CIRCULANTS OF FINITE GROUPS

by

M.G. Karpovsky*and E.A. Trachtenberg

Technical Report #67
December 1975

*) Department of Mathematics, Tel-Aviv University, Tel-Aviv, Israel.

A B S T R A C T

It is shown that properties of simple and composite circulant matrices may be generalized to circulants of finite groups. The closure porperties are investigated and simple methods for calculations of ranks, determinants, generalized inverses (Moor-Penrose), eigenvalues and eigenvectors of such a circulants are suggested. Methods of abstract harmonic ananlysis are used to solve these problems.

CIRCULANTS ON FINITE GROUPS

1. INTRODUCTION

The properties of circulants and composite circulants have been studied recently in a number of articles [1,2,3,4]. In this paper, we generalize the concepts of circulant and composite circulant to the case of an arbitrary finite group, study the properties of such circulants and, in particular, generalize some of the results of [1,2,3]. A circulant F on a finite group G with elements denoted by $1,\ldots,g$ is defined as a composite $kg \times kg$ matrix $F = \|F_{i,j}\| = \|f(j^{-1}i)\|$ $(i,j = 1,\ldots,g)$ where f is a matrix-valued function, $f: G \to M_{k,k}$, $M_{k,k}$ is the set of all $k \times k$ matrices over the field C of complex numbers and j^{-1} is the inverse of j in G. (If G is a cyclic group, a circulant on G is the same as an ordinary composite circulant [1,3].)

Circulants of finite groups G arise in the solution of synthesis and controllability problems for linear convolution-type systems whose input and output signals are functions defined on G (see, e.g., [5,6,7]). Thus a study of the properties of circulants on finite groups is of considerable importance.

II. PROPERTIES OF CIRCULANTS ON FINITE GROUPS

We first note some closure properties of the set

$$Cir(G,k) = \{\|f(j^{-1}i)\| \mid f: G \to M_{k,k}\}$$

of all circulants on a given group G with the respect to the basic algebraic operations.

Theorem 1 (i) If $F \in Cir(G,k)$, then $F^* \in Cir(G,k)$.

(ii) If $F_1,\ldots,F_n \in Cir(G,k)$ and $\alpha_1,\ldots,\alpha_n \in C$, then $(\sum_{i=1}^{n} \alpha_i F_i) \in Cir(G,k)$.

(iii) If $F_1, F_2 \in Cir(G,k)$, then $(F_1 \cdot F_2) \in Cir(G,k)$.

(iv) If $F_1,F_2 \in Cir(G,k)$, then $(F_1 * F_2 \in Cir(G,k)$ ($F_1 * F_2$ is the Hadamard product of F_1 and F_2).

(v) If $F_1 \in Cir(G,k_1)$ $F_2 \in Cir(G,k_2)$, then $(F_1 \otimes F_2)$ $Cir(G,k_1k_2g)$. ($F_1 \otimes F_2$ is the Kronecker product of F_1, F_2 and g is the order of G).

Proof. Properties (i), (ii), (iv), (v) follows immediately from the definition of $Cir(G,k)$.

We prove (iii). Let $F_1 = \|f_1(j^{-1}i)\|$, $F_2 = \|f_2(j^{-1}i)\|$, $F = \|F_{i,j}\| = F_1F_2$ and suppose that $j_1^{-1}i_1 = j_2^{-1}i_2$ for some $i_1,i_2,j_1,j_2 \in G$. Then

Theorem 2

(i) If the equation $FX = \phi$ $(F,\phi \in Cir(G,k))$ is solvable, then its set of solutions contains at least one circulant on G.

(ii) Let $S \in V(F,\phi)$. If $T \in V(F,\mathcal{O})$, then $(S + T) \in V(F,\phi)$; for every $X \in V(F,\phi)$ there exists a $T \in V(F,\mathcal{O})$ such that $X = S + T$.

