Reprinted from JOURNAL OF COMPUTER AND SYSTEM SCIENCES
All Rights Reserved by Academic Press, New York and London

Vol. 19, No. 3, December 1979
Printed in Belgium

Group Character Tables in Discrete Transform Theory

SHARAD V. KANETKAR

Computer Centre, Indian Institute of Technology, Bombay 400 076, India

AND

MEGHANAD D. WAGH

Department of Electrical Engineering, Concordia University, Montreal, Quebec H3G 1M8, Canada

Received June 10, 1977; revised June 6, 1979

It has been shown that a transform satisfying a generalized form of the convolution theorem can be described by the group character table of an appropriate finite Abelian group G. Exact correspondence between the transform properties and the underlying group properties is established and it has been demonstrated that many of the digital signal processing problems may be solved efficiently using the group theoretic approach. Sets of permutations are fully characterized such that a permutational convolution defined with respect to them can be converted into a transform product by some invertible transform.

1. INTRODUCTION

Recent years have seen a rapid development of digital signal processing (DSP) techniques. A major part of the activity in this field is confined to a search for efficient discrete orthogonal transforms and investigation of their properties. In this paper, it has been shown that all those transform matrices used in DSP which satisfy a generalized version of the convolution theorem can be identified with the character tables of finite Abelian groups. This allows a group theoretic approach in the solution of many DSP problems resulting in a considerable saving of effort.

This methodology, amply illustrated in this paper through examples, is not only more efficient as compared to the usual matrix methods, but also provides a better understanding and unified approach in dealing with many of the discrete orthogonal transforms.

2. GROUP THEORETIC PRELIMINARIES

All the groups considered here are finite Abelian. Let $G = \{g_0, g_1, \ldots, g_{N-1}\}$ be such a group.[1] Then it is known that there are exactly N homomorphisms $\phi_0, \phi_1, \ldots, \phi_{N-1}$

[1] Additive notations will be used (identity $\equiv 0$) throughout for the group and ng, $g \in G$, will denote $g + g + \cdots n$ times. Note that since G is Abelian, $n(g + h) = ng + nh$, for all $g, h \in G$.

0022-0000/79/060211-11$02.00/0

from G into the multiplicative group of the complex field. The complex character table of G is an $N \times N$ matrix M defined by

$$M(i,j) = \phi_i(g_j), \qquad i,j = 0, 1,..., N-1. \tag{1}$$

From (1), it is clear that the columns of M can be labeled with the elements of G and the rows with the homomorphisms.

The following properties of the group character tables are well known [5, Chap. 5; 9, Chap. 3]:

(P1) $\sum_{j=0}^{N-1} M(i,j) \cdot M^*(k,j) = N\delta(i,k)$, where the asterisk denotes the complex conjugate and δ is the Kronecker delta.

(P2) If $G = G_1 \times G_2 \times \cdots \times G_r$, then the character table of G is the Kronecker product of the character tables of $G_1, G_2,..., G_r$.

(P3) Since $\forall g \in G$, $g^N =$ identity of G, $(\phi_i(g))^N = 1$ $\forall i$. This implies that $M(i,j)$ is an Nth root of unity for $0 \leqslant i, j \leqslant N-1$ and $|M(i,j)| = 1$.

If

$$G \simeq C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}, \tag{2}$$

where $C_{n_k} = \langle a_k \rangle$ is a cyclic group of order n_k with generator a_k, the group elements may be ordered lexicographically as

$$g_j = j_1 a_1 + j_2 a_2 + \cdots + j_r a_r, \tag{3}$$

where $j_1, j_2,..., j_r$ are obtained from the unique representation of j

$$\begin{aligned} j &= \langle\!\langle j_1, j_2,..., j_r \rangle\!\rangle \\ &= j_1 n_2 n_3 \cdots n_r + j_2 n_3 n_4 \cdots n_r + \cdots + j_{r-1} n_r + j_r, \qquad 0 \leqslant j_k \leqslant n_k - 1, \end{aligned} \tag{4}$$

to give

$$M = F_{n_1} \otimes F_{n_2} \otimes \cdots \otimes F_{n_r}, \tag{5}$$

where F_{n_k} is a Fourier matrix of order n_k and $\otimes$ denotes the Kronecker product.

