E. I. Nechiporuk

1961

Abstract

Full Text

Cybernetics and Control Theory

E. I. Nechiporuk

On the Complexity of Superpositions in Bases Containing Nontrivial Linear Formulas with Zero Weights

(Presented by Academician A. I. Berg on 10 VIII 1960)

As Post showed ([1]), there exist altogether 5 classes of linear functions of the algebra of logic that are closed with respect to superpositions and contain functions of more than one argument. These classes are: the class L_1, generated by the basis $x \oplus y, 1$ (all linear functions); the class L_2 with basis $x \oplus y \oplus 1$ (functions of the form $\sum_{i=1}^{2t} x_i \oplus 1, \sum_{i=1}^{2t+1} x_i$); the class L_3 with basis $x \oplus y$ (functions of the form $\sum_{i=1}^{t} x_i$); the class L_4 with basis $x \oplus y \oplus z$ (functions of the form $\sum_{i=1}^{2t+1} x_i$); the class L_5 with basis $x \oplus y \oplus z \oplus 1$ (functions of the form $\sum_{i=1}^{2t+1} x_i \oplus 1, \sum_{i=1}^{2t+1} x_i$). The symbols $\oplus, \sum$ denote addition modulo 2.

It is obvious that

$$L_4 \subseteq L_i \subseteq L_1, \qquad i = 1, \dots, 5. \tag{1}$$

Let functions of the algebra of logic be realized by formulas that are superpositions of formulas from some basis. Consider bases $\Lambda_i, i = 1, \dots, 5$, consisting of formulas of weight 0 forming a basis of the class L_i, a formula of weight 1 realizing multiplication &, and, in the case where negation $\neg$ does not belong to L_i, a formula of weight 1 realizing negation. By the **weight of a formula** we shall mean the sum of the weights of all basic formulas entering into its expression. Denote by $L_i(n)$ the least number such that, by formulas in the basis Λ_i of weight not exceeding $L_i(n)$, one can realize any function of the algebra of logic of n arguments.

Lemma 1. *For any n, all n-tuples of zeros and ones distinct from the zero tuple can be ordered in such a way that any n consecutive tuples are linearly independent.*

Proof. Let ξ be a primitive root of the field $GF(2^n)$ ([2]). Then ξ is a root of some irreducible polynomial

$$\alpha_0 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1} + x^n$$

of degree n over $GF(2)$ (and therefore is not a root of any polynomial over $GF(2)$ of smaller degree). Hence

$$\xi^n = \alpha_0 + \alpha_1\xi + \cdots + \alpha_{n-1}\xi^{n-1},$$

and all powers of the root ξ are expressed as polynomials in ξ of degree not greater than $n-1$ (over $GF(2)$). Let

$$\xi^k = \alpha_{k,0} + \alpha_{k,1}\xi + \cdots + \alpha_{k,n-1}\xi^{n-1},$$

Since for $1 \leq k \leq 2^n - 1$ the elements ξ^k are distinct, all tuples $\tilde{\alpha}_k = (\alpha_{k,0}, \ldots, \alpha_{k,n-1})$ are also distinct. The tuples $\tilde{\alpha}_k, \tilde{\alpha}_{k+1}, \ldots, \tilde{\alpha}_{k+n-1}$ $(1 \leq k \leq 2^n - n)$ are linearly independent, since otherwise there would be a linear dependence (with the same coefficients) among $\xi^k, \xi^{k+1}, \ldots, \xi^{k+n-1}$, and ξ would satisfy a polynomial of degree at most $n-1$, which is impossible.

Consequence. For every n there exists a partition of some

$$n\left[\frac{2^n-1}{n}\right]$$

tuples of zeros and ones of length n into

$$\left[\frac{2^n-1}{n}\right]$$

groups of n tuples each, such that the tuples within any group are linearly independent.

Introduce the notation: $(x)^0 = \neg x$, $(x)^1 = x$,

$$K_{\tilde{\sigma}}(\tilde{x}) = (x^1)^{\sigma^1} \cdots (x^n)^{\sigma^n},$$

where $\tilde{x} = (x^1, \ldots, x^n)$, $\tilde{\sigma} = (\sigma^1, \ldots, \sigma^n)$.

