SPECTRAL METHODS FOR DECOMPOSITION, DESIGN AND TESTING OF MULTIPLE-VALUED LOGICAL NETWORKS*

Keynote paper at International Symposium on Multiple-valued Logic 1981

#32

M. Karpovsky
Computer Science Department
State University of New York
Binghamton, N. Y. 13901

In this paper we survey some new theoretical results on spectral methods for functional decomposition, synthesis and testing of multiple-valued (M-V) logical networks with many inputs and many outputs. In Section I we summarize the basic properties of spectral and correlation characteristics for M-V functions. These characteristics are widely used in spectral methods of decomposition, synthesis and testing for M-V networks. Section II is devoted to spectral methods for synthesis of M-V networks. In Section III we introduce several complexity criteria for systems of M-V functions. These criteria are used in Section IV for the solution of the problem of optimal linearization for systems of M-V functions. Section V is devoted to spectral methods for synthesis of reliable information transmission and processing systems. Spectral methods for testing of M-V networks are considered in Section VI. Advantages and limitations of spectral methods are discussed in Section VII. For the proofs, examples and applications the reader is referred to [1,2,6,7,8,9,10].

I. Basic Properties of Spectral and Correlation Characteristics for Multiple-Valued Logical Functions

Let

$$y^{(s)} = f^{(s)}(z^{(0)},\ldots,z^{(m-1)}) \quad (s=0,\ldots,K-1;\ y^{(s)},z^{(s)}\in\{0,1,\ldots,p-1\}) \quad (1)$$

be a system of K p-valued logical functions. We shall represent the system(1) as

$$y=f(Z) \quad \text{where } Z=\sum_{s=0}^{m-1} z^{(s)}\,p^{m-1-s},$$

$$y=\sum_{s=0}^{K-1} y^{(s)}\,p^{K-1-s}$$

$$(Z\in\{0,1,\ldots,\ p^m-1\}). \quad (2)$$

Let G be the group of all p-ary m-dimensional vectors with respect to componentwise addition modulo p.

D1: Any homomorphism of G into the multiplicative group of nonzero complex numbers is called a character of G or a generalized Walsh function or a Chrestenson function. [1,§1.3;2.]

The Chrestenson functions $\chi_\omega(Z)$ may be defined by the formula

$$\chi_\omega(Z) = u^{\langle\omega,Z\rangle}, \text{ where}$$

$$u=\exp\left(\frac{2\pi i}{p}\sqrt{-1}\right) \text{ and } \langle\omega,Z\rangle=\sum_{s=0}^{m-1} z^{(s)}\omega^{(m-1-s)}. \quad (3)$$

* This work was partially supported by the Division of Mathematical and Computer Sciences of the National Science Foundation under Grant No. MCS-8008339.

0195-623X/81/0000/0001$00.75 © 1981 IEEE

(We shall use the same letter represent a real number and a vector of its p-ary representation.)

The wide use of Chrestenson functions in the analysis and synthesis of multiple-valued logical networks [1-3,12,13], is partly due to some remarkable properties of these functions. We shall summarize below the most important properties of Chrestenson functions [1,§1;3].

1) Completeness and Orthogonality

For any two functions f(Z) and $\psi(Z)$ $(Z\in\{0,\ldots,N-1;N=p^m\})$ let

$$\langle f,\psi\rangle=\sum_{Z=0}^{N-1} f(Z)\psi(Z). \quad (4)$$

T.1 The set of Chrestenson functions is a complete orthogonal system

$$N^{-1}\langle\chi_t,\overline{\chi_q}\rangle=\delta_{t,q} \quad (5)$$

(where $\delta_{t,q}$ the Kronecker delta),

and $\overline{\chi_q(Z)}$ is the complex conjugate of $\chi_q(Z)$).

If f(Z) represents a system of p-valued functions of m arguments such that

$$\langle f,\chi_t\rangle=0 \qquad (t=0,\ldots,N-1), \quad (6)$$

then f(Z)=0 for all $Z\in\{0,\ldots,N-1\}$.

2) Finiteness of Representing Series

T.2 Let f(Z) represent a system of p-valued functions of m arguments. Then

$$f(Z)=\sum_{\omega=0}^{N-1}\hat{f}(\omega)\,\chi_\omega(Z) \quad (N=p^m), \quad (7)$$

where

$$\hat{f}(\omega)=N^{-1}\langle f,\overline{\chi_\omega}\rangle. \quad (8)$$

D2: We shall call $\hat{f}(\omega)$ the spectrum of f(Z) and ω the generalized frequency.

Many problems in analysis, synthesis and testing of multiple-valued networks may be simplified by changing from the original domain Z to the generalized frequency domain ω. Some of these problems will be discussed later in this paper.

3) Symmetry of Index and Argument

T.3 For any $\omega, Z\in\{0,\ldots,N-1\}$

$$\chi_\omega(Z)=\chi_Z(\omega). \quad (9)$$

4) Translation of Arguments

T.4 For any $\omega,Z \in \{0,\ldots,N-1\}$

$$\chi_\omega(Z \oplus \tau) = \chi_\omega(Z)\ \chi_\omega(\tau)\ . \qquad (10)$$

where $\oplus$ stands for componentwise addition mod p of m-dimensional p-ary vectors.

5) Isomorphism between Linear p-valued Functions and the Chrestenson Functions

D3: A p-valued logical function $f(Z)=f(Z^{(0)},\ldots,Z^{(m-1)})$ is linear if there exist $C_0,\ldots,C_{m-1} \in \{0,\ldots,p-1\}$ such that

$$f(Z^{(0)},\ldots,Z^{(m-1)}) = \bigoplus_{s=0}^{m-1} C_s Z^{(s)} \pmod p. \qquad (11)$$

The linear functions form a commutative group of order $N=p^m$ with respect to addition mod p.

T.5 The multiplicative group of Chrestenson functions is isomorphic to the group of linear p-valued logic functions. The isomorphism h is defined by

$$h(\chi_\omega(Z)) = \bigoplus_{s=0}^{m-1} \omega^{(m-1-s)} Z^{(s)} \pmod p. \qquad (12)$$

We shall describe now the basic properties of the Chrestenson transform $f \leftrightarrow \hat{f}$ which is also known as the Fourier transform over G [1,§1.4].

