIPLICATION OF THE SPACES Σ_g

We are going to introduce some preliminary results which follow roughly the same logical model of reasoning of the previous section. The conclusion will be different, because for $n=2\cdot r$ (r prime) the circulants do not constitute the only space Σ_g which is closed under multiplication. We shall show this in the final Theorem 3.1. In the following we denote by $j_{r,s}^{(p,q)}$ the element (r,s) of the matrix $J_p\cdot J_q$.

LEMMA 3.1. *Let $n=2\cdot r$ (r a prime >2). Let $\mathcal{J}=\{J_0,J_1,\ldots,J_{n-1}\}$ be closed under multiplication and satisfy $(*)$. Then $\Pi^{(k)}$ cannot be, for every $k\neq 0$, the product of 2-cycles. Also, there is a $k\neq 0$ such that J_k does not correspond to a product of 2-cycles.*

Proof. Let $\Pi^{(k)}$ be the product of 2-cycles for every $k\neq 0$. Then, from the assumption $j_{0,k}^{(k)}=1$ (see Section 2) and the equality $j_{k,k}^{(0)}=1$, we have $j_{k,0}^{(k)}=1$. By the closure of $\mathcal{J}$, $J_k^2=I$, i.e., all subcycles of the permutation corresponding to J_k $(k=1,2,\ldots,n-1)$ have length 2. Also if $j_{k,l}^{(k,l)}=1$, then we have $j_{l,k}^{(k,l)}=1$. Hence, from $j_{l,k}^{(l,k)}=1$ we deduce $J_k\cdot J_l=J_l\cdot J_{k'}$, i.e., the J_k commute, which is a contradiction by Lemma 2.2. ■

LEMMA 3.2. *Let $\mathcal{J}=\{J_0,J_1,\ldots,J_{n-1}\}$ be closed under multiplication and satisfy $(*)$. If $\Pi^{(l)}$, for some l, has two subcycles of length, respectively, r and s—i.e.*

$$j_{l,p_{k-1}}^{(p_k)}=1,\quad j_{l,q_{h-1}}^{(q_h)}=1,\qquad k=1,\ldots,r,\quad h=1,\ldots,s, \tag{3.1}$$

with $p_0 = p_r = 0$, $p_{r-1} = l$, $q_0 = q_s$*—then the following equalities are verified*:

$$J_{p_i} \cdot J_{p_h} = J_{p_{i+h}}, \qquad J_{p_i} \cdot J_{q_h} = J_{q_{i+h}}. \tag{3.2}$$

Proof. Observe that $j^{(k)}_{p,q} = 1$ if and only if $J_p \cdot J_k = J_q$. In fact, from $j^{(k)}_{p,q} = 1$ and $j^{(p)}_{0,p} = 1$ we have $j^{(p,k)}_{0,q} = 1$ and vice versa.

If (3.1) holds then we have

$$J_l \cdot J_{p_k} = J_{p_{k-1}}, \qquad k = 1, \ldots, r,$$

$$J_l \cdot J_{q_h} = J_{q_{h-1}}, \qquad h = 1, \ldots, s. \tag{3.3}$$

From (3.3) and $J_0 = I$ we obtain the following implications:

$$J_{p_1} \cdot J_l = J_0, \qquad J_l \cdot J_{q_h} = J_{q_{h-1}} \Rightarrow J_{p_1} \cdot J_{q_{h-1}} = J_{q_h}, \quad h = 1, \ldots, s,$$

$$J_{p_1} \cdot J_l = J_0, \qquad J_l \cdot J_{p_i} = J_{p_{i-1}} \Rightarrow J_{p_1} \cdot J_{p_{i-1}} = J_{p_i}, \quad i = 1, \ldots, r; \tag{3.4}$$

and then, from (3.4), the following recurrence relations:

$$\left\{ \begin{aligned} & J_{p_h} J_{p_1} = J_{p_{h+1}}, \\ & J_{p_1} \cdot J_{p_{i-h}} = J_{p_{i-h+1}}, \\ & J_{p_h} \cdot J_{p_{i-h+1}} = J_{p_{i+1}} \end{aligned} \right\}$$

$$\Rightarrow \quad J_{p_{h+1}} \cdot J_{p_{i-h}} = J_{p_{i+1}}, \qquad h = 1, \ldots, r-1, \quad i = h+1, \ldots, r+h; \tag{3.5}$$

$$\left\{ \begin{aligned} & J_{p_h} \cdot J_{p_1} = J_{p_{h+1}}, \\ & J_{p_1} \cdot J_{q_{i-h}} = J_{q_{i-h+1}}, \\ & J_{p_h} \cdot J_{q_{i-h+1}} = J_{q_{i+1}} \end{aligned} \right\}$$

$$\Rightarrow \quad J_{p_{h+1}} \cdot J_{q_{i-h}} = J_{q_{i+1}}, \qquad h = 1, \ldots, r-1, \quad i = h+1, \ldots, s+h,$$

where the indices are taken modulo r and s. ∎

PROPOSITION 3.1. *Let $\mathcal{J}=\{J_0, J_1,\dots, J_{n-1}\}$ be closed under multiplication and satisfy* $(*)$. *Then $\Pi^{(k)}$ is the product of subcycles of the same length. Also, if $\Pi^{(k)}$ is an n-cycle for some $k\neq 0$, then every J_k is an n-cycle and $\mathcal{J}$ satisfies* $(**)$.

