B. S. MITYAGIN, B. N. SADOVSKII

1965

SovietRxiv

Abstract

Full Text

B. S. MITYAGIN, B. N. SADOVSKII

ON LINEAR BOOLEAN OPERATORS

(Presented by Academician A. N. Kolmogorov, 17 IV 1965)

In the present paper the complexity of Boolean, mainly linear Boolean, operators is studied when they are realized by circuits of functional elements in the basis $(\dot{+}, \wedge; 1, 0)$.* A linear Boolean operator is an operator all of whose components are linear functions, i.e., functions of the form $a_1x_1\dot{+}a_2x_2\dot{+}\cdots\dot{+}a_nx_n$. In Sec. 1 it is proved that the complexity of any operator is not less than the complexity of its linear part. In Sec. 2 the order of Shannon' s function $\mathcal{L}(m, n)$ is determined for linear operators. Circuits of a special type are introduced (called free circuits —the complexity when they are used for realization is denoted by $\mathcal{L}^+(m, n)$), in which the inputs of any element are supplied with functions having no common essential variables. Under natural restrictions on m, n the relation

$$\mathcal{L}^+(m,n) \asymp \mathcal{L}(m,n), \quad \text{where } \mathcal{L}(m,n) = \max_{\substack{m(A)=m\\ n(A)=n}} \mathcal{L}(A), \quad \mathcal{L}^+(m,n) = \max_{\substack{m(A)=m\\ n(A)=n}} \mathcal{L}^+(A)$$

is proved.

The following sections are devoted to the study of the function $\lambda(n) = \max \mathcal{L}^+(A)/\mathcal{L}(A)$ (the maximum is taken over all square matrices of order n). It is proved that $\lambda(n) \to \infty$ as $n \to \infty$, and the lower estimate $\lambda(n) > n^{1/2-o(1)}$ is given. The following abbreviations are used in the paper: f.e.—functional element, f.c.—circuit of functional elements.

1. Let $F(\tilde{x}) = \{y_1(x_1, \dots, x_n), \dots, y_m(x_1, \dots, x_n)\}$ be a Boolean operator. Represent its components in the form of Zhegalkin polynomials ([3]):

$$y_j = \sum_{i=0}^{n} \sigma_i[y_j(\tilde{x})] \qquad (j = 1, 2, \dots, m),$$

where $\sigma_i(y_j)$ $(i = 0, \dots, n;\ j = 1, \dots, m)$ is the homogeneous part of degree i of the function $y_j(\tilde{x})$.

The linear operator

$$\Lambda(F)\tilde{x} = \{\sigma_1[y_1(\tilde{x})], \dots, \sigma_1[y_m(\tilde{x})]\}$$

will be called the **linear part of the operator** F.

Theorem 1. *The complexity of any Boolean operator in the basis* $(\dot{+}, \wedge; 1, 0)$ *is not less than the complexity of its linear part:* $\mathcal{L}(F) \geq \mathcal{L}[\Lambda(F)]$.

Proof. Consider an f.c. $\mathfrak{F}$ realizing the operator F, and perform such a global reconstruction of this circuit that, in the course of the reconstruction, the number of f.e.' s will not increase, and the resulting f.c. $\mathfrak{A}$ will realize the operator $\Lambda(F)$. This will prove Theorem 1.

---

* Definitions of the basic concepts can be found in ([1]). The operations $\dot{+}, \wedge$ denote, respectively, addition modulo 2 and conjunction. The constant 0 is not an independent basis element; its introduction facilitates the formulation of some results, while the complexity of any operator changes at most by one.

We shall first divide the set of all functional elements of the circuit into 6 classes in accordance with Table 1. The membership of an element in one or another class is determined by the following features: a) the operation performed by the element ($\dot{+}$ or $\wedge$); b) the number of inputs of the given element directly connected with pole 1 $(0, 1, 2)$; c) the number of inputs of the element to which functions having a nonzero constant term $(0, 1, 2)$ are fed in the circuit $\mathfrak{F}$.

Table 1

Class number	a)	b)	c)	Rebuilding	Notes
1	$\dot{+}$	0		$\dot{+}$	
2	$\dot{+}$	1		p.e.	Conducts that input which is not connected with plus 1
3	$\dot{+}$	2		n.e.	
4	$\wedge$		0	n.e.	

