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.
ABSTRACT

It is shown that properties of simple and composite circulant matrices may be generalized to circulants of finite groups. The closure properties 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 analysis are used to solve these problems.
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 $k g \times k g$ matrix $F = \|f_{i,j}\|$ $f_{i,j} = \|f(j^{-1}i)\|$ $(1, j = 1, \ldots, g)$ where $f$ is a matrix-valued function, $f: G \rightarrow M_{k,k}$, $M_{k,k}$ is the set of all $k \times k$ matrices over the field $\mathbb{C}$ 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

\[ \text{Cir}(G,k) = \{ \| f(j^{-1}i) \| \mid f: G \to \mathbb{K}_{k,k} \} \]

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

**Theorem 1**

(i) If \( F \in \text{Cir}(G,k) \), then \( F^n \in \text{Cir}(G,k) \).

(ii) If \( F_1, \ldots, F_n \in \text{Cir}(G,k) \) and \( \alpha_1, \ldots, \alpha_n \in \mathbb{C} \),

\[ \text{then} \quad (\sum_{i=1}^{n} \alpha_i F_i) \in \text{Cir}(G,k). \]

(iii) If \( F_1, F_2 \in \text{Cir}(G,k) \), then \( (F_1 \ast F_2) \in \text{Cir}(G,k) \).

(iv) If \( F_1, F_2 \in \text{Cir}(G,k) \), then \( (F_1 \# F_2) \in \text{Cir}(G,k) \)

\((F_1 \# F_2)\) is the Hadamard product of \( F_1 \) and \( F_2 \).

(v) If \( F_1 \in \text{Cir}(G,k_1) \), \( F_2 \in \text{Cir}(G,k_2) \), then \( (F_1 \otimes F_2) \in \text{Cir}(G,k_1 k_2) \).

\((F_1 \otimes F_2)\) is the Kronecker product of \( F_1, F_2 \) and \( g \) is the order of \( G \).

**Proof.** Properties (i), (iii), (iv), (v) follows immediately from the definition of \( \text{Cir}(G,k) \).

We prove (iii). Let \( F_1 = \| f_1(j^{-1}i) \|, F_2 = \| f_2(j^{-1}i) \|, F = \| F_1, j \| = F_1 \cdot F_2 \)

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 $FX = \phi$ ($F, \phi \in \text{Cir}(G,k)$) is solvable, then its set of solutions contains at least one circulant on $G$.

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

(iii) \[ \dim V(F, \phi) = k(kg - \text{rank}F). \] (1)

Proof. (i) Let

\[ F = \| F_{i,j} \|, \quad X = \| X_{i,j} \|, \quad \phi = \| \phi_{i,j} \|, \quad (F_{i,j}, X_{i,j}, \phi_{i,j} \in M_{k,k}) \]

$i, j = 1, \ldots, g$. If $FX = \phi$ is solvable, there exist $X_{q,i}$ such that

\[ \sum_{q=1}^{g} F_{i,q} X_{q,i} = \phi_{i,i} \] (2)

Let

\[ X_{p,r} = X_{r^{-1}p,1} \] \hspace{1cm} $(p, r = 1, \ldots, g)$ (3)

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

\[ F_{p,r} = F_{r^{-1}p,1}, \quad \phi_{p,r} = \phi_{r^{-1}p,1} \] \hspace{1cm} $(p, r = 1, \ldots, g)$. Now let $i = r^{-1}j$, $q = r^{-1}p$ in (2) for some $r \in \{1, \ldots, g\}$. Then by (2), (3),
\[ \phi_{j,r} = \sum_{p=1}^{g} F_{-r_1,j,-r_1}^* X_{-r_1}^* = \sum_{p=1}^{g} F_{-r,p}^* X_{-r}^* = \sum_{p=1}^{g} F_{j,p} X_{p,r} \]

and so \( X \in \mathcal{V}(F, \phi) \).

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

(iii) Conditions (2), (3) hold for every \( X \in \mathcal{V}(F, \phi) \); hence putting

\[ \phi_{1,1} = 0 \quad (i = 1, \ldots, g) \]

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 \( \psi + \hat{\psi} \) on \( G \) for matrix-valued functions \( \psi(j) = \| \psi_{m,\xi}(j) \| \) \( (j \in G; m = 1, \ldots, k_1; \xi = 1, \ldots, k_2) \)

\[ \hat{\psi}(\omega) = \| \hat{\psi}_{m,\xi}(\omega) \| = \| \frac{d\omega}{g} \sum_{j=1}^{g} \psi_{m,\xi}(j) R_{\omega}(j^{-1}) \|, \quad (4) \]

where \( R_{\omega} \) is the \( \omega \)-th irreducible unitary representation of \( G \) of dimension \( d\omega \) over the field \( \mathbb{C} \) 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.

