

On Group Theoretic Transforms and the Automorphism Groups

HEMACHANDRA B. KEKRE, MEGHANAD D. WAGH, AND SHARAD V. KANETKAR

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

An exact correspondance between the signal sample permutations described by group automorphisms and the Group Theoretic Transform (GTT) sample permutations is established. This enables one to find the permutation matrices which commute with the transform kernel. It is also shown that the signal and the transform samples can be partitioned into sets (called orbits) such that if all the signal samples in every orbit are identical then all the transform samples in every orbit are also identical.

1. INTRODUCTION

Recent advances in digital technology have triggered an arousal of a deep interest in discrete linear transform theory. A study of these transforms using classical matrix methods is not only complicated, but is also restricted to transforms with rather simple and suitable kernels.

It has been shown that many of these transform kernels are the character tables of appropriate finite abelian groups and are amenable to group theoretical methods (Kanetkar and Wagh, 1977). We therefore, refer to them as the Group Theoretic Transforms (GTT), although some authors (Apple, 1970; Karpovsky, 1976) prefer the name 'Fourier transforms over abelian groups'. The GTT's include, among others, the Discrete Fourier Transform (DFT), the Hadamard Transform (HT) and the Generalised Walsh Transform (GWT) of Chang and Thomas (1972) which are character tables of a cyclic group, a group $C_2 \times C_2 \cdots \times C_2$ and an elementary abelian group $C_p \times C_p \times C_p \cdots \times C_p$ respectively. In general, all GTT's are the Butson's generalised Hadamard transforms (1962).

Consider an abelian group¹ $G = \{g_0, g_1, \dots, g_{N-1}\}$. It is known that there are exactly N homomorphisms $\phi_0, \phi_1, \dots, \phi_{N-1}$ of G into the multiplicative group of complex numbers, C^* . An $N \times N$ matrix defined by

$$M(i, j) = \phi_i(g_j), \quad 0 \leq i, j \leq N-1$$

is called the character table of G . If $G = C_N$, a cyclic group of order N and the group elements are ordered as $g_j = ja$ where $\langle a \rangle = G$, then the matrix M is

¹ Group operation will be denoted by $+$.

the Fourier matrix and will be denoted by F_N . Further, the character table of $G \simeq G_1 \times G_2$ is the Kronecker product of the character tables of G_1 and G_2 . This suggests that the character table of $G \simeq C_{n_1} \times C_{n_2} \cdots \times C_{n_r}$ is given by $F_{n_1} \otimes F_{n_2} \cdots \otimes F_{n_r}$ where \otimes denotes Kronecker product and the group elements are ordered lexicographically as:

$$g_j = j_1 a_1 + j_2 a_2 + \cdots + j_r a_r \quad (1)$$

where $\langle a_i \rangle = C_{n_i}$ and j_1, j_2, \dots, j_r are obtained from the unique representation of j as

$$j = \langle j_1, j_2, \dots, j_r \rangle \\ = j_1 n_2 n_3 \cdots n_r + j_2 n_3 n_4 \cdots n_r + \cdots + j_{r-1} n_r + j_r, \quad 0 \leq j_i \leq n_i - 1 \quad (2)$$

It is obvious that the ordering of the homomorphisms also plays an important part in establishing the matrix F_N or in general, a matrix $F_{n_1} \otimes F_{n_2} \cdots \otimes F_{n_r}$ as the character table of the group C_N or $C_{n_1} \times C_{n_2} \cdots \times C_{n_r}$ respectively. Firstly, since the number of homomorphisms is exactly equal to the order of the group, the homomorphisms may also be indexed by the group elements, e.g. $\phi_{g_0}, \phi_{g_1}, \dots, \phi_{g_{N-1}}$. Thus, in the case of cyclic group C_N , the homomorphism $\phi: G \rightarrow C^*$ defined by $\phi(g_j) = \omega^{kj}$, $0 \leq j \leq N-1$, where ω is the primitive N th root of unity and k is a fixed integer $0 \leq k \leq N-1$, is denoted by ϕ_{g_k} . This also allows one to compute any element in the matrix M , which is the character table of a cyclic group C_N since,