Class number	a)	b)	c)	Rebuilding	Notes
5	$\wedge$		1	p.e.	Conducts that input whose function has zero constant term
6	$\wedge$		2	$\dot{+}$	Change of operation

The last two columns of Table 1 show in what way the elements of each class are rebuilt. For convenience we introduce fictitious elements: a conducting element (p.e.), whose output is considered to be one of its inputs, and a zero element (n.e.), at whose output a function identically equal to zero is formed. The rebuilding $\dot{+}$ consists in assigning to the given element the operation $\dot{+}$, independently of what operation it performed in the circuit $\mathfrak{F}$. After the indicated transformations it is necessary to discard the fictitious elements. If some outputs of the obtained circuit are taken directly from input pole 1, then they must be transferred to pole 0. It is clear that as a result of the described rebuilding a circuit $\mathfrak{A}$ will be obtained whose complexity is no greater than $\mathcal{L}(F)$. It remains to prove that $\mathfrak{A}$ realizes the operator $\Lambda(F)$. Let y be the output function of some functional element a of the circuit $\mathfrak{F}$, and let z_1, z_2 be the functions of its inputs. Then

$$\sigma_1(y) = \begin{cases} \sigma_1(z_1)\dot{+}\sigma_1(z_2), & \text{if } a \text{ realizes the operation } \dot{+}, \\ \sigma_0(z_1)\sigma_1(z_2)\dot{+}\sigma_0(z_2)\sigma_1(z_1), & \text{if } a \text{ realizes } \wedge\,. \end{cases}$$

By direct verification we are convinced that if the indicated rebuilding is applied to a, and the functions of the inputs are replaced by the functions $\sigma_1(z_1), \sigma_1(z_2)$, then at the output of the element the function $\sigma_1(y)$ is obtained. Hence, by induction on $\mathcal{L}(F)$, the required assertion is easily obtained.

The circuit $\mathfrak{A}$ obtained as a result of the described rebuilding contains only addition elements, and the input pole 1 is not used in this circuit. In view of this remark the following is true.

Proposition 1. Let $A : D^n \to D^m$ be a Boolean linear operator and let $\mathfrak{A}$ be a circuit realizing this operator in the basis $(\dot{+}, \wedge; 1, 0)$. Then there exists a

circuit $\mathfrak{B}$ in the basis $(\dot{+}, 0)$ that also realizes the operator A, and moreover

$$\mathcal{L}(\mathfrak{B}) \leqslant \mathcal{L}(\mathfrak{A}).$$

Corollary 1. If A is a linear Boolean operator, then

$$\mathcal{L}(A; \dot{+}, \wedge; 1, 0) = \mathcal{L}(A; \dot{+}; 0).$$

2. In what follows, as usual, we shall represent linear operators by matrices. It should be borne in mind that when multiplying a Boolean matrix by a Boolean vector, all operations are performed modulo 2. The symbols $m(A)$ and $n(A)$ will denote, respectively, the number of nonzero rows and the number of columns in the matrix A.

Definition 1. We shall call a circuit $\mathfrak{A}$ free (f.c.) if functions having no common essential variables are fed to the inputs of each element in it. The complexity of an operator A when realized by an f.c. will be denoted by $\mathcal{L}^+(A)$. It is clear that

$$\mathcal{L}^+(A) \geqslant \mathcal{L}(A). \tag{1}$$

Lemma 1. If A is a Boolean matrix and A' is the transposed matrix, then

$$\mathcal{L}(A') = \mathcal{L}(A) + m(A) - n(A), \qquad \mathcal{L}^+(A') = \mathcal{L}^+(A) + m(A) - n(A).$$

Lemma 2. For any Boolean matrix A the estimate

$$\mathcal{L}^+(A) \leqslant 2^{n(A)}$$

holds.

Lemma 3. If $n/\log m \to \infty,\ m/\log n \to \infty$, then

$$\mathcal{L}^+(m, n) \preccurlyeq 4mn/\log mn.$$

For the proof, an arbitrary $(m \times n)$-matrix A is divided into vertical strips of width $[\log m]$. The complexity of each strip is estimated with the aid of Lemma 2, and addition between strips is performed directly. From these considerations one obtains the estimate $\mathcal{L}^+(m, n) \preccurlyeq 2mn/\log m$. If the construction described is first carried out for the matrix A', and then Lemma 1 is applied, we obtain $\mathcal{L}^+(m, n) \preccurlyeq 2mn/\log n$. The assertion of the lemma follows from these two inequalities.

