Reprinted from INFORMATION AND CONTROL
All Rights Reserved by Academic Press, New York and London

Vol. 34, No. 3, July 1977
Printed in Belgium

Some Optimization Problems for Convolution Systems over Finite Groups

M. G. KARPOVSKY

Department of Mathematics, Tel Aviv University, Tel Aviv, Israel

AND

E. A. TRACHTENBERG

Department of Computer Science, Technion—Israel Institute of Technology, Haifa, Israel

We define and study many-dimensional linear invariant discrete systems over finite groups. We consider the problem of optimum synthesis of such systems computing a given input/output pair. The optimum solution (or estimates for them) are obtained on the basis of two very simply computed criteria. Conditions are studied for the existence of an idempotent impulse function of a linear system over a group, computing a given input/output pair. The best approximation is found for many-dimensional linear invariant systems, defined on a finite interval of discrete time by systems over the given finite group.

1. SYSTEMS OVER FINITE GROUPS

We consider linear systems with m inputs and k outputs, constructed as follows. Let G be an arbitrary abstract finite group with elements 0, 1,..., $g-1$ (0 is the identity of the group). $\bar{G} = g$ is the order of G (throughout, $\bar{A}$ denotes the cardinality of the set A). Let $L_{a,b}$ be the set of all functions defined on G with values in a set of $(a \times b)$ matrices $M_{a,b}$ over the field of complex numbers C.

DEFINITION 1. A linear invariant discrete system S over a finite group G is defined as a quadruple $S = (L_{m,1}; L_{k,1}; h; \circledast)$, where the operation $\circledast$ is defined for any $u \in L_{m,1}$, $y \in L_{k,1}$ as follows:

$$y(t) = (h \circledast u)(t) = \sum_{\zeta \in G} h(\zeta^{-1} \circ t)\, u(\zeta). \tag{1}$$

i.e., $\circledast$ is the operation of group convolution of two matrix-valued functions; $h \in L_{k,m}$, $u \in L_{m,1}$; $y \in L_{k,1}$; ζ^{-1} is the inverse of ζ in G and $\circ$ denotes the group operation.

ISSN 0019-9958

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:

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

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

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

In other words, S consists of the set $L_{m,1}$ of mappings $G \to M_{m,1}$ (the set of input signals), the set $L_{k,1}$ of mappings $G \to M_{k,1}$ (the set of output signals) and a mapping h from $L_{m,1}$ to $L_{k,1}$ (impulse function). If (1) is true for a given system S, $u \in L_{m,1}$ and $y \in L_{k,1}$, we say that system S computes the input/output pair (u, y).

Equation (1) may be realized either as a network or as a computer program. One possible network realization, computing $y(t)$ by a sequential procedure, is illustrated in Fig. 1.

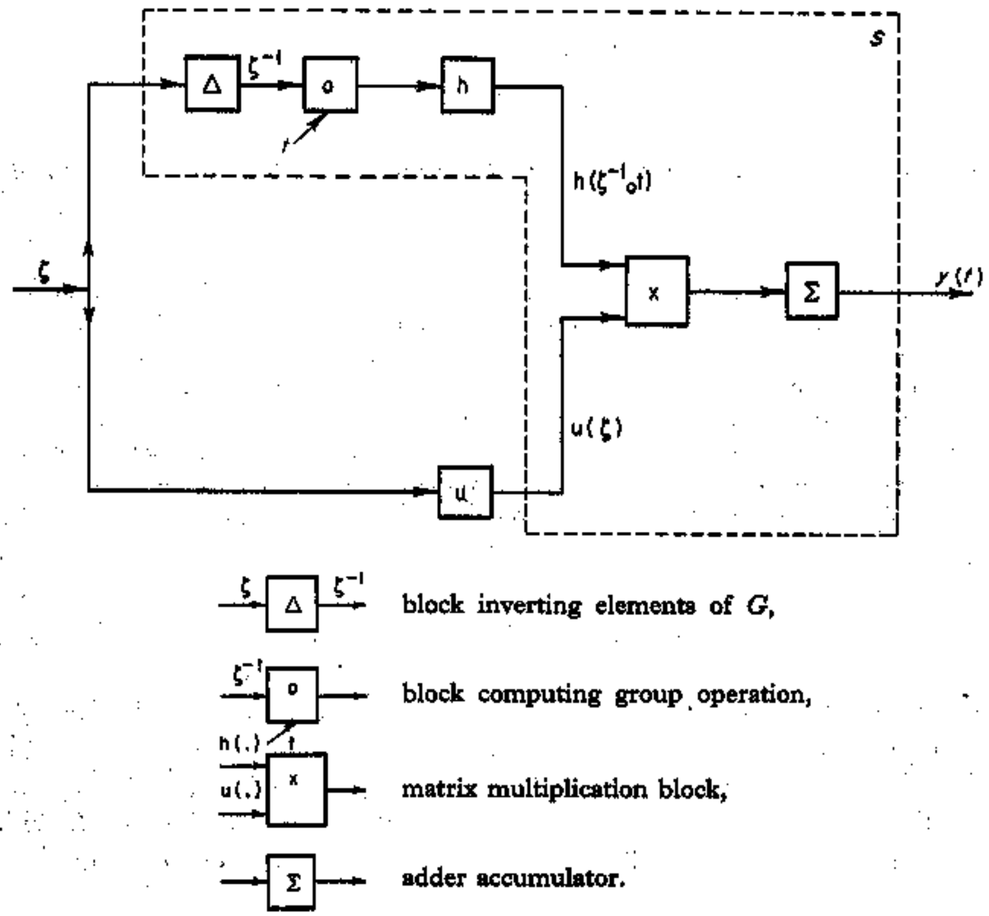


FIGURE 1

For each $t \in G$, all elements $\zeta = 0, 1, \ldots, g-1$ of G are fed to the input of the network, and blocks h and u compute $h(\zeta^{-1} \circ t)$ and $u(\zeta)$, respectively. After the right-hand member of (1) has accumulated in the adder Σ, the output produces the signal $y(t)$, $t = 0, 1, \ldots, g-1$.

From the standpoint of systems theory, S is a linear input/output system whose input and output signals are defined over an arbitrary finite group G. When G is the dyadic group (the group of binary vectors relative to componentwise

addition mod 2), such systems are considered by Pichler (1971), Pearl (1975). Systems over locally compact Abelian groups were studied by Falb and Friedman (1970). The systems considered by Tsypkin, Faradjev (1966), were defined over groups in such a way that the input and output were functions from the infinite cyclic group of integers into $GF(2^q)$ the (Galois field of 2^q elements).

Systems over a finite group G may be regarded as a special class of digital filters or a special class of systems with variable structure (Nailor, 1965), operating in discrete time and defined on a finite interval $[0, g-1]$, such that at each instant of time t the impulse function is readjusted according to the rule $h(t, \zeta) = h(\zeta^{-1} \circ t)$.

Some problems connected with the analysis of impulse matrices of systems over arbitrary (not necessarily commutative) finite groups were considered by Karpovsky and Trachtenberg (1975).

Systems over finite groups to compute a given input/output transformation may be very useful, particularly when the input and output have a natural interpretation as functions on a group as is often the case for Abelian groups, in switching theory, the theory of error-correcting codes, image processing, etc. (Hartmuth, 1970; Karpovsky and Moskalev, 1970; Lechner, 1971; Karpovsky, 1976.).

As examples of such problems for non-Abelian groups we note 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 (Benes, 1964) and a problem of synthesis of rearrangeable switching networks, whose outputs depend on the permutation of input terminals (Harada, 1973). Another example of a problem of this type is a problem of approximation of the linear time-invariant system by the system whose input and output are functions defined on group. In the case of the dyadic groups this problem was solved by Pearl (1975). The replacement of the dyadic group by some non-Abelian group may result in considerable simplification of the approximating system. This problem will be solved in Section 5.

Simulation of Eq. (1) by a computer program greatly expands the possible applications of systems over finite groups.