As is evident from (5), when $G = C_N$, M is the discrete Fourier transform (DFT) kernel of order N. If $G = C_2 \times C_2 \times \cdots \times C_2$ (n times), M is the kernel of the Hadamard transform (HT) of order 2^n. If $G = C_p \times C_p \times \cdots \times C_p$ (n times), M is the kernel of the class of generalized Walsh transforms studied by Chang and Thomas [4]. Finally, it may be pointed out that any character table M as given by (5) is the generalized Hadamard transform (lcm$\{n_1, n_2,..., n_r\}$, $n_1 n_2 \cdots n_r$) of Butson [2].

The transform whose kernel M is a character table of some finite Abelian group (not necessarily with ordered elements which give M in the form (5)) will be referred to as the Group Theoretic Transform (GTT) in this work although some authors

[1, 3, 10, 11] have called it "Fourier transform over Abelian groups" or "a system of Walsh functions in a generalized sense" [12].

The transform vector X is related to the signal vector x through (1) as

$$X(i) = \sum_{j=0}^{N-1} \phi_i(g_j)\, x(j), \qquad 0 \leqslant i \leqslant N-1.$$

Relabeling $X(i)$ as X_ϕ, where ϕ is the homomorphism corresponding to the ith row, and $x(j)$ as x_g, where g is the jth element of the group (given by (3) and (4)) and hence the element associated with the jth column of M, one gets

$$X_\phi = \sum_{g \in G} \phi(g)\, x_g .$$

From (P1), the inverse transform could be defined as

$$x_g = \frac{1}{N} \sum_{\phi} \phi(-g)\, X_\phi , \tag{6}$$

where the summation is taken over all the homomorphisms ϕ.

3. Permutational Properties of the Group Theoretic Transforms

Let $\bar{x}$ be a vector obtained by

$$\bar{x}_g = x_{\sigma^{-1}g} ,$$

where σ^{-1} is a permutation of the elements of G. $\bar{x}$ is thus clearly a sequence obtained by permuting the components of x. Let $\bar{X}$ be the transform of $\bar{x}$, i.e.,

$$\bar{X}_\phi = \sum_{g \in G} \phi(g)\, x_{\sigma^{-1}g} = \sum_{g \in G} \phi(\sigma g)\, x_g .$$

In this section, we determine σ's under some relations between $\bar{X}$ and X.

THEOREM 1. *$|\bar{X}_\phi| = |X_\phi|$ for all ϕ and all complex signal vectors iff $\sigma(g) = g + h$ for some fixed $h \in G$ for all $g \in G$.*

Proof. Obvious. ∎

Since h is an arbitrary element of G, there are exactly N permutations of complex signal components which preserve the transform component's modulus.

In the case of a DFT, the group elements are ordered as $g_j = ja$, where $G = \langle a \rangle$. In this case, if $h = ka$, $0 \leqslant k \leqslant N-1$, then these permutations are $g_j \to g_j + h = (j + k)a = g_{(j+k) \bmod N}$ which is a cyclic shift of the signal samples by $-k$ units. In the case of the HT, these permutations turn out to be dyadic shifts.

THEOREM 2. *A permutation σ^{-1} of the signal components merely permutes the* GTT *components iff σ is an automorphism of the group G.*

Proof. If $\bar{X}$ is a permuted version of X, the component $\bar{X}_\phi$ of $\bar{X}$ is the same as some component $X_{\bar{\phi}}$ of X. Then

$$\sum_{g\in G} \phi(\sigma g)\, x_g = \sum_{g\in G} \bar{\phi}(g)\, x_g\,.$$

Since this equation is true for all x sequences,

$$\phi(\sigma g) = \bar{\phi}(g).$$

Now, $\forall g, h \in G$,

$$\begin{aligned}\phi(\sigma(g+h)) &= \bar{\phi}(g+h) = \bar{\phi}(g)\,\bar{\phi}(h)\\ &= \phi(\sigma g)\,\phi(\sigma h)\\ &= \phi(\sigma g + \sigma h).\end{aligned}$$

