Fast Fourier Transforms on Finite Non-Abelian Groups

M. G. KARPOVSKY

***Abstract*—Recent works [1]–[9] were devoted to the properties and application of Fourier transforms over finite Abelian groups and fast Fourier transforms for calculation of the corresponding spectra. In this correspondence we describe Fourier transforms on finite non-Abelian groups and appropriate algorithms of fast Fourier transforms.**

***Index Terms*—Fast Fourier transforms and fast inverse Fourier transforms on finite non-Abelian groups, fast Hadamard–Walsh and fast Hadamard–Chrestenson transforms, Fourier transforms on finite non-Abelian groups, irreducible representations of groups.**

I. Introduction

Several authors have considered the properties and applications of Walsh and Chrestenson functions and their generalizations on arbitrary finite Abelian groups, and fast Fourier transforms (FFT) for calculation of the corresponding spectra [1]–[9]. In this correspondence we describe Fourier transforms on finite non-Abelian groups and appropriate FFT. The main difference between these transforms and the Hadamard–Walsh or Hadamard–Chrestenson transforms is that instead of Walsh or Chrestenson functions, which are group characters, irreducible representations of the appropriate groups must be used.

The transforms discussed in this correspondence are generalizations of the Hadamard–Walsh and Hadamard–Chrestenson transforms. They may be used in the problems involving functions that depend on permutations, on matrices over finite field, etc. As examples of such problems we note an assignment problem for automata, a traveling-salesman problem, a problem of pattern recognition for two-colored pictures, which may be considered as a problem of realization of a function defined on the group of binary matrices, a problem of interconnecting telephone lines [10], and a problem of synthesis of rearrangeable switching networks whose outputs depend on the permutation of input terminals [11], [12]. Another example of a problem of this type is a problem of approximation of the linear system by the system whose input and output are functions defined on group. In the case of the dyadic groups this problem was solved in [9]. The replacement of the dyadic group by some non-Abelian group may result in considerable simplification of the approximating system. This problem will be considered in [13].

Manuscript received September 3, 1975; revised April 23, 1976, and August 20, 1976.

The author is with the Computer Science Division, Department of Mathematics, Tel-Aviv University, Ramat Aviv, Tel-Aviv, Israel.

II. Fourier Transforms on Finite Non-Abelian Groups

Let G be a (non-Abelian) group of order g; V be a vector space of dimension d over the field C of complex numbers; and $GL(V)$ be the group of all nonsingular $d \times d$ matrices with elements in C. A representation of G with representation space V is a homomorphism $R{:}G \to GL(V)$; that is, $R(xy) = R(x) \cdot R(y)$, $x,y \in G$. A representation R is irreducible if there are no nontrivial subspaces of V which are mapped into themselves by all matrices $R(x)$, $x \in G$. Two representations R_ω and R_q are equivalent if there exists a $Q \in GL(V)$ such that $R_\omega(x) = Q^{-1}R_q(x)Q$ for all $x \in G$. Every representation is equivalent to some unitary representation (i.e., a representation R such that $R(x)$ is a unitary matrix for all $x \in G$ [14, p. 3]). Methods for constructing the representations of a given group are considered in detail in algebraic literature (see, e.g., [14]). The number of sets of irreducible unitary representations for some specific groups may be found in [14, pp. 47–54]. Let $R_\omega^{(s,t)}(x)$ denote the (s,t)th element of $R_\omega(x)$; then we have the orthogonality relations [14, pp. 11–14]

$$g^{-1} \sum_{x \in G} R_\omega^{(s,t)}(x)\overline{R_q^{(p,n)}(x)} = d_\omega^{-1} \cdot \delta_{\omega q} \cdot \delta_{sp} \cdot \delta_{tn} \tag{1}$$

$$\sum_{R_\omega \in R(G)} d_\omega \operatorname{Tr} R_\omega(x) = g \cdot \delta_{x,e} \tag{2}$$

where d_ω is the dimension of R_ω; $R(G)$ is the set of all irreducible unitary representations of G; e is the identity of G; δ is the Kronecker symbol; and Tr A trace of A. Thus the direct and inverse Fourier transforms on G may be defined as follows. If $f{:}G \to C$, then