By letting the elements of an abstract finite group play the role of time, one can not only extend the results and methods of linear systems theory to systems over groups but also prove some new results for such systems.

For our investigation of systems over groups, we use the techniques of abstract harmonic analysis, which will play a role analogous to that of Fourier transform techniques for ordinary linear systems. This method is employed by Lechner (1971), Karpovsky (1976) as applied to problems in the analysis, synthesis, and optimization of devices whose input and output signals are functions on finite Abelian groups.

This paper comprises five sections. The next section presents some prere-

quisites from harmonic analysis on finite groups. Section 3 solves the problem of synthesis of optimum systems over groups computing a given input/output pair, for two easily computed optimality criteria. Section 4 is devoted to the synthesis of a special class of systems (systems with idempotent impulse function), which display significant advantages as regards the simplicity of their network or program realization.

In Section 5 we solve the problem of the best approximation to a given linear many-dimensional system operating on a finite interval of discrete time by a system on a finite group.

2. Preliminaries

Let $L_{1,1}$ denote the space of functions defined on an arbitrary finite (not necessarily commutative) group G with values in the field of complex numbers C. We use the elements of the nonequivalent irreducible unitary representations of G as a complete orthonormal basis for this space. Recall (Hewitt and Ross, 1963) that a representation of degree d in a linear space $V(\dim V = d)$ over C is defined as a homomorphism R: $G \to GL(V)$, where $GL(V)$ is the group of automorphisms of V. A representation R is said to be irreducible in V if V has no proper R-invariant subspaces, and unitary if $R(t)$ is a unitary matrix for every $t \in G$. Two representations R_1 and R_2 of the same degree are said to be equivalent if there exists an invertible matrix Q such that $QR_1(t)\,Q^{-1} = R_2(t)$ for every $t \in G$.

Let $R(G) = \{R_\omega\}$ denote the set of all nonequivalent irreducible unitary representations of G in the space $L_{1,1}$, indexed so that R_ω is of degree d_ω (Henceforth we write $\omega \in R(G)$ as an abbreviation for $R_\omega \in R(G)$.) $R(G)$ is the dual object of the group G. It is known (Hewitt and Ross, 1963) that

$$\sum_{\omega \in R(G)} d_\omega^2 = g. \tag{2}$$

Moreover, d_ω is a divisor of g for all $\omega \in R(G)$, and if G is not commutative, its dual object $R(G)$ contains at least one R_ω such that $d_\omega > 1$.

Let $R_\omega^{(i,k)}(\cdot)$ denote the (i, k)th element of the matrix $R_\omega(\cdot)$ $(1 \leqslant i, k \leqslant d_\omega)$. We recall the orthogonality relations for the components of the matrix functions of the dual object $R(G)$:

$$\frac{1}{g} \sum_{t \in G} d_\omega^{1/2} \overline{R_\omega^{(i,k)}(t)}\, d_\nu^{1/2} R_\nu^{(j,r)}(t) = \delta_{\omega\nu}\delta_{ij}\delta_{kr}\,. \tag{3}$$

$(\omega, \nu \in R(G);\ 1 \leqslant i, k \leqslant d_\omega;\ 1 \leqslant j, r \leqslant d_\nu$. The bar in (3) denotes complex conjugation; the expression on the right is a product of Kronecker symbols.)

The character χ_ω of the representation R_ω is defined as follows:

$$\chi_\omega(t) = \operatorname{trace} R_\omega(t). \tag{4}$$

The characters satisfy the following orthogonality relations (Hewitt and Ross, 1963):

$$\frac{1}{g} \sum_{t \in G} \overline{\chi_\omega(t)}\, \chi_\nu(t) = \delta_{\omega\nu}\,, \tag{5}$$

$$\frac{1}{g} \sum_{\omega \in R(G)} \overline{\chi_\omega(t)}\, \chi_\omega(\zeta) = \frac{\delta_{t\zeta}}{p_t}\,. \tag{6}$$

where p_t is the number of elements in the conjugate class of G, which contains t. (Recall that the number of conjugate classes of a group G is equal to the number of elements in the set $R(G)$.)

Methods for the construction of representations and characters of finite groups are described in the algebraic literature (see, e.g., Dornhoff, 1971).

Let $f \in L_{k,m}$, i.e., f: $G \to M_{k,m}$. It follows from (3) and from the Peter–Weyl theorem (Hewitt and Ross, 1963), that the Fourier and inverse Fourier transforms in $L_{k,m}$ may be defined as follows:

$$\hat{f}(\omega) = (\hat{f}^{(n,l)}(\omega)) = \Big(\frac{d_\omega}{g} \sum_{\zeta \in G} f^{(n,l)}(\zeta)\, R_\omega(\zeta^{-1})\Big), \tag{7}$$

$$f(\zeta) = (f^{(n,l)}(\zeta)) = \Big(\sum_{\omega \in R(G)} \operatorname{trace}(\hat{f}^{(n,l)}(\omega)\, R_\omega(\zeta))\Big), \tag{8}$$

$$(\hat{f}(\omega) \in M_{kd_\omega, md_\omega};\qquad 1 \leqslant n \leqslant k;\ 1 \leqslant l \leqslant m).$$

We now list some fundamental properties of Fourier transforms over a given finite group G.

(i) *Linearity.* If $f_1, f_2 \in L_{k,m}$ and $c_1, c_2 \in C$, then

$$\widehat{(c_1 f_1 + c_2 f_2)}(\omega) = c_1 \hat{f}_1(\omega) + c_2 \hat{f}_2(\omega). \tag{9}$$

(ii) *Left translation.* If $f_1(t \circ \zeta) = f_2(\zeta)$ for all $\zeta \in G$; $f_1, f_2 \in L_{k,m}$ (where t is a fixed element of G), then

$$\hat{f}_1^{(n,l)}(\omega) = \hat{f}_2^{(n,l)}(\omega)\, R_\omega(t^{-1});\qquad (1 \leqslant n \leqslant k,\ 1 \leqslant l \leqslant m). \tag{10}$$

(iii) *Group convolution.* If $f \in L_{k,m}$, $\varphi \in L_{k,\nu}$, and $\psi \in L_{\nu,m}$, then

$$f(t) = (\varphi \circledast \psi)(t) = \sum_{\zeta \in G} \varphi(\zeta^{-1} \circ t)\, \psi(\zeta),$$

iff

$$\hat{f}(\omega) = \frac{g}{d_\omega}\, \hat{\varphi}(\omega)\, \hat{\psi}(\omega). \tag{11}$$

(iv) *Plancherel Theorem.* If $f_1, f_2 \in L_{k,m}$, then

$$\frac{1}{g}\sum_{t\in G}\operatorname{trace}(f_1^*(t)\,f_2(t)) = \sum_{\omega\in R(G)}\frac{1}{d_\omega}\operatorname{trace}(\hat{f}_1^*(\omega)\,\hat{f}_2(\omega)), \tag{12}$$

where $f_1^*(\cdot)$ is the adjoint matrix (transposed complex-conjugate) of $f_1(\cdot)$.

(v) *Wiener–Khinchin Theorem.* Let $f_1 \in L_{k,m}$, $f_2 \in L_{k,\nu}$, $\tau \in G$ and

$$B_{f_1,f_2}(\tau) = \sum_{\zeta\in G} f_1^*(\tau^{-1}\circ\zeta)\,f_2(\zeta); \qquad B_{f_1,f_2}\in L_{m,\nu}. \tag{13}$$

Then $B_{f_1,f_2}(\cdot)$ 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 logical or dyadic correlation functions described, for example, by Karpovsky, Moskalev (1970), and Lechner (1971).

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

$$B_{f_1,f_2}(\tau) = g(F_G^{-1}\{d_\omega^{-1}F_G{}^*\{f_1\}\,F_G\{f_2\}\})(\tau). \tag{14}$$

The proof of Wiener–Khinchin Theorem (14) follows from (7), unitary of $R_\omega(\cdot)$ and (11).