Thus σ is a homomorphism and therefore an automorphism of G. Conversely, if σ is an automorphism,

$$\phi(\sigma g) = (\phi\sigma)(g) = \bar{\phi}(g).$$

Since $\phi\sigma$ is clearly a homomorphism and the character table covers all the homomorphisms,

$$\bar{X}_\phi = X_{\bar{\phi}}\,. \quad \blacksquare$$

In the case of a DFT, $G = C_N = \langle a\rangle$ and therefore the automorphism group $A(G)$ of G is the group of mappings defined by $\sigma g_j = kg_j = (kj)a = g_{kj}$, where $\gcd(k, N) = 1$. This result matches with that of Gold and Rader [8, p. 170]. When $G = C_p \times C_p \times \cdots$ (n times), $A(G)$ is known to be the general linear group $GL_n(p)$, the group of $n \times n$ nonsingular matrices over $GF(p)$. Thus in the case of the generalized Walsh transform [4] or HT (for $p = 2$), these permutations can be easily determined and their number is [7, p. 223]

$$|A(G)| = (p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1}).$$

In general, the automorphism $\sigma \in A(G)$ is uniquely related to a matrix T transforming the basis of G through

$$\sigma g_j = g_{j'} \Leftrightarrow \langle\!\langle j'\rangle\!\rangle = \langle\!\langle j\rangle\!\rangle T,$$

where $\langle\!\langle j'\rangle\!\rangle$ and $\langle\!\langle j\rangle\!\rangle$ are the row vectors corresponding to the representations of j' and j, respectively, given by (3) and (4). If $G \simeq C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$, where n_i's are prime powers for $1 \leqslant i \leqslant r$, then the matrix T satisfies the following conditions [7, Sects. 55, 58 and Exercise 15 on p. 229]:

(i) $0 \leqslant T(i,j) < n_i$.

(ii) $T(i,j) = 0$, if $\gcd(n_i, n_j) = 1$.

(iii) $(n_i/n_j) \mid T(i,j)$, if $n_j \mid n_i$.

(iv) For any prime $p \mid\mid G \mid$, if set S_p is defined as $S_p = \{i \mid p \mid n_i\}$, then the matrix T_p obtained by restricting T to the rows and columns belonging to S_p is nonsingular modulo p.

This enables one to compute all the automorphisms of any Abelian group.

4. Convolutional Property of the Group Theoretic Transforms

When G is a cyclic group, the sequence

$$z_h = \sum_{g \in G} x_g y_{h-g}, \qquad h \in G, \tag{7}$$

turns out to be the cyclic convolution of x and y. Therefore, in general, (7) may be called a convolution associated with a group G. It is easy to show from (7) that

$$Z_\phi = X_\phi Y_\phi \qquad \text{for all } \phi, \tag{8}$$

where X, Y, and Z are the GTT's of x, y, and z, respectively, w.r.t. G. Conversely, (8) implies (7). Thus every GTT is uniquely associated with a convolution as in (7).

The concept of convolution may be further generalized by defining the permutational convolution of x and y w.r.t. a set Σ of N permutations σ_j's of $\Delta = \{0, 1, 2, \ldots, N-1\}$ to be a sequence z given by

$$z(j) = \sum_{i=0}^{N-1} x(i)\, y(\sigma_j i), \qquad j = 0, 1, \ldots, N-1. \tag{9}$$

A transform is said to satisfy a permutational convolution theorem (PCT) w.r.t. Σ if

$$Z = X \cdot Y, \tag{10}$$

where X, Y, and Z are the transforms of x, y, and z, respectively, and $(\cdot)$ denotes the componentwise product (i.e., $Z(k) = X(k)\, Y(k)$, $k = 0, 1, \ldots, N-1$).

5. Characterization of Group Theoretic Transforms

Theorem 3. *An invertible transform which satisfies a* PCT *must be a* GTT.