Lemma 2. Let $\chi(\tilde{x})$ be the characteristic function of a system of linearly independent tuples $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_n$ of length n. Then for any conjunction $K_{\tilde{\sigma}_i}(\tilde{x})$ there exists a linear function (without constant term) $l_i(\tilde{x})$ such that

$$\chi(\tilde{x})l_i(\tilde{x}) = K_{\tilde{\sigma}_i}(\tilde{x}), \tag{2}$$

and, for $i \neq j$,

$$\chi(\tilde{x})l_i(\tilde{x})l_j(\tilde{x}) = 0. \tag{3}$$

Finding the coefficients of the linear function reduces to solving a system of linear equations whose matrix is nonsingular by virtue of the linear independence of the tuples $\tilde{\sigma}_1, \dots, \tilde{\sigma}_n$. Relation (3) follows from (2) and the orthogonality of the conjunctions $K_{\tilde{\sigma}_i}(\tilde{x})$.

Theorem*.

$$L_i(n) \sim \frac{2^{n-1}}{n}, \qquad i = 1, \dots, 5.$$

Proof. From (1) it follows that

$$L_1(n) \leq L_i(n) \leq L_4(n), \qquad i = 1, \dots, 5.$$

Lower bound for $L_1(n)$. To each formula we associate a tree in the manner of R. E. Krichevskii ([3]) (the root of the tree is placed at the top). The vertices of the tree corresponding to conjunctions will be called &-vertices; the vertices corresponding to linear formulas will be called $\oplus$-vertices. To each edge of the tree we assign the number 1 or 2, depending on the number of the input of the &-vertex closest to that edge and located between it and the root. Edges whose lower endpoint is an $\oplus$-vertex are contracted to a single point; the type of this vertex coincides with the type of the upper endpoint of the edge. As a result of successive application of the indicated operation we obtain a tree consisting only of &-vertices, except possibly for the root of the tree. Edges of the tree into which the terminal edges of the original tree pass are removed, and to the vertices is assigned one of the numbers $1, \dots, 2^{2(n+1)}$, depending on the combination of variables assigned to the removed edges incident with the given vertex. The tree thus constructed uniquely determines the function represented by the original formula. The number of such trees containing h edges does not exceed $8^h 2^{2(n+1)h}$. Hence the lower bound follows.

---

* As is known ([5]), in the case of positivity of the weights of all basis formulas, $L(n)$ has order $2^n/\lg n$.

Upper bound for $L_4(n)$ (and the synthesis method). The arguments are divided into groups $\tilde{x} = (\tilde{x}_1, \tilde{x}_2, \tilde{x}_3)$, $\tilde{x}_1 = (x^1, \dots, x^s)$; $\tilde{x}_2$ contains $t = n - s - u$ letters, $\tilde{x}_3 = (z^1, \dots, z^u)$, $u = 2^r$. In the set of nonzero value tuples of the arguments $\tilde{x}_1$, choose a system of disjoint groups $V_k = \{\tilde{\sigma}_{k,1}, \dots, \tilde{\sigma}_{k,s}\}$, $k = 1, \dots, \left[\frac{2^s-1}{s}\right]$, with s tuples in each group, so that all tuples of one group are linearly independent (a consequence of Lemma 1). Denote by $\chi_k(\tilde{x}_1)$, $k = 1, \dots, \left[\frac{2^s-1}{s}\right]$, the characteristic function of the set V_k, and let $l_{k,i}(\tilde{x}_1)$ be such a linear function that $\chi_k(\tilde{x}_1) l_{k,i}(\tilde{x}_1) = K_{\tilde{\sigma}_{k,i}}(\tilde{x}_1)$ (Lemma 2). The remaining tuples, including the zero tuple, will be denoted by $\tilde{\tau}_t$, $t = 1, \dots, d$; $d \leqslant s$.

