Reprinted from INFORMATION AND CONTROL
Vol. 33, No. 2, February 1977
Printed in Belgium

Harmonic Analysis over Finite Commutative Groups in Linearization Problems For Systems of Logical Functions

M. G. KARPOVSKY

Tel-Aviv University, Romat-Aviv, Tel-Aviv, Israel

In this paper we consider the linearization problems for systems of two- and many-valued logical functions by methods of abstract harmonic analysis. By an optimal linearization we mean a representation of the original system as a superposition of linear and nonlinear vectorfunctions, such that the complexity of the nonlinear part is minimized. The problems are solved for the three most simply computed criteria of the complexity of systems of logical functions. Logical functions are treated as functions defined on finite commutative groups. The solutions of the linearization problems involve the use of Fourier expansions of these functions in terms of the group characters. The spectral characteristics thus arising, as well as the correlation characteristics obtained from the original function by double spectral transforms, are used as a working tool in solving linearization problems. The solutions are exact and convenient from the computational standpoint.

The paper illustrates the effectiveness of the methods of abstract harmonic analysis in problems of synthesis and optimization of digital devices.

INTRODUCTION

This paper deals with the linearization of systems of functions defined on finite commutative groups, the principal topic being linearization of systems of two-valued and many-valued logical functions. Two classes of structures are studied: structures with the linear and nonlinear blocks connected in series and in parallel. The problems treated are optimization problems, in the sense that their solutions determine structures with nonlinear parts of minimal complexity.

The main tools are methods of harmonic analysis on finite commutative groups. These methods yield solutions which are both exact and convenient for computational purposes.

The paper falls into four sections.

The first section discusses harmonic analysis on finite commutative groups. We define the spectral and correlation characteristics of functions

ISSN 0019–9958

on such groups and study their properties. Spectral transforms of functions are defined by expanding them in generalized Fourier series in terms of the group characters. Correlation characteristics are obtained from the original functions by double spectral transforms.

In the second section we introduce and justify various criteria for the complexity of systems of logical functions. These criteria will subsequently be used in the linearization problems.

The third section formulates and solves linearization problems for the case of series-connected linear and nonlinear blocks. The main tools utilized here are the correlation characteristics.

The fourth section is devoted to linearization when the linear and nonlinear blocks are connected in parallel. The main tools are the spectral characteristics.

In order to make the exposition more systematic, we include in this paper certain results of Karpovsky and Moskalev (1970, 1973), slightly generalized. Related questions, concerning the linearization of systems of logical functions and the synthesis of logical networks using orthogonal transformations, were dealt with in Karpovsky and Moskalev (1967, 1970), Karpovsky (1971), Lechner (1971), Kitahashi and Tanaka (1972). The use of harmonic analysis on finite commutative groups in problems of analysis, synthesis, and optimization of digital devices is also discussed in the monograph of Karpovsky (1976).

I. Harmonic Analysis on Finite Commutative Groups

Let G be a finite commutative group. A character of G is defined to be a homomorphism of G into the multiplicative group of complex numbers. The set of characters of G is a complete orthogonal basis in the space of functions mapping G into the field C of complex numbers, and on the other hand the set of characters of G is a multiplicative group isomorphic to G (Curtis and Reiner, 1962). Thus if $\chi_\omega(x)$ is the character mapped onto an element $\omega \in G$ under this isomorphism and $f: G \to C$, then

$$f(x) = \sum_{\omega \in G} S_f(\omega)\, \chi_\omega(x), \tag{1}$$

where

$$S_f(\omega) = g^{-1} \sum_{x \in G} f(x)\, \overline{\chi_\omega(x)}, \tag{2}$$

g is the order of G and $\overline{\chi_\omega(x)}$ is the function complex–conjugate to $\chi_\omega(x)$. Formulas (1) and (2) define the generalized Fourier transform over G,

a function $f(x)$ being associated with its spectrum $S_f(\omega)$. The basic properties of the generalized Fourier transform are analogous to the corresponding properties of the classical Fourier transform (Curtis and Reiner, 1962).

We now indicate an explicit method of constructing characters for finite commutative groups.

Express G as a direct product of cyclic subgroups, $G = \prod_{i=0}^{m-1} G_i$. Let e_i denote a generator of G_i, q_i the order of G_i and q_i prime ($i = 0, 1, \ldots, m-1$). Then for any $x \in G$ there is a unique vector $x = (x^{(0)}, \ldots, x^{(m-1)})$ such that $0 \leqslant x^{(i)} < q_i$ and

$$x = x^{(0)}e_0 * \cdots * x^{(m-1)}e_{m-1} = \underset{i=0}{\overset{m-1}{*}} x^{(i)}e_i ,$$

where

$$x^{(i)}e_i = \underbrace{e_i * \cdots * e_i}_{x^{(i)}};$$

$0e = e$, the identity of G. (We let $*$ denote the group operation in G.)

THEOREM 1 (Curtis and Reiner, 1962). *Let* $G = \prod_{i=0}^{m-1} G_i$, $x = *_{i=0}^{m-1} x^{(i)}e_i$, $\omega = *_{i=0}^{m-1} \omega^{(i)}e_i$, $(0 \leqslant x^{(i)}, \omega^{(i)} < q_i ; i = 0, 1, \ldots, m-1)$. *Then*

$$\chi_\omega(x) = \exp\left(\sum_{i=0}^{m-1} (2\pi/q_i)\, j\omega^{(i)}x^{(i)}\right), \tag{3}$$

(where $j = (-1)^{1/2}$, q_i *is the order of* G_i*) and the multiplicative group* $\{\chi_\omega(x)\}$ *is isomorphic to* G.

It follows from Theorem 1 that if $q_i = q$ $(i = 0, \ldots, m-1)$, then $\{\chi_\omega(x)\}$ is the system of Chrestenson functions; if $q = 2$ we get the system of Walsh functions (Karpovsky and Moskalev, 1970).

We now define correlation function on a group. The cross-correlation function $B^{(2)}_{f^{(1)}(x), f^{(2)}(x)}(\tau)$ for functions $f^{(1)}: G \to C$, $f^{(2)}: G \to C$, is defined as:

$$B^{(2)}_{f^{(1)}(x), f^{(2)}(x)}(\tau) = \sum_{\tau \in G} f^{(1)}(x)\, \overline{f^{(2)}(x * \tau^{-1})}, \tag{4}$$

where $\tau^{-1} \in G$ the inverse of τ in G.

The next theorem will show the relationship between the cross-correlation function and the generalized Fourier transform. Denote $S_f(\omega) = \mathscr{F}(f(x))$ and $f(x) = \mathscr{F}^{-1}(S_f(\omega))$.

THEOREM 2 (Curtis and Reiner, 1962). *For any* $f^{(1)}$, $f^{(2)}: G \to C$, *the following diagram is commutative* (g *is the order of* G):

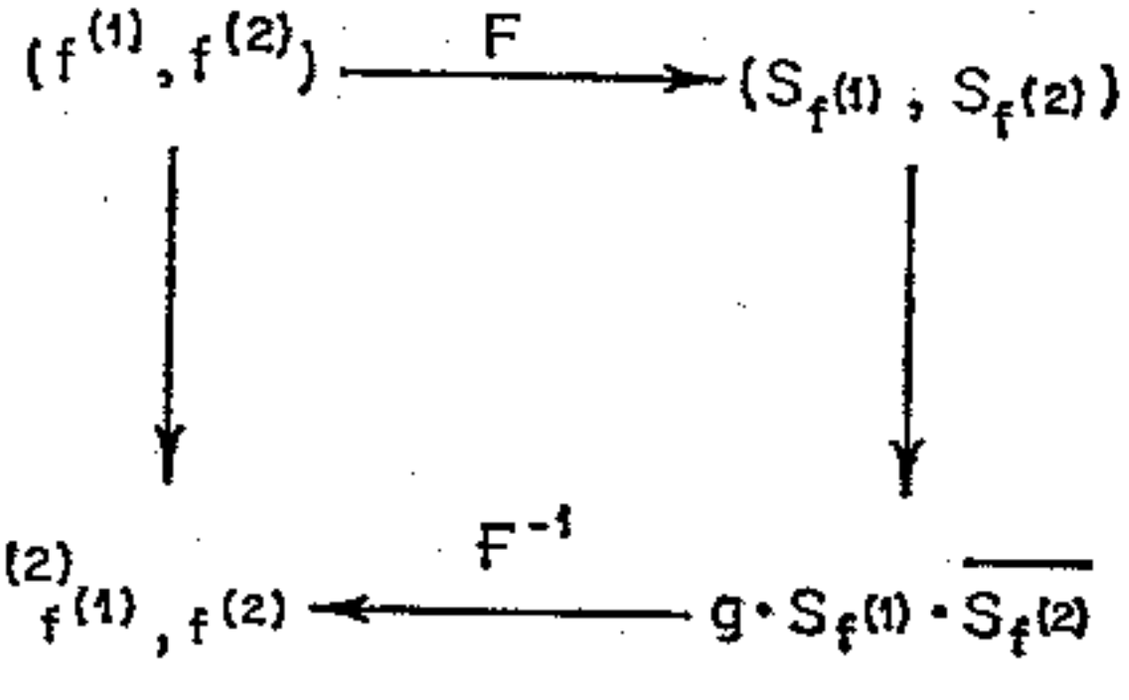

FIG. 1. Diagram of Theorem 2.

