The obtained data indicate that the machine performance is optimum.

The results of these investigations indicate that it is possible to choose a stochastic automatic machine with variable structure and optimum behavior in a composite medium, whose switching can be accomplished by its own operations. Studies of machine performance in media of this type are useful in conjunction with studies of automatic administrative models, for example. A description of the model of an administrative network, as well as some specific examples, can be found in reference 4.

Submitted January 15, 1973

REFERENCES

1. V. I. Varshavskiy and I. P. Vorontsova, Behavior of stochastic automata with a variable structure. Avtomatika i Telemekhanika (Automat. Remote Control), 1963, 24, No. 3.
2. B. Chandrasekaran and D. W. C. Shen, On expediency and coherence in variable structure automata. Proc. Nat. Electron. Conf., Chicago, Ill., 1966, 22.
3. I. P. Vorontsova, Algorithms for variation of the transition probabilities in stochastic automata, Problemy Peredachi Informatsii (Probs. Information Trans.), 1965, No. 3.
4. A. K. Pulatov, Automatic model of an administrative network, in the collection Decentralized Methods of Control, F. E. Dzerzhinski Moscow Publishing House of Scientific-Technical Propaganda, 1972.

□◆◆◆□

Methods of Estimating the Correcting Capacity of Functions of the Algebra of Logic

M. G. KARPOVSKIY, E. S. MOSKALEV AND A. A. TROYANOVSKIY

(Leningrad)

Methods of analyzing the correcting capacity of functions of the algebra of logic are described. The apparatus of discrete functional transformations is used to estimate this capacity on the set of arithmetic and nonarithmetic errors. Certain classes of Boolean functions are examined from the point of view of their correcting capacity for errors of given multiplicity.

* * *

1. Suppose that we are given completely determined functions of the algebra of p-ary logic:

$$y^{(j)}=f^{(j)}(x) \quad (j=0, 1, \ldots, r-1), \tag{1.1}$$

where $x = (x^{(0)}, x^{(1)}, \ldots, x^{k-1}) \in X$ for $X \in \{0, 1, \ldots, p-1\}^k$.

By an error for the system of functions defined by (1.1) we mean an ordered pair $(x, x') \in X^2$, where x and x' belong to X. The system of functions (1.1) corrects the set of errors R if and only if $f^{(j)}(x) = f^{(j)}(x')$ for $j = 0, 1, \ldots, r-1$ and for arbitrary $(x, x') \in R$, where $R \subseteq X^2$.

Below we shall consider two classes of errors, the class of arithmetic errors and the class of nonarithmetic errors.

We shall denote a nonarithmetic error (x, x') (where $x, x' \in \{0, 1, \ldots, p-1\}^k$) by γ, and we shall assume that

$$\gamma = x - x' \pmod p. \tag{1.2}$$

(By (1.2) we mean the operation of component-wise subtraction of the vectors modulo p.)

We shall refer to a nonarithmetic error γ as an error of multiplicity l if and only if

$$\|x - x'\| = l \pmod p, \tag{1.3}$$

where $\|d\|$ is the number of nonzero components of the p-ary vector d.

We shall denote an arithmetic error (x, x') (where x, $x' \in \{0, 1, \ldots, p-1\}^k$) by γ_a, with $\gamma_a = x - x'$, where x and x' are numbers whose p-ary expansions are respectively the vectors x and x'.

By the weight of an arithmetic error γ_a we mean the minimum number of nonzero terms in the representation of $|x - x'|$ in the form of an algebraic sum of terms of the form $\alpha_i p^i$ (where $\alpha_i \in \{0, 1, \ldots, p-1\}$ for $i = 0, 1, \ldots, k-1$). We denote the arithmetic weight by $\|x - x'\|_a$.

We shall call an arithmetic error γ_a an error of multiplicity l if and only if $\|x - x'\|_a = l$.