(1) Let \( f : G \rightarrow M_{k_1, k_2}, x : G \rightarrow M_{k_2, k_3}, \psi : G \rightarrow M_{k_1, k_3} \).
Then

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

iff

$$\hat{f}(\omega) \hat{x}(\omega) = \text{diag}^{-1}(\Psi(\omega)) \quad \forall R_\omega \in R(G)$$  \hspace{1cm} (5)

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

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

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

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

(i) $\text{rank } F = \sum_{R_\omega \in R(G)} \text{durerank } \hat{f}(\omega)$ ; \hspace{1cm} (7)

(ii) $\text{det } F = g^{kg} \sum_{R_\omega \in R(G)} \omega^{-k} \omega^{-2} (\text{det } \hat{f}(\omega)) \omega$ ; \hspace{1cm} (8)

(iii) Let $Q_{i,j} = \|q_{m,k}(j^{-1}i)\| = \| \sum_{R_\omega \in R(G)} \omega^{2} \text{Trace } (f_{m,k}^+(\omega) R_{j^{-1}i}(j^{-1}i)) \|$, \hspace{1cm} (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

\[
F^* \begin{bmatrix} \|x(1)\| \\ \vdots \\ \|x(g)\| \end{bmatrix} = \begin{bmatrix} \|\Psi(1)\| \\ \vdots \\ \|\Psi(g)\| \end{bmatrix}. \tag{10}
\]

Then

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

and by (5),

\[
\hat{f}(\omega)\hat{x}(\omega) = d_{og}^{-1}\hat{\Psi}(\omega) \quad \forall \omega \in R(G) \tag{12}
\]

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

(i) Let \( \Psi = 0 \). Then for every \( \omega \in R(G) \), \( \hat{\Psi}(\omega) = 0 \) and the space of solutions \( \hat{x}(\omega) \) of (12) has dimension \( kd\omega \cdot \text{rank} \hat{f}(\omega) \).

Since \( \hat{x}(\omega) \) is the Fourier transform for \( x(i) \), the dimension of the null-space of \( F \) is \( \sum_{\omega \in R(G)} \Sigma \omega \cdot \text{rank} \hat{f}(\omega) \). Hence, since [8]:

\[
\sum_{\omega \in R(G)} \Sigma \omega^2 = g, \tag{13}
\]

we have (7).
(11) Let $\Psi(i) = \lambda x(i) = (i = 1, \ldots, g)$. Then by (12),

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

(14)

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

$$
det F = \prod_{\omega \in R(G)} \frac{kdu}{S=1} (\lambda_S(\omega))^{d\omega} = \prod_{\omega \in R(G)} \left(\frac{g^{-1}}{d\omega} kdu \right)^{d\omega} \prod_{S=1} (\mu_S(\omega))^{d\omega} =
$$

$$
g^{kg} \prod_{\omega \in R(G)} d\omega^{-kdu} (det F(\omega))^{d\omega}.
$$

(11) Let $F \in Clr(G, k), f : G \rightarrow M, X = \begin{bmatrix} x(1) \\ \vdots \\ x(g) \end{bmatrix}, \Psi = \begin{bmatrix} \Psi(1) \\ \vdots \\ \Psi(g) \end{bmatrix}$. Then

$$(x(i), \Psi(i)) \in M_k, \quad i = 1, \ldots, g.
$$

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

$$
\min_{M_2} |M_1 M_2 - M_3|^2 = |M_1^* M_3 - M_3|^2 \quad \text{iff} \quad M_4 = M_1^*
$$

(15)

we have by (5), (6)
\[
\min_{\mathbf{X}} |F \mathbf{X} - \Phi|^2 = \min_{\mathbf{X}} \sum_{i=1}^{\mathcal{Z}} \sum_{j=1}^{\mathcal{C}} f(j^{-1}i) x(j) - \Psi(i)|^2 = \\
= g \sum_{R_\omega \in \mathcal{R}(G)} dw^{-1} \min_{\hat{x}(\omega)} |g dw^{-1} \hat{f}(\omega) \hat{x}(\omega) - \hat{\Psi}(\omega)|^2 = \\
= g \sum_{R_\omega \in \mathcal{R}(G)} dw^{-1} |\hat{f}(\omega) \hat{x}(\omega) - \hat{\Psi}(\omega)|^2. \tag{16}
\]