1) Linearity

T.6 Let

$$f(Z) = \sum_{i=1}^{s} a_i f_i(Z), \qquad (13)$$

where the a_i are arbitrary real numbers. Then

$$\hat{f}(\omega) = \sum_{i=1}^{s} a_i \hat{f}_i(\omega)\ . \qquad (14)$$

2) Translation of Arguments

T.7 Let $\psi(Z) = f(Z \ominus \tau)$ for some $\tau \in \{0,\ldots,N-1\}$, where $\ominus$ stands for componentwise subtraction mod p, then

$$\hat{\psi}(\omega) = \bar{\chi}_\tau(\omega)\ \hat{f}(\omega). \qquad (15)$$

3) Involution Theorem

T.8 We have

$$\hat{\hat{f}}(Z) = N^{-1} f(Z). \qquad (16)$$

4) Convolution Theorem

Let $(f_1 * f_2)(\tau) = \sum_{Z=0}^{n-1} f_1(Z)\ f_2(\tau \ominus Z)$.

T.9 We have

$$\widehat{f_1 \cdot f_2} = \hat{f}_1 * \hat{f}_2, \text{ and} \qquad \widehat{f_1 * f_2} = \hat{f}_1 \cdot \hat{f}_2. \qquad (17)$$

5) Linear Transformation of the Input Space

Let p be a power of ,a prime, and let $\sigma = (\sigma_{is})$ $(i,s=0,\ldots,m-1)$ be a matrix over GF(p) with non-vanishing determinant.

Let $\sigma \otimes Z$ be the product of σ with a p-ary m-dimensional column-vector Z and let σ^{-1} be the inverse of σ (all arithmetical operations are modulo p).

T.10 Let $f_\sigma(Z) = f(\sigma \otimes Z)$. Then

$$\hat{f}_\sigma(\omega) = \hat{f}(\overleftarrow{\omega \otimes \sigma^{-1}}), \qquad (18)$$

where if $\omega = (\omega^{(0)}, \omega^{(1)},\ldots, \omega^{(m-1)})$, then $\overleftarrow{\omega} = (\omega^{(m-1)}, \omega^{(m-2)},\ldots,\omega^{(0)})$.

6) Plancherel Theorem

T.11 We have

$$N^{-1} \langle f_1, f_2 \rangle = \langle \bar{\hat{f}}_1, \hat{f}_2 \rangle. \qquad (19)$$

7) Poisson Summation Theorem

T.12 Let V be a subspace of a G, considered as a vector space over GF(p), and let $V^\perp$ be the subspace orthogonal to V. Then

$$|V|^{-1} \sum_{Z \in V} f(Z) = \sum_{\omega \in V^\perp} \hat{f}(\omega)\ , \qquad (20)$$

where $|V|$ is the cardinality of V.

The Poisson summation formula (20) is widely used in the theory of non-binary error-correcting codes [11,Ch.5].

Some additional properties of the Chrestenson transform may be found in [12] and for p = 3 in [13].

For the solution of design problems for multiple-valued logical networks implementing f(Z) we shall use not only the spectrum $\hat{f}(\omega)$ but also the logical correlation functions $B(\tau)$, which we shall define now.

D4: The cross-correlation function $B^{(2)}_{f_1,f_2}(\tau)$ for functions $f_1,f_2: G \to \{0,\ldots,p^K-1\}$ is defined by

$$B^{(2)}_{f_1,f_2}(\tau) = \sum_{Z=0}^{N-1} f_1(Z)\ f_2(Z \ominus \tau). \qquad (21)$$

The next theorem [1, §1.5] will show the relationship between the cross-correlation function and the Chrestenson transform. This relationship is similar to the representation of the classical correlation functions as the double Laplace transform of the original functions (the Wiener-Khinchin theorem in the theory of stechastical processes [20]).

T.13 We have $B^{(2)}_{f_1,f_2} = N\ \hat{f}_1\ \bar{\hat{f}}_2$. (22)

D5: If $f_1 = f_2 = f$, then the function $B^{(2)}_{f,f}(\tau) = B^{(2)}_f(\tau)$ is known as the logical autocorrelation function.

We now proceed to generalize this concept.

Consider the system of autocorrelation functions:

$$B_f^{(t)}(\tau) = \sum_{Z=0}^{N-1} f(Z)\, f(Z \oplus \tau) \ldots f(Z\underbrace{\oplus\tau\oplus\ldots\oplus\tau}_{t}) = \sum_{Z=0}^{N-1} \prod_{i=0}^{t} f(Z \oplus i\tau). \qquad (23)$$

The function $B_f^{(t)}(\tau)$ may be viewed as the cross-correlation function of $f(Z)$ and its $t-1$ successive translations on G. We now describe its main properties [6].

T.14 (i)

$$\text{We have } B_f^{(t)}(0) = \sum_{Z=0}^{N-1} f(Z). \qquad (24)$$

(ii) Evenness Relation

For any $\tau=(\tau^{(0)},\ldots,\tau^{(m-1)})$ define $\tau^{-1} =$

$$(p-1-\tau^{(0)},\ldots,p-1-\tau^{(m-1)}).$$

Then

$$B_f^{(t)}(\tau^{-1}) = B_f^{(t)}(\tau). \qquad (25)$$

(iii) Translation of Arguments

Let $\psi(Z) = f(Z \oplus \alpha)$. Then

$$B_\psi^{(t)}(\tau) = B_f^{(t)}(\tau). \qquad (26)$$

(iv) Linear Transformation of the Input Space

Let $f_\sigma(Z) = f(\sigma \oplus Z)$. Then

$$B_{f_\sigma}^{(t)}(\tau) = B_f^{(t)}(\sigma \oplus \tau). \qquad (27)$$

The spectral and correlation characteristics described above are widely used in spectral methods of analysis, synthesis and testing of multiple-valued networks. To calculate the spectrum one can use the very efficient algorithm of the fast Chrestenson transform [14; 2; 1,§1.3]. This algorithm requires for a system of p-ary functions of m arguments $m \cdot p^m$ arithmetical operations and p^m memory cells. To calculate the correlation functions $B^{(2)}_{f_1,f_2}$ one can use the fast Chrestenson transform and T.13.