Thus the set R_a (resp. R) of arithmetic (resp. nonarithmetic) errors of multiplicity l is defined as follows:

$$R_a \equiv \{(x, x') \mid x, x' \in \{0, 1, \ldots, p-1\}^k;\ \|x - x'\|_a = l\}, \tag{1.4}$$

$$R \equiv \{(x, x') \mid x, x' \in \{0, 1, \ldots, p-1\}^k;\ \|x - x'\| = l\} \pmod p. \tag{1.5}$$

We denote by $\xi_{R_a}^{(p)}(f)$ [resp. $\eta_R^{(p)}(f)$] the number of arithmetic (resp. nonarithmetic) errors in the set R_a (resp. R) defined by (1.4) [resp. (1.5)], and we shall call it the correcting capacity of the system of functions of the algebra of logic on the set of errors R_a (resp. R). We denote by $\xi_l^{(p)}(f)$ [resp. $\eta_l^{(p)}(f)$] the correcting capacity of the system of functions on the set of all arithmetic (nonarithmetic) errors of multiplicity l.

In the present article, we shall consider problems of analyzing the correcting capacity for different classes of systems of functions of the algebra of logic, and different classes of errors.

2. For the systems of functions of the algebra of logic (1.1), let us construct the lattice function [1] $y = f(x)$, with

$$x = \sum_{i=0}^{k-1} x^{(i)} p^{k-i-1}, \qquad y = \sum_{j=0}^{r-1} y^{(j)} p^{r-j-1},$$

Let us then construct the system of characteristic functions $\{f_s(x)\}$ for $s = 0, 1, \ldots, p^r - 1$:

$$f_s(x) = \begin{cases} 1 & \text{for } f(x) = s, \\ 0 & \text{otherwise.} \end{cases}$$

Then, from the definition of correcting capacity of functions of the algebra of logic $\eta_R^{(p)}(f)$ on the set R of nonarithmetic errors, we get:

Theorem 1.

$$\eta_R^{(p)}(f) = \sum_{\gamma \in R} \sum_{s=0}^{p^r-1} B_{p,s}(\gamma), \tag{2.1}$$

$$B_{p,s}(\gamma) = \sum_x f_s(x) f_s(x - \gamma) \pmod p. \tag{2.2}$$

(Here and below, when there is no ambiguity, we denote numbers and the vectors corresponding to their p-ary expansions in the same way.)

We shall call the function $B_{p,s}(\gamma)$ an autocorrelation function modulo p of the characteristic function $f_s(x)$.

Example. The table shows one function f(x) of ternary logic of two arguments ($k = 2$, $p = 3$, $r = 1$), the characteristic functions $f_0(x)$, $f_1(x)$, and $f_2(x)$, the autocorrelation functions (modulo 3) $B_{3,1}(\gamma)$ and $B_{3,2}(\gamma)$ ($B_{3,0}(\gamma) = 0$), and their sum. From the table we get $\eta_1^{(3)}(f) = 20$ and $\eta_2^{(3)}(f) = 12$.

Theorem 2.

$$B_{p,s}(\gamma) = B_{p,s}(0 - \gamma) \pmod p. \tag{2.3}$$

Equation (2.3) enables us to cut in half the amount of calculation for finding $\eta_l^{(p)}(f)$.

As one can easily note from (1.1), (1.3), and (1.5), the set of sets of arguments of the system of functions of the algebra of logic, together with the set of nonarithmetic errors of multiplicity l,

x, γ	$x^{(0)}$	$x^{(1)}$	$f(x)$	$f_0(x)$	$f_1(x)$	$f_2(x)$	$B_{3,1}(\gamma)$	$B_{3,2}(\gamma)$	$\sum_{s=0}^{2} B_{3,s}(\gamma)$
0	0	0	1	0	1	0	5	4	9
1	0	1	2	0	0	1	2	1	3
2	0	2	1	0	1	0	2	1	3
3	1	0	1	0	1	0	4	3	7
4	1	1	2	0	0	1	2	1	3
5	1	2	2	0	0	1	2	1	3
6	2	0	1	0	1	0	4	3	7
7	2	1	2	0	0	1	2	1	3
8	2	2	1	0	1	0	2	1	3

constitute a commutative group G_k with subtraction modulo p as group operation. Thus the system of functions can be represented in the form of a linear combination of characters [2] of the group G_k. The coefficients of this combination are the Fourier coefficients [3]. By virtue of the completeness and orthogonality of the system of characters, and also since the system of characters forms a multiplicative group isomorphic to G_k, it is convenient to use a discrete functional transformation, assigning to the original system of functions (the operand of the transformation) a sequence of coefficients (the spectra of its expansion in a generalized Fourier series of the characters of the group G_k (the transform), for analysis of the correcting capacity $\eta_l^{(p)}(f)$. A discrete functional transformation assigning, to the original function $f_s(x)$, its autocorrelation function $B_{p,s}(\gamma)$, is a functional transformation of the convolution type [3] on the group G_k. Therefore, the connection between the original function $f_s(x)$ and the function $B_{p,s}(\gamma)$, in terms of the dual spectral transformation of the function $f_s(x)$, is useful for simplifying the construction of $B_{p,s}(\gamma)$.

