A LOWER BOUND FOR THE COMPUTATIONAL COMPLEXITY OF A SET OF DISJUNCTIVES IN A MONOTONE BASIS

D. Yu. Grigor'ev

UDC 518.5:519.1

A set of disjunctions of some variables is constructed and a nonlinear lower bound is proved for the circuit complexity of this set in systems of functional elements (s. f. e.)* in a fixed monotone basis. The proposed method for proving the lower bound of circuit complexity in the s. f. e. differs from previously known methods (in a monotone basis).

1. A monotone Boolean function is the composition of conjunctions and disjunctions. In [1-4] the authors examine the problem of finding a lower bound for the computational complexity of a set of monotone Boolean functions in systems of functional elements (s.f.e.) in a fixed monotone basis, i.e., a basis of monotone functions. Nechiporuk [1] was the first to construct a set of disjunctions with a nonlinear lower bound for their computational complexity in s. f. e. in a monotone basis. The disjunctions constructed by Nechiporuk had the property that no two had more than one common variable. The set of disjunctions in [2] has the same property.

In the present paper we construct a set of disjunctions for which we prove a nonlinear strict (to within a multiplicative constant) lower bound for the computational complexity in an s. f. e. in a fixed monotone basis. The method of proving the lower bound may therefore also be of interest. This method was used to obtain the lower bound for the computational complexity of a set of linear forms (see [5, Sec. 1]).

Nechiporuk (see [1]) proved that in computing a set of disjunctions in an s. f. e. in a monotone basis we can, without increasing the complexity, restrict ourselves to a basis consisting of one two-place disjunctive. We represent each s. f. e. in the usual way (see [5]) in the form of a directed graph with the number of vertices equal to the number of elements of the s. f. e., counting the variables which occur in it. Each vertex of the graph therefore corresponds to a Boolean function. We shall say that the functions corresponding to the vertices of a graph are computed by a given s. f. e. The complexity of an s. f. e. is the number of vertices in its corresponding graph. Therefore, we shall consider systems of functional elements in a basis of one two-place disjunction, which compute sets of disjunctions.

2. We proceed to the construction of the required set of disjunctions. Let M be a natural number, I be any nonempty subset of the set $\{1, \ldots, M\}$. We denote by A_I the disjunction of all variables x_i $(0 \le i < 2^M)$, such that if $i = i_1 \ldots i_M$ is the expansion of i in the binary scale, then the sum $\sum_{j\in I} i_j$ is even. Thus, we construct the set $\{A_I\}_{\emptyset \ne I \subset \{1,\ldots,M\}}$, consisting of $2^M - 1$ disjunctions of 2^M variables. We shall calculate the computational complexity of this set in s. f. e. in the basis $\{V\}$.

The number of variables that occur in any disjunction $\mathfrak{D}$ is the weight of $\mathfrak{D}$, and we denote it by $|\mathfrak{D}|$. We note that for every $I \ne \emptyset, I \subset \{1,\ldots,M\}$, $|A_I| = 2^{M-1}$ holds.

First we obtain an upper bound for the computational complexity of $\{A_I\}_{\emptyset \ne I \subset \{1,\ldots,M\}}$ in an s. f. e. in the basis $\{V\}$. We denote by K_I^ε $(\varepsilon = 0, 1)$ the following subset of the set $\{0, 1, \ldots, 2^M - 1\}$: $K_I^\varepsilon = \{i\colon i = i_1 \ldots i_M$ is the binary expansion of i and $\sum_{j\in I} i_j \equiv \varepsilon \pmod 2\}$.

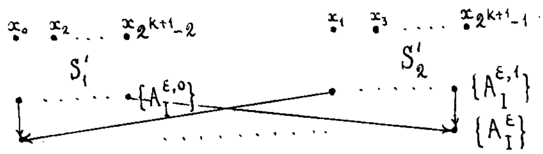
We put $A_I^\varepsilon = \bigvee_{i\in K_I^\varepsilon} x_i$, where $\varepsilon = 0, 1$. Obviously, $A_I^0 = A_I$ for every $\emptyset \ne I \subset \{1,\ldots,M\}$. We construct in the basis $\{V\}$ the s. f. e. of complexity $\le M \cdot 2^{M+1}$ which computes the set of disjunctions $\{A_I^\varepsilon\}$, $I \subset \{1,\ldots,M\}$, $\varepsilon = 0, 1$. We produce the construction by induction on M. For M = 1 the construction is obvious. Let the required s. f. e. S be already constructed for M = K.