The set of value tuples of the arguments $\tilde{x}_3$ is divided into spheres of radius 1, U_p, $p = 1, \dots, 2^u/u$, with centers at the tuples $\tilde{\xi}_p = (\xi^{p,1}, \dots, \xi^{p,u})$ (4). Denote the characteristic function of the sphere U_p by $\psi_p(\tilde{x}_3)$, and let

$$\tilde{\xi}_{p,j} = (\xi^{p,1}, \dots, \xi^{p,j-1}, \overline{\xi}^{p,j}, \xi^{p,j+1}, \dots, \xi^{p,u}).$$

Every function of the algebra of logic $f(\tilde{x})$ is represented in the form

$$f(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3) = \sum_{t=1}^{d} K_{\tilde{\tau}_t}(\tilde{x}_1) f(\tilde{\tau}_t, \tilde{x}_2, \tilde{x}_3) \oplus \\ \oplus \sum_{k=1}^{\left[\frac{2^s-1}{s}\right]} \chi_k(\tilde{x}_1) \left(\sum_{p=1}^{\frac{2^u}{u}} \psi_p(\tilde{x}_3) \left(\sum_{\tilde{\sigma}_2} K_{\tilde{\sigma}_2}(\tilde{x}_2) \left(\sum_{j=1}^{u} (z^j)^{\overline{\xi}^{p,j}} \right) \ \& \right.\right. \\ \left.\left. \& \left(\sum_{i=1}^{s} l_{k,i}(\tilde{x}_1) f(\tilde{\sigma}_{k,i}, \tilde{\sigma}_2, \tilde{\xi}_{p,j}) \right) \right) \right) \Bigg). \tag{4}$$

Denote

$$A_{k,p,\tilde{\sigma}_2,j} = (z^j)^{\overline{\xi}^{p,j}} \oplus \sum_{i=1}^{s} l_{k,i}(\tilde{x}_1) f(\tilde{\sigma}_{k,i}, \tilde{\sigma}_2, \tilde{\xi}_{p,u/2+j}),$$

$$B_{k,p,\tilde{\sigma}_2,j} = (z^{u/2+j})^{\overline{\xi}^{p,u/2+j}} \oplus \sum_{i=1}^{s} l_{k,i}(\tilde{x}_1) f(\tilde{\sigma}_{k,i}, \tilde{\sigma}_2, \tilde{\xi}_{p,j}),$$

$$C_{k,p,\tilde{\sigma}_2} = \sum_{j=1}^{u/2} \sum_{i=1}^{s} l_{k,i}(\tilde{x}_1) f(\tilde{\sigma}_{k,i}, \tilde{\sigma}_2, \tilde{\xi}_{p,j}) f(\tilde{\sigma}_{k,i}, \tilde{\sigma}_2, \tilde{\xi}_{p,u/2+j}).$$

From (3), (4) it follows that

$$f(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3) = \sum_{t=1}^{d} K_{\tilde{\tau}_t}(\tilde{x}_1) f(\tilde{\tau}_t, \tilde{x}_2, \tilde{x}_3) \oplus \\ \oplus \sum_{k=1}^{\left[\frac{2^s-1}{s}\right]} \chi_1(\tilde{x}_1) \left(\sum_{p=1}^{\frac{2^u}{u}} \psi_p(\tilde{x}_3) \left(\sum_{\tilde{\sigma}_2} K_{\tilde{\sigma}_2}(\tilde{x}_2) \left(C_{k,p,\tilde{\sigma}_2} \oplus \sum_{j=1}^{u/2} A_{k,p,\tilde{\sigma}_2,j} B_{k,p,\tilde{\sigma}_2,j} \right) \right) \right). \tag{5}$$

Transform expression (5) so that the linear functions $A_{k,p,\tilde{\sigma}_2,j}$, $B_{k,p,\tilde{\sigma}_2,j}$, which play the main role, become linear functions from L_4. Let δ be an arbitrary operator. Denote

$$D^{(\delta)}_{k,p,\tilde{\sigma}_2} = \sum_{j=1}^{u/2} \delta(A_{k,p,\tilde{\sigma}_2,j})(B_{k,p,\tilde{\sigma}_2,j} \oplus \delta(B_{k,p,\tilde{\sigma}_2,j})) \oplus$$

$$\oplus\, \delta(B_{k,p,\tilde{\sigma}_2,j})(A_{k,p,\tilde{\sigma}_2,j} \oplus \delta(A_{k,p,\tilde{\sigma}_2,j})) \oplus \delta(A_{k,p,\tilde{\sigma}_2,j})\delta(B_{k,p,\tilde{\sigma}_2,j}).$$