(iii) $$\dim V(F,\mathcal{O}) = k(kg - \operatorname{rank} F). \tag{1}$$

Proof. (i) Let

$F = \|F_{i,j}\|$, $X = \|X_{i,j}\|$, $\phi = \|\phi_{i,j}\|$, $(F_{i,j},X_{i,j},\phi_{i,j} \in M_{k,k}$ $i,j = 1,\ldots,g)$. If $FX = \phi$ is solvable, there exist $X_{q,1}$ $(q = 1,\ldots,g)$ such that

$$\sum_{q=1}^{g} F_{i,q} X_{q,1} = \phi_{i,1} \tag{2}$$

Let

$$X_{p,r} = X_{r^{-1}p,1} \qquad (p,r = 1,\ldots,g) \tag{3}$$

Then $X \in Cir(G,k)$ and, since $F,\phi \in Cir(G,k)$, we have also

$F_{p,r} = F_{r^{-1}p,1}$, $\phi_{p,r} = \phi_{r^{-1}p,1}$ $(p,r = 1,\ldots,g)$. Now let $i = r^{-1}j$, $q = r^{-1}p$ in (2) for some $r \in \{1,\ldots,g\}$. Then by (2), (3),

$$\phi_{j,r} = \sum_{p=1}^{g} F_{r^{-1}j,r^{-1}p} \cdot X_{r^{-1}p,1} = \sum_{p=1}^{g} F_{p^{-1}j,1} X_{p,r} = \sum_{p=1}^{g} F_{j,p} X_{p,r}$$

and so $X \in V(F,\phi)$.

Part (ii) follows from (ii) of Theorem 1.

(iii) Conditions (2), (3) hold for every $X \in V(F,\phi)$; hence putting $\phi_{j,1} = 0$ $(i = 1,\ldots,g)$ in (2), we obtain (1).

We now consider the calculation of ranks, determinants and generalized inverses of circulants on a finite group.

We shall use the generalized Fourier transform $\psi \to \hat{\psi}$ on G for matrix-valued functions $\psi(j) = \|\psi_{m,\ell}(j)\|$ $(j \in G;\ m = 1,\ldots,k_1;\ \ell = 1,\ldots,k_2)$

$$\hat{\psi}(\omega) = \|\hat{\psi}_{m,\ell}(\omega)\| = \| \frac{d\omega}{g} \sum_{j=1}^{g} \psi_{m,\ell}(j) R_{\omega}(j^{-1}) \|, \qquad (4)$$

where R_{ω} is the ω-th irreducible unitary representation of G of dimension $d\omega$ over the field C of complex numbers, $\hat{f}(\omega) \in M_{k_1 d\omega \times k_2 d\omega}$ [8].

The following two important properties of the Fourier transform (4) will be used in what follows.

(i) Let $f: G \to M_{k_1,k_2}$, $x: G \to M_{k_2,k_3}$, $\Psi: G \to M_{k_1,k_3}$.

Then

$$\sum_{j=1}^{g} f(j^{-1}i)x(j) = \Psi(i) \qquad (i = 1,\ldots,g)$$

iff

$$\hat{f}(\omega)\hat{x}(\omega) = d\omega g^{-1}\hat{\Psi}(\omega) \qquad \forall R_\omega \in R(G) \tag{5}$$

where $R(G)$ is the set of all irreducible nonequivalent unitary representations of G.

(ii) If $M \in M_{k_1,k_2}$, denote $|M|^2 = \text{Trace } M^*M$. Then for every

$$f: G \to M_{k,k}$$

$$\sum_{i=1}^{g} |f(i)|^2 = g \sum_{R_\omega \in R(G)} d\omega^{-1} |\hat{f}(\omega)|^2 \quad . \tag{6}$$

Theorem 3. Let $F = \|f(j^{-1}i)\|$ $(f(j^{-1}i) = \|f_{m,\ell}(j^{-1}i)\|$; $i,j = 1,\ldots,g$; $m,\ell = 1,\ldots,k)$ be a circulant on finite group G, with g elements. Then:

(i) $$\text{rank } F = \sum_{R_\omega \in R(G)} d\omega \text{rank} \hat{f}(\omega) \quad ; \tag{7}$$

(ii) $$\det F = g^{kg} \prod_{R_\omega \in R(G)} d\omega^{-kd\omega^2} (\det \hat{f}(\omega))^{d\omega} \quad ; \tag{8}$$

(iii) Let $Q_{ij} = \|q_{m,\ell}(j^{-1}i)\| = \| \sum_{R_\omega \in R(G)} \frac{d\omega^2}{g^2} \text{Trace } (\hat{f}^+_{m,\ell}(\omega) R_\omega(j^{-1}i))\|$, (9)

Then $F^+ = Q$. (F^+ is the Moore-Penrose inverse of F).