$$S_f(\omega) = d_\omega \cdot g^{-1} \sum_{x \in G} f(x)R_\omega(x^{-1}) \tag{3}$$

$$f(x) = \sum_{R_\omega \in R(G)} \operatorname{Tr}\,(S_f(\omega) \cdot R_\omega(x)) \tag{4}$$

where x^{-1} is the inverse of x in G. The verification that (3) and (4) define an invertible transform may be done by (2) and (3) as follows:

$$\sum_{R_\omega \in R(G)} \operatorname{Tr}\,((S_f(\omega)R_\omega(x))$$

$$= g^{-1} \sum_{R_\omega \in R(G)} d_\omega \operatorname{Tr}\left(\sum_{y \in G} f(y)R_\omega(y^{-1}x)\right)$$

$$= g^{-1} \sum_{y \in G} f(y) \sum_{R_\omega \in R(G)} d_\omega \operatorname{Tr} R_\omega(y^{-1}x) = f(x).$$

The Hadamard–Walsh and Hadamard–Chrestenson transforms are special cases of (3) and (4) obtained when G is the additive group of binary or $p$ary ($p > 2$) vectors (in this case, group is Abelian and so representations have dimension 1 and coincide with the Walsh or Chrestenson functions).

We now describe the main properties of the transforms (3) and (4).

1) *Linearity:* For all $\alpha_1,\alpha_2 \in C, f_1,f_2: G \to C$

$$S_{\alpha_1 f_1(x)+\alpha_2 f_2(x)}(\omega) = \alpha_1 S_{f_1(x)}(\omega) + \alpha_2 S_{f_2(x)}(\omega). \tag{5}$$

2) *(Right) Group Translation:* For all $\tau \in G$

$$S_{f(x\tau)}(\omega) = R_\omega(\tau) \cdot S_{f(x)}(\omega). \tag{6}$$

3) *Group Convolution:* Let $f_1,f_2: G \to C$ and

$$(f_1 * f_2)(\tau) = \sum_{x \in G} f_1(x) \cdot f_2(\tau x^{-1}). \tag{7}$$

Then

$$d_\omega \cdot g^{-1} \cdot S_{(f_1 * f_2)(\tau)}(\omega) = S_{f_1(x)}(\omega) \cdot S_{f_2(x)}(\omega). \tag{8}$$

Properties 1)–3) follow immediately from (3) and (4).

4) *Parseval's Theorem:* For all $f_1,f_2: G \to C$

$$\sum_{x \in G} f_1(x) \cdot \overline{f_2(x)} = g \cdot \sum_{R_\omega \in R(G)} d_\omega^{-1} \cdot \mathrm{Tr}\,(S_{f_1(x)}(\omega) \cdot S^*_{f_2(x)}(\omega)) \tag{9}$$

where $S^*_{f_2(x)}(\omega)$ is the conjugate transposed to $S_{f_2(x)}(\omega)$ with elements $S^{*(p,q)}_{f_2(x)}(\omega) = \overline{S^{(q,p)}_{f_2(x)}}(\omega)$ ($S^{(q,p)}_{f_2(x)}(\omega)$ is the (q,p)th element of $S_{f_2(x)}(\omega)$). The proof of Parseval's theorem may be done by (2), (3), and unitarity of $R_\omega(x)$

$$\begin{aligned} & g \sum_{R_\omega \in R(G)} d_\omega^{-1} \mathrm{Tr}\,(S_{f_1}(\omega) S^*_{f_2}(\omega)) \\ & = g^{-1} \sum_{R_\omega \in R(G)} d_\omega \,\mathrm{Tr}\left(\left(\sum_{x_1 \in G} f_1(x_1) R_\omega(x_1^{-1})\right)\right. \\ & \left. \cdot \left(\sum_{x_2 \in G} \overline{f_2(x_2)} R^*_\omega(x_2^{-1})\right)\right) = g^{-1} \sum_{x_1,x_2 \in G} f_1(x_1)\overline{f_2(x_2)} \\ & \cdot \sum_{R_\omega \in R(G)} d_\omega \,\mathrm{Tr}\,(x_1^{-1}x_2) = \sum_{x \in G} f_1(x)\overline{f_2(x)}. \end{aligned}$$

5) *Correlation Functions and the Wiener–Khinchin Theorem:* Let $f_1,f_2: G \to C$, $\tau \in G$ and

$$B_{f_1,f_2}(\tau) = \sum_{x \in G} f_1(x) f_2(\overline{x\tau^{-1}}). \tag{10}$$

Then B_{f_1,f_2} may be called the cross-correlation function on G; if $f_1 = f_2$, it is called the autocorrelation function. B_{f_1,f_2} is a generalization of the logical or dyadic correlation functions described, for example, in [3], [6], [7], [9].