But from (9), using (4), we deduce
\[
\hat{f}_{m, \mathcal{Z}}(\omega) = g^2 dw^{-2} \hat{q}_{m, \mathcal{Z}}(\omega) \quad (m, \mathcal{Z} = 1, \ldots, k) \tag{17}
\]

It now follows from (16), (17) in view of (5), (6) and \(Q \in \text{Cir}(G, k)\) that
\[
\min_{\mathbf{X}} |F \mathbf{X} - \Phi|^2 = g \sum_{R_\omega \in \mathcal{R}(G)} dw^{-1} g^2 dw^{-2} \hat{f}(\omega) \hat{q}(\omega) \hat{x}(\omega) - \hat{\Psi}(\omega)|^2 = \\
= \sum_{S=1}^{\mathcal{G}} \sum_{i=1}^{\mathcal{C}} q(j^{-1}i) \sum_{j=1}^{\mathcal{C}} q(j^{-1}i) \Psi(j) - \Psi(i)|^2 = |FQ \Psi - \Psi|^2
\]

and thus, by (15), \(Q = F^*\).

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

**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 $kdw \times kdw$ 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 calculations 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 $j, l \in G$

$F_{ij} = f(j^{-1} i)$ is a circulant on some group $G_1$ of the order $g_1$, i.e., $f: G \rightarrow \text{Cir}(G_1, k_1)$ and $k = k_1g_1$. 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 $f(j^{-1} i) \in \text{Cir}(G_1, k_1)$ for every $j, i \in G$, then it follows from (4) and (ii) of Theorem 1, that $\hat{f}(\omega) \in \text{Cir}(G_1, k_1d\omega)$ 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 $f: G \rightarrow M_{k_1, k_2}$ and $k_1 \neq k_2$. 
III. CIRCULANTS ON ABELIAN GROUPS FOR $k=1$

We now consider the case of circulants $F = \|f(j^{-1}i)\|$, $f: G \to \mathbb{C}$, 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 $M = \|M_{ij}\|$ ($M_{ij} \in \mathbb{C}$; $1, j, \ldots, g$) and any Abelian group $G$ of order $g$, there exists a unique circulant $F_M \in \text{Cir}(G,1)$ on $G$ which is unitarily similar to $M$.

**Proof.** Since $G$ is Abelian, $\omega = 1$ 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 $f_M(\omega) = g^{-1}\lambda_M(\omega)$. Then

$$f_M(i) = g^{-1} \sum_{R_{\omega} \in R(G)} \lambda_M(\omega)R_{\omega}^{-1}$$

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

**Corollary 3.** Let $F = \|f(j^{-1}i)\|$ ($f: G \to \mathbb{C}$; $i, j = 1, \ldots, g$) be a circulant on an Abelian group $G$. Then:
(i) \[ \text{rank } F = \sum_{R \in \mathcal{R}(G)} \delta^{t} \hat{f}(\omega), 0 \quad \text{where} \quad \delta^{t} \hat{f}(\omega), 0 = \begin{cases} 1, \text{if } \hat{f}(\omega) \neq 0 \\ 0, \text{if } \hat{f}(\omega) = 0 \end{cases} \] \quad ; \quad (18)

(ii) \[ \text{det } F = g^{\mathfrak{g}} \prod_{R \in \mathcal{R}(G)} \hat{f}(\omega); \] \quad (19)

(iii) \[ F^{\dagger} = \| F_{ij} \| = g^{-2} \sum_{R \in \mathcal{R}(G)} \hat{f}^{\star}(\omega) R_{i}(j^{-1}) \|, \text{ where} \] \[ \hat{f}^{\star}(\omega) = \begin{cases} \hat{f}^{-1}(\omega), \text{if } \hat{f}(\omega) \neq 0 \\ 0, \text{if } \hat{f}(\omega) = 0 \end{cases} \] \quad (20)

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

**Proof.** The proof follows from Theorem 3 and Corollary 1 with \( k=1 \) since in our case \( dw = 1 \) for every \( R \in \mathcal{R}(G) \). Thus, for Abelian groups, calculation of the rank, eigenvalues, determinant and generalized inverse of a circulant \( F = \| f(j^{-1}) \| \) 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 \( G \) [39]). 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

\[ g + 2g \sum_{s=1}^{D} g_s \] additions and multiplications.

ACKNOWLEDGEMENT

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