Proof. Let $x: G \to M_{k,1}$, $\Psi: G \to M_{k,1}$ and

$$F \cdot \begin{Vmatrix} x(1) \\ \vdots \\ x(g) \end{Vmatrix} = \begin{Vmatrix} \Psi(1) \\ \vdots \\ \Psi(g) \end{Vmatrix} . \tag{10}$$

Then

$$\sum_{j=1}^{g} f(j^{-1}i)x(j) = \Psi(i) \qquad (i = 1,\ldots,g) \tag{11}$$

and by (5),

$$\hat{f}(\omega)\hat{x}(\omega) = d\omega g^{-1}\hat{\Psi}(\omega) \qquad \forall R_\omega \in R(G) \tag{12}$$

$(\hat{f}(\omega) \in M_{kd\omega \times kd\omega}$; $\hat{x}(\omega), \hat{\Psi}(\omega) \in M_{kd\omega \times d\omega})$.

(i) Let $\Psi = 0$. Then for every $R_\omega \in R(G)$, $\hat{\Psi}(\omega) = 0$ and the space of solutions $\hat{x}(\omega)$ of (12) has dimension $d\omega(kd\omega - \text{rank}\hat{f}(\omega))$. Since $\hat{x}(\omega)$ is the Fourier transform for $x(i)$, the dimension of the null-space of F is $\sum_{R_\omega \in R(G)} d\omega(kd\omega - \text{rank}\hat{f}(\omega))$. Hence, since [8]:

$$\sum_{R_\omega \in R(G)} d\omega^2 = g, \tag{13}$$

we have (7).

(ii) Let $\Psi(i) = \lambda x(i) =$ $(i = 1,\ldots,g)$. Then by (12),

$$(\hat{f}(\omega) - \lambda \frac{d\omega}{g} E)\ \hat{x}(\omega) = 0, \quad \forall R_\omega \in R(G) \quad (E = \begin{Vmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{Vmatrix}). \tag{14}$$

Hence, by (10), (14), the numbers $\mu_S(\omega)$ $(S = 1,\ldots,kd\omega)$ are eigenvalues of matrix $\hat{f}(\omega)$ iff $\lambda_S(\omega) = gd\omega^{-1}\mu_S(\omega)$ are eigenvalues of F; in that case, in view of (13) the multiplicity of $\lambda_S(\omega)$ $(S = 1,\ldots,kd\omega)$ is $d\omega$. Thus, by (13),

$$\det F = \prod_{R_\omega \in R(G)} \prod_{S=1}^{kd\omega} (\lambda_S(\omega))^{d\omega} = \prod_{R_\omega \in R(G)} (\frac{g}{d\omega})^{kd\omega^2} \prod_{S=1}^{d\omega} (\mu_S(\omega))^{d\omega} =$$

$$= g^{kg} \prod_{R_\omega \in R(G)} d\omega^{-kd\omega^2} (\det \hat{f}(\omega))^{d\omega}.$$

(iii) Let $F \in Cir(G,k)$, $f: G \to M_{k,k}$, $X = \begin{Vmatrix} x(1) \\ \vdots \\ x(g) \end{Vmatrix}$, $\Psi = \begin{Vmatrix} \Psi(1) \\ \vdots \\ \Psi(g) \end{Vmatrix}$

$$(x(i),\ \Psi(i) \in M_{k,1};\quad i = 1,\ldots,g).$$

Since for every $M_1 \in M_{k_1,k_1}$, $M_2 \in M_{k_1,k_2}$, $M_3 \in M_{k_1,k_2}$

$$\min_{M_2} |M_1M_2 - M_3|^2 = |M_1M_4M_3 - M_3|^2 \qquad \text{iff} \quad M_4 = M_1^+ \tag{15}$$

we have by (5), (6)

$$\min_X |FX-\phi|^2 = \min_x \sum_{i=1}^{g} \Big| \sum_{j=1}^{g} f(j^{-1}i))x(j)-\Psi(i)\Big|^2 =$$

$$= g \sum_{R_\omega \in R(G)} d\omega^{-1} \min_{\hat{x}(\omega)} |gd\omega^{-1}\hat{f}(\omega)\hat{x}(\omega)-\hat{\Psi}(\omega)|^2 =$$

$$= g \sum_{R_\omega \in R(G)} d\omega^{-1} |\hat{f}(\omega)\hat{f}^{+}(\omega)\hat{\Psi}(\omega)-\hat{\Psi}(\omega)|^2. \qquad (16)$$