$$M(k, j) = \phi_{g_k}(g_j) = \omega^{kj} \quad (3)$$

Now if $G \simeq C_{n_1} \times C_{n_2} \times C_{n_3} \cdots \times C_{n_r}$, one can associate a $r \times r$ diagonal matrix D with G such that

$$d_{ii} = \text{lcm}(n_1, n_2, \dots, n_r)/n_i \quad i = 1, 2, \dots, r \\ d_{ij} = 0, \quad i \neq j.$$

Then the fact that the character table of G is $F_{n_1} \otimes F_{n_2} \otimes \cdots \otimes F_{n_r}$ yields

$$M(k, j) = \phi_{g_k}(g_j) = \omega_1^{k_1 j_1} \cdot \omega_2^{k_2 j_2} \cdots \omega_r^{k_r j_r}, \quad 0 \leq k_i, j_i \leq n_i - 1 \quad (4)$$

where ω_i is the primitive n_i th root of unity and k_1, k_2, \dots, k_r and j_1, j_2, \dots, j_r are mixed radix representation coefficients of k and j obtained from (1) and (2). Using matrix D and the notation

$$\langle\langle k \rangle\rangle = (k_1, k_2, \dots, k_r) \quad \text{and} \quad \langle\langle j \rangle\rangle = (j_1, j_2, \dots, j_r), \quad (4)$$

may be written compactly as

$$M(k, j) = \phi_{g_k}(g_j) = \omega^{\langle\langle k \rangle\rangle D \langle\langle j \rangle\rangle^t} \quad 0 \leq k, j \leq N-1, \quad (5)$$

where t denotes the transpose and ω is the primitive $\text{lcm}(n_1, n_2, \dots, n_r)$ th root of unity. It may be observed that (3) is a special case of (5) when $G = C_N$. Equation (5) determines the character table M completely.

Given a sequence $x(j)$, $j = 0, 1, \dots, N-1$ one may define its GTT $X(k)$, $k = 0, 1, \dots, N-1$ via the character table M of an abelian group G of order N as

$$X(k) = \sum_{j=0}^{N-1} M(k, j) x(j), \quad 0 \leq k \leq N-1. \quad (6)$$

Further M being symmetric and orthogonal, M^* , the complex conjugate of M , is $N \cdot M^{-1}$ and the inverse transform may be defined as

$$x(j) = \frac{1}{N} \sum_{k=0}^{N-1} M^*(k, j) X(k), \quad 0 \leq j \leq N-1.$$

Relabeling $x(j)$ and $X(k)$ as x_{g_j} and X_{g_k} respectively and using (3), (6) becomes,

$$X_h = \sum_{g \in G} \phi_h(g) x_g, \quad h \in G \quad (7)$$

For a permutation α of the elements of G , (7) gives

$$X_h = \sum_{g \in G} \phi_h(g) x_{\alpha^{-1}g} = \sum_{g \in G} \phi_h(\alpha g) x_g, \quad (8)$$

where \bar{X} is the transform of the sequence $x_{\alpha^{-1}g}$. Kanetkar and Wagh (1977) have shown that if $\alpha \in A(G)$, the automorphism group of G , then \bar{X} is merely a shuffled version of X , i.e.,

$$\bar{X}_h = X_{\mu h}, \quad h \in G, \quad (9)$$

where μ is a permutation of the group elements.

In this paper, it is shown that $\mu \in A(G)$ and can therefore be described by a matrix S_μ transforming the basis of G . The relationship between S_μ and matrix S_α describing $\alpha \in A(G)$ is found out. Finally, all the permutations to which the transform is invariant are found out.