Proof. We claim that $r\neq s$ in (3.1) contradicts $(*)$. In fact, let $r>s$; then from (3.2) we have $J_{p_s}\cdot J_{q_1}=J_{q_{s+1}}=J_{q_1}$, which is impossible. If $r<s$, then we have, from (3.2), $J_{p_{r-1}}\cdot J_{q_1}=J_{q_r}$, which is a contradiction with the equality $J_l\cdot J_{q_1}=J_{q_0}$ that is deduced from (3.1) [recall that $p_{r-1}=l$ in (3.1) and $q_0\neq q_r$]. For the second part of the proposition, if $\Pi^{(k)}$ is an n-cycle for some k, then the J_i commute by Lemma 3.2 and its proof with $r=n$. By Proposition 2.1, $\mathcal{J}$ satisfies $(**)$, and hence each J_k is an n-cycle. ∎

LEMMA 3.3. *Let $n=2r$ (r a prime >2). Let $\mathcal{J}=\{J_0, J_1,\dots, J_{n-1}\}$ be closed under multiplication and satisfy* $(*)$. *Then there is a $k\neq 0$ such that $\Pi^{(k)}$ is an n-cycle or the product of 2-cycles.*

Proof. Let $\Pi^{(k)}$ be a product of r-cycles ($k=1,\dots,n-1$). In particular let (2.18) hold. Consider $\Pi^{(q_h)}$ and let $j^{(l)}_{q_{h,0}}=1$. We first show that $l\neq p_i$ for every p_i. In fact let $j^{(p_i)}_{q_h,0}=1$ for some p_i; then $J_{q_h}\cdot J_{p_i}=J_{p_i}\cdot J_{q_h}=J_0=I$, so we have $j^{(q_h)}_{p_i,0}=1$. But this leads to a contradiction because the equality $J_{p_i}\cdot J_{p_h}=J_{p_{i+h}}$ of Lemma 2.2 implies $j^{(p_h)}_{p_i,p_{i+h}}=1$ and $j^{(p_t)}_{p_i,0}=1$ for some p_t such that $t+i=0$ modulo r. Then we have $l=q_i$ for some index q_i. Now observe that $j^{(0)}_{q_h,q_h}=1$. Also, by the equality $j^{(q_i)}_{q_h,0}=1$ and the second equality in (3.2), $j^{(l)}_{q_h,q_i}=1$ implies $l=p_k$ for some p_k. Similarly, by the first equality in (3.2), if $j^{(l)}_{q_h,p_i}=1$, then $l=q_k$ for some q_k. This means that $\Pi^{(q_i)}$ must contain an m-cycle where m is even, which is a contradiction. ∎

THEOREM 3.1. *Let $n=2\cdot r$, where r is a prime >2. Let $\mathcal{J}=\{J_0, J_1,\dots, J_{n-1}\}$ be closed under multiplication and satisfy* $(*)$. *Then $\mathcal{J}$ is a finite cancellative semigroup, and hence a group. Moreover,*

(i) $(**)$ *holds, or*

(ii) *there exist indices $p_0, p_1,\dots, p_r$ ($p_r=p_0=0$) and $q_0, q_1,\dots, q_r$ ($q_0=q_r$) such that, for all $i=1,\dots,r$ and all $j=1,\dots,r$,*

$$\begin{aligned} J_{q_j}\cdot J_{p_i}&=J_{q_{j-i}},\\ J_{q_j}\cdot J_{q_i}&=J_{p_{j-i}},\\ J_{p_i}\cdot J_{q_j}&=J_{q_{i+j}},\\ J_{p_i}\cdot J_{p_j}&=J_{p_{i+j}}. \end{aligned} \tag{3.6}$$

Also, the matrices J_k are completely defined, and the space Σ_g of matrices $A(\mathbf{a})=\Sigma a_k J_k$ is a monoid (with neutral element $J_0=I$). This implies that Σ_g is closed under inversion.