Lemma 4. If $n \to \infty,\ m/\log n \to \infty$, then

$$\mathcal{L}(m, n) \succcurlyeq mn/\log mn.$$

The proof of this lemma is carried out by the Shannon–Lupanov method ([1]). From Lemmas 3, 4 and inequality (1) the following follows.

Theorem 2. If $m/\log n \to \infty,\ n/\log m \to \infty$, then

$$\mathcal{L}(m,n) \asymp mn/\log mn.$$

A natural question arises: can it be asserted that the relation $\mathcal{L}(A_i) \asymp \mathcal{L}^+(A_i)$ is valid for any sequence of Boolean matrices $\{A_i\}$? A negative answer to this question is given by Theorem 3.

3. Here we shall single out one class of Boolean matrices for which $\mathcal{L}^+(A)$ is computed simply. We shall denote the rows of the matrix A by $\tilde{a}_i$ $(i = 1, 2, \dots, m(A))$; the symbol $(\tilde{a}_i, \tilde{a}_j)$ denotes the ordinary (and not modulo 2) scalar product of the vectors $\tilde{a}_i, \tilde{a}_j$; $R(A)$ is the number of ones in the matrix A.

Definition 2. A Boolean matrix A will be called **sparse** if for it the inequalities

$$(\tilde{a}_i, \tilde{a}_j) \leqslant 1 \qquad (i, j = 1, 2, \dots, m(A);\ i \neq j)$$

hold.

Proposition 2. If A is a sparse matrix, then

$$\mathcal{L}^+(A) = R(A) - m(A).$$

The proof is by induction on the value of $\mathcal{L}^+(A)$. For the case $\mathcal{L}^+(A) = 0$ the assertion is obvious. Further, if $\mathcal{L}^+(A) = k + 1$, we discard an element of a minimal s.f.s. $\mathfrak{A}$ realizing the matrix A, whose output is not fed to the inputs of other elements, and declare its inputs to be outputs of the circuit. It is not hard to see that the resulting f.s. $\hat{\mathfrak{A}}$ will be a minimal s.f.s. for the matrix $\hat{A}$ which it realizes. Moreover, since the functions of the added outputs have no common essential variables, $\hat{A}$, like A, will be sparse. But then, by the induction hypothesis,

$$\mathcal{L}^+(\hat{A}) = R(\hat{A}) - m(\hat{A}).$$

Finally, by direct verification we are convinced that

$$R(A) - m(A) = R(\hat{A}) - m(\hat{A}) + 1.$$

The required result follows from these two relations.

4. Consider the operator

$$F_n(\tilde{x}, \tilde{y}) = \{z_0(\tilde{x}, \tilde{y}), \dots, z_{2n-1}(\tilde{x}, \tilde{y})\}$$

of multiplication of two n-digit binary numbers $|\tilde{x}|$ and $|\tilde{y}|$, which is defined by the relation

$$|\tilde{z}| = |\tilde{x}| \cdot |\tilde{y}|, \qquad |\tilde{w}| = \sum w_i 2^i.$$

Lemma 5.

$$\mathcal{L}(F_n) \preccurlyeq n^{1+o(1)}.$$

This fact (in a stronger form) was proved by A. Toom ([2]). Consider the operator

$$F_n^0(\tilde{x}) = F_n(\tilde{x}, \tilde{y}_0),$$

where $\tilde{y}_0$ is a fixed vector of length n,

$$|\tilde{y}_0| = \sum_{k=0}^{t} 2^{r_k}. \tag{2}$$

It is clear that for any such $\tilde{y}_0$

$$\mathcal{L}(F_n) \geqslant \mathcal{L}(F_n^0). \tag{3}$$

Our next task is to extract the linear part of the operator F_n^0.