To conclude this section, we note that calculations of spectral and correlation characteristics utilize operations over the field of complex numbers. However, all of the results above may be easily generalized to the case when the operations are defined over finite fields [1,§1.6].

II. Spectral Methods for Synthesis of Multiple-Valued Logical Networks

Let $f(Z)$ represent a system $\{f^{(s)}(Z)\}$ of K p-ary logical functions of m arguments (see (1), (2)). Based on the Chrestenson expansion (7) of $f(Z)$, we can set up a block-diagram of a device implementing $\{f^{(s)}(Z)\}$, as illustrated in Fig. 1.

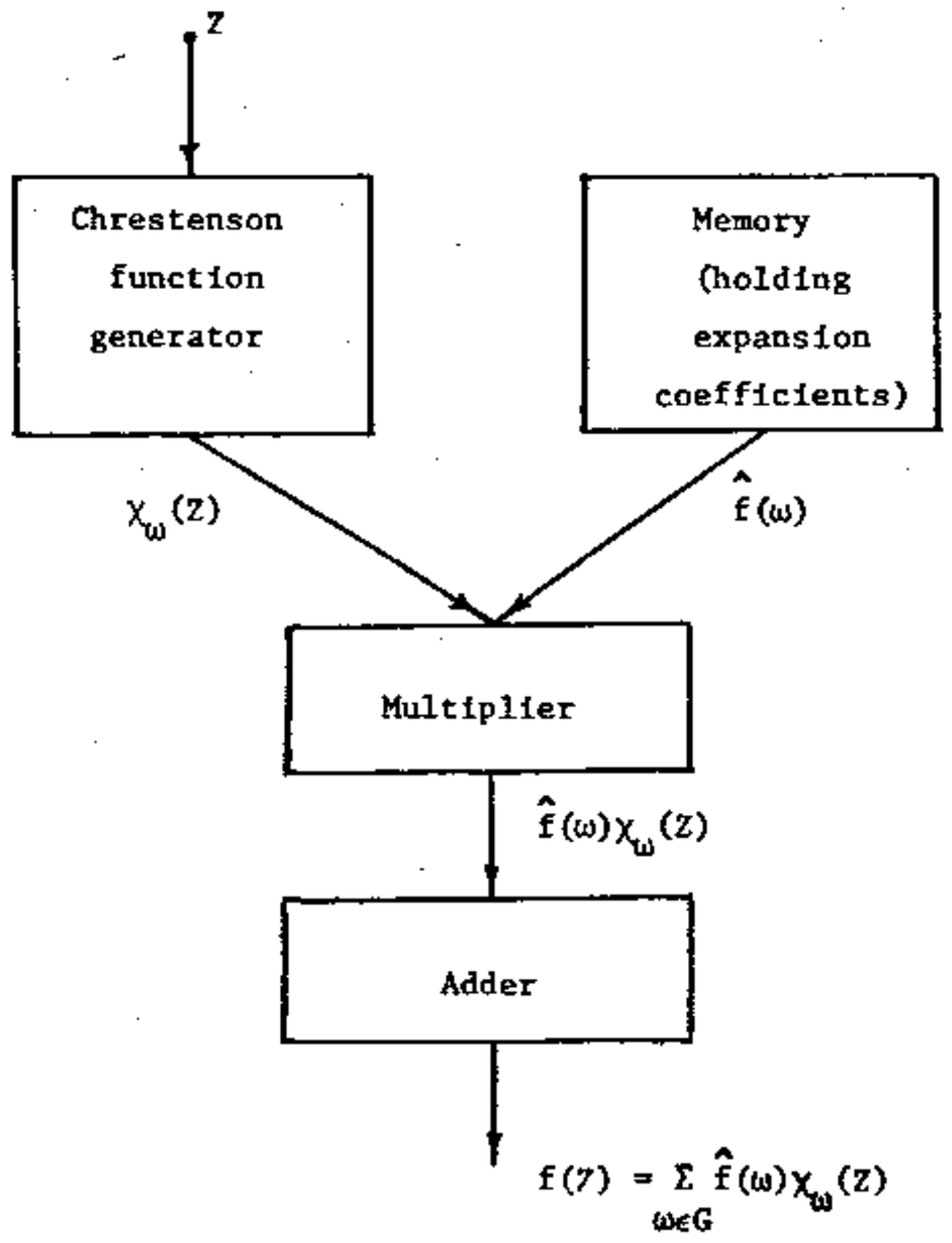


Fig. 1 Block-diagram of a device implementing a system of multiple-valued logical function

In view of the isomorphism between the Chrestenson and linear functions, the Chrestenson function generator in Fig. 1 may be implemented using only elements for two-input addition and multiplication by constants mod p.

The summation of terms in expansion (7) may be implemented sequentially or in parallel. The following theorem [1,§3.4] provides us with the complexity estimations for the parallel Chrestenson functions generator.

T.15

Let $L^{(p)}_{\oplus}(m)$ be the minimal number of two-input mod p adders necessary to implement all Chrestenson functions $\{\chi_\omega(Z)\}$ $(\omega=0,\ldots,p^m-1)$. Then

$$L^{(p)}(m) = p^m - (p-1)\, m-1. \qquad (28)$$

The complexity of the memory block in Fig. 1 depends on the number $L(f)$ of nonzero coefficients $\hat{f}(\omega)$ in the expansion (7) of $f(Z)$. Thus, the proposed approach will be efficient for small $L(f) = |\{\omega \mid \hat{f}(\omega)\neq 0\}|$. To estimate $L(f)$ we introduce

the notion of the inertia group (group of symmetries) for the given f(Z):

$$G_I(f) = \{x \in G \mid f(Z \theta x) = f(Z),\ \forall Z \in G\}. \tag{29}$$

T.16[6]