Theorem 2 enables one to calculate the correlation function as an iterated generalized Fourier transform.

Throughout the sequel, we shall consider functions $f(x)$ taking values in the field R of real numbers.

If $f^{(1)}(x) = f^{(2)}(x) = f(x)$, then function $B^{(2)}_{f,f}(\tau) = B^{(2)}_{f}(\tau)$ is known as the autocorrelation function. We now proceed to generalize this concept.

Consider the system of autocorrelation functions

$$B^{(p)}_{f}(\tau) = \sum_{x \in G} f(x) f(x * \tau^{-1}) \cdots f(x * \tau^{-(p-1)}) = \sum_{x \in G} \prod_{i=0}^{p-1} f(x * \tau^{-i}) \quad (5)$$

where, if $G = \prod_{i=0}^{m-1} G_i$, q_i is the order of G_i, then $p = 2, 3, \ldots, \min_{(i)} q_i - 1$.

The function $B^{(p)}_{f}(\tau)$ may be viewed as the cross-correlation function of $f(x)$ and its $p - 1$ successive translations on the group G. We now describe its main properties.

THEOREM 3 (Karpovsky and Moskalev, 1973). *Let $f: G \to R$; let e be the identity in $G = \prod_{i=0}^{m-1} G_i$, $\alpha \in G$. Then for any $p \in \{2, 3, \ldots \min_i q_i - 1\}$:*

$$B^{(p)}_{f(x)}(e) = \sum_{x \in G} f^{p}(x), \quad (6)$$

$$B^{(p)}_{f(x)}(\tau^{-1}) = B^{(p)}_{f(x)}(\tau) \quad (7)$$

(analog of the evenness relation for the classical autocorrelation function),

$$B^{(p)}_{f(x*\alpha)}(\tau) = B^{(p)}_{f(x)}(\tau) \quad (8)$$

(group-translation invariance).

Let σ be a group isomorphism for G, then

$$B^{(p)}_{f(\sigma(x))}(\tau) = B^{(p)}_{f(x)}(\sigma(\tau)). \quad (9)$$

Theorems 1–3 may be used to calculate the functions $S_f(\omega)$ and $B_f^{(p)}(\tau)$, which will be used constantly for solutions of linearization problems.

To conclude this section, we note that calculations of the values of functions, spectral characteristics, and correlation characteristics utilize operations over these values in the field of complex numbers. However, the results may be generalized to the case that the operations are defined over finite fields.

II. Complexity of Systems of Logical Functions

Let G_q denote the group $\{0,..., q-1\}$ with respect to addition modulo q (the operation will be denoted by $\oplus \pmod q$), and

$$G_q^m = \underbrace{G_q \times \cdots \times G_q}_{m} \qquad (q \geqslant 2).$$

By a system of k q-valued logical functions of m arguments we mean a system of K mappings $f^{(i)}: G_q^m \to G_q$ $(i = 0,..., k-1)$. The complexity of a system is defined as the sum of complexities of the functions entering into the system.

We shall consider various criteria for complexity of logical functions.

The simplest and most natural complexity criterion for a q-valued logical function $f(x^{(0)},..., x^{(m-1)})$, $x^{(i)} \in G_q$ $(i = 0,..., m-1)$ is the number $\xi_0(f)$ $(\xi_0 \leqslant m)$ of arguments on which $f(x^{(0)},..., x^{(m-1)})$ depends essentially. (The function depends essentially on $x^{(i)}$ if there exist $\alpha, \beta \in G_q$ such that for some $(x^{(0)},..., x^{(i-1)}, x^{(i+1)},..., x^{(m-1)})$ $f(x^{(0)},..., x^{(i-1)}, \alpha, x^{(i+1)},..., x^{(m-1)}) \neq f(x^{(0)},..., x^{(i-1)}, \beta, x^{(i+1)},..., x^{(m-1)})$.)

The criterion $\xi_0(f)$ is very easy to evaluate but is only weakly connected with the specific properties of the function f.

We now define a criterion $\xi_1(f)$, first for the case of Boolean functions $(q = 2)$.

If $x_1 = (x_1^{(0)},..., x_1^{(m-1)})$, $x_2 = (x_2^{(0)},..., x_2^{(m-1)})(x_1^{(i)}, x_2^{(i)} \in \{0, 1\})$, we set

$$d(x_1, x_2) = \sum_{i=0}^{m-1} | x_1^{(i)} - x_2^{(i)} |.$$

Then $\xi_1(f)$ is the number of pairs $\{x_1, x_2\}$ such that $f(x_1) \neq f(x_2)$ and $d(x_1, x_2) = 1$.

The criteria $\xi_0(f)$ and $\xi_1(f)$ are used in the case $q = 2$, for example, in Sholomov (1966), Pospelov (1968), Karpovsky and Moskalev (1970); some considerations from which one can determine the relation between $\xi_0(f)$,

$\xi_1(f)$ and the complexity of a minimal network implementing the mapping f may be found in Sholomov (1966), Karpovsky and Moskalev (1970).

We now proceed to introduce two natural generalizations $\xi_{1,L}(f)$ and $\xi_{1,H}(f)$ of $\xi_1(f)$ to the case $q \geqslant 2$, arising from two different metrizations of the space of q-adic vectors of arguments.

We shall use the two most familiar metrics (Berlekamp, 1968): the Lee metric $d_L(x_1, x_2)$ and the Hamming metric $d_H(x_1, x_2)$:

$$d_L(x_1, x_2) = \sum_{i=0}^{m-1} |x_1^{(i)} - x_2^{(i)}|, \qquad |x_1^{(i)} - x_2^{(i)}| \equiv \pm(x_1^{(i)} - x_2^{(i)}) \pmod q,$$

$$0 \leqslant |x_1^{(i)} - x_2^{(i)}| \leqslant 0.5q; \quad (10)$$

$$d_H(x_1, x_2) = \sum_{i=0}^{m-1} d_H(x_1^{(i)}, x_2^{(i)}), \; d_H(x_1^{(i)}, x_2^{(i)})$$

$$= \begin{cases} 1, & x^{(i)} \neq x_2^{(i)}, \\ 0, & x_1^{(i)} = x_2^{(i)}. \end{cases} \quad (11)$$

We introduce the following notation: (i) $\xi_{1,L}(f)$ is the number of pairs $\{x_1, x_2\}$ such that $d_L(x_1, x_2) = 1$ and $f(x_1) \neq f(x_2)$; (ii) $\xi_{1,H}(f)$ is the number of q-tuples of vectors $\{x_1, \ldots, x_q\}$ such that $d_H(x_i, x_s) = 1$ $(i, s \in \{1, \ldots, q\}, i \neq s)$ and there exist $\alpha, \beta \in \{1, \ldots, q\}$ $(\alpha \neq \beta)$ such that $f(x_\alpha) \neq f(x_\beta)$. When $q = 2$, we have $\xi_{1,L}(f) = \xi_{1,H}(f) = \xi_1(f)$).

The complexity criteria $\xi_{1,L}(f)$ and $\xi_{1,H}(f)$ are related to the error-correcting capability of the function f. The function f (and any device implementing it) will correct an error $\{x_1, x_2\}$ $(x_1 \neq x_2)$ if $f(x_1) = f(x_2)$. An error $\{x_1, x_2\}$ is called a single Lee error (Hamming error) if $d_L(x_1, x_2) = 1$ $(d_H(x_1, x_2) = 1)$. (The probability of either type of error—Lee or Hamming—depends on the physical representation (i.e., type of modulation) of the signal x (Berlekamp, 1968).)

Given a function f, we let $\eta_{1,L}(f)$ and $\eta_{1,H}(f)$ denote the number of corrected single Lee and Hamming errors, respectively. Then by (10), (11):

$$\eta_{1,L}(f) = \gamma_q q^m m - \xi_{1,L}(f), \qquad \gamma_q = \begin{cases} 1, & q \geqslant 2, \\ 0.5, & q = 2; \end{cases} \quad (12)$$

$$\eta_{1,H}(f) = \binom{q}{2}(q^{m-1}m - \xi_{1,H}(f)). \quad (13)$$

The criteria $\xi_0, \xi_{1,L}, \xi_{1,H}$ will be used below for linearization problems. Of course, these are not the only possible criteria; our choice is dictated primarily by considerations of computational simplicity.

III. Series Linearization of Systems of Logical Functions

Let $f(x) = \{f^{(i)}(x)\}$ $(i = 0,\ldots, k-1;\ x = (x^{(0)},\ldots, x^{(m-1)}),\ x^{(s)} \in \{0,\ldots, q-1\})$ be a system of k q-valued logical functions which depend essentially on all their arguments. We first assume that q is a prime.