From (5) it follows that

$$\begin{aligned} f(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3) = {} & \bigoplus_{t=1}^{d} K_{\tilde{\tau}_t}(\tilde{x}_1)\, f(\tilde{\tau}_t, \tilde{x}_2, \tilde{x}_3) \\ & \oplus \bigoplus_{k=1}^{\left[\frac{2^s-1}{s}\right]} \chi_1(\tilde{x}_1) \left(\bigoplus_{p=1}^{\frac{2^u}{u}} \psi_p(\tilde{x}_3) \left(\bigoplus_{\tilde{\sigma}_2} K_{\tilde{\sigma}_2} \right.\right. \\ & \left.\left. \& \left(C_{k,p,\tilde{\sigma}_2} \oplus D^{(\delta)}_{k,p,\tilde{\sigma}_2} \oplus \bigoplus_{j=1}^{u/2} \left((A_{k,p,\tilde{\sigma}_2,j} \oplus \delta(A_{k,p,\tilde{\sigma}_2,j}))(B_{k,p,\tilde{\sigma}_2,j} \oplus \delta(B_{k,p,\tilde{\sigma}_2,j})) \right) \right) \right) \right) \end{aligned}$$

Let φ be a function of the algebra of logic, and let $\tilde{0}$ (respectively $\tilde{1}$) be the set of values of its arguments consisting entirely of zeros (respectively ones). Put

$$\delta(\varphi) = \varphi(\tilde{0}) \oplus x(\varphi(\tilde{1}) \oplus \neg\varphi(\tilde{0})).$$

Then

$$D^{(\delta)}_{k,p,\tilde{\sigma}_2} = x l^1_{k,p,\tilde{\sigma}_2} \oplus l^2_{k,p,\tilde{\sigma}_2},$$

where $l^1_{k,p,\tilde{\sigma}_2}$, $l^2_{k,p,\tilde{\sigma}_2}$ are linear functions. If φ is a linear function, then

$$\varphi \oplus \delta(\varphi) \in L_4.$$

Denote by $P(\varphi)$ the least number such that the function φ can be realized by a formula in the basis Λ_4 with weight $P(\varphi)$. Obviously,

$$P(K_{\tilde{\tau}_t}(\tilde{x}_1)) < 2s, \qquad P(K_{\tilde{\sigma}_2}(\tilde{x}_2)) < 2t, \qquad P(f(\tilde{\tau}_t, \tilde{x}_2, \tilde{x}_3)) \le (t+u)2^{t+u+1},$$

$$P(\chi_k(\tilde{x}_1)) < Cs^2, \qquad P(\psi_p(\tilde{x}_3)) < Cu^2, \qquad P(D^{(\delta)}_{k,p,\tilde{\sigma}_2}) \le C',$$

where C, C' are constants. We have

$$P(f) < P(0) + d(2s + 1 + (t + u)2^{t+u+1}) +$$

$$+\frac{2^s}{s}\left\{Cs^2 + 1 + \frac{2^u}{u}\left(Cu^2 + 1 + 2^t\left(2t + 3 + C' + \frac{u}{2}\right)\right)\right\}.$$

Put

$$r = [\lg_2 \lg_2 n] + 3, \qquad t = 2[\lg_2 \lg_2 n], \qquad s = n - t - u;$$

then

$$P(f) \lesssim \frac{2^{n-1}}{n}.$$

The theorem is proved.

Received
5 VIII 1960

CITED LITERATURE

([1]) E. Post, *Two-valued iterative systems*, 1941.
([2]) B. L. Van der Waerden, *Modern Algebra*, 1947.
([3]) R. E. Krichevskii, DAN, 126, No. 6, 1191 (1959).
([4]) O. B. Lupanov, DAN, 119, No. 1, 23 (1958).
([5]) O. B. Lupanov, DAN, 128, No. 3, 464 (1959).

Note: Figure translations are in progress. See original paper for figures.