We have

$$L(f) \le p^m / |G_I(f)| \ . \tag{30}$$

We can use autocorrelation functions to construct the inertia group $G_I(f)$. First, we construct the following system of characteristic functions for the given $f(Z) = \{f^{(s)}(Z)\}$.

$$\text{Define } f_i^{(s)}(Z) = \begin{cases} 1, & f^{(s)}(Z)=i; \\ 0, & f^{(s)}(Z)\neq i. \end{cases} \quad (i=0,\dots,p-1;s=0,\dots,K-1) \tag{31}$$

Let $B_{i,s}^{(2)}$ be the autocorrelation function of $f_i^{(s)}(Z)$ (see (21)) and $B^{(2)}(\tau)$ be the total autocorrellation function of f(Z):

$$B_f^{(2)}(\tau) = \sum_{i,s} B_{i,s}^{(2)}(\tau) = \sum_{i,s} \sum_{Z=0}^{N-1} f_i^{(s)}(Z) f_i^{(s)}(Z \theta \tau) \pmod p. \tag{32}$$

T.17[6]

For any system of K p-ary logical functions of m arguments $\tau \in G_I(f)$ iff

$$B_f^{(2)}(\tau) = \max_{\tau \in G} B_f^{(2)}(\tau) = B_f^{(2)}(0) = K \cdot p^m. \tag{33}$$

To conclude this section we note again that the application of the block-diagram in Fig. 1 is useful in case f(Z) has a large group of symmetries $G_I(f)$.

III. Complexity Criteria of Multiple-Valued Logical Functions

In this section we shall introduce the complexity criteria which will be used later for the functional decomposition of systems of multiple-valued logical functions. These criteria were used in [1,2,6] and also in [3,4,15] for the case of p=2. Of course, these are not the only possible criteria; our choice is dictated primarily by considerations of computational simplicity. We note also that the complexity criteria we are going to introduce describe the so called "abstract" complexity of systems of multiple-valued logical functions rather than the complexity of a realization of the corresponding networks based on some specific technology. Some relationships between abstract complexity and realization complexity were discussed in [16]. The complexity of a system $f(Z) = \{f^{(s)}(Z^{(0)},\dots,Z^{(m-1)})\}$ is defined as the sum of the complexities of the functions entering into the system.

The simplest and most natural complexity criterion for a p-valued logical function $\psi(Z^{(0)},\dots Z^{(m-1)})$ is the number $\xi_0(\psi)$ of arguments on which ψ depends essentially (ψ depends essentially on $Z^{(i)}$ iff there exists $\alpha,\beta \in \{0,\dots,p-1\}$ such that for some $(Z^{(0)},\dots,Z^{(i-1)},Z^{(i+1)},\dots,Z^{(m-1)})$ we have

$$\psi(Z^{(0)},\dots,Z^{(i-1)},\alpha,Z^{(i+1)},\dots,Z^{(m-1)}) \neq \psi(Z^{(0)},\dots,Z^{(i-1)},\beta,Z^{(i+1)},\dots,Z^{(m-1)}).$$

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

We now introduce two more criteria, ξ_L and ξ_H, arising from two different metrizations of G. We shall use two widely used metrics [11]: the Lee metric $d_L(Z_1,Z_2)$ and the Hamming metric $d_H(Z_1,Z_2)$ $(Z_i=(Z_i^{(0)},\dots,Z_i^{(m-1)});\ i=1,2;\ Z_i^{(s)} \in \{0,\dots,p-1\})$:

$$d_L(Z_1,Z_2) = \sum_{i=0}^{m-1} |Z_1^{(i)}-Z_2^{(i)}|, \quad |Z_1^{(i)}-Z_2^{(i)}| \equiv^{+} (Z_1^{(j)}-Z_2^{(j)}) \pmod p \tag{34}$$
$$(0 \le |Z_1^{(i)} - Z_2^{(i)}| \le 0.5p);$$

$$d_H(Z_1,Z_2) = \sum_{i=0}^{m-1} d_H(Z_1^{(i)},Z_2^{(i)}), \quad d_H(Z_1,Z_2) = \begin{cases} 1, & Z_1^{(i)} \neq Z_2^{(i)}, \\ 0, & Z_1^{(i)} = Z_2^{(i)}. \end{cases} \tag{35}$$

We introduce the following notations:

(i) $\xi_L(\psi)$ is the number of pairs $\{Z_1,Z_2\}$ such that $d_L(Z_1,Z_2) = 1$ and $\psi(Z_1) \neq \psi(Z_2)$.

(ii) $\xi_H(\psi)$ is the number of p-tuples $\{Z_1,Z_2,\dots,Z_p\}$ such that $d_H(Z_i,Z_j)=1$ $(i,j=1,\dots,p;i\neq j)$ and and there exist $\alpha,\beta \in \{1,\dots,p\}$ such that $\psi(Z_\alpha) \neq \psi(Z_\beta)$.

We shall use the criteria ξ_0, ξ_L and ξ_H for the solution of decompcsition problems in the next section.

IV. Linearization of Systems of Multiple-Valued Logical Functions

Let $f(Z) = \{f^{(s)}(Z)\}$ represent a system of K p-valued logical functions each of which depends essentially on all m arguments. We first assume that p is a power of a prime.

Let $\sigma=(\sigma_{ij})$ $(\sigma_{ij} \in \{0,\dots,p-1\})$ be a nonsingular $(m\times m)$ matrix over GF(p). We construct a system $\{f_\sigma^{(s)}(Z)\}$ as follows:

$$f_\sigma^{(s)}(\sigma \theta Z) = f^{(s)}(Z) \pmod p \quad (s=0,\dots,K-1). \tag{36}$$

Formula (36) generates a scheme for synthesis of a device implementing the system $\{f^{(s)}(Z)\}$ by serial connection of two blocks: linear σ and nonlinear

$\{f_\sigma^{(s)}\}$. The linear block σ may be implemented using only adders mod p and multipliers by constants mod p.

The following theorem [1,§3.4] provides us with the complexity estimations of the linear part σ.