Let $\sigma = (\sigma_{is})(\sigma_{is} \in \{0,\ldots, q-1\};\ i, s = 0,\ldots, m-1)$ be a nonsingular $m \times m$ matrix over $GF(q)$. We construct a system $f_\sigma(x) = \{f_\sigma^{(i)}(x)\}$ as follows:

$$f_\sigma^{(i)}(\sigma \otimes x) = f^{(i)}(x) \pmod q \qquad (i = 0,\ldots, k-1). \tag{14}$$

(Here and below the symbol $\otimes$ and the notation (mod q) to the right of an expression signify matrix multiplication over $GF(q)$.)

Formula (14) generates a scheme for synthesis of a device implementing the function $f(x)$ by series connection of two blocks: linear σ and nonlinear $f_\sigma(x)$.

By series linearization we mean the determination of a matrix σ, minimizing the complexity of $f_\sigma(x)$ for the given system $f(x)$. The reason that we are minimizing the complexity of the nonlinear part $f_\sigma(x)$ only is that for almost all $f(x)$ and almost all σ the complexity $L(f)$ of the minimal network implementing $f(x)$ is much more than the complexity $L(\sigma)$ of a minimal network implementing σ. For example, let $q = 2$ and $m \to \infty$; then for almost all systems of k Boolean functions of m arguments, the complexities $L(f)$ and $L(\sigma)$ (measured by the minimal number of single-input and two-input logical elements) satisfy the conditions (Nechiporuk, 1963)

$$L(f) \sim k \cdot 2^m/m, \tag{15}$$

$$L(\sigma) \sim m^2/\log_2 m. \tag{16}$$

(The expression "for almost all functions of m arguments in class ϕ satisfying condition A" means that the fraction of functions in ϕ satisfying condition A tends to unity as $m \to \infty$.)

Thus, the problem of series linearization with respect to a criterion ξ_α may be formulated as follows: Given a system $f(x)$, find a matrix σ_α such that

$$\min_{\sigma \in \Xi_q} \xi_\alpha(f_\sigma) = \xi_\alpha(f_{\sigma_\alpha}), \tag{17}$$

where $f_\sigma(x)$ is defined in terms of $f(x)$ by (14) and Ξ_q is the class of all nonsingular $m \times m$ matrices over $GF(q)$.

We denote the complexity $\xi_\alpha(f_{\sigma_\alpha})$ of the nonlinear part for the best linearization σ_α by $\xi_\alpha^{(n)}(f)$.

The theorems established below furnish constructive methods to determine σ_α and estimates of $\xi_\alpha^{(n)}(f)$ $(\alpha = 0; 1, L; 1, H)$.

We shall seek a solution to the series linearization problems using the autocorrelation characteristics $B_f^{(2)}(\tau)$ and $B_f^{(q)}(\tau)$ on the group $G = G_q{}^m$.

We first consider linearization with respect to ξ_0.

Construct the following system of characteristic functions for given $\{f^{(i)}(x)\}$:

$$f_t^{(i)}(x) = \begin{cases} 1, & f^{(i)}(x) = t, \\ 0, & f^{(i)}(x) \neq t. \end{cases} \tag{18}$$

Let $B_{i,t}^{(2)}(\tau)$ be the autocorrelation function of $f_t^{(i)}(x)$ $(t = 0,\ldots, q-1; i = 0,\ldots, k-1)$ on $G = G_q{}^m$ (see (4)), and let $B_f^{(2)}(\tau)$ be the total autocorrelation function of $f(x)$:

$$B_f^{(2)}(\tau) = \sum_{i,t} B_{i,t}^{(2)}(\tau) = \sum_{i,t} \sum_{x \in G} f_t^{(i)}(x) f_t^{(i)} \qquad (x \ominus \tau) \pmod q. \tag{19}$$

(The symbols $\oplus$ and $\ominus$ (mod q) denote componentwise addition and subtraction modulo q). We set $\tau_s \in G_I(f)$ if and only if

$$B_f^{(2)}(\tau_s) = \max_{t \in G} B_f^{(2)}(\tau) = B_f^{(2)}(0,\ldots,0) = k \cdot q^m. \tag{20}$$

Then $G_I(f)$ is a subgroup of G, which we call the inertia group of $f(x)$ (since it follows from (19) and (20) that $\tau_s \in G_I(f)$ if and only if $f(x) = f(x \oplus \tau_s) \pmod q$).

Now let $b_I(f)$ be the number of elements in an arbitrary basis for $G_I(f)$ (in other words, in an arbitrary maximal set of elements of $G_I(f)$ linearly independent over $GF(q)$).

THEOREM 4. *Let $T_0 \in \Xi_q$ be a matrix whose set of columns contains some basis for the inertia group of a system $f(x)$ of k q-valued logical functions of m arguments. Then*

$$\sigma_0 \otimes T_0 = E \qquad (\text{mod } q), \qquad \left(E = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right), \tag{21}$$

$$\xi_0^{(n)}(f) = k(m - b_I(f)). \tag{22}$$

Proof. By (14) and (21), we have $f_{\sigma_0}(x) = f(T_0 \otimes x) \pmod q$. Set

$$e_s = (\underbrace{0,\ldots,0}_{s}, 1, 0,\ldots,0) \qquad (s = 0,\ldots, m-1).$$

Then $f_{\sigma_0}(x)$ depends on $x^{(s)}$ nonessentially if and only if $B^{(2)}_{f_\sigma}(e_s) = k \cdot q^m$.

Then, if $\tau_0,\ldots,\tau_{b_I(f)-1}$ is a basis for $G_I(f)$ and τ_s is the sth column of T_0 $(s = 0,\ldots, b_I(f) - 1)$, we have $\tau_s = T_0 \otimes e_s \pmod q$ and by (14), (20), and Theorem 3 (for $\sigma = \sigma_0$ and $p = 2$):

$$kq^m = B^{(2)}_{f(x)}(\tau_s) = B^{(2)}_{f(x)}(T_0 \otimes e_s) = B_{f(T_0 \otimes x)}(e_s) = B^{(2)}_{f_{\sigma_0}(x)}(e_s)$$

$$(s = 0, 1,\ldots, b_I(f) - 1) \pmod q.$$

Consequently, $\xi_0^{(n)}(f) = \xi_0(f_{\sigma_0}) \leqslant m - b_I(f)$.

We now show that for any $\sigma \in \Xi_q$ $\xi_0(f_\sigma) \geqslant m - b_I(f)$, whence it will follow that σ_0 is the best linearization with respect to ξ_0. Let $\xi_0(f_\sigma) = m - b_I(f) - \epsilon$ $(\epsilon > 0)$. Then there exist vectors e_{i_r} $(r = 0,\ldots, b_I(f) + \epsilon - 1)$ such that

$$k \cdot q^m = B^{(2)}_{f_\sigma(x)}(e_{i_r}) = B^{(2)}_{f(\sigma^{-1} \otimes x)}(e_{i_r}) = B^{(2)}_{f(x)}(\sigma^{-1} \otimes e_{i_r}) \pmod q$$

and so $(\sigma^{-1} \otimes e_{i_r}) \in G_I(f)$. But since the vectors e_{i_r} $(r = 0,\ldots, b_I(f) + \epsilon - 1)$ are linearly independent and the matrix σ is nonsingular over $GF(q)$, this contradicts the assumption that the basis of $G_I(f)$ contains only $b_I(f)$ vectors. This completes the proof.

Thus, series linearization with respect to the criterion ξ_0 reduces to the following operations:

1. construct the total autocorrelation function $B^{(2)}_f(\tau)$;
2. using the maxima of $B^{(2)}_f(\tau)$, construct the inertia group $G_I(f)$;
3. select an arbitrary basis in $G_I(f)$;
4. construct a matrix $T_0 \in \Xi_q$ whose set of columns contains the basis of $G_I(f)$ and invert T_0 over $GF(q)$.

EXAMPLE 1. Table I defines a system $\{f^{(0)}, f^{(1)}\}$ of two Boolean functions of 4 arguments and values of the corresponding total autocorrelation function, $B^{(2)}_f(\tau)$ $(q = 2, m = 4, k = 2, G = G_2^4)$. We see from Table I that $G_I(f) =$

$\{(0, 0, 0, 0), (0, 1, 0, 1), (1, 0, 1, 0), (1, 1, 1, 1)\}$. As a basis we take $\tau_0 = (0, 1, 0, 1)$, $\tau_1 = (1, 0, 1, 0)(b_I(f) = 2)$. Now set

$$T_0 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{so that} \quad \sigma_0 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The functions $f^{(0)}_{\sigma_0}$ and $f^{(1)}_{\sigma_0}$ are also shown in Table I.