Let F_G be the direct and F_G^{-1} the inverse Fourier transforms on G, and F^*_G the transform such that $(F^*_G(f))(\omega) = S^*_f(\omega)$. Then

$$B_{f_1,f_2} = g \cdot F_G^{-1}(d_\omega^{-1} \cdot F_G(f_1) \cdot F^*_G(f_2)). \tag{11}$$

The proof of (11) follows from unitarity of $R_\omega(x)$, (3), and (8).

Formulas (5)–(11) generalize the analogous properties of the Hadamard–Walsh or Hadamard–Chrestenson transforms [2], [3], [6]–[8].

III. Fast Fourier Transform (FFT) for Finite Non-Abelian Groups

Calculation of the spectrum $S_f(\omega)$ by (3) involves $g \cdot d_\omega^2$ multiplications for a given ω (not counting normalization by $d_\omega g^{-1}$). Since [14, p. 43] $\Sigma_{R_\omega \in R(G)} d_\omega^2 = g$, the number of multiplications required to calculate S_f for all ω is g^2. We describe another method for the calculation of S_f, a generalization of the fast Hadamard–Walsh or fast Hadamard–Chrestenson transforms [4], [5]. Let G be a direct product of groups G_j ($j = 0, \cdots, m-1$), $G = \Pi_{j=0}^{m-1} G_j$. Then 1) if $x \in G$, then $x = (x_0, \cdots, x_{m-1}), x_j \in G$; 2) $g = \Pi_{j=0}^{m-1} g_j$, where g_j is the order of G_j; 3) if $R_\omega \in R(G)$, then [14, p. 27]

$$R_\omega(x) = R_\omega(x_0, \cdots, x_{m-1}) = \bigotimes_{j=0}^{m-1} R_{\omega_j}(x_j), \qquad R_{\omega_j} \in R(G_j) \tag{12}$$

where $R(G_j)$ is the set of all irreducible unitary representations of G_j and $\otimes$ denotes the Kronecker product of matrices. Thus, for every $R_\omega \in R(G)$, we denote $\omega = (\omega_0, \cdots, \omega_{m-1})$. By (3) and (12)

$$\begin{aligned} S_f(\omega) &= S_f(\omega_0, \cdots, \omega_{m-1}) \\ &= d_\omega g^{-1} \sum_{x_0,\cdots,x_{m-1}} f(x_0, \cdots, x_{m-1}) \cdot \bigotimes_{j=0}^{m-1} R_{\omega_j}(x_j^{-1}) \\ &= d_\omega g^{-1} \sum_{x_{m-1}} \left(\cdots \left(\sum_{x_1} \left(\sum_{x_0} f(x_0, \cdots, x_{m-1}) \right.\right.\right. \\ &\left.\left.\left. \cdot R_{\omega_0}(x_0^{-1})\right) \otimes R_{\omega_1}(x_1^{-1})\right) \cdots\right) \otimes R_{\omega_{m-1}}(x_{m-1}^{-1}). \end{aligned} \tag{13}$$

Let

$$f_0(x_0, \cdots, x_{m-1}) = f(x_0, \cdots, x_{m-1}) \tag{14}$$

$$f_1(\omega_0, x_1, \cdots, x_{m-1}) = \sum_{x_0} f_0(x_0, \cdots, x_{m-1}) R_{\omega_0}(x_0^{-1}) \tag{15}$$

$$\cdots$$

$$\begin{aligned} & f_l(\omega_0, \cdots, \omega_{l-1}, x_l, \cdots, x_{m-1}) \\ & = \sum_{x_{l-1}} f_{l-1}(\omega_0, \cdots, \omega_{l-2}, x_{l-1}, \cdots, x_{m-1}) \\ & \otimes R_{\omega_{l-1}}(x_{l-1}^{-1}) (l = 1, \cdots, m). \end{aligned} \tag{16}$$