We now present a spectral method of analysis of the correcting capacity $\eta_l^{(p)}(f)$, based on calculation of the autocorrelation functions $B_{p,s}(\gamma)$ in terms of the dual spectral transformation of Krestenson [3]. Krestenson's functions are the characters of the group G_k, and they are defined for arbitrary natural numbers ω and k by

$$\chi_\omega^{(p)}(x) = \exp\left(\frac{2\pi}{p} j \sum_{i=0}^{k-1} \omega^{(k-i-1)} x^{(i)}\right),$$

where $j = \sqrt{-1}$, and $\omega^{(i)}$ and $x^{(i)}$ are the components of the p-ary expansions of ω and x.

Krestenson's transformation of the lattice function f(x) for $x \in \{0, 1, \ldots, p^k - 1\}$ assigns the spectrum $\chi^{(p)}(f) = S(\omega)$ (for $\omega \in \{0, 1, \ldots, p^k - 1\}$), where $S(\omega) = p^{-k} \sum_{x=0}^{p^k-1} f(x) \overline{\chi_\omega^{(p)}(x)}$ and $\overline{\chi^{(p)}}$ is the complex conjugate of $\chi^{(p)}$.

<u>Theorem 3.</u>

$$B_{p,s}(\gamma) = p^{2k} (\chi^{(p)})^{-1} (\chi^{(p)}(f) \overline{\chi^{(p)}}(f)) (\gamma), \tag{3.1}$$

where $(\chi^{(p)})^{-1}$ is the discrete functional transformation inverse to the transformation $\chi^{(p)}$.

Theorem 3 provides a comparatively simple method of calculating the correcting capacity of systems of functions of p-ary logic by repeated application of the "fast" Hadamard-Krestenson transformation [3]. Application of the fast Hadamard-Krestenson transformation for calculating $B_{p,s}(\gamma)$ from formula (3.1) requires $p^{k+1}(k+1)$ arithmetic operations, whereas calculation of $B_{p,s}(\gamma)$ from formula (2.2) requires p^{2k} such operations [3].

We now present an important property of $\eta_l^{(p)}(f)$.

<u>Theorem 4.</u> *Suppose that we are given the four systems of functions of the algebra of logic:* $f_1(x)$, $f_2(x)$, $f_3(x)$, $f_4(x)$, where

$$x \in \{0, 1, \ldots, p-1\}^k; \; f_1(x), \; f_2(x), \; f_3(x), \; f_4(x) \in \{0, 1, \ldots, p-1\}^r.$$

$$f_2(x)=f_1(x-\alpha)\pmod p\quad(\alpha\in\{0,1,\ldots,p-1\}^k),$$
$$f_3(x)=f_1(\sigma x),$$
$$f_4(x)=f_1(x)-\beta\pmod p\quad(\beta\in\{0,1,\ldots,p-1\}^r), \tag{3.2}$$

where σ is a permutation of $(x^{(0)}, x^{(1)}, x^{(2)}, \ldots, x^{(k-1)})$. Then, for arbitrary l, with $1\leqslant l\leqslant k$,

$$\eta_l^{(p)}(f_1)=\eta_l^{(p)}(f_2)=\eta_l^{(p)}(f_3)=\eta_l^{(p)}(f_4). \tag{3.3}$$

Theorem 4 indicates the invariance of the correcting capacity $\eta_l^{(p)}(f)$ under displacements with respect to the modulus and under permutations of the arguments of the system of Boolean functions.

Let us look briefly at the case in which the set R_a of errors consists of arithmetic errors of multiplicity l. One can easily show that, for the case of arithmetic errors, all the relationships given above remain valid, except that the operation of subtraction modulo p is replaced with the operation of subtraction modulo p^k. The autocorrelation function $B_{p^k,s}(\gamma_a)$ is also connected with the function $f_s(x)$ by a dual discrete transformation. This connection has the same form as in (3.1).