TABLE I

x, τ	$x^{(0)}$	$x^{(1)}$	$x^{(2)}$	$x^{(3)}$	$f^{(0)}$	$f^{(1)}$	$B^{(2)}_f$	$f^{(0)}_{\sigma_0}$	$f^{(1)}_{\sigma_0}$
0	0	0	0	0	0	0	32	0	0
1	0	0	0	1	1	0	16	0	0
2	0	0	1	0	1	0	16	0	0
3	0	0	1	1	1	1	16	0	0
4	0	1	0	0	1	0	16	1	0
5	0	1	0	1	0	0	32	1	0
6	0	1	1	0	1	1	16	1	0
7	0	1	1	1	1	0	16	1	0
8	1	0	0	0	1	0	16	1	0
9	1	0	0	1	1	1	16	1	0
10	1	0	1	0	0	0	32	1	0
11	1	0	1	1	1	0	16	1	0
12	1	1	0	0	1	1	16	1	1
13	1	1	0	1	1	0	16	1	1
14	1	1	1	0	1	0	16	1	1
15	1	1	1	1	0	0	32	1	1

It is evident from Table I that $f^{(0)}_{\sigma_0}$ and $f^{(1)}_{\sigma_0}$ do not depend essentially on $x^{(2)}$, $x^{(3)}$. Consequently, in accordance with (22), $\xi^{(n)}_0(f) = \xi_0(f^{(0)}_{\sigma_0}) + \xi_0(f^{(1)}_{\sigma_0}) = 4$, (whereas $\xi_0(f) = 8$).

A network realizing σ_0 is illustrated in Fig. 2. Thus the efficiency of the serial linearization with respect to the criterion ξ_0 depends only on the order of the inertia group $G_I(f)$.

The class of systems possessing a nontrivial linearization with respect to ξ_0 is relatively small. We therefore proceed to linearization with respect to $\xi_{1,L}$ and $\xi_{1,H}$.

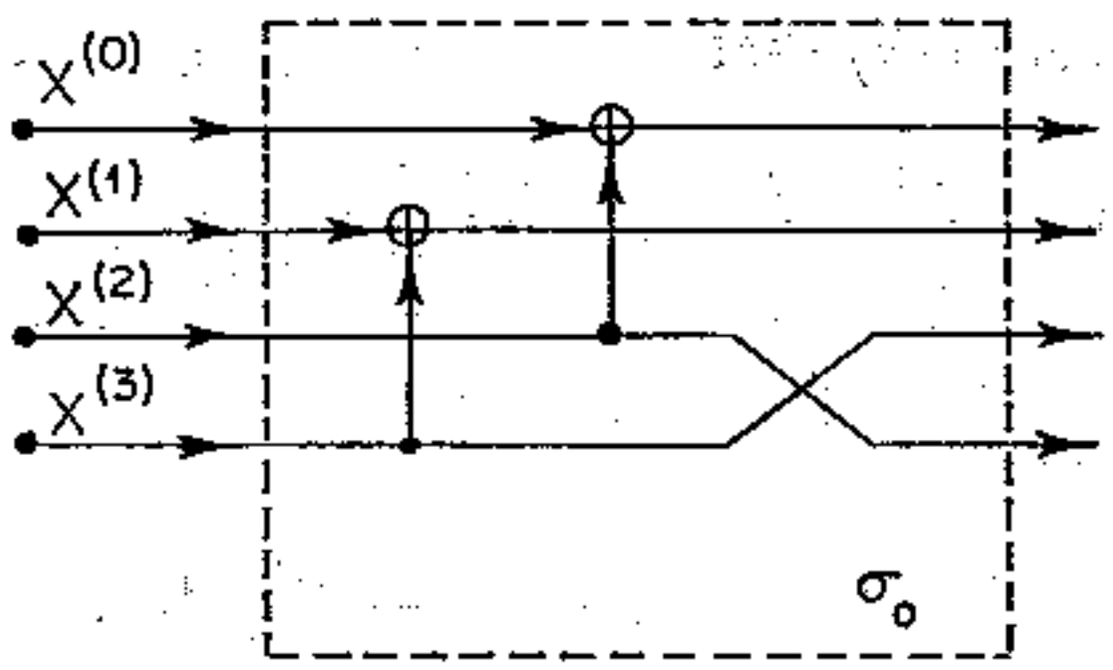

FIG. 2. A linear example of Example 1.

We first consider linearization with respect to $\xi_{1,L}$, based on use of the Lee metric.

Given a system $f(x)$, we construct $B_f^{(2)}(\tau)$ as before (see (18), (19)). Then, if $\tau_0, \ldots, \tau_{m-1} \in G_q^m$ and T is the $m \times m$ matrix with columns $\tau_0, \ldots, \tau_{m-1}$, we set

$$B_f^{(2)}(T) = \sum_{s=0}^{m-1} B_f^{(2)}(\tau_s). \tag{23}$$

THEOREM 5. *Given a system $f(x)$ of k q-valued logical functions of m arguments, let*

$$\max_{T \in S_q} B_f^{(2)}(T) = B_f^{(2)}(T_{1,L}). \tag{24}$$

Then

$$\sigma_{1,L} \otimes T_{1,L} = E \pmod q, \tag{25}$$

$$\xi_{1,L}^{(n)}(f) = \gamma_q(q^m mk - B_f^{(2)}(T_{1,L})) \qquad \left(\gamma_q = \begin{cases} 1, & q > 2 \\ 0.5, & q = 2 \end{cases}\right). \tag{26}$$

Proof. We first show the connection between the total autocorrelation function $B_f^{(2)}$ and $\xi_{1,L}$-complexity of the system f.

Let $N^{(2)}$ denote the number of pairs $\{x_1, x_2\}$ such that $d_{1,L}(x_1, x_2) = 1$, and $N_i^{(2)}$ $(i = 0, \ldots, k-1)$ the number of pairs $\{x_1, x_2\}$ such that

$$d_{1,L}(x_1, x_2) = 1 \quad \text{and} \quad f^{(i)}(x_1) \neq f^{(i)}(x_2) \quad (x_1, x_2 \in G_q^m).$$

Then, by (10), (18), (19), and (23),

$$N^{(2)} = \gamma_q \cdot q^m \cdot m, \qquad N_i^{(2)} = N^{(2)} - \gamma_q \cdot \sum_{t=0}^{q-1} B_{i,t}^{(2)}(E).$$

Further, it follows from (19) that

$$\xi_{1,L}(f) = \sum_{i=0}^{k-1} N_i^{(2)} = \sum_{i=0}^{k-1} \gamma_q\left(q^m m - \sum_{t=0}^{q-1} B_{i,t}^{(2)}(E)\right) = \gamma_q(q^m mk - B_f^{(2)}(E)).$$

Similarly, for any $\sigma \in \Xi q$,

$$\xi_{1,L}(f_\sigma) = \gamma_q(q^m mk - B_{f_\sigma}^{(2)}(E)).$$

Now, by (14), we have for any $\sigma \in \Xi_q$,

$$f_\sigma(x) = f(\sigma^{-1} \otimes x) \qquad (\text{mod } q),$$

and so, in view of (9), it follows from Theorem 3, (24), and (25), that

$$\xi_{1,L}^{(n)}(f) = \xi_{1,L}(f_{\sigma_{1,L}}) = \min_{\sigma \in \Xi_q} \gamma_q(q^m mk - B_{f_\sigma}^{(2)}(E))$$

$$= \gamma_q(q^m mk - \max_{\sigma \in \Xi_q} B_f^{(2)}(E)) = \gamma_q(q\ \ mk - \max_{\sigma \in \Xi_q} B_f^{(2)}(\sigma^{-1}))$$

$$= \gamma_q(q^m mk - B_f^{(2)}(T_{1,L})),$$

and $\sigma_{1,L} \otimes T_{1,L} = E \pmod q$. The proof is complete.

Thus, the process of linearization with respect to $\xi_{1,L}$ amounts to the following operations:

1. construct the total autocorrelation function $B_f^{(2)}(\tau)$;
2. determine a matrix $T_{1,L}$ maximizing $B_f^{(2)}(T)$ over all $T \in \Xi_q$;
3. invert $T_{1,L}$ over $GF(q)$.

The question of economical techniques for calculation $B_f^{(2)}(\tau)$ will be discussed later; for the moment we indicate a recursive m-step procedure to compute the columns $\tau_0^{(1,L)}, \ldots, \tau_{m-1}^{(1,L)}$ of matrix $T_{1,L}$, satisfying (23), (24).

Set

$$\max_{\tau \neq (0,\ldots,0)} B_f^{(2)}(\tau) = B_f^{(2)}(\tau_0^{(1,L)}). \tag{27}$$

Assuming that $\tau_0^{(1,L)}, \ldots, \tau_{s-1}^{(1,L)}$ $(s = 1, \ldots, m-1)$ are already known, and letting L_s be the set of all vectors $\bigoplus_{i=0}^{s-1} c_i \tau_i^{(1,L)} \pmod q$, $c_i \in \{0, \ldots, q-1\}$

$$(c_i \tau_i^{(1,L)} = \underbrace{\tau_i^{(1,L)} \oplus \cdots \oplus \tau_i^{(1,L)}}_{c_i} \pmod q),$$

we have

$$B_f^{(2)}(\tau_s^{(1,L)}) = \max_{\tau \notin L_s} B_f^{(2)}(\tau) \qquad (s = 1, \ldots, m-1). \tag{28}$$

Some data about the implementations of the above algorithm for the case of systems of Boolean functions may be found in Karpovsky, Moskalev (1970).

EXAMPLE 2. Table II defines a function f and the appropriate $B_f^{(2)}(\tau)$ ($q = 3, m = 2, k = 1$). Using the procedure (27), (28), we have, for example,

$$T_{1,L} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Then

$$\sigma_{1,L} = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}.$$

The function $f_{\sigma_{1,L}}$ is also shown in Table II.