*Translator's note: For "functional elements" read "Boolean circuits."

Translated from Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR, Vol. 68, pp. 19-24, 1977. Original article submitted January 29, 1976.

0090-4104/81/1501-0011$07.50

We take two samples of S (denoted by S_1 and S_2), and we replace every index i of the variable occurring in S_1 by 2i. Correspondingly, in S_2 we replace i by 2i + 1. We denote the systems thus formed by S_1' and S_2', respectively. We denote the output of the s. f. e. S_1' by $\{A_I^{\varepsilon,0}\}$, and the output of S_2' by $\{A_I^{\varepsilon,1}\}$, $I \subset \{1, \ldots, K\}$, $\varepsilon = 0,1$. We now combine S_1' and S_2' and obtain an s. f. e. with input variables $x_0, x_1, \ldots, x_{2^{k+1}-1}$. We construct the output for the resulting s. f. e., $\{A_I^{\varepsilon}\}$, $I \subset \{1, \ldots, k+1\}$, $\varepsilon = 0,1$ (see clarification below)



(where $A_\emptyset^0$ is the disjunction of all the variables, and $A_\emptyset^1$ is the empty disjunction). Let $I \subset \{1, \ldots, k+1\}$. We consider two cases:

1) $k+1 \notin I$. Then $A_I^0 = A_I^{0,0} \vee A_I^{0,1}$ and $A_I^1 = A_I^{1,0} \vee A_I^{1,1}$;

2) $k+1 \in I$. We put $I' = I \setminus \{k+1\}$. Then

$$A_I^0 = A_{I'}^{0,0} \vee A_{I'}^{1,1} \quad \text{and} \quad A_I^1 = A_{I'}^{1,0} \vee A_{I'}^{0,1}.$$

Thus, we have constructed an s. f. e. (see Fig. 1) on the basis $\{V\}$ with complexity no greater than $2 \cdot 2^{k+1} + k \cdot 2 \cdot 2^{k+1} = (k+1)2^{k+2}$, which computes the set $\{A_I\}_{\emptyset \neq I \subset \{1, \ldots, k+1\}}$, $\varepsilon = 0,1$. This proves the inductive statement for M = k + 1.

3) We proceed to establish the lower bound.

<u>THEOREM.</u> The computational complexity of the set $\{A_I\}_{\emptyset \neq I \subset \{1, \ldots, M\}}$ in s. f. e. in a monotone basis is not less than $(M-1)(2^{M-1} - 1/2)$. As a preliminary, we prove some subsidiary lemmas.

A directed graph G is ordered if it has the following properties:

1) It contains no directed cycles (see [6]);

2) no more than two arcs enter each vertex of the graph G.

The letter G will denote ordered graphs.

Vertices that are entered by no arc are input; vertices from which no arc leaves are output. We shall say that the vertex B is situated above the vertex C in the graph G, if there exists a directed chain in the graph G from B to C (see [6]). For every vertex A of the graph G we put $\beta_{G'}(A)$ equal to the number of input vertices of the graph G which are situated above A in the subgraph G' of the graph G. The following lemma is well-known in coding theory.

<u>LEMMA 1.</u> Let G' be a subtree of an ordered graph G, having one outgoing vertex R. Then

$$\sum_{A \in G} \beta_{G'}(A) \geq \beta_{G'}(R) \log_2 \beta_{G'}(R).$$

Lemma 1 can be proved by induction on the number of vertices of G', using the convexity of the function $x \log_2 x$ on the positive semiaxis.

<u>LEMMA 2.</u> Let G be an ordered graph with a single output vertex R. Then

$$\sum_{A \in G} \beta_G(A) \geq \beta_G(R) \log_2 \beta_G(R).$$

<u>Proof.</u> Let $G = G_0, G_1, \ldots, G_m$ be some chain of ordered graphs, such that

(1) G_i is obtained from G_{i-1} by the deletion of some arc $i = 1, \ldots, m$;

(2) G_m has a unique output vertex R and is a tree.