In contrast with $\eta_l^{(p)}(f)$, $\xi_l^{(p)}(f)$ is not invariant under permutation of the arguments. With regard to displacement, we have:

Theorem 5. Suppose that $f_1(x)$ $f_2(x)$, and $f_3(x)$ are three systems of functions of p-ary logic of k arguments, and that for every $x\in\{0, 1, \ldots, p^k-1\}$ we have $f_2(x) = f_1(x-\alpha) \pmod{p^k}$ (for $\alpha\in\{0, 1, \ldots, p^k-1\}$) and $f_3(x) = f_1(x) = f_1(x) - \beta \pmod p$ (for $\beta\in\{0, 1, \ldots, p^r-1\}$). Then for every l, $1\leqslant l\leqslant k$, we have $\xi_l^{(p)}(f_1) = \xi_l^{(p)}(f_2) = \xi_l^{(p)}(f_3)$.

4. Because of its practical importance, let us look in greater detail at the case in which the system of functions (1.1) is a system of Boolean functions (p = 2), and let us examine the properties of $\eta_l^{(2)}(f)$ for several classes of Boolean functions.

We note that (3.3) implies invariance of $\eta_l^{(2)}(f)$ under inversion and permutation of the arguments of the Boolean functions, and also under inversion of the individual functions of the system. Equation (3.1) with p = 2 is put in the form $B_{2,s}(\gamma) = 2^{2k}W[W^2(f_s)](\gamma)$, where W is the spectral transformation of Walsh [3].

Before analyzing the correcting capacity of particular frequently used classes of Boolean functions, we point out the connection between the complexity and the correcting capacity of the system of Boolean functions. It was shown in [1, 4, 5] that it is expedient to take as criterion N(f) of complexity of a Boolean function the number of unordered pairs of constituents of unity "glued" with respect to some variable. (Since the possibility of simplifying the expressions by gluing increases with increase in N(f), it would be more accurate to call N(f) the criterion of simplicity of the Boolean function.) The complexity of the system of Boolean functions is equal to the sum of the complexities of all functions appearing in the system. Then, for an arbitrary system of Boolean functions F(x), we have

$$N(F)={}^1/_2\eta_1^{(2)}(F). \tag{4.1}$$

It follows from (4.1) that increasing the number of identical errors to be corrected increases the value of the criterion N(F), so that the complexity of the minimal scheme realizing the given system of Boolean functions almost always decreases asymptotically.

Let us now look at the question of Boolean functions having a given power $\|f(x)\| = \sum_{x=0}^{2^k-1} f(x)$, and a maximal correcting capacity. We denote by $\eta^{(2)}(f)$ the total number of errors of all multiplicities exceeding zero corrected by the function f(x):

$$\eta^{(2)}(f)=\sum_{l=1}^{k}\eta_l^{(2)}(f).$$

Theorem 6. For a Boolean function f(x) with power $\|f(x)\|$,

$$\eta^{(2)}(f)=2^{2k}-2^k-2^{k+1}\|f(x)\|+2\|f(x)\|^2. \tag{4.2}$$

It follows from Theorem 6 that all Boolean functions of k arguments of given power exhaust the same total number of errors $\eta^{(2)}(f)$. However, for a fixed power, the correcting capacity of some functions can be concentrated in a region of errors of small multiplicity, and that of others in a region of errors of high multiplicity. Let us look, for example, at the nonincreasing functions [6]:

$$R_t(x) = \begin{cases} 1 & \text{for } x \leqslant t, \\ 0 & \text{for } x > t \end{cases} \qquad (4.3)$$

$$(x \in \{0, 1\}^k;\ x, t \in \{0, 1, \ldots, 2^k - 1\}).$$

For functions $R_t(x)$ satisfying (4.3), we have:

Theorem 7.

$$\eta_l^{(2)}(R_t) = 2\sum_{u=0}^{t}\sum_{i=0}^{k-1} x^{(i)} C_i^{l-1} + 2\sum_{u=t+1}^{2^k-1}\sum_{i=0}^{k-1} \overline{x^{(i)}} C_i^{l-1}, \qquad (4.4)$$

where

$$u = \sum_{i=0}^{k-1} x^{(i)} 2^i, \quad x^{(i)} \in \{0, 1\}, \quad \overline{x^{(i)}} = 1 - x^{(i)}.$$