TABLE II

x, τ	$x^{(0)}$	$x^{(1)}$	f	$B_f^{(2)}$	$f_{\sigma_{1,L}}$
0	0	0	0	9	0
1	0	1	2	2	1
2	0	2	0	2	0
3	1	0	1	2	0
4	1	1	0	3	2
5	1	2	1	3	0
6	2	0	2	2	1
7	2	1	0	3	2
8	2	2	1	3	1

It is readily seen that, in accordance with (26), $\xi_{1,L}^{(n)}(f) = 12$, whereas $\xi_{1,L}(f) = 14$.

The methods just described for linearization with respect to ξ_0 and $\xi_{1,L}$ were based on the correlation characteristics.

$$B_f^{(2)}(\tau) = \sum_{i,t} B_{i,t}^{(2)}(\tau).$$

To calculate $B_f^{(2)}(\tau)$ itself, one can use formula (19) and the evenness relation (7), but for large m and $k \ll m$ it is more advantageous to use Theorem 2, calculating $B_{i,t}^{(2)}(\tau)$ in terms of iterated generalized Fourier transforms over the group $G_q{}^m$. Since the characters of $G_q{}^m$ are the Chrestenson functions or, if $q = 2$, the Walsh functions, the generalized Fourier transforms may be calculated in this case by using the highly effective

algorithm of the fast Hadamard–Chrestenson or Hadamard–Walsh transform (Andrews and Caspari, 1970).

To end the discussion for $\xi_{1,L}$, we observe that an optimal linearization with respect to $\xi_{1,L}$ is always optimal with respect to ξ_0 (but not conversely), and so the class of systems admitting a nontrivial linearization with respect to $\xi_{1,L}$ always contains the corresponding class for ξ_0.

We now consider linearization with respect to the criterion $\xi_{1,H}$, based on the use of the Hamming metric.

Given a system $f(x) = \{f^{(i)}(x)\}$ of k q-valued logical functions of m arguments, we construct the characteristics $f_t^{(i)}(x)$ (see (18)) ($i = 0,..., k-1$; $t = 0,..., q-1$) and the total autocorrelation function $B_f^{(q)}(\tau)$ on the group G_q^m:

$$B_f^{(q)}(\tau) = \sum_{i,t} B_{i,t}^{(q)}(\tau) = \sum_{i,t} \sum_{x \in G_q^m} \prod_{p=0}^{q-1} f_t^{(i)}(x - p\tau) \pmod q. \tag{29}$$

Furthermore, if T is the $m \times m$ matrix with columns $\tau_0, ..., \tau_{m-1}$, then

$$B_f^{(q)}(T) = \sum_{s=0}^{m-1} B_f^{(q)}(\tau_s). \tag{30}$$

THEOREM 6. *Given a system f of k q-valued logical functions of m arguments, assume that*

$$\max_{T \in \Xi_q} B_f^{(q)}(T) = B_f^{(q)}(T_{1,H}). \tag{31}$$

Then

$$\sigma_{1,H} \otimes T_{1,H} = E \pmod q, \tag{32}$$

$$\xi_{1,H}^{(n)}(f) = q^{m-1}mk - q^{-1}B_f^{(q)}(T_{1,H}). \tag{33}$$

The proof is analogous to that of Theorem 5; to find $\sigma_{1,L}$ one can employ a procedure similar to that used for $\sigma_{1,L}$. The only difference is that $B_f^{(2)}(\tau)$ should be replaced by $B_f^{(q)}(\tau)$ (for Boolean functions, $\sigma_{1,L} = \sigma_{1,H}$).

EXAMPLE 3. Table III defines a function f and the appropriate $B_f^{(3)}$ ($q = 3, m = 2, k = 1$). Using the procedure (27), (28), we have $T_{1,H} = \left(\begin{smallmatrix} 2 & 1 \\ 2 & 2 \end{smallmatrix}\right)$, and then $\sigma_{1,H} = \left(\begin{smallmatrix} 1 & 1 \\ 2 & 1 \end{smallmatrix}\right)$; the corresponding $f\sigma_{1,H}$ is also shown in Table III. In accordance with (33), we have $\xi_{1,H}^{(n)}(f) = \xi_{1,H}(f_{\sigma_{1,H}}) = 4$, whereas $\xi_{1,H}(f) = 6$.

To conclude this section, we generalize the above linearization procedures to the case that q is not a prime.

TABLE III

x, τ	$x^{(0)}$	$x^{(1)}$	f	$B_f^{(3)}$	$f_{\sigma_{1,H}}$
0	0	0	0	9	0
1	0	1	1	0	0
2	0	2	0	0	0
3	1	0	0	0	2
4	1	1	2	3	1
5	1	2	0	3	0
6	2	0	1	0	2
7	2	1	0	3	1
8	2	2	2	3	0

Let R_q denote the ring of residue classes modulo q. In the previous case (q a prime), the σ's were linear operators in an m-dimensional vector space over $GF(q)$; in the case of composite q, they will be linear operators in an m-dimensional vector space over the ring R_q (i.e., in an R_q-module). We know (Lang, 1965) that under these circumstances a matrix σ over R_q is invertible if and only if its determinant $|\sigma|_q$ and q are relatively prime $((|\sigma|_q, q) = 1$, where (a, b) denotes the greatest common divisor of a and $b)$.

Thus, we have $\sigma \in \Xi_q$ if and only if $(|\sigma|_q, q) = 1$. The theorems established above remain valid (except that the relations (27), (28) can no longer be used to find $T_{1,L}$ or $T_{1,H}$).

EXAMPLE 4. We carry out the linearization procedure for the 4-valued logical function defined by Table IV ($q = 4$, $m = 2$, $k = 1$).

The functions $B_f^{(2)}(\tau)$ and $B_f^{(q)}(\tau) = B_f^{(4)}(\tau)$ are also shown in Table IV. Since $G_I(f) = \{(0, 0)\}$, there is no nontrivial linearization with respect to ξ_0. In accordance with Table IV, and (24), (31), we put $T_{1,L} = T_{1,H} = \begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}$ ($T_{1,L} \in \Xi_4$, since $|T_{1,L}|_4 = 3$ and $(3, 4) = 1$).

Then $\sigma_{1,L} = \sigma_{1,H} = \sigma_1 = \begin{pmatrix} 1 & 3 \\ 1 & 2 \end{pmatrix}$. The function f_{σ_1} is shown in Table IV. By (26) and (33), we have $\xi_{1,L}^{(n)}(f) = \xi_{1,L}(f_{\sigma_1}) = 20$, $\xi_{1,H}^{(n)}(f) = \xi_{1,H}(f_{\sigma_1}) = 7$, whereas $\xi_{1,L}(f) = 27$, $\xi_{1,H}(f) = 8$.

For the case of functions of one argument, which is of importance in applications, $\sigma \in \{0, \ldots, q-1\}$, and $\sigma \in \Xi_q$ if and only if $(\sigma, q) = 1$. In this case it is worth noting that linearization with respect to $\xi_{1,L}$ minimizes the number $\sum_{x=0}^{q-1} |f(x) - f(x \ominus 1)| \pmod q$ of discontinuities of the function

TABLE IV

x, τ	$x^{(0)}$	$x^{(1)}$	f	$B_f^{(2)}$	$B_f^{(q)}$	f_{σ_1}
0	0	0	2	16	16	2
1	0	1	1	3	0	1
2	0	2	2	4	0	4
3	0	3	3	3	0	4
4	1	0	3	2	0	2
5	1	1	4	7	4	3
6	1	2	1	3	0	3
7	1	3	4	2	0	3
8	2	0	1	0	0	2
9	2	1	2	5	0	3
10	2	2	4	6	2	1
11	2	3	1	5	0	4
12	3	0	1	2	0	1
13	3	1	3	2	0	1
14	3	2	3	3	0	1
15	3	3	1	7	4	1

$f(x)$; this is useful, for example, when one is calculating $f(x)$ by summation mod q of its finite differences.

$$\Delta_q f(x) = f(x) - f(x \ominus 1) \pmod q.$$

IV. Parallel Linearization of Systems of Logical Functions

We first formulate the parallel linearization problem for the case of greatest practical importance—systems of Boolean functions ($q = 2$).

Given a system $f(x) = \{f^{(i)}(x^{(0)}, \ldots, x^{(m-1)})\}$ $(i = 0, \ldots, k-1)$ of k Boolean functions depending essentially on all their m arguments, let

$$\{l_r(x)\} = \left\{\bigoplus_{s=0}^{m-1} l_r^{(s)} x^{(s)}\right\} \pmod 2 \quad (l_r^{(s)} \in \{0, 1\}, r = 0, \ldots, b-1)$$

be a system of some b linear Boolean functions. If there exist $t_r \in \{0, 1\}$ and $f_{\mathscr{L}}^{(i)}(x)$ such that

$$f^{(i)}(x) = f_{\mathscr{L}}^{(i)}(x) \prod_{r=0}^{b-1} (l_r(x) \oplus t_r) \tag{34}$$

$(\mathrm{mod}\ 2)$ $(i = 0,\ldots, k-1)$, $(x = (x^{(0)},\ldots, x^{(m-1)})$, then we shall call $\mathscr{L}(x) = \prod_{r=0}^{b-1}(\ell_r(x) \oplus t_r)\ (\mathrm{mod}\ 2)$ a parallel linearization for $f(x)$.