Proof. By Lemma 3.1 and Lemma 3.3, the closure of $\mathcal{G}$ and $(*)$ imply that one of the following residual possibilities must be verified (see proof of Theorem 2.1):

(δ) there is an l such that $\Pi^{(l)}$ is an n-cycle;

(γ) no permutation $\Pi^{(l)}$ is an n-cycle; there is an l such that $\Pi^{(l)}$ is the product of two r-cycles. In this case (3.1) holds with $r=s$ and, by the proof of Lemma 3.3, every $\Pi^{(q_i)}$ is the product of 2-cycles.

If (δ) holds, then (i) holds by Proposition 3.1.

Now let (γ) hold and let $l=1$ (without loss of generality). Then we have

$$j_{1,p_{k+1}}^{(p_k)}=j_{1,q_{k+1}}^{(q_k)}=1, \tag{3.7}$$

with $p_0=p_r=0$, $p_{r-1}=1$, $q_0=q_r$. As $J_{q_k}^2=I$ for every q_k, we obtain, from $J_{p_i}\cdot J_{q_j}=J_{q_{i+j}}$ [see (3.2)],

$$J_{p_i}=J_{q_{i+j}}\cdot J_{q_j},$$

$$J_{q_{i-j}}\cdot J_{p_i}=J_{q_j},$$

so all the equalities (3.6) are satisfied. The choice of $\Pi^{(1)}$ and the condition on the permutations $\Pi^{(q_k)}$ define all matrices J_k. In fact from (3.6) we have

$$j_{q_h,q_{h+i}}^{(p_i)}=j_{q_h,p_{h+i}}^{(q_i)}=j_{p_h,q_{i+h}}^{(q_i)}=j_{p_h,p_{i+h}}^{(p_i)}=1; \tag{3.8}$$

and it is easy to see, from the dislocation of the indices in (3.8), that (3.8) is consistent with $(*)$.

Now let $A(\mathbf{a})=\Sigma_{k=0}^{n-1}a_k J_k$ and Σ_g be the space of matrices $A(\mathbf{a})$. Consider the matrix X whose first row $[x_0\ x_1\ \cdots\ x_{n-1}]$ is the first row of A^{-1}, computed for a particular choice of a_k (say $a_k=\alpha_k\in\mathbb{C}$), and such that $X=\Sigma_{k=0}^{n-1}x_k J_k$. As $\mathcal{G}$ is a group, $XA\in\Sigma_g$. Also, the first row of $X\cdot A$ is the first row of the identity. This implies $XA=I$ and $X=A^{-1}$. ■

Observe that, if (3.6) holds, then the J_k do not commute with each other. More precisely, the J_{q_i} are not commutative and the J_{p_i} do not commute with the J_{q_i}. We can state the following equalities:

$$\begin{aligned} J_{p_i}^T \cdot J_{q_i} &= J_{q_i} \cdot J_{p_i}, \\ J_{q_i} \cdot J_{p_i}^T &= J_{p_i} \cdot J_{q_i}, \\ J_{q_i} \cdot J_{q_i} &= \left(J_{q_i} \cdot J_{q_i}\right)^T. \end{aligned} \tag{3.9}$$

Now we can extend Theorem 4.2 in [2] to the following

THEOREM 3.2. *The only spaces of matrices* $A(\mathbf{a}) = \sum_{k=0}^{n-1} a_k J_k$ $(n = \delta \cdot r,$ $\delta \in \{1,2\}$, *r a prime* $>2)$ *which constitute a commutative algebra are the spaces of the form* $P^T CP$ *where C is circulant and P is a permutation matrix or the identity.*

EXAMPLE 3.1. In the following matrix $A(\mathbf{a})$, $J_0, J_1, \ldots, J_{n-1}$ obey condition (ii) of Theorem 3.1 and do not commute with each other (more precisely, J_1 and J_4 do not commute with J_2, J_3, J_5, and J_2, J_3, J_5 do not commute with each other):

$$A(\mathbf{a}) = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_0 & a_5 & a_2 & a_1 & a_3 \\ a_2 & a_5 & a_0 & a_4 & a_3 & a_1 \\ a_3 & a_2 & a_1 & a_0 & a_5 & a_4 \\ a_1 & a_4 & a_3 & a_5 & a_0 & a_2 \\ a_5 & a_3 & a_4 & a_1 & a_2 & a_0 \end{bmatrix}.$$

It is easy to see that all J_k are defined through the second row $[a_4\ a_0\ a_5\ a_2\ a_1\ a_3]$ and the equalities $J_2^2 = J_3^2 = J_5^2 = I$.

REFERENCES

1 Chong-Yun Chao, On circulant matrices, submitted for publication.
2 P. Zellini, On some properties of circulant matrices, *Linear Algebra and Appl.* 26:31–43 (1979).

Received 15 November 1979; revised 27 May 1980