Since analysis of the correcting capacity of the functions $R_t(x)$ with the aid of Theorem 7 for large k is rather laborious, let us introduce a lower bound for the correcting capacity $\eta_l^{(2)}(R_t)$:

$$\eta_l^{(2)}(R_t) \geqslant 2\sum_{x: f(x)=0} C^l_{k-\|x\|} + 2\sum_{x: f(x)=1} C^l_{\|x\|}. \qquad (4.5)$$

We note that the bound defined by (4.5) is attained if the power of the function $R_t(x)$ is a power of 2.

Inequality (4.5) indicates a high correcting capacity of the functions $R_t(x)$ in the region of errors of small multiplicity. One can easily see that completely analogous results are obtained for nondecreasing functions [6].

Theorem 8. Suppose that f(x) is a linear Boolean function [3]:

$$\left(f(x) = \sum_{i=0}^{k-1} d_i x^{(i)} \pmod 2\right).$$

Then, for every l, $1 \leqslant l \leqslant k$,

$$\eta_l^{(2)}(f) = 2^k \sum_{n=0}^{[l/2]} C_{k-\|d\|}^{l-2n} C_{\|d\|}^{2n} \qquad (4.6)$$

Here $C_a^b = 0$ for $b > a$, $\|d\| = \sum_{i=0}^{k-1} d_i$, $d_i \in \{0, 1\}$, and $[l/2]$ denotes the greatest integer not exceeding $l/2$.

Equation (4.6) shows that, in a linear Boolean function, all nonarithmetic errors of even multiplicities are corrected.

Theorem 9. The Boolean function f(x) for $x \in \{0, 1\}^k$ is self-dual (anti-self-dual) if and only if

$$\eta_k^{(2)}(f) = 0 \quad (\eta_k^{(2)}(f) = 2^k). \qquad (4.7)$$

5. Conclusions. 1. Autocorrelation functions modulo p define a convenient and natural method of analyzing the correcting capacity of systems of functions of the algebra of logic. The connection between autocorrelation functions and the original functions by means of the dual spectral transformation determines a simple machine method of calculating them by repeated use of the fast Hadamard-Krestenson transformation (the Walsh transformation, for p = 2). In contrast with minimization problems, for example, the analysis of the correcting capacity of systems of functions of many-place logic does not differ greatly in complexity from the corresponding analysis for systems of Boolean functions. The proposed methods of analysis of the correcting capacity require no sorting.

2. To increase the number of errors of low multiplicity to be corrected in the scheme realizing a system of Boolean functions, it is convenient to use representations of individual functions of the system

in the form of a superposition of nondecreasing or nonincreasing functions. Corresponding to such a representation, for example, is the realization of a systems of Boolean functions using threshold elements, and, in particular, threshold elements with weights in the set $\{\pm 2^0, \pm 2^1, \ldots, \pm 2^{k-1}\}$ [7].

3. If it is necessary to correct errors of multiplicity k in the scheme realizing a system of Boolean functions, where k is the number of arguments of the system, it is expedient to construct the scheme in accordance with the representation of the individual functions of the system in the form of a superposition of anti-self-dual functions.

4. If correction of errors of even multiplicity is necessary in a scheme realizing a system of Boolean functions, it is expedient to use "sum modulo 2" for the synthesis elements.

5. Spectral methods of analyzing the correcting capacity of Boolean functions can be used for estimating the complexity of the scheme realizing a given Boolean function.