It is not difficult to construct such a chain from G. For every vertex A of the graph G, the inequality

$$\beta_G(A) \geq \beta_{G_1}(A) \geq \ldots \geq \beta_{G_m}(A)$$

is satisfied. In addition, by virtue of property (2), for G_m the equality $\beta_G(R) = \beta_{G_m}(R)$ is satisfied. Taking account of this, and applying Lemma 1 for the graph G_m, we get

$$\sum_{A\in G}\beta_G(A)\geqslant\sum_{A\in G_m}\beta_{G_m}(A)\geqslant\beta_G(R)\log_2\beta_G(R).$$

Lemma 2 is proved.

Variation. By using the Lemma 2 just proved, we can avoid the restriction (**) in the condition of Theorem 1 in [5].

4. We now consider the s. f. e. in the basis $\{V\}$ which computes the set of disjunctions $\{A_I\}_{\varnothing\neq I\subset\{1,\dots,M\}}$, and its corresponding ordered graph G. We denote by v(A) the vertex of the graph G which corresponds to the disjunction A. We denote by G_I the subgraph of the graph G which is generated by the vertices of the graph G which are situated above $v(A_I)$. For each disjunction A which is an element of the s. f. e. we denote by d(A) the number of graphs G_I in which the vertex v(A) occurs.

LEMMA 3.

$$\sum_{v(A)\in G}|A|\cdot d(A)\geqslant(2^M-1)\cdot 2^{M-1}\cdot(M-1). \tag{1}$$

Proof. The left part of (1) equals

$$\sum_{\varnothing\neq I\subset\{1,\dots,M\}}\sum_{v(A)\in G_I}|A|$$

We apply Lemma 2 to each G_I and obtain

$$\sum_{v(A)\in G_I}|A|\geqslant|A_I|\cdot\log_2|A_I|=2^{M-1}(M-1)$$

whence we deduce (I). Lemma 3 is proved.

Note. Let $A=\vee_{i\in F}x_i$ be computed in some vertex of the graph G. Then vertex v(A) can occur in the graph G_I only in the case where $F\subset K_I^0$.

This follows from the monotonicity of the disjunction.

We introduce one more definition. We say that the subsets $I_1,\dots,I_K$ of the set $\{1,\dots,M\}$ are Δ-independent, if for every nonempty subset L of the set $\{1,\dots,K\}$, the inequality $\Delta_{j\in L}I_j\neq\varnothing$ is satisfied, where Δ denotes the symmetric difference of the sets.

LEMMA 4. Let the subsets $\{I_1,\dots,I_K\}$ of the set $\{1,\dots,M\}$ be Δ-independent and let the disjunction α (element of the s. f. e.) be such that $v(\alpha)$ occurs in all the graphs G_{I_i} $(1\le i\le K)$. Then $|\alpha|\le 2^{M-K}$.

Proof. If $\alpha=\vee_{i\in I}x_i$, then by virtue of the note given above, $I\subset\bigcap_{1\leqslant i\leqslant K}K^0_{I_i}$ is satisfied. By definition of K^0_T this means that for every element i of I which has the binary expansion $i=i_1\dots i_M$ the sum

$$\sum_{j\in I_p}i_j\quad\text{is even for all}\quad p\quad\text{, where } 1\leqslant p\leqslant k.$$

Thus, the digits of the binary expansion of every element of the set I are the solution of the following system k of linear equations, over a field of two elements:

$$\begin{cases}a_{1,1}W_1+\dots+a_{1,M}W_M=0\\ \vdots\qquad\qquad\vdots\qquad\quad\vdots\\ a_{K,1}W_1+\dots+a_{K,M}W_M=0\end{cases} \tag{2}$$

where $a_{i,j}=1\Leftrightarrow j\in I_i$.

By virtue of the Δ-independence of $\{I_1,\dots,I_K\}$ the rank of system (2) equals k. Therefore, by means of elementary transformations (in a field of two elements), (2) can be reduced to the form:

$$\begin{aligned}W_{p_1}+b_{1,2}W_{p_2}+\dots+b_{1,k}W_{p_k}+\dots&=0\\ W_{p_2}+\dots+b_{2,k}W_{p_k}+\dots&=0\\ \vdots\qquad\qquad&\ \ \vdots\\ W_{p_k}+\dots&=0\end{aligned} \tag{3}$$

The variables $W_{p_{k+1}},\dots,W_{p_M}$ can be chosen arbitrarily, after which $W_{p_1},\dots,W_{p_k}$ are uniquely defined. Consequently, the number of solutions of system (3), and therefore also of (2), equals 2^{M-K}, therefore the number of elements of the set I does not exceed 2^{M-K}. Lemma 4 is proved.