But from (9), using (4), we deduce

$$\hat{f}^{+}_{m,\ell}(\omega) = g^2 d\omega^{-2}\hat{q}_{m,\ell}(\omega) \qquad (m,\ell = 1,\ldots,k) \qquad (17)$$

It now follows from (16), (17) in view of (5), (6) and $Q \in Cir(G,k)$ that

$$\min_X |FX-\phi|^2 = g \sum_{R_\omega \in R(G)} d\omega^{-1} |g^2 d\omega^{-2}\hat{f}(\omega)\hat{q}(\omega)\hat{\Psi}(\omega)-\hat{\Psi}(\omega)|^2 =$$

$$= \sum_{S=1}^{g} \Big| \sum_{i=1}^{g} f(i^{-1}S) \sum_{j=1}^{g} q(j^{-1}i)\Psi(j)-\Psi(S)\Big|^2 = |FQ\Psi-\Psi|^2$$

and thus, by (15), $Q = F^{+}$.

Corollary 1 A circulant $F = \|f(j^{-1}i)\|$ $(f: G \to M_{k,k})$ on G is nonsingular iff $\hat{f}(\omega)$ nonsingular for every $R_\omega \in R(G)$.

Proof. The proof follows from (i) of Theorem 3 in view of $F \in M_{kg\times kg}$, $\hat{f}(\omega) \in M_{kd\omega\times d\omega}$ and (13).

Thus. it follows from Theorem 3 that calculation of ranks, eigenvalues, determinants and generalized inverses of a $kg \times kg$ circulant F may be reduced to the analogous calculation for $kd\omega \times kd\omega$ matrices $\hat{f}(\omega)$ for all $R_\omega \in R(G)$. Since all the numbers $d\omega$ are divisors of g [8] and $\sum_{R_\omega \in R(G)} d\omega^2 = g$, the caluclations for $\hat{f}(\omega)$ $(R_\omega \in R(G))$ involve considerably less operations than the direct calculations for the original circulant F.

We now consider the case in which for every $j,i \in G$ $F_{ij} = f(j^{-1}i)$ is a circulant on some group G_1 of the order g_1, i.e., $f: G \to Cir(G_1,k_1)$ and $k = k_1 \cdot g_1$. The special case of these circulants F in which G_1 is a cyclic group and $k_1 = 1$ have been studied in [3]).

If $f(j^{-1}i) \in Cir(G_1,k_1)$ for every $j,i \in G$, then it follows from (4) and (ii) of Theorem 1, that $\hat{f}(\omega) \in Cir(G_1,k_1d\omega)$ for every $R_\omega \in R(G)$. Thus for calculation of ranks, eigenvalues, determinants and generalized inverses of $\hat{f}(\omega)$ for every $R(\omega) \in R(G)$ may be used again Theorem 3.

To end this section, we note that most of the results of Theorems 1,2,3 may easily be generalized to the case of circulants $F = \|f(j^{-1}i)\|$, where $f: G \to M_{k_1,k_2}$ and $k_1 \neq k_2$.

III CIRCULANTS ON ABELIAN GROUPS FOR k=1

We now consider the case of circulants $F = \|f(j^{-1}i)\|$, $f: G \to C$, where G is a finite Abelian group (this is the most important case for control theory [5,6,7]).

Corollary 2. For any normal matrix $M = \|M_{ij}\|$ $(M_{ij} \in C;\ i,j,\ldots,g)$ and any Abelian group G of order g, there exists a unique circulant $F_M \in Cir(G,1)$ on G which is unitarily similar to M.

Proof Since G is Abelian, $d\omega = 1$ for every $R_\omega \in R(G)$. Hence, if $\lambda_M(\omega)$ $(\omega = 1,\ldots,g)$ are the eigenvalues of M, then, as in the proof of (ii) of Theorem 3, we put $\hat{f}_M(\omega) = g^{-1}\lambda_M(\omega)$. Then

$$f_M(i) = g^{-1} \sum_{R_\omega \in R(G)} \lambda_M(\omega) R_\omega(i^{-1})$$ for every $i \in G$ and $F_M = \|f_M(j^{-1}i)\|$

is a circulant on G which is unitarily similar to M.

We also note that if $F \in Cir(G,1)$ then

$$\begin{pmatrix} R_\omega(1) \\ \vdots \\ R_\omega(g) \end{pmatrix}$$ for all $R_\omega \in R(G)$ are eigenvectors of F and if

$F_1, F_2 \in Cir(G,1)$ then $F_1F_2 = F_2F_1$.