A network realizing $f(x)$ may be obtained by connecting in parallel networks implementing the linear functions $\ell_r(x) \oplus t_r\ (\mathrm{mod}\ 2)$ $(r = 0,\ldots, b-1)$ and the nonlinear part $f_{\mathscr{L}}(x)$.

There exists a nontrivial linearization for $f^{(i)}(x)$ if and only if $\sum_x f^{(i)}(x) \leqslant 2^{m-1}$. In order to extend the problem to the case $\sum_x f^{(i)}(x) > 2^{m-1}$, we need only replace the multiplication operation in (34) throughout by logical addition (this follows from the DeMorgan laws).

The linearization $\mathscr{L}_\alpha(x)$ will be called a best linearization with respect to a criterion ξ_α if it minimizes the complexity $\xi_\alpha(f_{\mathscr{L}})$ of the nonlinear part $f_{\mathscr{L}}(x) = \{f^{(i)}_{\mathscr{L}}(x)\}$.

We now generalize the parallel linearization problem to systems $f(x) = \{f^{(i)}(x)\}$ $(i = 0,\ldots, k-1)$ of q-valued logical functions (where q is an arbitrary integer $\geqslant 2$, not necessarily prime), depending essentially on all their m arguments. Let

$$\ell_r(x) = \bigoplus_{s=0}^{m-1} \ell_r^{(s)} x_r^{(s)} \qquad (\mathrm{mod}\ q)\ (\ell_r^{(s)} \in \{0,\ldots, q-1\},\ r = 0,\ldots, b-1)$$

be a system of some b linear q-valued logical functions. Let $\{d_t(\ell_r(x))\}$ $(t = 0,\ldots, q-1)$ denote a system of characteristic functions for $\ell_r(x)$:

$$d_t(\ell_r(x)) = \begin{cases} 1, & \ell_r(x) = t, \\ 0, & \ell_r(x) \neq t \end{cases} \tag{35}$$

(if $q = 2$, we have $d_0(\ell_r(x)) = \ell_r(x) \oplus 1\ (\mathrm{mod}\ 2)$, $d_1(\ell_r(x)) = \ell_r(x)$).

If there exist $t_r \in \{0,\ldots, q-1\}$ and $f^{(i)}_{\mathscr{L}}(x)$ such that

$$f^{(i)}(x) = f^{(i)}_{\mathscr{L}}(x) \prod_{r=0}^{b-1} d_{t_r}(\ell_r(x))\ (i = 0,\ldots, k-1), \tag{36}$$

then $\mathscr{L}(x) = \prod_{r=0}^{b-1} d_{t_r}(\ell_r(x))$ is a parallel linearization for $f(x)$, and we denote

$$f(x) = f_{\mathscr{L}}(x) \cdot \mathscr{L}(x). \tag{37}$$

Our problem is to determine a best linearization with respect to a criterion ξ_α $(\alpha = 0;\ 1, L;\ 1, H)$.

Let $\mathscr{F}_{\mathscr{L}}$ denote the set of systems $f_{\mathscr{L}}(x) = \{f^{(i)}_{\mathscr{L}}(x)\}$ satisfying (37) for given $f(x)$ and $\mathscr{L}(x)$, and

$$\min_{f_{\mathscr{L}} \in \mathscr{F}_{\mathscr{L}}} \xi_\alpha(f_{\mathscr{L}}) = \xi\alpha(\tilde{f}_{\mathscr{L}}). \tag{38}$$

We shall say that a linearization $\mathscr{L}_\alpha$ is best if it minimizes $\xi_\alpha(\tilde{f}_{\mathscr{L}})$. As before, we let $\xi_\alpha^{(n)}(f)$ denote the ξ_α-complexity $\xi_\alpha(\tilde{f}_{\mathscr{L}_\alpha})$ of the nonlinear part for a best linearization $\mathscr{L}_\alpha$.

In constrast to the previous treatment, the solution of the problem will involve not correlation functions but rather spectral characteristics of the system $\{f^{(i)}(x)\}$.

By Theorem 1, the characters of the group $G = G_q{}^m$ are

$$\chi_\omega(x) = \exp\left((2\pi/q)\, j \sum_{s=0}^{m-1} x^{(s)}\omega^{(s)}\right),$$

$$(x = (x^{(0)},\ldots, x^{(m-1)});\quad \omega = (\omega^{(0)},\ldots, \omega^{(m-1)});\quad x^{(s)}, \omega^{(s)} \in \{0,\ldots, q-1\}). \quad (39)$$

Let $\ell_r = (l_r^{(0)},\ldots, l_r^{(m-1)}) \in G$. We stipulate that $\ell_r \in G_{\mathscr{L}}(f)$ if and only if there exist $t_r \in \{0,\ldots, q-1\}$ and $f_{\mathscr{L}}(x) = \{f_{\mathscr{L}}^{(i)}(x)\}$ such that

$$f^{(i)}(x) = f_{\mathscr{L}}^{(i)}(x) \cdot d_{t_r}\left(\bigoplus_{s=0}^{m-1} \ell_r^{(s)} x^{(s)}\right) \pmod q\ (i = 0,\ldots, k-1). \quad (40)$$

Then $G_{\mathscr{L}}(f)$ is a subgroup of G, which we call the linearity group of $f(x) = \{f^{(i)}(x)\}$.

LEMMA 1. *A system $f(x)$ $(x \in G_q{}^m)$ is expressible in the form (40) if and only if*

$$S_{f^{(i)}}(\ell_r) = q^{-m} \exp(-(2\pi/q)\, jt_r) \sum_{x \in G_q{}^m} f^{(i)}(x), \quad (41)$$

where $S_{f^{(i)}}$ is the spectrum of the Fourier expansion of $f^{(i)}(x)$ in terms of characters of $G_q{}^m$.

Proof. In view of (39), we have

$$S_{f^{(i)}}(\ell_r) = q^{-m} \sum_{x \in G_q{}^m} f^{(i)}(x)\, \chi_{\ell_r}(x)$$

$$= q^{-m} \sum_{x \in G_q{}^m} f^{(i)}(x) \exp\left(-(2\pi/q)\, j \bigoplus_{s=0}^{m-1} \ell_r^{(s)} x^{(s)}\right)$$

(mod q) and therefore

$$S_{f^{(i)}}(\ell_r) = q^{-m} \exp(-(2\pi/q)\, jt_r) \sum_{x \in G_q{}^m} f^{(i)}(x)$$

if and only if $\bigoplus_{s=0}^{m-1} \ell_r^{(s)} x^{(s)} = t_r \pmod q$ or $d_{t_r}(\bigoplus_{s=0}^{m-1} \ell_r^{(s)} x^{(s)}) = 1$ for any x such that $f^{(i)}(x) \neq 0$, hence if and only if condition (40) holds.

Lemma 1 provides a simple procedure for constructing the linearity group $G_{\mathscr{L}}(f)$: $l_r \in G_{\mathscr{L}}(f)$ if and only if

$$|S_{f(i)}(\ell_r)| = \max_{\omega \in G_q^m} |S_{f(i)}(\omega)| = S_{f(i)}(0,\ldots,0) = q^{-m} \sum_{x \in G_q^m} f^{(i)}(x)$$

$$(i = 0,\ldots,k-1). \quad (42)$$

Comparing (42) and (20), we see that whereas the maxima of $B_f^{(2)}(\tau)$ defined the inertia group $G_I(f)$ of $f(x)$, the maxima of $\sum_{i=0}^{k-1} |S_{f(i)}(\omega)|$ define the linearity group $G_{\mathscr{L}}(f)$ of $f(x)$. Moreover, if q is a prime, then for any $f^{(i)}(x)$ $(x \in G_q^m)$ the number of points at which $B_{f(i)}^{(2)}(\tau)$ and $|S_{f(i)}(\omega)|$ assume their maximal values is always a power of q; hence we have yet another simple check on the correctness of a calculation of autocorrelation characteristics and spectra.