Proof. Let $m_0, m_1, \ldots, m_{N-1}$ denote the columns of M. Then the transform vector X is given by

$$X = \sum_{i=0}^{N-1} m_i x(i).$$

If $x(i) = \delta(i, i_1)$ and $y(i) = \delta(i, i_2)$, then $X = m_{i_1}$ and $Y = m_{i_2}$. As the transform satisfies the PCT,

$$m_{i_1} \cdot m_{i_2} = X \cdot Y = Z = \sum_{j=0}^{N-1} m_j z(j)$$

$$= \sum_{j=0}^{N-1} \sum_{i=0}^{N-1} m_j x(i)\, y(\sigma_j i)$$

$$= \sum_{j=0}^{N-1} m_j y(\sigma_j i_1)$$

$$= \sum_{j \in A(i_1, i_2)} m_j , \tag{11}$$

where $A(i_1, i_2) = \{j \mid \sigma_j i_1 = i_2\}$. The set A satisfies the following properties:

$$A(i_1, i_2) \cap A(i_1, i_3) = \phi \qquad \text{if} \quad i_2 \neq i_3 , \tag{12}$$

for $j \in A(i_1, i_2) \cap A(i_1, i_3)$ implies $\sigma_j(i_1) = i_2 = i_3$. Further,

$$\bigcup_{i_2 \in \Delta} A(i_1, i_2) = \Delta \tag{13}$$

because for any $j \in \Delta$, $\sigma_j(i_1)$ equals some i_2 in Δ implying $j \in A(i_1, i_2)$. It can now be shown that for any $i, j \in \Delta$, $A(i, j) \neq \phi$ because otherwise from (12) and (13), there exist some $s, t \in \Delta$ such that

$$A(i, j) = \phi \qquad \text{or} \qquad m_i \cdot m_j = 0, \tag{14}$$

$$A(i, s) \neq \phi \qquad \text{or} \qquad m_i \cdot m_s \neq 0, \tag{15}$$

$$s \in A(j, t) \qquad \text{or} \qquad m_j \cdot m_t = m_s + \cdots, \tag{16}$$

where the RHS of (16) is the sum of distinct columns of M (including m_s). Multiplying (16) by m_i (componentwise), the LHS $= 0$, but from (12) and (15), the RHS is the sum of one or more distinct columns of M. This contradicts the nonsingularity of M. Hence, $A(i_1, i_2) \neq \phi$ for any $i_1, i_2 \in \Delta$ and from (12) and (13), $|A(i_1, i_2)| = 1$ and Σ is transitive. Let $A(i_1, i_2) = \{i_3\}$. Then (11) shows that $m_{i_1} \cdot m_{i_2} = m_{i_3}$. Thus the columns of M are closed under component-by-component multiplication. Also, no element of M is zero because otherwise the transitivity of Σ and (11) would imply that the row which has a zero is a zero row, again contradicting the nonsingularity of M. Since the set of columns is finite and each component of a column is nonzero, it is obvious that the columns form a group G. Each row of M is therefore a homomorphic image of G. These rows are also linearly independent as M is invertible. M is therefore the character table of G and hence M is the kernel of the GTT with the underlying Abelian group G. ∎

Without loss of generality, it may be assumed that the column which acts as the

identity of the group G is the leftmost column of M, i.e., m_0. Obviously, all the components of m_0 are equal to unity.

From Theorem 3, it is clear that G is related to Σ, the set of N permutations defining the convolution as in (9). The following corollary explicitly defines G in terms of Σ.

COROLLARY 1. *Any $\sigma \in \Sigma$ is of order 2 and the set $\sigma_0\Sigma$ forms a group $G' \simeq G$.*

Proof. From the proof of Theorem 3 and especially (11), it is obvious that $\sigma_k(i) = j$ iff $m_i \cdot m_j = m_k$. Because m_i and m_j commute, σ_k is of order 2. Further, $\sigma_0(i) = j$ iff $m_i = m_j^{-1}$ and $\sigma_0\sigma_k(i) = t$ iff $m_t = m_i \cdot m_k^{-1}$.

