ON A BOOLEAN FUNCTION

1966

SovietRxiv

Abstract

Full Text

UDC 519.95

MATHEMATICS

E. I. NECHIPORUK

ON A BOOLEAN FUNCTION

(Presented by Academician P. S. Novikov on 26 III 1965)

It is known ($^{1-3}$) that, as $n \to \infty$, almost all Boolean functions of n arguments admit only realizations whose complexity is greater than $\exp Cn$, where C is some constant. However, only for very few explicitly specified functions f has it been possible to show that their complexity $L(f)$ has order greater than linear. All these examples ($^{4-7}$) are connected with certain restrictions on the basis. Until now, for no function had it been proved that it admits only "superlinear" realizations in the class of superpositions over an arbitrary basis or in the class of arbitrary contact circuits. Below an example of a function is constructed that fills this gap.

1°. Let $m = [\log n] + 2^*$, $\tilde{x} = \{\tilde{x}_i\}_1^{[n/m]}$, $\tilde{x}_i = \{x_{i,j}\}_1^m$ for $1 \le i \le [n/m]$, $x_{i,j}$ being pairwise distinct Boolean arguments. By $\|\tilde{\sigma}\|$ we denote the number of ones in the Boolean vector $\tilde{\sigma}$. Let $\tilde{\sigma}_{i,j}$ be pairwise distinct Boolean vectors of dimension m such that $\|\tilde{\sigma}_{i,j}\| > 1$. By $K^+_{\tilde{\sigma}_{i,j}}(\tilde{x}_k)$ we denote the conjunction without negations of all arguments from $\tilde{x}_k$ corresponding to the unit components of the vector $\tilde{\sigma}_{i,j}$. Put, for $1 \le i, k \le [n/m]$, $1 \le j \le m^{**}$,

$$f_n(\tilde{x}) = \sum_{i,j} x_{i,j} \sum_{\substack{k \\ (k \ne i)}} K^+_{\tilde{\sigma}_{i,j}}(\tilde{x}_k).$$

Lemma. For every i, all functions obtained from the function $f_n(\tilde{x})$ by replacing all arguments from $\tilde{x} \setminus \tilde{x}_i$ by arbitrary Boolean constants are distinct.

Proof follows from the uniqueness of the resulting Zhegalkin polynomials.

2°. **Theorem 1.** For superpositions over any finite irreducible basis (^{3}), the estimate

$$L(f_n) \succcurlyeq n^2 / \log n.$$

is valid.

Fig. 1

Figure 1: Fig. 1

Proof. Let $\mathfrak{A}$ be a superposition on which $L(f_n)$ is attained; let h be the number of its edges along which arguments are fed. Then there exists a constant C, depending only on the basis, such that $L(f_n) \succcurlyeq Ch$. Choose a number i_0 such that $h \geq [n/m]h_0$, where h_0 is the number of edges along which arguments from $\tilde{x}_{i_0}$ are fed.

Divide $\mathfrak{A}$ into two nonintersecting groups of elements: in the first group place all elements *** to each input of each of which there is fed argument from $\tilde{x} \setminus \tilde{x}_{i_0}$ or the output of an element of the 1st group; to the 2nd group we assign all elements in each of which an argument from $\tilde{x}_{i_0}$ or the output of an element of the 2nd group is fed to one input, while to each of the remaining inputs an argument from $\tilde{x} \setminus \tilde{x}_{i_0}$ or the output of an element of the 1st group is fed. The elements of the 2nd group form disjoint chains. We remove from $\mathfrak{A}$ all arguments from $\tilde{x} \setminus x_{i_0}$ and all elements of the 1st group; the inputs thereby formed will be called **free**. After this, each chain of elements of the 2nd group* is replaced by one element with three inputs, realizing the function $x\varphi + \psi$ (Fig. 1). Here the argument x is the same as in the chain, and the inputs φ, ψ (which we shall also call **free**) correspond to the functions $\varphi(\tilde{x} \setminus \tilde{x}_{i_0})$, $\psi(\tilde{x} \setminus \tilde{x}_{i_0})$ produced by the free inputs in the chain. We denote the resulting superposition by $\mathfrak{A}_0$.

Fig. 1

Every function obtained from the function $f_n(\tilde{x})$ by replacing all arguments from $\tilde{x} \setminus \tilde{x}_{i_0}$ by constants is determined by an assignment of certain Boolean constants at the free inputs of the superposition $\mathfrak{A}_0$. By the lemma, the number of these functions is equal to $2^{m[n/m]-m}$, and therefore the total number of free inputs is not less than $m[n/m]-m$.

We shall call an element of the superposition $\mathfrak{A}_0$ **terminal** if an argument is fed to at least one of its inputs. Since in $\mathfrak{A}_0$ there are no elements of the 1st and 2nd groups, it follows, by dichotomy (chains of terminal elements are not counted), that the proportion of terminal elements is not less than 1/2. Therefore there exists a constant C, depending only on the basis, such that the number of free inputs is not greater than h_0/C. Finally,

$$L(f_n) \geq C^2[n/m](m[n/m]-m) \asymp n^2/\log n.$$

---

* Logarithms are taken to base 2.
** The symbol $\sum$ denotes addition modulo 2.
*** In particular, elements without outputs.

3°. Theorem 2. For contact circuits the estimate

$$L(f_n) \succ (n/\log n)^2$$

holds.

Proof. Choose a number i_0 such that $L(f_n) \geq [n/m]h_0$, where h_0 is the number of contacts from $\tilde{x}_{i_0}$. Every function obtained from the function $f_n(\tilde{x})$ by replacing all arguments from $\tilde{x} \setminus \tilde{x}_{i_0}$ by constants is determined by a circuit consisting of h_0 contacts. Therefore, by the lemma of the present paper and Lemma 13 of (2),

$$2^{m[n/m]-m} \leq (30h_0)^{h_0}(2m)^{h_0},$$

whence

$$h_0 \succ n/\log n,$$

from which the assertion of the theorem follows.

Leningrad State University
named after A. A. Zhdanov

Received
23 III 1965

CITED LITERATURE

1. C. E. Shannon, Bell Syst. Techn. J., 28, 1, 59 (1949).
2. O. B. Lupanov, collection *Problems of Cybernetics*, issue 10, Moscow, 1963, p. 63.
3. I. I. Nechiporuk, collection *Problems of Cybernetics*, issue 14, "Nauka," 1965, p. 111.
4. B. A. Subbotovskaya, DAN, 136, No. 3, 553 (1961).
5. A. A. Markov, collection *Problems of Cybernetics*, issue 8, Moscow, 1962, p. 117.
6. G. Hansel, C. R., 258, 25, 6037 (1964).
7. R. E. Krichevsky, collection *Problems of Cybernetics*, issue 12, "Nauka," p. 45.

[*] In particular, one element.

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