3. Synthesis of Optimal Systems over a Group for a Given Input/Output Pair

Consider the kmg-dimensional linear space $L_{k,m}$ over C. The norm $\|\cdot\|_2$ in $L_{k,m}$ (Hilbert–Schmidt norm) is defined by

$$\|f\|_2 = \Big(\sum_{t\in G}\operatorname{trace}(f^*(t)\,f(t))\Big)^{1/2} \tag{15}$$

(if $B \in M_{a,b}$, then $\|B\|_2 = (\operatorname{trace} B^*B)^{1/2}$).

Solutions of optimization problems for systems on groups relative to criteria based on the norm $\|\cdot\|_2$ are usually unique and fairly simple to find (see, e.g., Theorem 1); in some cases, however, such criteria do not faithfully represent the complexity of realization of the block diagram of system S (by complexity we mean, for example, the number of elementary units needed to realize the block diagram). We, therefore, define $\|f\|_0$ as a number of nonzero elements in all matrices $f(t)$ for all $t \in G$, $(0 \leqslant \|f\|_0 \leqslant kmg)$. (Note that $\|\cdot\|_0$ may be regarded as a generalization of the Hamming metric.)

Now, consider the original system S over the group G:

$$y(t) = (h \circledast u)(t), \quad (u \in L_{k,1};\ h \in L_{k,m};\ y \in L_{k,1}). \tag{16}$$

If Eq. (16) is solvable for h for a given pair (u, y), we consider the problem of finding $h_{21} \in H(u, y)$ and $h_{01} \in H(u, y)$ (where $H(u, y)$ is the set of solutions of Eq. (16)) minimizing $\|h\|_2$ and $\|h\|_0$, respectively.

If Eq. (16) is unsolvable, we let e_h denote the error function

$$e_h(t) = y(t) - (h \circledast u)(t), \tag{17}$$

and consider the problem of finding $h_{22} \in L_{k,m}$ and $h_{02} \in L_{k,m}$ minimizing $\|e_h\|_2$ and $\|e_h\|_0$.

THEOREM 1. *The impulse functions h_{21}, h_{22} of optimal systems over a given group G, computing a given pair (u, y), satisfy the condition*

$$\hat{h}_2(\omega) = \hat{h}_{21}(\omega) = \hat{h}_{22}(\omega) = \frac{d_\omega}{g}\,\hat{y}(\omega)\,\hat{u}^+(\omega), \qquad \forall\omega \in R(G) \tag{18}$$

$$(\hat{y}(\omega) \in M_{kd_\omega,d_\omega};\ \hat{u}^+(\omega) \in M_{d_\omega,md_\omega}),$$

where $\hat{u}^+(\omega)$ denotes the generalized Moore-Penrose inverse (Ben Israel and Greville, 1974) of $\hat{u}(\omega)$.

Proof. For any $h \in L_{k,m}$, it follows from the Plancherel Theorem (12) and from the group convolution theorem (11) that

$$(\|e_h\|_2)^2 = \sum_{\omega\in R(G)}\frac{g}{d_\omega}(\|\hat{e}_h(\omega)\|_2)^2 = \sum_{\omega\in R(G)}\frac{g}{d_\omega}\Big(\Big\|\hat{y}(\omega) - \frac{g}{d_\omega}\hat{h}(\omega)\,\hat{u}(\omega)\Big\|_2\Big)^2. \tag{19}$$

Consequently,

$$(\|e_h\|_2)^2 = (\|e_{h_2}\|_2)^2 = \min_{h\in L_{k,m}}\{(\|e_h\|_2)\}^2$$

iff

$$\|\hat{y}(\omega) - \frac{g}{d_\omega}\hat{h}_2(\omega)\,\hat{u}(\omega)\|_2 = \min_{\hat{h}(\omega)\in M_{kd_\omega,md_\omega}}\Big\{\Big\|\hat{y}(\omega) - \frac{g}{d_\omega}\hat{h}(\omega)\,\hat{u}(\omega)\Big\|_2\Big\}; \tag{20}$$

for all $\omega \in R(G)$.

Condition (18) now follows from (20) by the definition of the generalized Moore–Penrose inverse.

The following corollary of Theorem 1 sometimes facilitates the computation of $h_2 = h_{21} = h_{22}$.

COROLLARY. *If the matrices $\hat{u}^*(\omega)\,\hat{u}(\omega)$ are invertible for all $\omega \in T$, where T is some subset of $R(G)$, then*

$$\hat{h}_2(\omega) = \frac{d_\omega}{g}\,\hat{y}(\omega)(\hat{u}^*(\omega)\,\hat{u}(\omega))^{-1}\,\hat{u}^*(\omega); \tag{21}$$

for all $\omega \in T$.

Indeed, if $\hat{u}^*(\omega)\,\hat{u}(\omega)$ is invertible, then $\hat{u}^+(\omega) = (\hat{u}^*(\omega)\,\hat{u}(\omega))^{-1}\,\hat{u}^*(\omega)$.

Theorem 1 and Corollary together with (8) solve the problem of synthesis of optimal systems over a finite groups relative to criteria based on the norm $\|\cdot\|_2$.

The next theorem gives upper bounds for the optimal impulse functions h_{01} and h_{02} (optimal with respect to criteria based on $\|\cdot\|_0$).

THEOREM 2. *Let (u, y) be a given input/output pair, $u \in L_{m,1}$, $y \in L_{k,1}$.*

(i) *If Eq. (16) is solvable for the given pair (u, y), then*

$$\| h_{01} \|_0 \leqslant k \sum_{\omega \in R(G)} d_\omega \operatorname{rank} \hat{u}(\omega). \tag{22}$$

(ii) *If Eq. (16) is unsolvable for the given pair (u, y), then*

$$\| e_{h_{02}} \|_0 \leqslant kg - k \sum_{\omega \in R(G)} d_\omega \operatorname{rank} \hat{u}(\omega). \tag{23}$$

Proof. (i) Any solution h of Eq. (16) may be written as

$$h(t) = \varphi(t) + \sum_{i=1}^{p} c_i \psi^{(i)}(t), \tag{24}$$

where φ is a fixed particular solution of the equation, $\psi^{(i)}$ are linearly independent solutions of the homogeneous equation corresponding to (16) ($i = 1, 2, \ldots, p$). To determine p, we use (11) to write the homogeneous equation as

$$\hat{h}(\omega)\,\hat{u}(\omega) = \mathbb{0} \tag{25}$$

$$(\hat{h}(\omega) \in M_{kd_\omega, md_\omega}\,;\ \hat{u}(\omega) \in M_{md_\omega, d_\omega}).$$

In view of (2), there results from (25)

$$p = \sum_{\omega \in R(G)} kd_\omega(md_\omega - \operatorname{rank} \hat{u}(\omega)) = kmg - k \sum_{\omega \in R(G)} d_\omega \operatorname{rank} \hat{u}(\omega). \tag{26}$$

Consequently, the required relation (22) follows from the fact that the least number of elements in the values of $h(\cdot)$ that can be equated to zero (by suitable choice of the coefficients c_i) in system (24) is $kmg - k \sum_{\omega \in R(G)} d_\omega \operatorname{rank} \hat{u}(\omega)$.

(ii) The proof is analogous.

We now consider a special class of systems over a given group G, which admit simpler program and network realizations than in the general case.

Let $k = m$; let G_1 be a group of order k, and

$$h^{(i,j)}(\zeta) = h^{(j^{-1}i)}(\zeta), \qquad (\zeta \in G;\ 1 \leqslant i, j \leqslant k), \tag{27}$$

where $i, j \in G_1$ and the group operation in G_1 is written as multiplication. Then

the methods outlined in the proofs of Theorems 1 and 2 may be used to synthesize systems of this class, by successive application of Fourier transforms on the groups G and G_1.

Given a function $f: G \to M_{k,1}$, we let $\tilde{f}$ denote the result of successive applications of the Fourier transforms on G and G_1. We then have $\tilde{f}(\omega, \theta) = \hat{f}(\theta, \omega)$, $(\omega \in R(G), \theta \in R(G_1))$.