T.18

Let $L_\sigma^{(p)}(m)$ denote the minimum number of two-input adders and multipliers by constants mod p necessary to design a linear network realizing any $(m\times m)$-matrix σ.

Then for $m\to\infty$,

$$L_\sigma^{(p)}(m) \sim \frac{m^2}{\log_p m}. \qquad (37)$$

Since the nonlinear part $f_\sigma = \{f_\sigma^{(s)}\}$ has "almost always" an exponential complexity[6], we shall try to minimize the complexity of that nonlinear part f_σ.

Thus, the problem of linearization with respect to a criterion ξ_i may be formulated as follows:

Given a system $f(Z)$, find a nonsingular matrix σ_i such that

$$\min_\sigma \xi_i(f_\sigma) = \xi_i(f_{\sigma_i}). \qquad (38)$$

We denote by η_i the complexity $\xi_i(f_{\sigma_i})$ of the nonlinear part for the best linearization σ_i.

T.19[6]

Let T_0 be a matrix whose set of columns contains some basis for the inertia group $G_I(f)$ of the given system $f(Z)$ (see (29)). Then

$\sigma_0 \theta T_0 = E \pmod p$, where E is the $(m\times m)$ identity matrix, and (39)

$$\eta_0 = K\,(m - \log_p |G_I(f)|). \qquad (40)$$

Thus, in view of T.17 and T.19 linearization with respect to ξ_0 reduces to the following operations:

1. Construct by (31), (32) the total autocorrelation function $B_f^{(2)}(\tau)$.

2. Using the maxima of $B_f^{(2)}(\tau)$, construct by T.17 the inertia group $G_I(f)$.

3. Select an arbitrary basis in $G_I(f)$.

4. Construct a nonsingular matrix T_0 whose set of columns contain the basis of $G_I(f)$ chosen in step 3 and invert T_0 over GF(p).

The class of systems of p-valued logical functions possessing a nontrivial linearization with respect to ξ_0 is relatively small. We therefore proceed to linearization with respect to ξ_L based on the Lee metric.

If $B_f^{(2)}(\tau)$ is the total autocorrelation function for $f(Z)$ (see (31), (32)) and $\tau_0,\ldots,\tau_{m-1}\in G$ are linearly independent over GF(p), we denote by T the $(m\times m)$ matrix with columns $\tau_0,\ldots,\tau_{m-1}$ and

$$B_f^{(2)}(T) = \sum_{i=0}^{m-1} B_f^{(2)}(\tau_i). \qquad (41)$$

T.20[6]

Let

$$\max_T B_f^{(2)}(T) = B_f^{(2)}(T_L). \qquad (42)$$

Then

$$\sigma_L \theta T_L = E \pmod p, \qquad (43)$$

and for $p>2$ $\eta_L = (p^m m K - B_f^{(2)}(T_2))$. (44)

To conclude the discussion for ξ_H, based on the Hamming metric.

Given a system $f(Z) = \{f^{(s)}(Z)\}$ we construct the characteristic functions $f_i^{(s)}(Z)$ (see (31)) and the total autocorrelation function $B_f^{(p)}(\tau)$ where

$$B_f^{(p)}(\tau) = \sum_{i,s} B_{i,s}^{(p)}(\tau) = \sum_{i,s}\sum_{Z\in G} f_i^{(s)}(Z) f_i^{(s)}(Z\theta\tau)\ldots f_i^{(s)}(Z\theta\underbrace{\tau\theta\ldots\theta\tau}_{p-1}), \qquad (45)$$

and, if $\tau_0,\ldots,\tau_{m-1}\in G$, then $B_f^{(p)}(T) = \sum_{i=0}^{m-1} B_f^{(p)}(\tau_i)$.

T.21[6]

Let

$$\max_T B_f^{(p)}(T) = B_f^{(p)}(T_H). \qquad (46)$$

Then

$$\sigma_H \theta T_H = E \pmod p, \qquad (47)$$

and

$$\eta_H = p^{m-1} mK - p^{-1} B_f^{(p)}(T_H). \qquad (48)$$

A simple algorithm for the construction T_L satisfying (42) (or T_H satisfying (46)) is given in[6].

We note that the theorems established above may be easily generalized to the case when p is not a power of a prime. In this case matrices T_0, T_L and T_H have to satisfy the condition $(\mathrm{Det}\ T_i, p) = 1$ $(i=0,L,H$; (a,b) is the greatest common divisor of a and b and $\mathrm{Det}\ T_i$ is the determinant of T_i[6]).

Let us consider now the case of p-valued

functions of one argument. To implement a function $f(Z)$, $Z\in\{0,1,\ldots,p-1\}$, one can use adder-accumulator Σ mod p for the summation of its finite differences (see Fig. 2) [4,6].

$$\Delta f(Z) = f(Z) \ominus f(Z\ominus 1) \pmod p. \qquad (49)$$

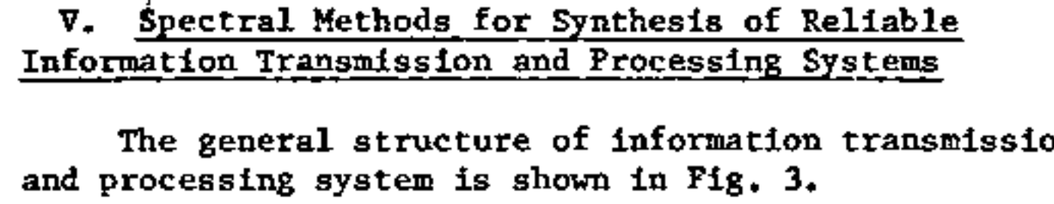


Fig. 2 Implementation of multiple-valued logical functions based on finite differences

In this case $T_i\in\{0,\ldots,p-1\}$, $(T_i,p)=1$ $(i=0,L,H)$, and linearization with respect to ξ_L minimizes the number of discontinuities of $f(Z)$ (or the number of nonzero values of $\Delta f(Z)$).

To conclude this section we note that the linearization defined by (36) results in the serial connection of linear and nonlinear blocks. Methods for the construction of optimal linearizations with respect to criteria ξ_0, ξ_L and ξ_H in the case of parallel connection of linear and nonlinear blocks are given in [1,§2.6; 6].