2. A COMPLETE SOLUTION TO THE PERMUTATION PROBLEM OF THE GTT

It is first shown that $\mu \in A(G)$. Combining (7), (8) and (9), which hold good for all the x sequences

$$\phi_{\mu h}(g) = \phi_h(\alpha g), \quad \forall g, \quad h \in G \quad (10)$$

Thus,

$$\begin{aligned}\phi_{\mu(h_1+h_2)}(g) &= \phi_{h_1+h_2}(\alpha g) \\ &= \phi_{h_1}(\alpha g) \cdot \phi_{h_2}(\alpha g) \\ &= \phi_{\mu h_1}(g) \cdot \phi_{\mu h_2}(g) = \phi_{\mu h_1 + \mu h_2}(g)\end{aligned}\quad (11)$$

Since (11) is true for all $g \in G$,

$$\mu(h_1 + h_2) = \mu h_1 + \mu h_2,$$

which shows that μ is a homomorphism. Moreover, as μ is a permutation, it is one-one. Thus $\mu \in A(G)$ and can be described by a $r \times r$ matrix S_μ which transforms the basis of $G \simeq C_{n_1} \times C_{n_2} \times C_{n_3} \times \cdots \times C_{n_r}$ as (Kanetkar and Wagh, 1977)

$$\mu g_k = g_{k'} \Leftrightarrow \langle\langle k' \rangle\rangle = \langle\langle k \rangle\rangle S_\mu. \quad (12)$$

Since $\alpha \in A(G)$, it can also be described by a matrix S_α as

$$\alpha g_j = g_{j'} \Leftrightarrow \langle\langle j' \rangle\rangle = \langle\langle j \rangle\rangle S_\alpha \quad (13)$$

Equations (5), (10), (12), and (13) then give

$$\langle\langle k \rangle\rangle D S_\alpha^t \langle\langle j \rangle\rangle^t = \langle\langle k \rangle\rangle S_\mu D \langle\langle j \rangle\rangle^t \quad (14)$$

Since (14) is true for all $\langle\langle k \rangle\rangle$ and $\langle\langle j \rangle\rangle$,

$$D S_\alpha^t = S_\mu D.$$

Matrix S_μ may therefore be obtained from S_α as

$$\begin{aligned}S_\mu(i, j) &= S_\alpha(j, i) d_{ii}/d_{jj} \\ &= S_\alpha(j, i) n_j/n_i, \quad 1 \leq i, j \leq r\end{aligned}\quad (15)$$

It is easy to show that the elements of S_μ obtained through (15) are indeed integers. Firstly, it is shown by Kanetkar and Wagh (1977) that to find S_α , G must be expressed as $C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$ where n_1, n_2, \dots, n_r are powers of primes. Consider the image of a_j under the automorphism α , $\alpha a_j = g_u$. Then from (13),

$$\langle\langle u \rangle\rangle = (0, 0, 0, 1, 0, \dots, 0) S_\alpha$$

where only j th component of the vector on the right hand side is nonzero. Thus

$$\langle\langle u \rangle\rangle = (S_\alpha(j, 1), S_\alpha(j, 2), \dots, S_\alpha(j, r))$$

and from (1),

$$g_u = S_\alpha(j, 1)a_1 + S_\alpha(j, 2)a_2 + \cdots + S_\alpha(j, r)a_r \quad (16)$$

But since α is an automorphism of G , order of g_u is equal to the order of a_j , i.e., n_j . Therefore, the order of each of the terms $S_\alpha(j, i)a_i$ must divide n_j . But the order of $S_\alpha(j, i)a_i$ also divides the order of a_i , i.e. n_i , and therefore if $\gcd(n_i, n_j) = 1$, $S_\alpha(j, i) = 0$ giving from (15) $S_\mu(i, j) = 0$.