Now consider a function $f: G \to \sigma_0\Sigma$ defined by $f(m_i) = \sigma_0\sigma_i$. It should then be shown that f is an isomorphism. Consider the image of $f(m_i \cdot m_j)$, where $m_p = m_i \cdot m_j$.

$$f(m_i \cdot m_j) = f(m_p) = \sigma_0\sigma_p .$$

But

$$\sigma_0\sigma_p(u) = v, \tag{17}$$

iff $m_v = m_u \cdot m_p^{-1} = m_u \cdot m_i^{-1} \cdot m_j^{-1}$. Substituting $m_u \cdot m_i^{-1} = m_w$ gives $\sigma_0\sigma_i(u) = w$ and $m_v = m_w \cdot m_j^{-1}$ gives $\sigma_0\sigma_j(w) = v$. Thus,

$$\sigma_0\sigma_j(\sigma_0\sigma_i(u)) = v. \tag{18}$$

Comparing (17) and (18), which are true for all u,

$$\sigma_0\sigma_p = \sigma_0\sigma_j \cdot \sigma_0\sigma_i$$

or

$$f(m_i \cdot m_j) = f(m_i) \cdot f(m_j).$$

Thus f is a homomorphism. Further, if $f(m_i) = f(m_j)$,

$$\sigma_0\sigma_i(u) = \sigma_0\sigma_j(u) = v \text{ (say)}.$$

This implies $m_v = m_u \cdot m_i^{-1} = m_u \cdot m_j^{-1}$ and gives $m_i = m_j$. This shows that f is an isomorphism and completes the proof. ∎

Note that since $\sigma_0\Sigma = G'$, for any $\sigma \in \Sigma$, $\sigma_0\sigma \in G'$ and therefore its inverse $\sigma\sigma_0 \in G'$. Hence

$$G' = (\sigma\sigma_0)\, G' = (\sigma\sigma_0)(\sigma_0\Sigma) = \sigma\Sigma.$$

The converse of this corollary is Theorem 4.

THEOREM 4. *Given a set Σ of N permutations of $\Delta = \{0, 1, \ldots, N-1\}$ such that σ^2 is an identity permutation for all $\sigma \in \Sigma$ and for some $\sigma \in \Sigma$, $\sigma\Sigma \simeq G$, an Abelian group, then the* GTT *over G satisfies the* PCT w.r.t. Σ.

Proof. Since $\sigma\Sigma$ is an Abelian group of order equal to $|\Delta|$, it is transitive. Hence Σ is transitive and one could denote by σ_i that $\sigma \in \Sigma$ which takes (some fixed) $s \in \Delta$ to i. Thus

$$\sigma_i(s) = i, \qquad i \in \Delta. \tag{19}$$

From the remark after Corollary 1 and the proof of Theorem 3, $\sigma_s\Sigma = \sigma\Sigma \simeq G \simeq$ group of columns of M. Let m_i be the image of $\sigma_s\sigma_i$ under this isomorphism. The convolution μ_k associated with the GTT takes i to j iff $m_i \cdot m_j = m_k$, i.e.,

$$\sigma_s\sigma_i\sigma_s\sigma_j = \sigma_s\sigma_k . \tag{20}$$

We now show that (20) leads to $\sigma_k(i) = j$ which would imply that σ's are the permutations associated with the GTT. Combining (19) and (20),

$$\begin{aligned} \sigma_s\sigma_k(i) &= (\sigma_s\sigma_i)(\sigma_s\sigma_j)(\sigma_i(s)) \\ &= \sigma_s\sigma_j\sigma_s(s) && \text{as } G \text{ is Abelian and the order of } \sigma_i \text{ is 2,} \\ &= \sigma_s(j) && \text{from (19).} \quad \blacksquare \end{aligned}$$

Theorem 4 identifies all those sets Σ of permutations for which there exist transforms which convert convolutions defined as in (9) into products of transforms as in (10).

The following two examples illustrate the determination of transform (if it exists) which satisfies the PCT w.r.t. the given set of permutations Σ.