APPENDIX

The proof of Theorem 2 follows from (2.2) on the basis of the relationship

$$f_s(x)f_s(x-\gamma)=f_s(x+\gamma)f_s(x)=f_s(x-(0-\gamma)) \pmod p.$$

Proof of Theorem 3. Let us denote by $S_s(\omega)$ the value of $\chi^{(p)}(f_s)$ at the point ω, and let us denote by $\chi_\omega^{(p)}(x)$ $(x \in \{0, 1, \ldots, p-1\}^k)$ the value of the ω-th character at the point x. Then, by virtue of relationships for the Fourier coefficients,

$$S_s(\omega)\overline{S_s(\omega)}=p^{-2k}\sum_{x,x'\in G_k} f_s(x)f_s(x')\overline{\chi_\omega^{(p)}(x)}\chi_\omega^{(p)}(x').$$

From this, the relationships $\chi_\omega^{(p)}(x)=\chi_x^{(p)}(\omega)$ and $\sum_{\omega\in G_k}\chi_\omega^{(p)}(x)=p^k$, and the isomorphism between the group G_k and the multiplicative group of its characters, we have

$$(\chi^{(p)})^{-1}(\chi^{(p)}(f_s))\overline{(\chi^{(p)}(f_s))}(\gamma)=p^{-k}\sum_{\omega\in G_k}S_s(\omega)\overline{S_s(\omega)}(\chi^{(p)})_\gamma^{-1}(\omega)=$$

$$=p^{-3k}\sum_{\omega\in G_k}\sum_{x,x'\in G_k}f_s(x)f_s(x')\overline{\chi_\omega^{(p)}(x-(x')^{-1}-\gamma^{-1})}=$$

$$=p^{-3k}\sum_{x,x'\in G_k}f_s(x)f_s(x')\sum_{\omega\in G_k}\overline{\chi_\omega^{(p)}(x-(x')^{-1}-\gamma^{-1})}=$$

$$=p^{-2k}\sum_{x\in G_k}f_s(x)f_s(x'-\gamma^{-1})+p^{-3k}\sum_{x'\neq x-\gamma^{-1}}f_s(x)f_s(x')\sum_{\omega\in G_k}\overline{\chi^{(p)}(x-(x')^{-1}-\gamma^{-1})}=$$

$$=p^{-2k}\sum_{x\in G_k}f_s(x)f_s(x-\gamma^{-1})=p^{-2k}B_{p,s}(\gamma)$$

(all the subtractions are modulo p).

Proof of Theorems 4 and 5. We note that (3.2) implies $f_1(x-\alpha)f_1(x-\alpha-\gamma)=f_1(x)f_1(x-\gamma) \pmod p$ (where $x, \alpha, \gamma \in \{0, 1, \ldots, p-1\}^k$). The validity of Theorem 4 now follows by virtue of Eqs. (2.1) and (2.2), and the fact that under a permutation (displacement modulo p) there will be the same permutation (displacement modulo p) of the arguments of the summary autocorrelation function of the corresponding system of Boolean functions.

Theorem 5 is proved analogously.

Proof of Theorem 6. The number of errors (of arbitrary multiplicities) to be corrected in the sets x for which f(x) = 1 is $\|f(x)\|(\|f(x)\|-1)$; in sets x for which f(x) = 0, it is $(2^k-\|f(x)\|)(2^k-\|f(x)\|-1)$. Equation (4.2) follows.

Proof of Theorem 7. We note that if $R_t(x^{(0)}, \ldots, x^{(i-1)}, 1, x^{(i+1)}, \ldots, x^{(k-1)})=0$ then (4.3) implies that $R_t(x^{(0)}, \ldots, x^{(i-1)}, 1, z^{(i+1)}, \ldots, z^{(k-1)})=1$ for arbitrary $z^{(i+1)}, \ldots, z^{(k-1)}$. Therefore the number of errors of multiplicity l to be corrected in the sets x such that $R_t(x)=1$ is

$$2\sum_{u=0}^{l}\sum_{i=0}^{k-1}x^{(i)}C_i^{l-u}.$$

Furthermore, if $R_t(x^{(0)}, \ldots, x^{(i-1)}, 1, x^{(i+1)}, \ldots, x^{(k-1)}) = 0$, then (4.3) implies that $R_t(x^{(0)}, \ldots, x^{(i-1)}, 1, z^{(i+1)}, \ldots, z^{(k-1)}) = 0$ for arbitrary $z^{(i+1)}, \ldots, z^{(k-1)}$. Consequently, the number of errors of multiplicity t to be corrected in sets x such that $R_t(x) = 0$ is

$$\sum_{x=i+1}^{2^k-1} \sum_{i=0}^{k-1} \overline{x^{(i)}} C_i^{t-1}.$$

Equation (4.4) follows.