A double application of Theorem 1 now shows that the optimal impulse functions h satisfying (27) (i.e., those giving the best $\| h \|_2$ or $\| e_h \|_2$) are defined by the condition

$$\tilde{h}_2(\omega, \theta) = \tilde{h}_2(\omega, \theta) = \tilde{h}_{22}(\omega, \theta) = \frac{d_\omega}{g} \frac{d_\theta}{k} \tilde{y}(\omega, \theta)\,\tilde{u}^+(\omega, \theta),$$

$$(\tilde{y}(\omega, \theta), \tilde{u}(\omega, \theta) \in M_{d_\omega d_\theta, d_\omega d_\theta}\,;\ \omega \in R(G),\ \theta \in R(G_1)). \tag{28}$$

Similarly, two applications of Theorem 2 show that the optimal (giving the best $\| h \|_0$ or $\| e_h \|_0$) impulse functions h of the form (27) satisfy the conditions

$$\| h_{01} \|_0 \leqslant \sum_{\omega \in R(G)} \sum_{\theta \in R(G_1)} d_\omega d_\theta \operatorname{rank} \tilde{u}(\omega, \theta), \tag{29}$$

$$\| e_{h_{02}} \|_0 \leqslant kg - \sum_{\omega \in R(G)} \sum_{\theta \in R(G_1)} d_\omega d_\theta \operatorname{rank} \tilde{u}(\omega, \theta). \tag{30}$$

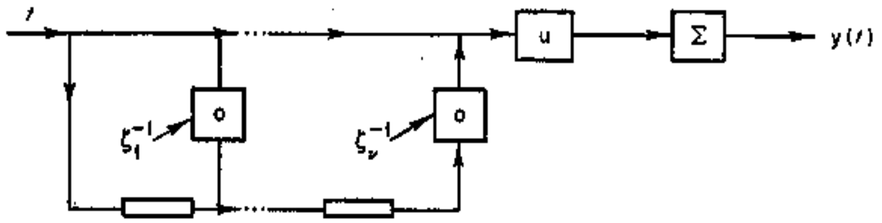
To conclude this section, we note that if we put $u(\zeta) = \zeta$ in (16) for all $\zeta \in G (k = m = 1)$, the synthesis methods considered in this and the following sections make it possible to design devices computing functions on groups (see Figs. 1 and 2) using only linear systems over groups.

4. Synthesis of Systems with Idempotent Impulse Function for a Given Input/Output Pair (u, y) $(k = m = 1)$

Suppose that, given an input $u: G \to C$ and an output signal $y: G \to C$ $(k = m = 1)$, there exists an idempotent impulse function $h: G \to C$, i.e., $h^2(\zeta) = h(\zeta)$ for all $\zeta \in G$, which satisfies (1). Then the block diagram for realization of system S assumes the very simple form shown in Fig. 2.

Here $t, \zeta_1^{-1}, \ldots, \zeta_\nu^{-1} \in G$ and $h(\zeta) = 1$ iff $\zeta \in \{0, \zeta_1, \ldots, \zeta_\nu\}$.

It was shown by Karpovsky (1977) for Abelian groups that if a given input/output pair (u, y) has an idempotent impulse function h, there is a simple and effective method for detecting errors for the appropriate system S. In this section, therefore, we consider necessary and sufficient conditions for the existence of idempotent impulse functions realizing a given input/output pair (u, y).



Here $t, \zeta_1^{-1}, \ldots, \zeta_\nu^{-1} \in G$ and $h(\zeta_i) = 1$ where $i = 1, 2, \ldots, \nu$.

FIGURE 2

THEOREM 3. *If a given input/output pair (u, y) is realizable by a system S with idempotent function h, then there exists an integer k_h $(1 \leqslant k_h \leqslant g)$ such that*

$$0 \leqslant \epsilon(u, y) \leqslant \frac{k_h}{g}\left(1 - \frac{k_h}{g}\right) \leqslant \tfrac{1}{4}. \tag{31}$$

Moreover, if $\hat{u}(1) \neq 0$, then $k_h = \hat{y}(1)/\hat{u}(1)$. Where

$$\epsilon(u, y) = \sum_{\substack{\omega \in R(G) \\ \omega \neq 1}} \left(\prod_{i=1}^{d_\omega} \Delta_i(\omega)\right)^{1/d_\omega}; \tag{32}$$

$$\Delta_i(\omega) = \frac{d_\omega^2}{g^2} \frac{|\alpha_i(\omega)|^2}{|\beta_i(\omega)|^2}, \qquad \beta_i(\omega) \neq 0;$$

$$= 0, \qquad \textit{otherwise.} \tag{33}$$

and $\alpha_i(\omega)$, $\beta_i(\omega)$ are the eigenvalues of the matrices $\hat{y}(\omega)$, $\hat{u}(\omega)$, respectively $(1 \leqslant i \leqslant d_\omega)$. (Note that $R_1(\zeta) = 1$ for all $\zeta \in G$.)

Proof. Using (11), we write (1) for system S in an equivalent form:

$$\hat{h}(\omega)\,\hat{u}(\omega) = \frac{d_\omega}{g}\,\hat{y}(\omega), \tag{34}$$

$(\hat{u}(\omega), \hat{y}(\omega), \hat{h}(\omega) \in M_{d_\omega, d_\omega})$.

Set $k_h = \sum_{t \in G} h(t)$; then by (7)

$$\hat{h}(1) = \frac{1}{g}\sum_{t \in G} h(t)\, R_1(t^{-1}) = \frac{1}{g}\sum_{t \in G} h(t) = \frac{1}{g}\,k_h. \tag{35}$$

It follows from (35) and (34) that $k_h = \hat{y}(1)/\hat{u}(1)$ if $\hat{u}(1) \neq 0$.

It remains to show that k_h satisfies inequality (31). Since $h(\cdot)$ is idempotent, it

follows from (35) by the Plancherel theorem (12) (for $k = m = 1$) and from the fact that $\hat{h}(1) = 1/g \sum_{t \in G} h(t) > 0$ that

$$\hat{h}(1) = \frac{k_h}{g} = \frac{1}{g}\sum_{t \in G} h(t)\, h(t) = \frac{1}{g}\sum_{\omega \in R(G)} \frac{g}{d_\omega}\,\mathrm{trace}(\hat{h}^*(\omega)\,\hat{h}(\omega))$$

$$= \frac{k_h^2}{g^2} + \sum_{\substack{\omega \in R(G) \\ \omega \neq 1}} \frac{1}{d_\omega}\,\mathrm{trace}(\hat{h}^*(\omega)\,\hat{h}(\omega)). \tag{36}$$

The expression following the summation symbol on the right of (36) is the sum of squares of the singular values of the matrices $\hat{h}(\omega)$. Thus, inequality (31) will follow from (36) if we replace the arithmetic mean of the squared singular values of $\hat{h}(\omega)$ by their geometric mean and use the Weyl inequality (Amir–Moez, 1956), together with (33) and (32). Note that the right-hand part of (31) is true for any k_h.

With a view to simplifying the search for an idempotent impulse function, given u and y, we impose a restriction on the class H_{1d} of idempotent functions, stipulating that $h \in H_{1d}$ if there exists a normal subgroup G_h of G such that $h(\zeta) = 1$, iff $\zeta \in G_h$.

Now, consider the problem of finding all idempotent impulse functions $h \in H_{1d}$ realizing a given pair (u, y) on the assumption that $y = 0$; i.e., we are considering the following equation in h:

$$(h \circledast u)(t) = 0 \tag{37}$$

for all $t \in G$.

Let $P \subseteq R(G)$, and denote

$$P^\perp = \bigcap_{\omega \in P} R_\omega^{\perp} = \bigcap_{\omega \in P} \mathrm{kern}\, R_\omega. \tag{38}$$

$(R_\omega^{\perp} = \mathrm{kern}\, R_\omega = \{t \mid R_\omega(t) = E_{d_\omega}\})$, $E_{d_\omega} - (d_\omega \times d_\omega)$ identity matrix.