EXAMPLE 1. Let $\Delta = \{0, 1, \ldots, 7\}$ and $\Sigma = \{\sigma_0, \sigma_1, \ldots, \sigma_7\}$, where in cycle notation,

$$\begin{aligned} \sigma_0 &= (1\ 3)(2\ 6), & \sigma_1 &= (0\ 4)(1\ 6)(2\ 3)(5\ 7), \\ \sigma_2 &= (0\ 1)(2\ 4)(3\ 5)(6\ 7), & \sigma_3 &= (0\ 5)(4\ 7), \\ \sigma_4 &= (0\ 7)(1\ 2)(3\ 6)(4\ 5), & \sigma_5 &= (0\ 3)(1\ 5)(2\ 7)(4\ 6), \\ \sigma_6 &= (0\ 6)(1\ 7)(2\ 5)(3\ 4) \quad \text{and} & \sigma_7 &= (0\ 2)(1\ 4)(3\ 7)(5\ 6). \end{aligned}$$

It can be observed that all the permutations are of order two and that $\sigma_4\Sigma$ forms an Abelian group isomorphic to $C_4 \times C_2 = \langle a \rangle \times \langle b \rangle$ with the following correspondence (any other $\sigma \in \Sigma$ in place of σ_4 would have given the same group by the remark after Corollary 1):

$$\begin{aligned} \sigma_4\sigma_0 &= (0\ 7)(1\ 6)(2\ 3)(4\ 5) \to b, \\ \sigma_4\sigma_1 &= (0\ 5)(1\ 3)(2\ 6)(4\ 7) \to 2a, \\ \sigma_4\sigma_2 &= (0\ 2\ 5\ 6)(1\ 7\ 3\ 4) \to a, \\ \sigma_4\sigma_3 &= (0\ 4)(1\ 2)(3\ 6)(5\ 7) \to 2a + b, \\ \sigma_4\sigma_4 &= \text{identity permutation} \to 0, \\ \sigma_4\sigma_5 &= (0\ 6\ 5\ 2)(1\ 4\ 3\ 7) \to 3a, \\ \sigma_4\sigma_6 &= (0\ 3\ 5\ 1)(2\ 4\ 6\ 7) \to a + b, \\ \sigma_4\sigma_7 &= (0\ 1\ 5\ 3)(2\ 7\ 6\ 4) \to 3a + b. \end{aligned}$$

From Theorem 4, the required transform kernel is thus the character table of $C_4 \times C_2$ whose columns are headed by the group elements $b, 2a, a, 2a + b, 0, \ldots$ (in that order). This transform kernel is given below:

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

Note that the ordering of rows is arbitrary. The eight homomorphisms are defined by $\phi(i_1 a + i_2 b) = (\phi(a))^{i_1}(\phi(b))^{i_2}$, where $\phi(a)$ could be 1, i, -1, or $-i$ and $\phi(b)$ could be 1 or -1 ($i = \sqrt{-1}$).

EXAMPLE 2. Let $\Delta = \{0, 1, 2, 3\}$ and $\Sigma = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, where

$$\sigma_0 = (1\ 3), \qquad \sigma_1 = (0\ 1)(2\ 3),$$
$$\sigma_2 = (0\ 2)(1\ 3), \quad \text{and} \quad \sigma_3 = (0\ 3)(1\ 2).$$

Then

$$\sigma_0\sigma_0 = \text{identity permutation}, \qquad \sigma_0\sigma_1 = (0\ 3\ 2\ 1),$$
$$\sigma_0\sigma_2 = (0\ 2), \qquad \sigma_0\sigma_3 = (0\ 1\ 2\ 3).$$

Since $\sigma_0\Sigma$ does not form a group ($(\sigma_0\sigma_1)(\sigma_0\sigma_2) = (0\ 1)(2\ 3) \notin \sigma_0\Sigma$), by Corollary 1, there is *no* invertible transform which would satisfy a PCT w.r.t. this Σ. Note that if the invertibility condition is relaxed, the transform defined by an all-zero matrix satisfies a PCT w.r.t. *any* given Σ.

6. Extensions over Finite Fields and Finite Rings

The GTT kernel M defined in earlier sections has rows which are homomorphisms from G into the complex field. If this field is replaced by any finite field F, then still there are exactly $|G|$ distinct homomorphisms provided that an rth primitive root of unity exists in that finite field (i.e., $r \mid (|F| - 1)$), where r is the exponent of the group (i.e., the maximum order of any group element). By setting the rows of M equal to the images of G under these homomorphisms, one can still get a perfectly valid definition of a character table and hence a GTT for which all the earlier results will apply (except that Theorem 1 will become modified as $\bar{X}_\phi = \phi(h)\, X_\phi$).