THEOREM 7. *Let $\ell_0,\ldots,\ell_{b_{\mathscr{L}}(f)-1}$ be an arbitrary basis for the linearity group $G_{\mathscr{L}}(f)$ of $f(x) = \{f^{(i)}(x)\}$ $(x \in G_q^m;\ i = 0,\ldots,k-1)$, and*

$$S_{f(i)}(\ell_r) = q^{-m} \exp(-(2\pi/q) j t_r) \sum_{x \in G_q^m} f^{(i)}(x)$$

$$(r = 0,\ldots,b_{\mathscr{L}}(f)-1; \qquad i = 0,\ldots,k-1). \quad (43)$$

Then

$$\mathscr{L}_0(x) = \mathscr{L}_{1,L}(x) = \mathscr{L}_{1,H}(x) = \prod_{r=0}^{b(f)-1} d_{t_r}\left(\bigoplus_{s=0}^{m-1} \ell_r^{(s)} x^{(s)}\right) \pmod q; \quad (44)$$

$$\xi_0^{(n)}(f) \leqslant m - b_{\mathscr{L}}(f);$$

$$\xi_{1,L}^{(n)}(f) \leqslant \gamma_q k q^{m-b_{\mathscr{L}}(f)}(m - b_{\mathscr{L}}(f)) \quad \left(\gamma_q = \begin{cases} 1, & q > 2 \\ 0.5, & q = 2 \end{cases}\right); \quad (45)$$

$$\xi_{1,H}^{(n)}(f) \leqslant k q^{m-b_{\mathscr{L}}(f)-1}(m - b_{\mathscr{L}}(f)).$$

Proof. It follows from Lemma 1 that

$$\mathscr{L}_{\text{opt}}(x) = \prod_{r=0}^{b_{\mathscr{L}}(f)-1} d_{t_r}\left(\bigoplus_{s=0}^{m-1} \ell_r^{(s)} x^{(s)}\right) \pmod q$$

is a linearization.

Set $x \in \mathscr{L}^{-1}(1)$ if and only if $\mathscr{L}(x) = 1$. Then, by (36), (38), if $\mathscr{L}_1^{-1}(1) \subseteq \mathscr{L}_2^{-1}(1)$, we have $\xi_\alpha(f_{\mathscr{L}_1}) \geqslant \xi_\alpha(f_{\mathscr{L}_2})$ $(\alpha = 0; 1, L; 1, H)$. If $\mathscr{L}(x)$ is a linearization for $f(x)$, then $\hat{\ell}_0,\ldots,\hat{\ell}_{b-1} \in G_{\mathscr{L}}(f)$ and, since $\ell_0,\ldots,\ell_{b_{\mathscr{L}}(f)-1}$ are a basis for

$G_{\mathscr{L}}(f)$, it follows by Lemma 1 that $\hat{\mathscr{L}}^{-1}(1) \subseteq \mathscr{L}_{\text{opt}}^{-1}(1)$, $\xi_\alpha(\tilde{f}_{\hat{\mathscr{L}}}) \geqslant \xi_\alpha(\tilde{f}_{\mathscr{L}_{\text{opt}}})$ and $\mathscr{L}_{\text{opt}}(x)$ is a best linearization ($\alpha = 0; 1, (L; 1, H)$.

We now prove that $\xi_0(\tilde{f}_{\mathscr{L}_{\text{opt}}}) \leqslant m - b_{\mathscr{L}}(f)$, whence the inequalities (45) will immediately follow.

For that we first construct the function $f_{\mathscr{L}_{\text{opt}}}(x)$ satisfying (37) for given $f(x)$, $\mathscr{L}(x) = \mathscr{L}_{\text{opt}}(x)$ and depending essentially on no more than $m - b_{\mathscr{L}}(f)$ arguments.

Consider the following nonsingular system of $b_{\mathscr{L}}(f)$ linear equations over $GF(q)$:

$$\bigoplus_{s=0}^{m-1} \ell_r^{(s)} x^{(s)} = t_r \pmod q \qquad (r = 0,\ldots, b_{\mathscr{L}}(f) - 1).$$

There exist i_s ($s = 0,\ldots, b_{\mathscr{L}}(f) - 1$) such that $x^{(i_s)} = g_s(x^{(0)},\ldots, x^{(m-1)})$ where the g_s are some linear functions over $GF(q)$, each of which is independent of all the arguments $x^{(i_s)}$ ($s = 0,\ldots, b_{\mathscr{L}}(f) - 1$). Furthermore, if $f(x) = f_{\mathscr{L}_{\text{opt}}}(x) \cdot \mathscr{L}_{\text{opt}}(x)$, we substitute the function g_s for $x^{(i_s)}$ in $f_{\mathscr{L}_{\text{opt}}}(x)$ ($s = 0,\ldots, b_{\mathscr{L}}(f) - 1$), to obtain $f'_{\mathscr{L}_{\text{opt}}}(x)$ such that

$$f(x) = f'_{\mathscr{L}_{\text{opt}}}(x) \cdot \mathscr{L}_{\text{opt}}(x),$$

$$\xi_0(f'_{\mathscr{L}_{\text{opt}}}) \leqslant m - b_{\mathscr{L}}(f),$$

and consequently

$$\xi_0^{(n)}(f) = \xi_0(\tilde{f}_{\mathscr{L}_{\text{opt}}}) \leqslant \xi_0(f'_{\mathscr{L}_{\text{opt}}}) \leqslant m - b_{\mathscr{L}}(f).$$

This proves the theorem.

Thus, the linearity group $G_{\mathscr{L}}(f)$ generates all parallel linearizations for the system f, the best parallel linearizations with respect to ξ_0, $\xi_{1,L}$, and $\xi_{1,H}$ coincide, and they may be determined by a procedure involving the following operations:

1. compute the spectral characteristics $S_{f(i)}(\omega)$ ($i = 0,\ldots, k - 1$);
2. using condition (42), construct the linearity group $G_{\mathscr{L}}(f)$;
3. select an arbitrary basis in $G_{\mathscr{L}}(f)$;
4. use formulas (43), (44) to compute the best linearization

$$\mathscr{L}_{\text{opt}} = \mathscr{L}_0 = \mathscr{L}_{1,L} = \mathscr{L}_{1,H}.$$

As before, the most convenient tool for calculation of the spectra $S_{f(i)}$ is the fast Hadamard–Chrestenson transform.

EXAMPLE 5. Table V defines a 3-valued logical function $f(x)$ ($q = 3$, $m = 2, k = 1$) and its spectrum $S_f(\omega)$ (we use the notation $\zeta_1 = \exp(2\pi j/3)$, $\zeta_2 = \exp(4\pi j/3)$). We have $G_{\mathscr{L}}(f) = \{(0, 0), (1, 2), (2, 1)\}$. As a basis we can take, say, the vector (1, 2) ($b_{\mathscr{L}}(f) = 1$). Since $S_f(1, 2) = (5/9)\zeta_1 = 3^{-2} \cdot \exp(-(2\pi/3) j2) \cdot 5$, it follows from Theorem 7 that

$$\mathscr{L}_{\text{opt}}(x) = d_2(x^{(0)} \oplus 2x^{(1)}) \pmod 3$$

and

$$\xi_0^{(n)}(f) \leqslant 1, \qquad \xi_{1,L}^{(n)} \leqslant 3, \qquad \xi_{1,H}^{(n)} \leqslant 1.$$

The functions $d_2(x^{(0)} \oplus 2x^{(1)}) \pmod 3$ and $\tilde{f}_{\mathscr{L}_{\text{opt}}}(x)$ are also shown in Table V. We see from the table that $\xi_0^{(n)}(f) = 1$, $\xi_{1,L}^{(n)}(f) = 2$, $\xi_{1,H}^{(n)} = 1$, whereas $\xi_0(f) = 2$, $\xi_{1,L}(f) = 12$, $\xi_{1,H}(f) = 6$.

TABLE V

x, ω	$x^{(0)}$	$x^{(1)}$	f	$g \cdot S_f$	$d_2(x^{(0)} \oplus 2x^{(1)})$ (mod 3)	$x^{(0)}$	$f_{\mathscr{L}_{\text{opt}}}$
0	0	0	0	5	0	0	2
1	0	1	2	$-\zeta_1$	1	1	1
2	0	2	0	$-\zeta_2$	0	2	2
3	1	0	0	$-\zeta_2$	0		
4	1	1	0	-1	0		
5	1	2	1	$5\zeta_1$	1		
6	2	0	2	$-\zeta_1$	1		
7	2	1	0	$5\zeta_2$	0		
8	2	2	0	-1	0		

We now generalize the parallel linearization procedure to arbitrary commutative groups.

Let $G = G_{q_0} \times \cdots \times G_{q_{m-1}}$, where the group G_{q_s} contains the elements $\{0,..., q_s - 1\}$, q_s is prime ($s = 0,..., m - 1$). Consider a system $\{f^{(i)}(x^{(0)},..., x^{(m-1)})\}$ ($i = 0,..., k - 1$; $x^{(s)} \in \{0,..., q_s - 1\}$). (A system of this type may describe, for example, the operation of networks constructed on elements with a different number of stable states, networks operating in systems of residue classes, and so on.) All the complexity criteria introduced previously may be applied to systems of this class. The definitions of ξ_0 and $\xi_{1,L}$ are entirely analogous to the previous definitions, while $\xi_{1,H}(f^{(i)})$ is the total number of sequences $\{x_0,..., x_{q_s-1}\}$ ($s = 0,..., m - 1$) of argument vectors

which differ only in their sth component and have the property: there exist $\alpha, \beta \in \{0,..., q_s - 1\}$ such that $f(x_\alpha) \neq f(x_\beta)$.