On the other hand if $n_i \mid n_j$, $S_\mu(i, j)$ of (15) is obviously an integer and if $n_j \mid n_i$, the order of $a_i S_\alpha(j, i)$ is $n_i / \gcd(n_i, S_\alpha(j, i))$ giving

$$\frac{n_i}{\gcd(n_i, S_\alpha(j, i))} \mid n_j \quad \text{or} \quad \frac{n_i}{n_j} \mid S_\alpha(j, i)$$

again showing that $S_\mu(i, j)$ in (15) is an integer. Finally, recall from (8) and (9) that a permutation α^{-1} of the x components described by $S_{\alpha^{-1}}$ results in a permutation μ of the X components described by S_μ of (15).

Some special cases of (15) are worth investigating. Consider an elementary abelian group $C_p \times C_p \times \cdots \times C_p$ which is the underlying group of a GWT. In this case, $n_j = n_i$, $1 \leq i, j \leq r$ and therefore S_μ is the transpose of the inverse of $S_{\alpha^{-1}}$ in mod p field, i.e.,

$$S_\mu = ((S_{\alpha^{-1}})^{-1})^t.$$

This result is already known (Karpovsky, 1976, Theorem 1.4.5).

The permutation which corresponds to the automorphism α^{-1} , when applied to the signal components will result in an identical permutation of the transform components if $\mu = \alpha^{-1}$. The transform, in this case is said to be invariant to the permutation α^{-1} .

In the case of a DFT, which is a GTT over a cyclic group C_N , $S_{\alpha^{-1}} = [c]$ where $\gcd(c, N) = 1$. Then $S_\mu = [c^{-1} \bmod N]$. Thus the transform is invariant to a permutation which correspond to an automorphism $S_{\alpha^{-1}} = [c]$ iff $c^2 = 1 \bmod N$. The number of such automorphisms can be easily found out. Let n be the number of prime divisors of N . Then the group $A(G)$ is a direct product of t cyclic groups of even order where (Schenkman, 1965, Theorem III.2.m)

$$t = \begin{cases} n - 1 & \text{if } 2 \mid N \text{ but } 4 \nmid N \\ n & \text{if } N \text{ is odd or } 4 \mid N \text{ but } 8 \nmid N \\ n + 1 & \text{if } 8 \mid N \end{cases}$$

The number of elements of $A(G)$ of order two, i.e., the number of permutations to which the transform is invariant, is then equal to 2^t .

It is also possible to show that if all of n_1, n_2, \dots, n_r are relative primes in pairs then the number of permutations to which the GTT is invariant is the product

of the number of such permutations of the individual cyclic groups. In this case the automorphism matrix $S_{\alpha^{-1}}$ has the form

$$S_{\alpha^{-1}}(i, j) = 0 \quad \text{if } i \neq j$$

and $S_{\alpha^{-1}}(i, i) = c_i$ where $\gcd(c_i, n_i) = 1$. Equation (15) then gives

$$S_{\mu}(i, j) = 0 \quad \text{if } i \neq j$$

and

$$S_{\mu}(i, i) = c_i^{-1} \bmod n_i, \quad 1 \leq i \leq r.$$

Thus, for $S_{\mu} = S_{\alpha^{-1}}$, $c_i^2 = 1 \bmod n_i$, $i = 1, 2, \dots, r$, which gives the number of permutations to which the GTT is invariant.

In the case of a more complicated transform kernel $F_3 \otimes F_2 \otimes F_2$, it may be shown that the automorphisms matrix $S_{\alpha^{-1}}$ is one of the following twelve matrices:

$$\begin{aligned} R_1 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, & R_2 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, & R_3 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \\ R_4 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, & R_5 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, & R_6 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \\ R_7 &= \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, & R_8 &= \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, & R_9 &= \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \\ R_{10} &= \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, & R_{11} &= \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, & R_{12} &= \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \end{aligned}$$

It is easy to verify that (15) gives the corresponding permutation S_{μ} in the transform domain as

$S_{\alpha^{-1}}$	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}	R_{11}	R_{12}
S_{μ}	R_1	R_3	R_2	R_4	R_6	R_5	R_7	R_9	R_8	R_{10}	R_{12}	R_{11}

Thus this GTT is invariant to the permutations described by the matrices R_1 , R_4 , R_7 and R_{10} .