Further, ensuring that $\gcd(|F|, N) = 1$ guarantees the invertibility of N. The inverse GTT can therefore be defined as in (6).

Fourier transform (GTT for a cyclic group) over finite fields has been studied by Pollard [13].

When the field is replaced by a finite ring R, one can still define a GTT in a generalized sense as the set of homomorphisms from G into the multiplicative group of R. Further, if I is any maximal ideal of R and r, the exponent of G, then R/I is isomorphic to a finite field and existence of an rth primitive root of unity in R/I is guaranteed if $r \mid (\mid R/I \mid - 1)$. Arguments in this direction lead one to the following necessary and sufficient condition for the existence of the GTT in a finite ring:

$$r \mid \gcd\{(\mid R/I_1 \mid - 1), (\mid R/I_2 \mid - 1),\ldots, (\mid R/I_s \mid - 1)\},$$

where $I_1, I_2, \ldots, I_s$ are all the maximal ideals of R. This result has also been proved by Dubios and Venetsanopoulos [6]. All the results of the earlier sections (except the minor modification of Theorem 1) are then applicable to these transforms.

7. Conclusions

It has been shown in this paper that some of the properties of the GTT can be easily determined if it is realized that the GTT matrix is really the character table of an appropriate Abelian group. The establishment of a correspondence between the group theory and the digital transform theory allows a free flow of ideas from the highly developed group algebra to the digital signal processing domain. For example, it has been shown that the signal component permutations which permute the transform components are really the automorphisms of the underlying group. Since the automorphism group of a finite Abelian group can be completely and easily determined, all such permutations may be specified. Further, investigation of the properties of the automorphism group might reveal more details of these permutations.

The GTTs are fully characterized. These are the only invertible transforms which satisfy a permutational convolution theorem. Conversely, the permutational convolutions which can be converted into the transform products by any invertible transform are also characterized.

References

1. G. Apple and P. Wintz, Calculation of Fourier transform on finite Abelian groups, *IEEE Trans. Information Theory* **IT-16** (1970), 233–234.
2. A. T. Butson, Generalized Hadamard matrices, *Proc. Amer. Math. Soc.* **13** (1962), 894–898.
3. T. W. Cairns, On fast Fourier transforms on finite Abelian groups, *IEEE Trans. Computers* **C-20** (1971), 569–571.
4. S. H. Chang and J. Thomas, On ordering of a class of generalized Walsh functions, *in* "Applications of Walsh Functions: 1972 Proceedings, Washington, D. C.," pp. 337–343.
5. C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, *in* "Pure and Applied Mathematics, Vol. 11, Interscience, New York, 1962.
6. E. Dubios and A. N. Venetsanopoulos, The discrete Fourier transform over finite rings with application to fast convolution, *IEEE Trans. Computers* **C-27** (1978), 586–593.

7. L. FUCHS, "Abelian Groups," Pergamon, Oxford, 1960.
8. B. GOLD AND C. M. RADER, "Digital Processing of Signals," McGraw–Hill, New York, 1969.
9. D. GORENSTEIN, "Finite Groups," Harper & Row, New York, 1968.
10. M. G. KARPOVSKY, "Finite Orthogonal Series in the Design of Digital Devices (Analysis, Synthesis and Optimization)," Wiley, New York, 1976.
11. P. J. NICHOLSON, Algebraic theory of finite Fourier transforms, *J. Comput. System Sci.* **5** (1971), 524–547.
12. F. PICHLER, Walsh functions, signals and systems, *in* "Proceedings, Symposium on Applications of Walsh Functions," pp. 177–190, Washington, D. C., March 1974.
13. J. M. POLLARD, The fast Fourier transform in a finite field, *Math. Comp.* **25** (1971), 365–374.

Printed by the St. Catherine Press Ltd., Tempelhof 37, Bruges, Belgium