Derivation of (4.5). A Boolean function f(x) is said to be nonincreasing (resp. nondecreasing) if $f(x^{(0)}, \ldots, x^{(i-1)}, 0, x^{(i+1)}, \ldots, x^{(k-1)}) \geq f(x^{(0)}, \ldots, x^{(i-1)}, 1, \ldots, x^{(k-1)})$ [resp. $f(x^{(0)}, \ldots, x^{(i-1)}, 0, x^{(i+1)}, \ldots, x^{(k-1)}) \leq f(x^{(0)}, \ldots, x^{(i-1)}, 1, \ldots, x^{(k-1)})$] for arbitrary $x^{(0)}, x^{(1)}, \ldots, x^{(k-1)}$ and arbitrary i in [0, k - 1]. It follows from the definition of a nondecreasing function f(x) that if f(x) = 1, then f(x') = 1 for every $x' \leq x$, and hence the error (x, x') is corrected. The number of such errors of multiplicity t to be corrected for fixed x is $2C_{\|x\|}$. Analogously, if f(x) = 0, then f(x') = 0 for every $x' \geq x$, and the error (x, x') is corrected. The number of errors of this kind of multiplicity t for fixed x is no less than $2C^t_{k-\|x\|}$. Inequality (4.5) follows.

Proof of Theorem 8. A Boolean function f(x) is linear [1] if $f(x) = \sum_{i=0}^{k-1} d_i x^{(i)} \pmod 2$ $(d_i \in \{0, 1\})$. It follows that f(x) actually depends only on $\|d\|$ with respect to k arguments. For any fixed x and an error of multiplicity j, $C^j_{k-\|d\|}$ such errors are corrected in the arguments on which f(x) does not depend, and $C^j_{\|d\|}$ errors if j is even, or no errors if j is odd in the $\|d\|$ arguments on which f(x) does actually depend. Now assuming that an error of multiplicity 2i occurs in the arguments on which f(x) actually depends, and that an error of multiplicity $t - 2i$ occurs in the other arguments, and summing over i and over all x we get (4.6).

Proof of Theorem 9. A Boolean function f(x) is said to be self-dual (resp. anti-self-dual) if and only if $f(x^{(0)}, \ldots, x^{(k-1)}) = \overline{f(\overline{x^{(0)}}, \ldots, \overline{x^{(k-1)}})}$ [resp. $f(x^{(0)}, \ldots, x^{(k-1)}) = f(\overline{x^{(0)}}, \ldots, \overline{x^{(k-1)}})$] for arbitrary $x \in \{0, 1\}^k$, where $\overline{f(x)}$ and $\overline{x^{(i)}}$ denote respectively the negation of the function f(x) and the i-th argument. Then it follows from the definitions that $B_{2,s}(2^k - 1) = B_{2,s}(\|\gamma\|_2 = k) = 0$ (resp. $B_{2,s}(2^k - 1) = 2 \sum_{x=0}^{2^k-1} f(x) = 2 \cdot 2^{k-1}$). Equations (4.7) now follow on the basis of (2.1) and (2.2).

Submitted February 28, 1973

REFERENCES

1. D. A. Pospelov, Logicheskiye Metody Analiza i Sinteza Skhem (Logical Methods of Analysis and Synthesis of Circuits), Sovetskoye Radio, 1967.
2. J. -P. Serre, Linear Representation of Finite Groups, Mir, 1971.
3. A. M. Trakhtman, Vvedeniye v Obobshchennyyu Spektral'nuyu Teoriyu Signalov (Introduction to Generalized Spectral Theory of Signals), Sovetskoye Radio, 1973.
4. V. I. Varshavskiy and L. Ya. Rozenblyum, On minimization of pyramidal schemes of majority elements, Izv. AN SSSR, Tekhnicheskaya Kibernetika (Engineering Cybernetics), 1964, No. 3.
5. M. G. Karpovskiy and E. S. Moskalev, Use of autocorrelational characteristics for realization of systems of functions of the algebra of logic, Avtomatika i Telemekhanika (Automat. Remote Control), 1970, No. 2.
6. G. Korn and T. Korn, Mathematics Handbook for Scientists and Engineers. (In Russian transl., Nauka, 1970.)
7. M. Dertouzos, Threshold Logic, MIT Press, 1965. (In Russian transl., Mir, 1967.)

◻◆◆◆◻