V. Spectral Methods for Synthesis of Reliable Information Transmission and Processing Systems

The general structure of information transmission and processing system is shown in Fig. 3.

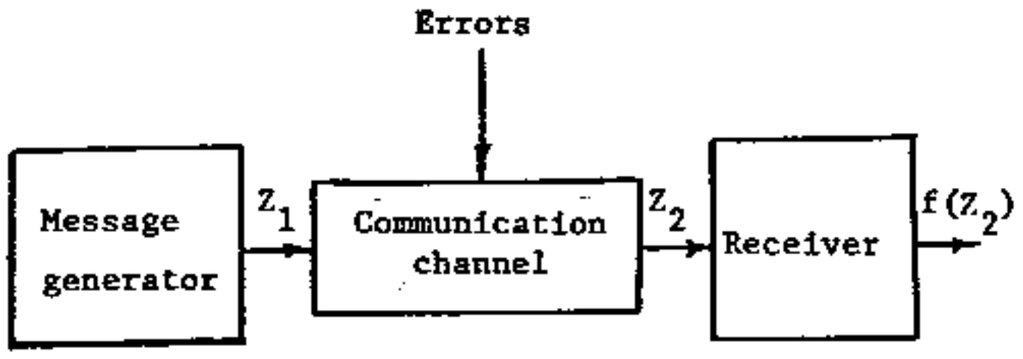


Fig. 3 Block diagram of an information transmission and processing system

The message generator produces information in the form of p-ary vectors $(Z^{(0)},\ldots,Z^{(m-1)})$. This information may be distorted because of errors in the communication channel or in the message generator itself; it then proceeds to the input of the receiver. We shall consider parallel transmission, i.e. all components $Z^{(i)}$ $(i=0,\ldots,m-1)$ reach the receiver input simultaneously, and the receiver itself is a p-valued logical network without memory which may be described by $f(Z)=\{f^{(s)}(Z)\}$ $(s=0,\ldots,K-1)$.

Two types of errors may appear in the communication channel, namely Lee errors and Hamming errors [11]. We shall say that there exists a Lee (Hamming) error with multiplicity t in the channel iff as a result of an error the transmitted message Z_1 is replaced by Z_2 and $d_L(Z_1,Z_2)=t$ $(d_H(Z_1,Z_2)=t)$ where d_L (d_H) is the Lee (Hamming) metric (see (34), (35). The probability of either type of error, Lee or Hamming, depends on the physical representation (i.e. type of modulation) of the transmitted signal Z_1 [11].

In this section we shall consider the most important case from the practical point of view, of single errors (t=1). The reliability of the system represented in Fig. 3 may be increased by using sophisticated methods from the theory of p-ary error-correcting codes [11]. The information $Z=(Z^{(0)},\ldots,Z^{(m-1)})$ is then transmitted in a redundant code and quite complex encoders and decoders are needed.

We shall use a different approach based on the fact that some errors may be corrected by the system represented in Fig. 3 without any redundancy, since any device implementing $f(Z)=\{f^{(s)}(Z)\}$ will correct an error $\{Z_1,Z_2\}$ if $f(Z_1)=f(Z_2)$.

In order to increase the reliability of the entire transmission and processing system we shall linearize $f(Z)$. This will result in the replacement of the original system by the system represented in Fig. 4.

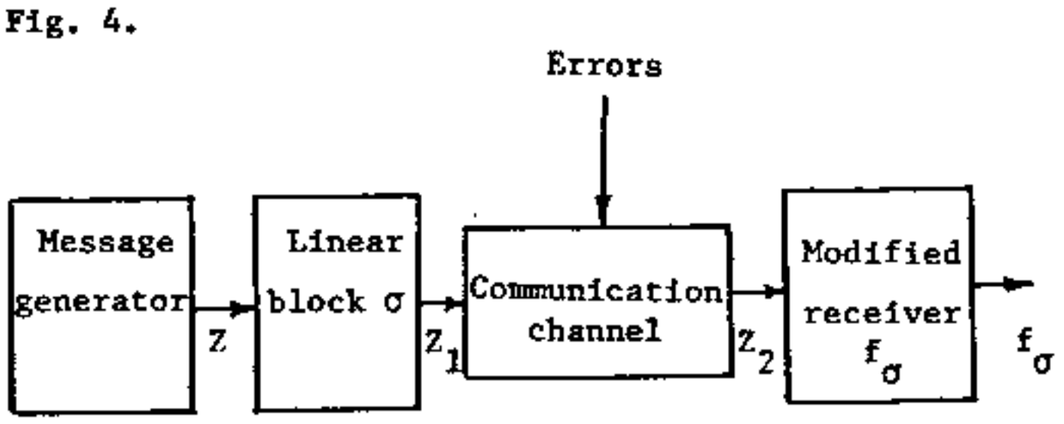


Fig. 4 Modified data transmission and processing system, $Z_1=\sigma\ominus Z$, $f_\sigma(\sigma\ominus Z)=f(Z)\pmod p$

Our problem is now to determine a matrix σ_{opt} minimizing the number of single Lee or Hamming errors uncorrected by the modified receiver f_σ.

Denote by α_L (α_H) the minimal number of Lee (Hamming) errors uncorrected by the modified receiver.

T.22 [1,§5.2; 6]

(i) For Lee errors

$$\sigma_{opt}=\sigma_L \text{ and } \alpha_L=B^{(2)}_f(T_L), \qquad (50)$$

where σ_L and T_L are defined by T.20.

(ii) For Hamming errors

$$\sigma_{opt}=\sigma_H \text{ and } \alpha_H=0.5\,(p-1)\,B^{(p)}_f(T_H), \qquad (51)$$

where σ_H and T_H are defined by T.21.

We note also that T.20, T.21 and T.22 illustrate the relationship between the concepts of complexity of systems of p-valued logical functions with respect to the criteria ξ_L and ξ_H and error-correcting capability of a device implementing these functions.