Then $P^\perp$ annihilator of P in G and it is obviously a normal subgroup of G.

DEFINITION 2. A subset $P \subseteq R(G)$ is said to be closed (notation: $P = [P]$), if, for any $R_\omega \notin P$ $(R_\omega \in R(G))$, we have $R_\omega^{\perp} \not\supset P^\perp$.

Note that if the representations in $R(G)$ are indexed so that $R_1(t) = 1$ for any $t \in G$, then $R_1 \in [P]$ for any $[P]$ in $R(G)$.

It can be shown (Hewitt and Ross, 1963), that for every normal subgroup G_h of G there is a unique $[P_h] \subseteq R(G)$ such that $[P_h]^\perp = G_h$. Moreover, any $[P]$ isomorphic to the dual object $R(G/[P]^\perp)$ of the factor group $G/[P]^\perp$, and the elements of the set $[P]$ are constant on the cosets of G modulo $[P]^\perp$; in addition,

$$\sum_{\omega \in [P]} d_\omega^2 = \overline{G/[P]^\perp}. \tag{39}$$

In other words, if K is any coset of G modulo $[P]^{\perp}$, then the relation between $R_\omega \in [P]$ and $\Gamma_\omega \in R(G/[P]^{\perp})$ is given by the formula:

$$R_\omega(t) = \Gamma_\omega(K), \qquad t \in K. \tag{40}$$

LEMMA 1. *For any $f: G \to M_{k,m}$ and any $[P] \subseteq R(G)$,*

$$1/\overline{\overline{[P]^{\perp}}} \sum_{\zeta \in [P]^{\perp}} f(\zeta) = \sum_{\omega \in [P]} \operatorname{Trace} \hat{f}(\omega), \tag{41}$$

$$(f(\zeta) \in M_{k,m}\,;\ \zeta \in G;\ \hat{f}(\omega) \in M_{kd_\omega, md_\omega}\,;\ \omega \in R(G)).$$

In this formula,

$$\operatorname{Trace} \hat{f}(\omega) = (\operatorname{trace} \hat{f}^{(n,l)}(\omega)), \qquad (1 \leqslant n \leqslant k,\ 1 \leqslant l \leqslant m). \tag{42}$$

Proof. In view of (42), it follows from (7) that

$$\operatorname{Trace} \hat{f}(\omega) = \frac{d_\omega}{g} \sum_{\zeta \in [P]^{\perp}} f(\zeta)\, \chi_\omega(\zeta^{-1}) + \frac{d_\omega}{g} \sum_{\zeta \notin [P]^{\perp}} f(\zeta)\, \chi_\omega(\zeta^{-1}). \tag{43}$$

We now sum (43) over $\omega \in [P]$. Then by the definitions of $[P]$ and $[P]^{\perp}$ and by (40),

$$\sum_{\zeta \in [P]^{\perp}} f(\zeta) \sum_{\omega \in [P]} \frac{d_\omega}{g}\, \chi_\omega(\zeta^{-1}) = \sum_{\zeta \in [P]^{\perp}} f(\zeta)\, \frac{1}{g} \sum_{\omega \in [P]} d_\omega^2$$

$$= \frac{1}{g}\, \overline{\overline{G/[P]^{\perp}}} \sum_{\zeta \in [P]^{\perp}} f(\zeta) = 1/\overline{\overline{[P]^{\perp}}} \sum_{\zeta \in [P]^{\perp}} f(\zeta). \tag{44}$$

On the other hand, by (40), (6), and the fact that $d_\omega = \chi_\omega(0)$:

$$\sum_{\zeta \notin [P]^{\perp}} f(\zeta) \sum_{\omega \in [P]} \frac{d_\omega}{g}\, \chi_\omega(\zeta^{-1}) = \frac{1}{g} \sum_{\zeta \notin [P]^{\perp}} f(\zeta) \sum_{\omega \in [P]} \chi_\omega(0)\, \overline{\chi_\omega(\zeta)} = 0. \tag{45}$$

Thus (41) follows from (43) and (45).

Lemma 1 may be considered an analog of the Poisson summation formula for matrix-valued functions on finite (not necessarily commutative) groups. It also illustrates the relationship between the closed subsets $[P]$ of the dual object $R(G)$ and the normal subgroups of G.

Our problem of finding solutions $h \in H_{1\mathrm{d}}$ of Eq. (37) is solved by the following theorem. Denote

$$\Omega_u = \{\omega \mid \hat{u}(\omega) = \mathbb{O}\} \cup \{1\}. \tag{46}$$

THEOREM 4. *Given an input $u: G \to C$, (such that $\sum_{t \in G} u(t) = 0$). There exists a one-to-one correspondence between the sets $[P]$ such that*

$$[P] \subseteq \Omega_u\,, \tag{47}$$

and the solutions $h \in H_{1\mathrm{d}}$ of Eq. (37), defined by

$$[P] \leftrightarrow h_{[P]}(\zeta) = 1, \qquad \zeta \in [P]^{\perp},$$

$$= 0, \qquad \zeta \notin [P]^{\perp}. \tag{48}$$

Proof. If $[P]$ satisfies (47), we set

$$\hat{h}(\omega) = \hat{h}_{[P]}(\omega) = \frac{\overline{\overline{[P]^{\perp}}}}{g}\, d_\omega E_{d_\omega}\,, \qquad \omega \in [P],$$

$$= \mathbb{O}, \qquad \omega \notin [P], \tag{49}$$

where E_{d_ω} the identity $(d_\omega \times d_\omega)$-matrix.

Then

$$\hat{h}(\omega)\, \hat{u}(\omega) = \mathbb{O}. \tag{50}$$

Now, using (49), one shows by direct computation that $h \in H_{1\mathrm{d}}$ and $G_h = [P]^{\perp}$.

Conversely, $h_{[P]} \in H_{1\mathrm{d}}$, then, by (7) and Definition 2,

$$\hat{h}_{[P]}(\omega) = \frac{g_h}{g}\, d_\omega E_{d_\omega}\,, \qquad \omega \in [P],$$

$$= \mathbb{O}, \qquad \omega \notin [P], \tag{51}$$

where $g_h = \bar{G}_h$ and $[P]$ is such that $G_h = [P]^{\perp}$.

It remains to show that P satisfies (47), but this follows from (50) and the definition of $H_{1\mathrm{d}}$, since $h_{[P]}$ is a solution of Eq. (37).

We now consider the analogous problem of finding $h \in H_{1\mathrm{d}}$ realizing a given pair (u, y), i.e., we are concerned with the nonhomogeneous equation ($k = m = 1$)

$$(h \circledast u)(t) = y(t). \tag{52}$$

Let $y(t)$ be expressible as

$$y(t) = (\rho \circledast f)(t) + d, \tag{53}$$

where $\rho \in H_{1\mathrm{d}}$ is an unknown function, $f: G \to C$ some known function, and d an unknown constant. In other words, instead of (52) we are studying the following equation:

$$(h \circledast u)(t) = (\rho \circledast f)(t) + d. \tag{54}$$

Let $\gamma \neq 0$, and denote

$$\Omega_{u,f}(\gamma) = \{\omega \mid \gamma \hat{u}(\omega) = \hat{f}(\omega)\}; \qquad \Omega_f = \{\omega \mid \hat{f}(\omega) = \mathbb{O}\} \cup \{1\}. \tag{55}$$