LEMMA 5. For any $k \geq 1$ and any t, if $t > 2^{k-1}$, then from any t mutually distinct subsets of the set $\{1, \ldots, M\}$ we can choose k which are Δ-independent.

Proof. Suppose the contrary is true and $\{A_1, \ldots, A_l\}$ is a maximal system of Δ-independent sets among the given t and let $l < t$. We consider 2^l sets of the form

$$A_{i_1} \Delta \ldots \Delta A_{i_p} \tag{4}$$

where i, j are mutually distinct. Since $t > 2^{k-1} \geq 2^l$, then among the original t sets there is one which cannot be represented in the form (4). We add this to $\{A_1, \ldots, A_l\}$ and again obtain a Δ-independent system, which contradicts the choice of $\{A_1, \ldots, A_l\}$. Lemma 5 is proved.

We will now prove the main theorem. We shall show that for every disjunction A which is computable in some vertex of the graph G, the statement $|A| \cdot d(A) \leq 2^M$ is satisfied. Let v(A) occur in the graphs G_{I_p} $(1 \leq p \leq d(A))$. Let k be a natural number such that $2^{k-1} < d(A) \leq 2^k$. Then by virtue of Lemma 5 we can choose from $\{I_p\}_{1 \leq p \leq d(A)}$ k subsets which are Δ-independent. Then, by Lemma 4, $|A| \leq 2^{M-K}$. Therefore $|A| \cdot d(A) \leq 2^M$. We now use Lemma 3 and find that $z \cdot 2^M \geq \sum_{v(A) \in G} |A| \cdot d(A) \geq (2^M - 1) 2^{M-1} (M-1)$, where z is the number of elements of the s. f. e. which is being examined. Whence $z \geq (2^{M-1} - 1/2)(M-1)$. The theorem is proved.

LITERATURE CITED

1. É. I. Nechiporuk, "On a Boolean matrix," Probl. Kibern., 21, 237-240 (1969).
2. E. A. Lamagna and J. E. Savage, "Computational complexity of some monotone functions," in: IEEE 15th Ann. Symp. Switch and Automata Theory, New Orleans, 1974, New York, (1974), pp. 140-144.
3. É. I. Nechiporuk, "On the realization of a disjunction and conjunction in some monotone bases," Probl. Kibern., 23, 291-293 (1970).
4. V. R. Pratt, "The power of negative thinking on multiplication of Boolean matrices," SIAM J. Comput., 4, No. 3, 326-330 (1975).
5. D. Yu. Grigor'ev, "The use of the concepts of separability and independence to obtain lower bounds for the complexity of circuits," Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, 60, 38-48 (1976).
6. A. A. Zykov, Theory of Finite Graphs [in Russian], Vol. I, Nauka (1969).

PROBLEM OF PATH CONNECTIONS IN GRAPHS

D. Yu. Grigor'ev

UDC 518.5.519.1

A generalization is considered of a problem that arises in the design of electronic equipment – the tracing of printed circuits. The generalization is proved to be NP-complete in the sense used by Cook and Karp.

We examine here a generalization of a problem in radioelectronics – the design of printed circuits (see [1]) – and we prove the NP-completeness of this generalization (see [2, 3]). The problem of designing printed circuits is as follows: in a printed circuit, which usually consists of one or more planar lattices combined in a specific way, a set of contacts (nodes) is selected and a list is drawn up of the necessary junctions of the selected contacts. It must be determined whether these connections can be made in the whole of the circuit without "shortings." A heuristic "algorithm" for the "solution" of this problem is proposed in [1].

There have been numerous unsuccessful attempts to find an algorithm for the design of printed circuits that would give results comparable to the present heuristic methods, and it has long been concluded that this problem is intrinsically complicated. The recent work of Cook [2] and Carp [3] makes it possible to prove the equivalence of the generalized problem of design with some other "hard" computer problems, e.g., the problem of integer linear programming, the rucksack problem, and verifying the satisfiability of propositional formulas (see [3]).

Translated from Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR, Vol. 68, pp. 26-29, 1977. Original article submitted December 9, 1975.