Let Q denote the lowest common multiple of $q_0, ..., q_{m-1}$ and $Q_s = Q/q_s$ $(s = 0,..., m - 1)$. Our class of linear functions in this case will consist of the functions

$$\ell_r(x) = \bigoplus_{s=0}^{m-1} Q_s \ell_r^{(s)} x^{(s)} \pmod{Q}, \text{ where } \ell_r^{(s)} \in \{0,..., q_s - 1\}. \quad (46)$$

The characters of $G = G_{q_0} \times \cdots \times G_{q_{m-1}}$ are, by Theorem 1,

$$\chi_\omega(x) = \exp\left((2\pi/Q) j \sum_{s=0}^{m-1} Q_s x^{(s)} \omega^{(s)}\right) (x^{(s)}, \omega^{(s)} \in \{0, 1,..., q_s - 1\}). \quad (47)$$

Then, as before, the group of linear functions (46) is isomorphic to the multiplicative group of characters (47), and the set of vectors $\ell_r = (\ell_r^{(0)}, ..., \ell_r^{(m-1)})$ for which there exist $t_r \in \{0,..., Q - 1\}$ and $f_{\mathscr{L}}^{(i)}(x)$ such that

$$f^{(i)}(x) = f_{\mathscr{L}}^{(i)}(x) \cdot d_{t_r}\left(\bigoplus_{s=0}^{m-1} Q_s \ell_r^{(s)} x^{(s)}\right) \quad (i = 0,..., k - 1) \pmod{Q} \quad (48)$$

is a linearity subgroup $G_{\mathscr{L}}(f)$ of G; moreover, $\{f^{(i)}(x)\}$ satisfies (48) if and only if

$$S_{f^{(i)}}(\ell_r) = \left(\prod_{s=0}^{m-1} q_s\right)^{-1} \exp(-(2\pi/Q) j t_r) \sum_{x \in G} f^{(i)}(x) \quad (i = 0,..., k - 1), \quad (49)$$

where $S_{f^{(i)}}$ is the spectrum of the expansion of $f^{(i)}$ in terms of characters (47).

Thus, as before, the maximum moduli of the spectra define the linearity group $G_{\mathscr{L}}(f)$. Let $\ell_0, ..., \ell_{b_{\mathscr{L}}(f)-1}$ be an arbitrary basis in $G_{\mathscr{L}}(f)$ (i.e., a maximal set of elements of $G_{\mathscr{L}}(f)$ satisfying the condition: $*_{s=0}^{b_{\mathscr{L}}(f)-1} c^{(s)} \ell_s = (0,..., 0)$ if and only if $c^{(s)} = 0 \pmod{Q}$, where

$$c^{(s)} \ell_s = \underbrace{\ell_s * \cdots * \ell_s}_{c^{(s)}} \text{ and } 0\, l_s = (0,..., 0) \; (s \in (0,..., b_{\mathscr{L}}(f) - 1)),$$

and $*$ denotes the group operation in G).

Then, by analogy with (44),

$$\mathscr{L}_{\text{opt}}(x) = \mathscr{L}_0(x) = \mathscr{L}_{1,L}(x) = \mathscr{L}_{1,H}(x) = \prod_{s=0}^{b_{\mathscr{L}}(f)-1} d_{t_r}\left(\bigoplus_{s=0}^{m-1} Q_s \ell_r^{(s)} x^{(s)}\right) \pmod{Q}. \quad (50)$$

Note that (49) and (50) generalize the results of Lemma 1 and Theorem 7 to arbitrary commutative groups. The spectra may be calculated using the algorithm of the fast Fourier transform for arbitrary finite commutative groups (Apple and Wintz, 1970).

EXAMPLE 6. Let $G = G_2 \times G_2 \times G_3$ ($q_0 = q_1 = 2$, $q_2 = 3$ and $x_1 * x_2 = x_3$ if and only if $x_3^{(0)} = x_1^{(0)} \oplus x_2^{(0)} \pmod 2$, $x_3^{(1)} = x_1^{(1)} \oplus x_2^{(1)} \pmod 2$ and $x_3^{(2)} = x_1^{(2)} \oplus x_2^{(2)} \pmod 3$. Table VI defines a function $f(x)$ ($x \in G$) and its spectrum $S_f(\omega)$ ($\zeta_1 = \exp(2\pi j/3)$, $\zeta_2 = 4\pi j/3$)).

TABLE VI

x, ω	$x^{(0)}$	$x^{(1)}$	$x^{(2)}$	f	$12 \cdot S_f$	$d_1(3x^{(0)} \oplus 3x^{(1)} \oplus 4x^{(2)}) \pmod 6$	$x^{(0)}$	$f_{\mathscr{L}_{\text{opt}}}$
0	0	0	0	0	4	0	0	3
1	0	0	1	0	$4\zeta_2$	0	1	1
2	0	0	2	0	$4\zeta_1$	0		
3	0	1	0	0	-2	0		
4	0	1	1	3	$-2\zeta_2$	1		
5	0	1	2	0	$-2\zeta_1$	0		
6	1	0	0	0	2	0		
7	1	0	1	1	$2\zeta_2$	1		
8	1	0	2	0	$2\zeta_1$	0		
9	1	1	0	0	-4	0		
10	1	1	1	0	$-4\zeta_2$	0		
11	1	1	2	0	$-3\zeta_1$	0		

We have

$$G_{\mathscr{L}}(f) = \{(0, 0, 0), (0, 0, 1), (0, 0, 2)(1, 1, 0), (1, 1, 1), (1, 1, 2)\}.$$

As a basis for $G_{\mathscr{L}}(f)$ we can take, e.g., the vector (1, 1, 2). Since $Q = 6$, $Q_0 = Q_1 = 3, Q_2 = 2$, and $S_f(1, 1, 2) = -\frac{1}{3}\zeta_1 = 12^{-1} \cdot \exp(-(2\pi/6) \cdot j \cdot 1) \cdot 4$, it follows from (42), (50) that $\mathscr{L}_{\text{opt}}(x) = d_1(3x^{(0)} \oplus 3x^{(1)} \oplus 4x^{(2)}) \pmod 6$; $d_1(3x^{(0)} \oplus 3x^{(1)} \oplus 4x^{(2)}) \pmod 6$ and $f_{\mathscr{L}_{\text{opt}}}(x)$ are also given in Table VI. We have $\xi_0^{(n)}(f) = 1$, $\xi_{1,L}^{(n)}(f) = 1$, $\xi_{1,H}^{(n)}(f) = 1$, whereas $\xi_0(f) = 3$, $\xi_{1,L}(f) = 8$, $\xi_{1,H}(f) = 6$.

Finally, we note that by successive application of our procedures for series and parallel linearization of systems of logical functions, one can construct

all the parallel–series networks implementing a given system and containing only one nonlinear block.

RECEIVED: June 6, 1975; REVISED: April 2, 1976

REFERENCES

ANDREWS, H. C. AND CASPARI, K. L. (1970), A generalized technique for spectral analysis, *IEEE Trans. Computers* **C-19**, 16–25.

APPLE, G. AND WINTZ, P. (1970), Calculation of Fourier transforms on finite abelian groups, *IEEE Trans. Information Theory* **IT-16**, 233–234.

BERLEKAMP, E. R. (1968), "Algebraic Coding Theory," McGraw–Hill, New York.

CURTIS, C. W. AND RAINER, I. (1962), "Representation Theory of Finite Groups and Associative Algebras," Halsted, New York/London.

KARPOVSKY, M. G. AND MOSKALEV, E. S. (1967), Realization of a system of logical functions by means of expansion in orthogonal series (in Russian), *Automatika i Telemakehanika* **12**, 119–129.

KARPVSKY, M. G. AND MOSKALEV, E. S. (1970), Utilization of autocorrelation characteristics for the realization of systems of logical functions (in Russian), *Automatika i Telemekhanika* **2**, 243–250.

KARPOVSKY, M. G. AND MOSKALEV, E. S. (1970), Realizations of partially defined functions of algebra of logic by expending in orthogonal series (in Russian), *Automatika i Telemekhanika* **8**, 89–99.

KARPOVSKY, M. G. (1971), Error-correction in automata, whose combinatorial parts are realized by expansion in orthogonal series (in Russian), *Automatika i Telemekhanika* **9**, 204–209.

KARPOVSKY, M. G. AND MOSKALEV, E. S. (1973), "Spectral Methods for Analysis and Synthesis of Digital Devices" (in Russian), Energia, Leningrad.

KARPOVSKY, M. G. (1976), "Finite Orthogonal Series in the Design of Digital Devices," Wiley, New York, IUP Press, Jerusalem.

KITAHASHI, T. AND TANAKA, K. (1972), Orthogonal expansion of many-valued logical functions and its applications to the realization with a single threshold element, *IEEE Trans. Computers* **C-21**, No. 2, short notes.

LANG, S. (1965), "Algebra," Addison–Wesley, New York.

LECHNER, R. Y. (1971), Harmonic analysis of switching functions, *in* "Recent Developments in Switching Theory" (A. Makhopadhyay, Ed.), Academic Press, New York.

NECHIPORUK, E. I. (1963), On synthesis of gating circutes (in Russian), *Problemy Kibernetiki* **9**.

POSPELOV, D. A. (1968), "Logical Methods of Analysis and Synthesis of Networks" (in Russian), Energia, Moscow.

SHOLOMOV, L. A. (1966), Criteria for complexity of Boolean functions (in Russian), *Problemy Kibernetiki* **17**

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