THEOREM 5. *For any u, $f: G \to C$, there exists h, $\rho \in H_{1\mathrm{d}}$ and a constant d*

such that h, u, ρ, f, d satisfy Eq. (54). Moreover, if there is $\gamma \neq 0$ such that the sets

$$\Omega_u \cup \Omega_{u,f}(\gamma) \quad \text{and} \quad \Omega_f \cup \Omega_{u,f}(\gamma) \tag{56}$$

contains sets $[P_u]$ and $[P_\delta]$, respectively, such that

$$\alpha([P_\delta]) = \gamma\alpha([P_u]), \quad \text{where} \quad \alpha[P] = \sum_{\omega\in[P]} d_\omega^2 \tag{57}$$

and

$$[P_u] \cap \Omega_{u,f}(\gamma) = [P_\delta] \cap \Omega_{u,f}(\gamma), \tag{58}$$

then

$$\sum_{\zeta\in G} h(\zeta) + \sum_{\zeta\in G} \rho(\zeta) = \frac{g}{\alpha([P_u])}\left(1 + \frac{1}{\gamma}\right). \tag{59}$$

Proof. Set

$$\begin{aligned} \hat{h}(\omega) &= \frac{\overline{[P_u]^\perp}}{g} d_\omega E_{d_\omega}, && \omega \in [P_u], \\ &= \mathbb{0}, && \omega \notin [P_u]. \end{aligned} \tag{60}$$

$$\begin{aligned} \hat{\rho}(\omega) &= \frac{\overline{[P_\delta]^\perp}}{g} d_\omega E_{d_\omega}, && \omega \in [P_\delta], \\ &= \mathbb{0}, && \omega \notin [P_\delta]. \end{aligned} \tag{61}$$

$$d = \frac{\overline{[P_u]^\perp}}{g} \sum_{t\in G} u(t) - \frac{\overline{[P_\delta]^\perp}}{g} \sum_{t\in G} f(t). \tag{62}$$

For any $\omega \in R(G)$, we have

$$\hat{h}(\omega)\,\hat{u}(\omega) = \hat{\rho}(\omega)\,\hat{f}(\omega) + \frac{d_\omega}{g}\,\hat{d}(\omega), \tag{63}$$

where $\hat{d}(\omega) = \mathbb{0}$ if $\omega \neq 1$ and $\hat{d}(1) = d/g$. Then it follows from Eqs. (60), (61) that for every $\zeta \in G$ $h(\zeta) \in \{0, 1\}$, $\rho(\zeta) \in \{0, 1\}$, and (59) follows from (60), (61), and (57) by Lemma 1.

Note that sets $[P_u]$ and $[P_\delta]$ satisfying (57) and (58) exist for any u and f (for example, $[P_u] = [P_\delta] = \{1\}$, $\gamma = 1$), and so there is always a solution h, ρ, d of Eq. (54) defined by (60), (61), and (62).

Note that sufficient condition of Theorem 4 follows from this theorem if we set $f = 0$, $d = 0$.

The advantage of idempotent systems over ordinary systems over a group lies in the maximal simplicity of the appropriate block diagram (see, e.g., Fig. 2). In addition (Karpovsky, 1977), in cases when there exist idempotent impulse functions there are simple and effective methods for detecting errors in system S. Note that the impulse functions h_{21} and h_{01} (see Section 3) coincide, if the corresponding optimum problems are to be solved in the class of idempotent functions. In that case the following corollary shows how to determine the optimal idempotent impulse function $h_{\text{opt}} \in H_{1d}$ (the case of Eq. (37)), realizing a pair (u, y) with $y = 0$.

COROLLARY. *Under the assumptions of Theorem 4, denote*

$$\alpha([P]_{\text{opt}}) = \max_{[P]\subseteq\Omega_u} \{\alpha([P])\}. \tag{64}$$

Then

$$\begin{aligned} h_{\text{opt}}(\zeta) &= 1, && \zeta \in [P]^\perp_{\text{opt}}; \\ &= 0, && \zeta \notin [P]^\perp_{\text{opt}}. \end{aligned} \tag{65}$$

Indeed, formula (65) follows from Lemma 1, Theorem 4, and (64).

5. Approximation of a Linear Invariant System by a System on a Given Finite Group G

Consider a given many-dimensional linear time-invariant system with zero initial state, m inputs, and k outputs, defined on a finite discrete time interval $[0, g-1]$ (where g is an integer):

$$x(t) = (w * u)(t) = \sum_{\zeta=0}^{g-1} w(t-\zeta)\,u(\zeta), \qquad (0 \leqslant t \leqslant g-1). \tag{66}$$

The symbol $*$ stands for convolution of the impulse function w: $[0, g-1] \to M_{k,m}$ and the input u: $[0, g-1] \to M_{m,1}$ of system (66); x: $[0, g-1] \to M_{k,1}$ is the output of system (66).

Now let G be some fixed (not necessarily commutative) group of order g. Treating the input u: $[0, g-1] \to M_{m,1}$ as a function defined on G, i.e., u: $G \to M_{m,1}$, we consider the system S on the group G:

$$y(t) = (h \circledast u)(t) = \sum_{\zeta\in G} h(\zeta^{-1} \circ t)\,u(\zeta). \tag{67}$$

We wish to find the best approximation of system (66) by a system (67) over the group G. This problem is solved by Pearl (1975) for a dyadic group G of order $g = 2^n$, with $k = m = 1$, by a method which is also applicable for systems S over arbitrary finite Abelian groups. In this section we generalize the method to many-dimensional systems ($k \geqslant 1$, $m \geqslant 1$) and on the case that the group is not commutative. It is noteworthy that the use of noncommutative groups may

considerably increase the accuracy of the approximation for a given system (66), or simplify the impulse function of the system over the group.

Given u: $[0, g-1] \to M_{m,1}$ and x: $[0, g-1] \to M_{k,1}$, we define column vectors $\mathbf{U}, \mathbf{Z}$ as follows:

$$\begin{aligned} \mathbf{U} &= (u_1(0)\, u_1(1) \cdots u_1(g-1) \cdots u_m(0)\, u_m(1) \cdots u_m(g-1))^T; \\ \mathbf{Z} &= (x_1(0) \cdots x_1(g-1) \cdots x_k(0) \cdots x_k(g-1))^T, \end{aligned} \tag{68}$$

i.e., $\mathbf{U} \in M_{mg,1}$ and $\mathbf{Z} \in M_{kg,1}$. Then the action of the impulse function w in system (66) is equivalent to

$$\mathbf{Z} = W\mathbf{U}. \tag{69}$$

Here W is a $(kg \times mg)$ matrix, whose elements are arranged in blocks $W^{(t,\zeta)}(0 \leqslant t, \zeta \leqslant g-1)$ of the form $(W^{(t,\zeta)})^{(n,l)} = w^{(n,l)}(t-\zeta)$, $(1 \leqslant n \leqslant k, 1 \leqslant l \leqslant m)$. The matrix $W = (w^{(n,l)}(t-\zeta))$ is called the impulse matrix of system (66). W is a Toeplitz block matrix, generated by the function w: $[0, g-1] \to M_{k,m}$. In similar fashion, we write Eq. (67) of the system S over the group G in matrix notation:

$$\mathbf{Y} = H\mathbf{U}. \tag{70}$$

The impulse matrix H of system S belongs to the set of circulant matrices defined as follows:

$$\begin{aligned} \mathrm{Cir}(G, k, m) = \{H \mid H = (H^{(t,\zeta)}),\ & \\ H^{(t,\zeta)} = (h^{(n,l)} = (h^{(n,l)}(\zeta^{-1} \circ t)),\ & \\ 1 \leqslant n \leqslant k,\ 1 \leqslant l \leqslant m,\ 0 \leqslant t, \zeta \leqslant g-1\} & \end{aligned} \tag{71}$$

Some properties of circulant matrices were considered by Karpovsky and Trachtenberg (1975).

We now state the best-approximation problem as follows.

Given a system (66) with impulse matrix W, and a group G, let $\{S\}$ be the class of all systems S over G with input $u \in L_{m,1}$. It is required to find a system S_{opt} in $\{S\}$ with an impulse matrix $H_{\mathrm{opt}} \in \mathrm{Cir}(G, k, m)$ such that

$$\| W - H_{\mathrm{opt}} \|_2 = \min_{H \in \mathrm{Cir}(G,k,m)} \{\| W - H \|_2\}. \tag{72}$$

(The choice of the Hilbert–Schmidt norm $\| \cdot \|_2$ as a measure of the "closeness" of two linear systems is justified by, e.g., Nailor (1965) and Pearl (1975)).