Corollary 3. Let $F = \|f(j^{-1}i)\|$ $(f: G \to C;\ i,j = 1,\ldots,g)$ be a circulant on an Abelian group G. Then:

$$\text{(i)}\quad \operatorname{rank} F = \sum_{R_\omega \in R(G)} \delta'\hat{f}(\omega),0\,, \quad \text{where} \quad \delta'\hat{f}(\omega),0 = \begin{cases} 1, & \text{if } \hat{f}(\omega) \neq 0 \\ 0, & \text{if } \hat{f}(\omega) = 0 \end{cases}; \tag{18}$$

$$\text{(ii)}\quad \det F = g^g \prod_{R_\omega \in R(G)} \hat{f}(\omega); \tag{19}$$

$$\text{(iii)}\quad F^+ = \|F_{ij}\| = g^{-2}\Big\| \sum_{R_\omega \in R(G)} \hat{f}^+(\omega) R_\omega(j^{-1}i)\Big\|, \quad \text{where}$$

$$\hat{f}^+(\omega) = \begin{cases} \hat{f}^{-1}(\omega), & \text{if } \hat{f}(\omega) \neq 0 \\ 0, & \text{if } \hat{f}(\omega) = 0 \end{cases} \tag{20}$$

(iv) F is nonsingular iff $\hat{f}(\omega) \neq 0$ for all $R_\omega \in R(G)$.

Proof. The proof follows from Theorem 3 and Corollary 1 with $k=1$ since in our case $d\omega = 1$ for ever $R_\omega \in R(G)$. Thus, for Abelian groups, calculation of the rank, eigenvalues, determinant and generalized inverse of a circulant $F = \|f(j^{-1}i)\|$ may be reduced to calculation of the Fourier transform $\hat{f}$.

Express G as a direct product of cyclic subgroups, $G = \prod_{S=1}^{n} G_S$. Let g_S be the order of G_S $(S = 1,\ldots,n)$. Then calculation of the Fourier transform on G involves only $g \sum_{S=1}^{n} g_S$ additions and multiplications (Fast Fourier Transform on G [9]). Consequently, by (18)-(20), calculation of the rank or determinant of a circulant on G requires only $g + g \sum_{S=1}^{n} g_S$ additions and multiplications, while

calculation of the generalized inverse of a circulant requires

$g + 2g \sum_{S=1}^{n} g_S$ additions and multiplications.

ACKNOWLEDGEMENT

The authors wish to thank Professor Minc and Dr. Rosinger from Technion, Israel Institute of Technology, for helpful discussions.

B I B L I O G R A P H Y

1. Ablow, C.M. and J.L. Brenner: "Roots and Canonical Forms of Circulant Matrices". Trans. Amer. Math. Soc., 107 (1963), pp. 360-373.

2. Charmonman, S. and R.S. Julius: "Explicit Inverses and Condition Numbers of Certain Circulants", Math. Comp., 22 (1968), pp. 428-430.

3. Pye, W.C., T.L. Boullion and T.A. Atchinson: "The Pseudoinverse of a Composite Matrix of Circulants", SIAM J. Appl. Math., 4, (1973), pp. 552-555.

4. Logofet, D.O.: "About Stability of One Class of Matrices Arising in the Mathematical Theory of Biological Associations", Dokladi Akademi Nauk USSR (1975), 221(6), pp. 1272-1275 (Russian).

5. Pearl, J.: "Optimal Dyadic Models of Time Invariant Systems", IEEE Trans. on Computers, Vol. C-24, No.6, June 1975, pp. 598-603.

6. Pichler, F.: "On State Space Description of Linear Dyadic - Invariant Systems". Proc. Symp. on the Appl. of Walsh Functions (Washington, D.C., April 1971), pp. 166-170.

7. Gethoffer, H.: "Algebraic Theory of Generalized Convolution on Cyclic Groups". Colloquium on Theory and Applications of Walsh Functions. (The Hatfield Polytechnic, June 1973.)

8. Hewitt, E. and K. Ross: "Abstract Harmonic Analysis". Vol.II, Springer-Verlag, Berlin, 1970.

9. Apple, G. and P. Wints: "Calculation of Fourier Transforms of Finite Abelian Groups", IEEE Trans. on Inf. Theory, Vol. IT-16, March 1970, pp. 233-236.