3. TRANSFORMS OF SIGNALS WHICH ARE CONSTANT OVER ORBITS

In this section the transforms of signals with a certain kind of redundancy are investigated. Consider the partitioning of group elements into what are known as orbits. Two group elements g_1, g_2 are in the same orbit T if $\exists \alpha \in A(G)$; s.t. $\alpha g_1 = g_2$. One can then prove the following theorem:

THEOREM 1. *If the signal is constant over each of the orbit, then so is the transform.*

Proof. It was shown in section 2 that if the signal components are permuted according to any $\alpha^{-1} \in A(G)$ then the transform components also permute according to some $\mu \in A(G)$. But if the signal components are constant over orbits, then the signal is invariant to α^{-1} , and the transform is also invariant to $\mu \in A(G)$. As α runs over $A(G)$, μ runs over $A(G)$. Thus transform is constant over each orbit. Q.E.D.

In the case of groups that one generally comes across, it is simple to determine the orbits. A cyclic group C_N (which is the underlying group of the Fourier transform of order N) has orbits defined by:

$$T_0 = \{0\} \quad \text{and} \quad T_d = \{(dq)a \mid \langle a \rangle = G, \gcd(q, N) = 1\}$$

where d is a divisor of N (including 1). Thus in the case of C_N , there are $s + 1$ orbits, where s is the number of divisors of N . For example, in the case of C_{12} the orbits are

$$\begin{aligned} T_0 &= \{0\}, \\ T_1 &= \{a, 5a, 7a, 11a\}, \\ T_2 &= \{2a, 10a\}, \\ T_3 &= \{3a, 9a\}, \\ T_4 &= \{4a, 8a\} \end{aligned}$$

and

$$T_6 = \{6a\}$$

where a is the generator of the group.

Recalling from (1) the labelling of the sequence elements by the group elements, theorem 1 can be applied to a sequence which satisfies

$$\begin{aligned} x(1) &= x(5) = x(7) = x(11), \\ x(2) &= x(10), \\ x(3) &= x(9) \end{aligned}$$

and

$$x(4) = x(8)$$

to give in the transform domain,

$$X(1) = X(5) = X(7) = X(11),$$

$$X(2) = X(10),$$

$$X(3) = X(9)$$

and

$$X(4) = X(8)$$

In the case of a transform with underlying group $C_{n_1} \times C_{n_2} \dots \times C_{n_r}$ where n_1, n_2, \dots, n_r are relative prime in pairs, the orbits may be obtained from the direct product of the orbits of individual cyclic groups. For example, the orbits of C_3 are: $\{0\}, \{b, 2b\}$ and those of C_4 are: $\{0\}, \{a, 3a\}$ and $\{2a\}$ where $\langle b \rangle = C_3$ and $\langle a \rangle = C_4$. Therefore, the orbits of $C_3 \times C_4$ are: $\{0\}, \{a, 3a\}, \{2a\}, \{b, 2b\}, \{b + a, b + 3a, 2b + a, 2b + 3a\}$ and $\{b + 2a, 2b + 2a\}$. Note that these orbits are similar to those in the case of C_{12} as the two groups are isomorphic. Again, recalling the association of the sequence and the group elements, theorem 1 is applicable to sequences which satisfy $x(1) = x(3), x(4) = x(8), x(5) = x(7), x(9) = x(11)$ and $x(6) = x(10)$.

In the case of the GWT with the underlying elementary abelian group $C_p \times C_p \dots \times C_p$ (n times), there are only two orbits $\{0\}, \{g \in G \mid g \neq 0\}$ because this group is a vector space over the field of integers mod p . Theorem 1 then states that if all the sequence components except perhaps the 0th component are identical then all components of the transform except the 0th, are also identical.