Let $\overline{\overline{R(G)}} = \sigma$ (i.e., the dual object $R(G)$ of G contains σ elements $R_1, \ldots, R_\sigma$).

We write $R(G)$ as a matrix $\tilde{R}$ of blocks $\tilde{R}_\omega$ $(1 \leqslant \omega \leqslant \sigma)$, where

$$\tilde{R}_\omega = \left(\frac{d_\omega}{g}\right)^{1/2} \begin{pmatrix} R_\omega^{(1,1)}(0) & R_\omega^{(1,2)}(0) & \cdots & R_\omega^{(1,d_\omega)}(0) & R_\omega^{(2,1)}(0) \\ \vdots & \vdots & & \vdots & \vdots \\ R_\omega^{(1,1)}(g-1) & R_\omega^{(1,2)}(g-1) & \cdots & R_\omega^{(1,d_\omega)}(g-1) & R_\omega^{(2,1)}(g-1) \\ \cdots & R_\omega^{(2,d_\omega)}(0) & \cdots & R_\omega^{(d_\omega,1)}(0) & \cdots \quad R_\omega^{(d_\omega,d_\omega)}(0) \\ & \vdots & & \vdots & \\ & R_\omega^{(2,d_\omega)}(g-1) & \cdots & R_\omega^{(d_\omega,1)}(g-1) & \cdots \quad R_\omega^{(d_\omega,d_\omega)}(g-1) \end{pmatrix} \tag{73}$$

$\tilde{R}_\omega \in M_{g,d_\omega^2}$. Here $R_\omega^{(p,q)}(\cdot)$ is the (p, q)th element of the matrix $R_\omega(\cdot)$ $(1 \leqslant p, q \leqslant d_\omega)$ and

$$\tilde{R} = (\tilde{R}_1 \tilde{R}_2 \cdots \tilde{R}_\sigma). \tag{74}$$

Note that $\tilde{R}$ is unitary (by the definition of the elements of $R(G)$ and $\tilde{R} \in M_{g,g}$ (in view of (2)). Letting $\otimes$ denote the Kronecker product, we define two unitary matrices $\tilde{R}^* \otimes E_k$ and $\tilde{R} \otimes E_m$, of dimensions $(kg \times kg)$ and $(mg \times mg)$, respectively (E_k, E_m identity matrices of dimensions $(k \times k)$ and $(m \times m)$). Then the following lemma furnishes a block-diagonal form for any matrix $H \in \mathrm{Cir}(G, k, m)$.

LEMMA 2. *For any matrix* $H \in \mathrm{Cir}(G, k, m)$

$$(\tilde{R}^* \otimes E_k)\, H (\tilde{R} \otimes E_m) = \bigoplus_{\omega=1}^{\sigma} \left(\frac{g}{d_\omega} E_{d_\omega} \otimes \hat{h}(\omega)\right), \tag{75}$$

where $\bigoplus$ *is the symbol for direct summation of matrices and* $\hat{h}(\omega)$ *is a block matrix* $\hat{h}(\omega) = (\hat{h}^{(n,l)}(\omega))$, *each* $\hat{h}^{(n,l)}(\omega)$ *being a* $(d_\omega \times d_\omega)$ *matrix* $(1 \leqslant n \leqslant k, 1 \leqslant l \leqslant m)$.

The proof of Lemma 2 proceeds by direct computation of the left-hand side of (75) using (3).

Given the impulse matrix $W \in M_{kg,mg}$ of system (66), defined in (69), we set

$$\Omega = (\tilde{R}^* \otimes E_k)\, W (\tilde{R} \otimes E_m). \tag{76}$$

In view of (2), we can define blocks $\Omega(1), \ldots, \Omega(\sigma)$ along the diagonal of Ω, where $\Omega(\omega) \in M_{kd_\omega^2, md_\omega^2}$ $(1 \leqslant \omega \leqslant \sigma)$ (see Fig. 3). In each block $\Omega(\omega)$, similarly, we determine diagonal blocks $\Omega_1(\omega), \ldots, \Omega_{d_\omega}(\omega)$, where $\Omega_i(\omega) \in M_{kd_\omega, md_\omega}$ $(1 \leqslant i \leqslant d_\omega)$ (see Fig. 3).

The following theorem shows how to select a system S_{opt} providing the best approximation to system (66) in the sense of the criterion (72).

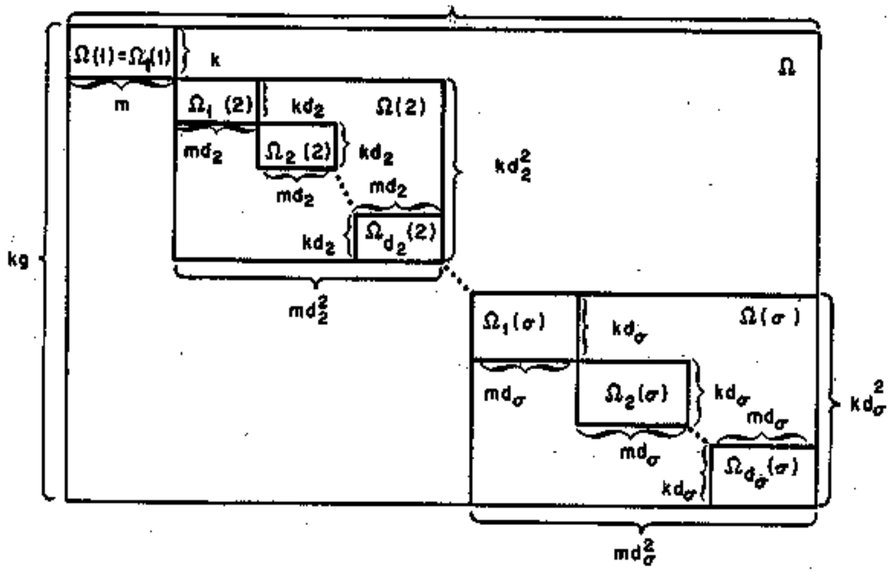


FIGURE 3

THEOREM 6. *Given a system* (66) *with impulse matrix* W *and a group* G *of order* g, *an optimal impulse function* $h_{\text{opt}} \in L_{k,m}$ *(in the sense of* (72)*) for system* S_{opt} *is defined by*

$$h_{\text{opt}}(\omega) = \frac{1}{g} \sum_{i=1}^{d_\omega} \Omega_i(\omega). \tag{77}$$

The norm of error e in (72) afforded by this approximation is given by

$$(\| e \|_2)^2 = \sum_{\omega=1}^{\sigma} \sum_{i=1}^{d_\omega} \left(\left\| \Omega_i(\omega) - \frac{1}{d_\omega} \sum_{j=1}^{d_\omega} \Omega_j(\omega) \right\|_2 \right)^2 + \left(\left\| \Omega - \bigoplus_{\omega=1}^{\sigma} \bigoplus_{i=1}^{d_\omega} \Omega_i(\omega) \right\|_2 \right)^2. \tag{78}$$

The proof based on the fact that $\|(\bar{R}^* \otimes E_k)\, W(\bar{R} \otimes E_m)\|_2 = \| W \|_2$ for any $W \in M_{kg,mg}$ and follows from Lemma 2.

We now present some relations that establish a direct relationship between the impulse function w of system (66) and the impulse function h_{opt} of the best approximation:

COROLLARY. *The impulse function* h_{opt} *of the best approximation* S_{opt} *to a given system* (66) *with impulse function* w *satisfies the condition*

$$h_{\text{opt}}(\zeta) = \frac{1}{g} \sum_{t \in G} w(t \circ \zeta - t). \tag{79}$$

The proof is by application of formula (8) to (77), using (76).