Then by (13)–(16)

$$S_f(\omega_0, \cdots, \omega_{m-1}) = d_\omega g^{-1} f_m(\omega_0, \cdots, \omega_{m-1}). \tag{17}$$

Formulas (14)–(17) define the FFT on a (non-Abelian) group G. Let us estimate the complexity of the FFT (14)–(17). If $\omega_0, \cdots, \omega_{l-1}, x_l, \cdots, x_{m-1}$ are fixed, then $f_{l-1}(\omega_0, \cdots, \omega_{l-2}, x_{l-1}, \cdots, x_{m-1})$ and $R_{\omega_{l-1}}(x_{l-1}^{-1})$ are matrices of dimensions $\Pi_{j=0}^{l-2} d_{\omega_j} \times \Pi_{j=0}^{l-2} d_{\omega_j}$ and $d_{\omega_{l-1}} \times d_{\omega_{l-1}}$, respectively. Since $\Sigma_{R_{\omega_j} \in R(G_j)} d_{\omega_j}^2 = g_j$, the number of the memory cells for storage f_l is $\bigcap_{j=0}^{m-1} g_j = g$ and the number of multiplications needed to calculate f_l by (16) is $g_{l-1} \cdot g$. Thus the number of multiplications for the FFT (14)–(17) is $g \cdot \Sigma_{j=0}^{m-1} g_j$ and generally less than g^2.

IV. Fast Inverse Fourier Transform (FIFT) for Finite Non-Abelian Groups

For non-Abelian groups the spectrum S_f is a matrix-valued function and the inverse transform (4) does not have the same form as the direct transform (3). Calculation of f by (4) involves g^2 multiplications. We describe another method for the calculation of f which involves only $g \cdot \Sigma_{j=0}^{m-1} g_j$ multiplications.

Let $G = \Pi_{j=0}^{m-1} G_j$. Then, by (12)

$$R_\omega^{(\alpha,\beta)}(x) = \prod_{j=0}^{m-1} R_{\omega_j}(\alpha_j,\beta_j)(x_j), \qquad \alpha_j,\beta_j \in \{1, \cdots, d_{\omega_j}\}. \tag{18}$$

Denote $\alpha = (\alpha_0, \cdots, \alpha_{m-1})$, $\beta = (\beta_0, \cdots, \beta_{m-1})$. Then by (4) and (18)

$$\begin{aligned} f(x) = f(x_0, \cdots, x_{m-1}) &= \sum_{R_\omega \in R(G)} \sum_{\alpha,\beta} S_f^{(\beta,\alpha)}(\omega) \cdot R_\omega^{(\alpha,\beta)}(x) \\ &= \sum_{R_{\omega_0},\cdots,R_{\omega_{m-1}}} \sum_{\substack{\alpha_0,\cdots,\alpha_{m-1} \\ \beta_0,\cdots,\beta_{m-1}}} S_f^{((\beta_0,\cdots,\beta_{m-1}),(\alpha_0,\cdots,\alpha_{m-1}))} \\ & \cdot (\omega_0, \cdots, \omega_{m-1}) \prod_{j=0}^{m-1} R_{\omega_j}^{(\alpha_j,\beta_j)}(x_j). \end{aligned} \tag{19}$$

Let analogously (14)–(16)

$$\hat{f}_0^{((\beta_0,\cdots,\beta_{m-1}),(\alpha_0,\cdots,\alpha_{m-1}))}(\omega_0,\cdots,\omega_{m-1}) = S_f^{((\beta_0,\cdots,\beta_{m-1}),(\alpha_0,\cdots,\alpha_{m-1}))}(\omega_0,\cdots,\omega_{m-1}) \quad (20)$$

$$\hat{f}_1^{((\beta_1,\cdots,\beta_{m-1}),(\alpha_1,\cdots,\alpha_{m-1}))}(x_0,\omega_1,\cdots,\omega_{m-1}) = \sum_{R_{\omega 0}} \sum_{\alpha_0,\beta_0} \hat{f}_0^{((\beta_0,\cdots,\beta_{m-1}),(\alpha_0,\cdots,\alpha_{m-1}))}(\omega_0,\cdots,\omega_{m-1})\, R_{\omega 0}^{(\alpha_0,\beta_0)}(x_0) \quad (21)$$