The analysis of this section holds good even if the orbits are defined with respect to a subgroup A_1 of the automorphism group $A(G)$. In order to partition the transform domain into orbits one may define

$$A_2 = \{\mu \in A(G) \mid \text{for some } \alpha \in A_1, \phi_h(\alpha g) = \phi_{\mu h}(g), \forall g, h \in G\}.$$

A_2 is also a subgroup of $A(G)$ because $1 \in A_2$ and $\mu_1, \mu_2 \in A_2$ imply the existence of $\alpha_1, \alpha_2 \in A_1$ such that $\forall g, h \in G$,

$$\phi_h(\alpha_1 g) = \phi_{\mu_1 h}(g)$$

and

$$\phi_h(\alpha_2 g) = \phi_{\mu_2 h}(g),$$

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

$$\phi_h(\alpha_2 \alpha_1 g) = \phi_{\mu_2 h}(\alpha_1 g) = \phi_{\mu_1 \mu_2 h}(g).$$

As $\alpha_2 \alpha_1 \in A_1, \mu_1 \mu_2 \in A_2$, which shows that A_2 is closed under multiplication and being finite, is a subgroup of G . The orbits in the transform domain then are defined with respect to A_2 consisting of μ 's related to α 's of A_1 through (10).

This yields a finer partitioning of the signal and transform domains. For example for $G = C_{12} = \langle a \rangle$ and $A(G) = \{\alpha_1, \alpha_5, \alpha_7, \alpha_{11}\}$ where $\alpha_i a = ia$, one may choose $A_1 = \{\alpha_1, \alpha_5\}$. Then $A_2 = \{\alpha_1, \alpha_5\}$ and the orbits in both signal and transform domain are: $\{0\}$, $\{a, 5a\}$, $\{2a, 10a\}$, $\{3a\}$, $\{4a, 8a\}$, $\{6a\}$, $\{7a, 11a\}$ and $\{9a\}$.

4. CONCLUSIONS

It was shown by Kanetkar and Wagh (1977) while discussing the properties of the GTT's that a permutation in the signal domain which results in a permutation in the transform domain of a GTT may be described by an automorphism of the underlying group. In this paper, this result is extended by showing that this permutation in the transform domain can also be described as an automorphism of the group.

The correspondence between the two automorphisms is established which brings out the relation between these permutations of the signal and transform samples. It also allows one to find out the permutations to which the GTT is invariant, i.e. the permutation matrices which commute with the transform kernel.

Finally, it is shown that the concept of orbits in group theory can be usefully employed in digital signal processing to compute the transforms of the signals which are constant over certain sets of samples.

It is obvious that the results obtained in this paper are valid even if the underlying field is not the complex field but is a finite field in which both e th primitive root of unity and N^{-1} exist, where N is the order of the group and e is the exponent, i.e. the maximum order of a group element in G .

RECEIVED: December 2, 1977; REVISED: September 13, 1978

REFERENCES

- G. APPLE AND P. WINTZ (1970), Calculation of Fourier transforms on finite abelian groups, *IEEE Trans. Inform. Theory* IT-16, 233-234.
- A. T. BUTSON (1962), Generalized Hadamard matrices, *Proc. Amer. Math. Soc.* 13, 894-898.
- S. H. CHANG AND J. THOMAS (1972), On ordering of a class of generalized Walsh transforms, in "Applications of Walsh Functions: 1972, Proc.," pp. 337-343.
- S. V. KANETKAR AND M. D. WAGH (1977), Group character tables in discrete transform theory, communicated.
- M. G. KARPOVSKY (1976), "Finite Orthogonal Series in the Design of Digital Devices," Wiley, New York.
- E. SCHENKMAN (1965), "Group Theory," Van Nostrand, Princeton, N. J.