We now consider the question when there is a one-to-one correspondence between the time system (66) and its best approximation S_{opt} over a given

group G. It is shown by Pearl (1975) that this is indeed the case if $k = m = 1$, G is a dyadic group and the impulse matrix W is symmetric (symmetric system (66)) or lower triangular (causal system (66)).

We are going to show that if system (66) is symmetric, the dyadic groups G are the only ones for which there is a one-to-one correspondence of this type. If (66) is a causal system, this is always the case for a commutative group G; if G is not commutative, there need not exist a one-to-one correspondence.

To simplify the exposition, we assume henceforth that $k = m = 1$.

If system (66) is symmetric ($W^{(t,\zeta)} = w(|\, t - \zeta \,|)$ or causal ($W^{(t,\zeta)} = 0$ for $t < \zeta$), we set

$$h_{\text{opt}} = \begin{pmatrix} h_{\text{opt}}(0) \\ \vdots \\ h_{\text{opt}}(g-1) \end{pmatrix}, \qquad \mathbf{W} = \begin{pmatrix} w(0) \\ \vdots \\ w(g-1) \end{pmatrix}. \tag{80}$$

We may thus rewrite (79) as follows:

$$h_{\text{opt}} = \frac{1}{g} C_G \mathbf{W}, \quad \text{where} \quad C_G \in M_{g,g}. \tag{81}$$

THEOREM 7. (i) *If system* (66) *is symmetric, then* C_G *is invertible iff* G *is a dyadic group.*

(ii) *If system* (66) *is causal and for any* $t, \zeta \in G$

$$t \circ \zeta \leqslant t + \zeta, \tag{82}$$

then C_G *is a nonsingular lower triangular matrix.*

Proof. (i) Sufficiency was proved by Pearl (1975). Suppose that G is not dyadic. By (79), if system (66) is symmetric

$$C_G^{(\zeta,p)} = \overline{\{t \mid |\, t \circ \zeta - t \,| = p\}}, \qquad (0 \leqslant \zeta, p \leqslant g-1), \tag{83}$$

then, putting $t \circ \zeta^{-1} = q$, we have for every $0 \leqslant p \leqslant g-1$

$$C_G^{(\zeta^{-1},p)} = \overline{\{t \mid |\, t \circ \zeta^{-1} - t \,| = p\}} = \overline{\{q \mid |\, q - q \circ \zeta \,| = p\}} = C_G^{(\zeta,p)}. \tag{84}$$

Since G is not dyadic there exists $\zeta \in G$ such that $\zeta^{-1} \neq \zeta$ and it follows from (84) that $\det C_G = 0$.

(ii) By (79), if system (66) is causal,

$$C_G^{(\zeta,p)} = \overline{\{t \mid \delta(t \circ \zeta - t) = p\}}, \tag{85}$$

where

$$\delta(x) = x, \qquad x \geqslant 0;$$
$$= 0, \qquad x \leqslant 0. \tag{86}$$

Then, $C_G^{(\zeta,\zeta)} > 0$ because $\delta(0 \circ \zeta - 0) = \zeta$.
By (86), using (82), we have

$$\delta(t \circ \zeta - t) \leqslant \zeta. \tag{87}$$

Consequently, by (85) $C_G^{(\zeta,p)} = 0$ for $\zeta < p$.
We note that if G is a commutative group then there always exists an enumeration of the elements of the group by numbers 0, 1,..., $g - 1$, such that condition (82) holds. (Since a commutative group may be represented as a direct product of its cyclic subgroups.)

For the causal system (66) in the case of a non-Abelian group G, the matrix C_G may be invertible or noninvertible. For example, if $G = S_8$, the symmetric group of the third order, then for the enumeration:

$$1 = 0; \quad (132) = 1; \quad (123) = 2; \quad (12) = 3; \quad (13) = 4; \quad (23) = 5; \tag{88}$$

we have $\det C_G = 0$. (1 is the identity of S_8.)
But for the enumeration:

$$1 = 2; \quad (132) = 1; \quad (123) = 3; \quad (12) = 4; \quad (13) = 0; \quad (23) = 5; \tag{89}$$

we have $\det C_G \neq 0$.
From Theorem 6, its Corollary and Theorem 7, we may conclude:

(1) The above search procedure enables us to find the best approximation for arbitrary discrete systems (including time variant ones).

(2) For an arbitrary discrete possibly time variant m input k output system, we may construct its best m input k output approximation in the class of all systems whose impulse matrices can be reduced to block-diagonal form by two unitary matrices Q and Q' of dimensions $(kg \times kg)$ and $(mg \times mg)$, respectively.

(3) The norm of the approximation error e for a given system defined on the interval $[0, g - 1]$ depends on the choice of the group G (in the set of all groups of the order g over which the approximating system S_{opt} is defined). This poses an apparently quite difficult problem: optimal selection of a group G of given order minimizing the norm of the approximation error.

The procedure we have described for solving optimum problems make use of Fourier transforms on finite groups. The actual computation of such transforms may be accomplished by means of suitable Fast Fourier Transform Algorithms. (Apple and Wintz (1970), Karpovsky (to appear).).

Received: June 4, 1976

References

Pichler, F. (1971), On State Space Description of Linear Dyadic Invariant Systems, *Proceedings Symposium*, Walsh Functions, Washington, D.C., pp. 166–170.

Pearl, J. (1975), "Optimal dyadic models of time-invariant systems," *IEEE Trans. Computers* **24**, 598–603.

Falb, P. L., and Friedman, M. I. (1970), "A generalized transform theory for causal operators," *SIAM J. Control*, 452–471.

Tsypkin, Ya. Z., and Faradjev, R. G. (1966), Laplas-Galois transformation in the theory of sequential machines, *Dokl. Akad. Nauk. USSR*, **166** (3), 507–573 (in Russian).

Nailor, A. W. (1965), A transform technique for multivariable, timevarying, discrete-time, linear systems, *Automatica*, **2**, 211–234.

Karpovsky, M. G., and Trachtenberg, E. A. (1975), Circulants on Finite Groups, Technical Report #67, Computer Science Dept. Technion-IIT, Haifa, Israel.

Hartmuth, H. F. (1970), "Transmission of Information by Orthogonal Functions," Springer, Berlin.

Karpovsky, M. G., and Moskalev, E. S. (1970), Utilization of autocorrelation characteristics for the realization of systems of logical functions, *Avtomatika i Telemekhanica*, **8**, 89–99 (in Russian). English Translation: *Automation and Remote Control* **31**, 1278–1288.

Lechner, R. Y. (1971), "Harmonic Analysis of Switching Functions," in *Recent Developments in Switching Theory* (A. Mahkopadhyay Ed.), Academic Press, New York.

Karpovsky, M. G. (1976), "Finite Orthogonal Series in the Design of Digital Devices," New York.

Benes, V. E. (1964), Optimal Rearrangeable multistage connecting Networks, *B.S.T.J.* **43**, 1641–1656.

Harada, K. (1973), Sequential Permutation Networks, *IEEE Trans. Computers* **21**, 472–479.

Hewitt, E., and Ross, K. A. (1963), "Abstract Harmonic Analysis." Springer, Berlin.

Dornhoff, L. (1971), "Group Representation Theory," Marcel Dekker, New York.

Ben Israel, A., and Greville, T. N. E. (1974), "Generalized Inverses," Wiley, New York.

Amir-Moez, A. R. (1956), Extreme properties of eigenvalues of hermitian transformation and singular values of the sum and product of linear transformations, *Duke Math. J.* **23**, 463–476.

Karpovsky, M. G. (1977), Error detection in digital devices and computer programs with the aid of recurrent equations over finite commutative groups, *IEEE Trans. Computers* **26**, N2.

Apple, G., and Wintz, P. (1970), Calculation of Fourier transforms on finite abelian groups, *IEEE Trans.* **IT-16**, 233–236.

Karpovsky, M. G. Fast Fourier transforms on finite non-abelian groups, *IEEE Trans. Computers*.

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