VI. Testing of Multiple-Valued Logical Networks

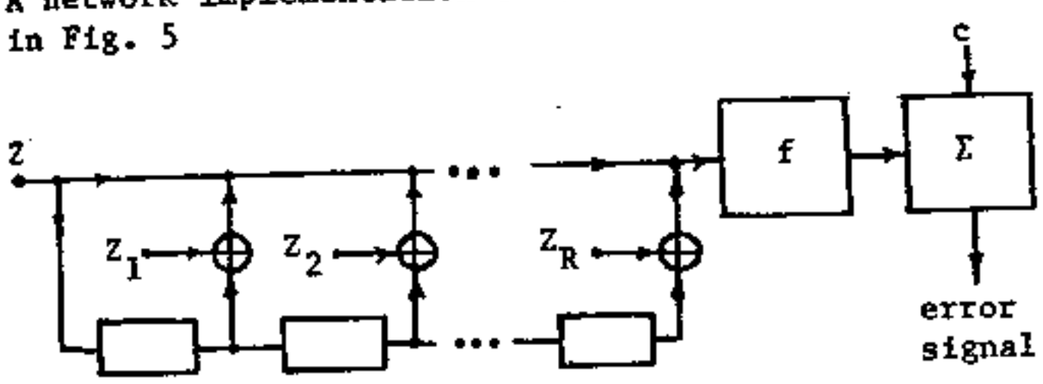
The problem of testing of multiple-valued networks was considered in [7,8,9,10,17,18]. We shall consider in this section the spectral approach to

to this problem. Details and proofs can be found in [7,8,9,10].

Suppose we are given a device computing $f(Z)=\{f^{(s)}(Z^{(0)},\ldots,Z^{(m-1)})(Z^{(i)}\in\{0,\ldots,p-1\})$. By errors in this device we mean catastrophic structural failures. To detect errors, one can compute $f(Z)$ for all $Z\in\{0,1,\ldots,p^m-1\}$ and then verify that $\sum_{Z\in G} f(Z)$ is equal to the given constant C. This method is used for the binary case[19] but usually it is very time-consuming. In this section we shall discuss another method of error detection, and error correction, according to which, given f one determines $Z_1,\ldots,Z_R\in G$ and constant C such that $T=\{Z_1,\ldots,Z_R\}$ is subgroup in G and

$$\sum_{i=1}^{R} f(Z\oplus Z_i)=C \pmod p \text{ for any } Z\in G. \qquad (52)$$

A network implementation of this method is illustrated in Fig. 5



delay element ;

Z
x
y
element for componentwise addition mod p ($Z = x \oplus y \pmod p$);

f
p-ary logical network under the test;

c
Σ
adder-accumulator with initial state -c,

Fig. 5 Error detection by equation (52)

The complexity and the testing time of a system represented by Fig. 5 depends on the cardinality $R=|T|$ of the check set $T=\{Z_1,\ldots,Z_R\}$. Thus, our problem is to find for the given f(Z) a set T of minimal cardinality and constant C such that (52) is satisfied for every $Z\in G$.

T.23[7]

For any $f(Z)=\{f^{(s)}(Z^{(0)},\ldots,Z^{(m-1)})\}$ there exists a subgroup $T=\{Z_1,\ldots,Z_R\}$ and a constant C such that (52) is satisfied for every Z and, in fact, we may choose

$$T=H^{\perp}=\{Z\mid \chi_\omega(Z)=1 \text{ for all } \omega\in H\},$$

$$C=|H|^{-1}\sum_{Z\in G} f(Z)\ ,\ R=|H|^{-1}p^m\ , \qquad (53)$$

where H is a maximal subgroup of G such that if $\omega\in H$ and $\omega\neq 0$ then $\hat f(\omega)=0$. Thus, the method for constructing a checking equation (52) reduces to the following operations: 1) Compute $\hat f(\omega)$ for the given $f(Z)$; 2) Construct a subgroup $H\subseteq\{\omega\mid\hat f(\omega)=0\}\cup\{0\}$. 3) Construct $T=H^{\perp}$ and compute $C=|H|^{-1}\sum_{Z\in G} f(Z)$.

Several generalizations of T.23 are given in[8,9].

Let us consider now the important special case when our device f computes a polynomial of degree d and input signals are represented in p-ary form

$$(f(Z)=\sum_{i=0}^{d} a_i Z^i).$$

T.24[10]

If $f(Z)=\sum_{i=0}^{d} a_i Z^i (Z\in\{0,\ldots,p^m-1\})$, then T is a dual to the maximal p-ary error-correcting code with the length of codewords equal to m and the Hamming distance d+1[11].

Let

$$\sum_{\tau\in T_i} f(Z\oplus\tau)=C_i \quad (i=1,\ldots,M) \qquad (54)$$

be a system of linear checks constructed by T.23.

A system of checks (54) is said to be orthogonal if $T_i\cap T_j=0$ $(i\neq j)$. We shall estimate now the error-detecting and error-correcting capabilities of systems of M orthogonal checks:

An error e(Z) is said to be present in a device computing the given system of p-valued functions f(Z) if for the latter f(Z)+e(Z) is computed instead of f(Z). By the multiplicity of an error e(Z), we mean number of non-zero values for the function e(Z). (Such a definition of multiplicity is natural, if errors in computing f(Z) are indepent for different Z's.)

We shall define the syndrome

$s^{(e)}(Z)=(s_1^{(e)}(Z),\ldots,s_M^{(e)}(Z))$ of the error e(Z) for the check system (54) by

$$s_i^{(e)}(Z)=\sum_{\tau\in T_i}(f(Z\oplus\tau)+e(Z\oplus\tau))-C_i=\sum_{\tau\in T_i} e(Z\oplus\tau). \qquad (55)$$

By error-correction we mean the computation of error e using the previously computed syndrome $s^{(e)}$.

We shall consider two methods for detection and correction of an error e by the syndrome $s^{(e)}$, namely memoryless and memory-aided decoding.

For memoryless decoding error detection or error correction for any given Z is implemented by $s^{(e)}(Z)$. For memory-aided decoding we first compute $s^{(e)}(Z)$ for all Z and then detect or correct errors.