$$\cdots$$

$$\hat{f}_l^{((\beta_l,\cdots,m-1),(\alpha_l,\cdots,\alpha_{m-1}))}(x_0,\cdots,x_{l-1},\omega_l,\cdots,\omega_{m-1})) = \sum_{R_{\omega l-1}} \sum_{\alpha_{l-1},\beta_{l-1}} \hat{f}_{l-1}^{((\beta_{l-1},\cdots,\beta_{m-1}),(\alpha_{l-1},\cdots,\alpha_{m-1}))} \cdot (x_0,\cdots,x_{l-2},\omega_{l-1},\cdots,\omega_{m-1})\, R_{\omega l-1}^{(\alpha_{l-1},\beta_{l-1})}(x_{l-1}), \quad (l=1,\cdots,m). \quad (22)$$

Then by (19)–(22)

$$f(x_0,\cdots,x_{m-1}) = \hat{f}_m(x_0,\cdots,x_{m-1}). \quad (23)$$

Formulas (20)–(23) defined the fast inverse Fourier transform (FIFT) on G.

The number of memory cells for storage $\hat{f}_l$ is g, and calculation of f_l by (22) involves $g_{l-1} \cdot g$ multiplications. The total number of multiplications for the FIFT is $g \cdot \Sigma_{j=0}^{m-1} g_j$; i.e., the same as for FFT.

V. Conclusions

We have considered the properties of Fourier transforms on finite non-Abelian groups, FFT, and FIFT algorithms for such groups and estimations for the complexity of these algorithms have been presented.

Acknowledgment

The author wishes to thank Dr. B. Moroz for useful discussions.

References

[1] M. G. Karpovsky and E. S. Moskalev, "Realization of a system of logical functions by means of an expansion in orthogonal series," *Automat. Remote Contr.*, vol. 28, pp. 1921–1932, 1967, (Translated from: *Automat. Telemekh.*, no. 12, pp. 119–129, 1967).

[2] B. L. N. Kennet, "A note on the finite Walsh transform," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 489–491, July 1970.

[3] M. G. Karpovsky and E. S. Moskalev, "Utilization of autocorrelation characteristics for realization of systems of logical functions," *Automat. Remote Contr.*, vol. 31, pp. 243–250, 1970 (Translated from: *Automat. Telemekh.*, no. 2, pp. 83–90, 1970).

[4] K. C. Andrews and K. L. Caspari, "A generalized technique for spectral analysis," *IEEE Trans. Comput.*, vol. C-19, pp. 16–25, Jan. 1970.

[5] G. Apple and P. Wintz, "Calculation of Fourier transforms on finite Abelian groups," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 233–236, Mar. 1970.

[6] R. J. Lechner, "Harmonic analysis of switching functions," in *Recent Development in Switching Theory*, A. Makhopadhyay, Ed. New York: Academic, 1971.

[7] M. G. Karpovsky and E. S. Moskalev, *Spectral Methods for Analysis and Synthesis of Digital Devices* (Monograph), "Energia" (in Russian), 1973.

[8] M. G. Karpovsky, *Finite Orthogonal Series in the Design of Digital Devices* (Monograph). New York: Wiley, and IUP Press, Jerusalem, 1976.

[9] J. Pearl, "Optimal dyadic models of time invariant systems," *IEEE Trans. Comput.*, vol. C-24, June 1975.

[10] V. E. Benes, "Optimal rearrangeable multistage connecting networks," *Bell Syst. Tech. J.*, vol. 43, pt. 2, pp. 1641–1656, July 1964.

[11] D. C. Opferman and N. T. Tsao-Wu, "On class of rearrangeable switching networks," *Bell Syst. Tech. J.*, vol. 50, pp. 1579–1618, May 1971.

[12] K. Harada, "Sequential permutation networks," *IEEE Trans. Comput.*, vol. C-21, pp. 472–479, May 1972.

[13] M. G. Karpovsky and E. A. Trakhtenberg, "Some optimization problems for generalized convolution systems over finite groups," *Informat. Contr.*, to be published.

[14] E. Hewitt and K. Ross, *Abstracts Harmonic Analysis* (Monograph), vol. II. Berlin: Springer, 1963.