Lemma 6. Let $\tilde{u}, \tilde{v}$ be Boolean vectors of length n, and let the Boolean operator

$$\tilde{z}(\tilde{u}, \tilde{v}) = \{z_0(\tilde{u}, \tilde{v}), \dots, z_n(\tilde{u}, \tilde{v})\}$$

be defined by the relation

$$\sum_{i=0}^{n} z_i(\tilde{u}, \tilde{v}) 2^i = |\tilde{u}| + |\tilde{v}|.$$

Then

$$\sigma_1(z_i) = u_i + v_i \quad (i = 0, 1, \dots, n).$$

Using the "by columns" multiplication algorithm and Lemma 6, one can show that the following is valid.

Lemma 7. The elements of the matrix A of the operator $\Lambda(F_n^0)$ are computed by the formulas

$$a_{ij} = \sum_{k=0}^{t} \delta(i - r_k - j) \quad (i = 1, 2, \dots, 2n;\ j = 1, 2, \dots, n),$$

where r_k are the exponents in (2); $\delta(x) = 1$ if $x = 0$; $\delta(x) = 0$ if $x \neq 0$.

Proposition 3. The complexity $\mathcal{L}(F_n)$ of the multiplication operator is not less than the complexity of the linear operator with matrix

$$A = (a_{ij})_n^{2n} = \left(\sum_{k=0}^{t} \delta(i - r_k - j) \right)_n^{2n},$$

where $\{r_k\}$ is a set of integers such that

$$0 \le r_0 < r_1 < \cdots < r_t \le n.$$

The following lemmas determine under what conditions the matrix of the operator $\Lambda(F_n^0)$ is sparse, and give a lower estimate for the quantity $R(A)$.

Definition 3. A set of nonnegative integers

$$R = \{r_0, r_1, \dots, r_t\}$$

will be called **nonuniform** if

$$r_{k_1} - r_{k_2} \ne r_{k_3} - r_{k_4}$$

for $k_1 \ne k_2,\ k_1 \ne k_3$. The set R will be called a **nonuniform n-set** if $r_k \le n$ $(k = 0, \dots, t)$. The maximum possible length of a nonuniform n-set will be denoted by $g(n)$.

Lemma 8. In order that the matrix A of the operator $\Lambda(F_n^0)$ be sparse, it is necessary and sufficient that the n-set of exponents in (2) be nonuniform.

Lemma 9.

$$g(n) \succcurlyeq n^{1/2}.$$

It is quite easy to construct a nonuniform n-set containing $\succcurlyeq n^{1/3}$ numbers. The estimate stated in the lemma was essentially proved by Singer ([4]).

Corollary 2. For any n, the vector $\tilde{y}_0$ can be chosen so that the matrix A_n of the operator $\Lambda(F_n^0)$ is sparse and satisfies the inequality

$$R(A_n) \succcurlyeq n^{3/2}.$$

Theorem 3.

$$\lambda(n) \succ n^{1/2 - o(1)}.$$

Proof. Let $\{A_n\}$ be the sequence of matrices constructed in Corollary 2. The matrices A_n are not square:

$$m(A_n) = 2n, \qquad n(A_n) = n.$$

We obtain square matrices B_n from A_n by deleting certain n rows so that

$$R(B_n) \ge \frac{1}{2} R(A_n).$$

Note that B_n, like A_n, are sparse; therefore, from Proposition 2 and Corollary 2 we obtain

$$\mathcal{L}^+(B_n) = R(B_n) - n \ge \frac{1}{2} R(A_n) - n \succ n^{3/2}.$$

On the other hand, obviously,

$$\mathcal{L}(B_n) \leq \mathcal{L}(A_n).$$

Therefore

$$\lambda(n) \geq \frac{\mathcal{L}^+(B_n)}{\mathcal{L}(B_n)} \succ n^{3/2} : n^{1+o(1)} = n^{1/2-o(1)},$$

and the theorem is proved.

Voronezh State University

Received
17 IV 1965

REFERENCES

1. O. B. Lupanov, *Problems of Cybernetics*, **10**, 63 (1963).
2. A. L. Toom, DAN, **150**, 496 (1963).
3. V. M. Glushkov, *Synthesis of Digital Automata*, Moscow, 1962, p. 218.
4. J. Singer, *Trans. Am. Math. Soc.*, **43**, 347 (1938); P. Erdős, *Matem. prosveshch.*, **6**, 315 (1961).

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