The following two theorems describe error-

detecting and correcting capabilities of M orthogonal checks for memoryless and memory-aided decoding.

T.25[9]

For any system of M orthogonal checks we have for memoryless decoding:

(i) All errors with multiplicity at most M are detected, and all those with multiplicity at most [M/2] are corrected.

(ii) There exist errors with multiplicity M+1 and [M/2], which are not detected and not corrected, respectively. (Here [M/2] is the greatest integer $\leq M/2$)

T.26[9]

For any system of M orthogonal checks we have for memory-aided decoding:

(i) All errors with multiplicity at most 2^M-1 are detected, and all those with multiplicity at most $2^{M-1}-1$ are corrected.

(ii) There exist errors with multiplicity 2^M and 2^{M-1}, which are not detected and not corrected, respectively. Thus, it follows from T.25, T.26 that error-detecting and error-correcting capabilities of M orthogonal checks do not depend on the function f(Z) implemented by our device, do not depend on p, and increase exponentially on transition from memoryless decoding to memory-aided decoding.

Generalizations of T.25 and T.26 are given in [7, 8 and 9].

VII. Closing Remarks

Spectral methods provide us with simple solutions of many difficult problems in the design, decomposition and testing of multiple-valued logical networks. These solutions are based on the spectral or correlation characteristics of the original system $\{f^{(s)}(Z)\}$ of multiple-valued logical functions.

The main advantage of spectral methods is in their simplicity and convenience for computer implementation even for problems of quite high dimension. In addition, the spectral methods provide easy estimations for the complexity of the network being designed.

If the original system $\{f^{(s)}(Z)\}$ is defined analytically, the solutions also may often be found analytically. If the functions $\{f^{(s)}(Z)\}$ are specified in tabular form, the solutions may be sought by employing the very effective fast Chrestenson algorithm.

For the spectral methods of synthesis described in Section II the specific features of the multiple-valued functions implemented by a network (given the number of inputs and outputs) have an effect only on the content of the memory (see Fig. 1). This makes for easy readjustment of the network to the implementation of any system of multiple-valued functions. Readjustment may be accomplished by replacing the information stored in the memory by the expansion coefficients of the new logical system. A similar principle may be employed to adapt the network to changes in its environment.

Another advantage of spectral methods is their weak dependence on the number p of stable states of the basic components, so that one obtains a unified set of solutions for devices that operate in p-ary systems for any $p \geq 2$. This universal property makes spectral methods particularly suitable for the design and testing of multiple-valued logical networks.

References

1. Karpovsky, M. G., "Finite Orthogonal Series in the Design of Digital Devices", Wiley NY, 1976.

2. Karpovsky, M. G. and Moskalev, E. S., "Spectral Methods for Analysis and Synthesis of Digital Devices", (in Russian), Energia, Leningrad, 1973.

3. Karpovsky, M. G. and Moskalev, E. S., "Realization of a System of Logical Functions by Means of Expansion in Orthogonal Series", Automat. and Remote Control, Vol. 28, No. 12, 1921-1932, Dec. 1967.

4. Karpovsky, M. G. and Moskalev, E. S., "Utilization of Autocorrelation Characteristics for the Realization of Systems of Logical Functions", Automat. and Remote Control, Vol. 31, No. 2, 243-250, Feb. 1970.

5. Karpovsky, M. G., "Error-Correction in Automata, whose Combinational Parts are Realized by Expansion in Orthogonal Series", Automat. and Remote Control, Vol. 32, No. 93 part 2, 1524-1528, Sept. 1971.

6. Karpovsky, M. G., "Harmonic Analysis over Finite Commutative Groups in Linearization Problems for Systems of Logical Functions", Information and Control, Vol. 33, N2, 142-165, Feb. 1977.

7. Karpovsky, M. G., "Error Detection" in Digital Devices and Computer Programs with the Aid of Linear Recurrent Equations over Finite Commutative Groups", IEEE Trans. on Computers, C-26, N3, 208-219, 1977.

8. Karpovsky, M. G. and Trachtenberg, E. A., "Linear Checking Equations and Error-Correcting Capability for Computation Channels", Proc. 1977 IFIP Congress, North Holland 1977.

9. Karpovsky, M. G. and Trachtenberg, E. A., "Fourier Transforms over Finite Groups for Error Detection and Error Correction in Computation Channels", Information and Control, Vol. 40, N3, 1979.

10. Karpovsky, M. G., "Error Detection for Polynomial Computations", IEE J. on Computer and Digital Techniques, Vol. 2, No. 1, Feb. 1979.

11. MacWilliams, F. Y. and Sloane, N. J. A., "The Theory of Error-Correcting Codes", North Holland, 1977.

12. Moraga, C., "Complex Spectral Logic", Proc. of the Eight Int. Symposium on Multiple-Valued Logic, 149-156, Rosemont, Ill. 1978.

13. Tokmen, V. H.,"Some Properties of the Spectra of Ternary Logic Functions", Proc. of the Nineth Int. Symposium on Multiple-Valued Logic, 88-93, Bath,

England, 1979.

14. Andrews, H. C. and Caspari, K. L., "A Generalized Technique for Spectral Analysis", IEEE Trans. Computers C-19, 16-25, 1970.

15. Sholomov, L. A., "Criteria for Complexity of Boolean Functions" (in Russian), Problems of Cybernetics, 17, 1966.

16. Moraga, C., "Comment on a Method of Karpovsky", Information and Control, 39, 243-246, 1978.

17. Spillman, R., "Single Stuck-at Faults in Multi-Valued Combinational Circuits", Proc. of Sixth Int. Symposium on Multiple-Valued Logic, 97-101, 1976.

18. Coy, W. and Moraga, C., "Description and Detection of Faults in Multiple-Valued Logic Networks", Proc. of Nineth Int. Symposium on Multiple-Valued Logic, 74-81, 1979.

19. Savir, J., "Syndrome Testable Design of Combinational Circuits", IEEE Trans. on Computers, C-29, No. 6, 442-451, June 1980.

20. Lange, F. H., "Correlation Techniques", Princeton, N. J., VanNostrand, 1967.