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 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 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, ..., M}. We denote by $A_I$ the disjunction of all variables $x_i (0 \leq i < 2^M)$, such that if $i = i_1 ... i_M$ is the expansion of $i$ in the binary scale, then the sum $\sum_{i_1 \leq 0} i_1$ is even. Thus, we construct the set $\{A_I, \varphi \in \{1, ..., M\}\}$ 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 $D$ is the weight of $D$, and we denote it by $|D|$. We note that for every $I \neq \emptyset, I \subset \{1, ..., M\}, |A_I| = 2^M - 1$ holds.

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

We put $A_I^e = \bigvee_{i \in K_I^e} x_i$, where $e = 0, 1$. Obviously, $A_I^0 = A_I$ for every $\varphi \in \{1, ..., M\}$. We construct in the basis $\{V\}$ the s.f.e. of complexity $\leq M \cdot 2^{M+1}$ which computes the set of disjunctions $\{A_I^e, 1 \in \{1, ..., M\}, e = 0, 1\}$. 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."
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 $\{A^1_i\}_i$, and the output of $S'_2$ by $\{A'^1_i\}_i$, $i \in \{i, ..., k\}$, $t \in 0, i$. We now combine $S'_1$ and $S'_2$ and obtain an s.f.e. with input variables $x_0, x_1, ..., x_{2k+1-l}$. We construct the output for the resulting s.f.e., $\{A''_i\}_i$, $i \in \{i, ..., k+l\}$, $t \in 0, i$ (see clarification below).

![Diagram](image1)

(where $A^0_0$ is the disjunction of all the variables, and $A^0_0$ is the empty disjunction). Let $I \subset \{i, ..., k+l\}$. We consider two cases:

1) $k+l \not\in I$. Then $A''_i = A^0_i \lor A^{'0}_i$ and $A''_i = A^0_i \lor A^{'0}_i$;

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

$$A''_i = A^0_i \lor A^{'0}_i$$

Thus, we have constructed an s.f.e. (see Fig. 1) on the basis $\{V\}$ with complexity no greater than $2 \cdot 2^{k+1} + k \cdot 2^{k+1} = (k + 1)2^{k+1}$, which computes the set $\{A''_i\}_{i \in \{i, ..., k+l\}, t \in 0, i}$. This proves the inductive statement for $M = k + 1$.

3) We proceed to establish the lower bound.

**THEOREM.** The computational complexity of the set $\{A_i\}_{i \in \{i, ..., k+l\}}$ 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 $G$, the inequality $\beta_G(A) \geq \beta_G(R) \cdot \log \beta_G(R)$ is satisfied. In addition, by virtue of property (2), for $G_m$ the inequality $\beta_G(R) = \beta_{G_m}(R)$ is satisfied. Taking account of this, and applying Lemma 1 for the graph $G_m$, we get

**LEMMA 1.** Let $G'$ be a subtree of an ordered graph $G$, having one outgoing vertex $R$. Then

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

**LEMMA 2.** Let $G$ be an ordered graph with a single output vertex $R$. Then

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

**Proof.** 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
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_1, \ldots, A_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.**

\[
\sum_{v(A) \in G} |A| \cdot d(A) \cdot \Phi^{K - i} \cdot \Phi^{M - i} (M - i).
\]

**Proof.** The left part of (1) equals

\[
\sum_{v(A) \in G} |A| \cdot d(A) \cdot \Phi^{K - i} \cdot \Phi^{M - i} (M - i).
\]

We apply Lemma 2 to each \(G_i\) and obtain

\[
\sum_{v(A) \in G_i} |A| \cdot \Phi^{K - i} \cdot \Phi^{M - i} (M - i)
\]

whence we deduce (1). Lemma 3 is proved.

**Note.** Let \(A = \bigvee_{i \in F} x_i\) 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 \(F \subseteq K^i\).

This follows from the monotonicity of the disjunction.

We introduce one more definition. We say that the subsets \(I_1, \ldots, I_K\) of the set \(\{1, \ldots, M\}\) are \(\Delta\)-independent, if for every nonempty subset \(L\) of the set \(\{1, \ldots, K\}\), the inequality \(\Delta \subseteq L, I \neq \emptyset\) is satisfied, where \(\Delta\) denotes the symmetric difference of the sets.

**Lemma 4.** Let the subsets \(\{I_1, \ldots, I_K\}\) of the set \(\{1, \ldots, M\}\) be \(\Delta\)-independent and let the disjunction \(\alpha\) (element of the s.f.e.) be such that \(v(\alpha)\) occurs in all the graphs \(G_{i1}\) (\(1 \leq i \leq K\)). Then \(|\alpha| \leq 2^{M - K} - 1\).

**Proof.** If \(\alpha = \bigvee_{i \in F} x_i\), then by virtue of the note given above, \(1 \subseteq \bigcup_{i \in F} K^i\) is satisfied. By definition of \(K^0\) this means that for every element \(i\) of \(I\) which has the binary expansion \(1 = i_1 \ldots i_M\) the sum

\[
\sum_{j \in I} i_j
\]

is even for all \(p\), where \(i \leq p \leq k\).

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:

\[
\begin{align*}
\begin{cases}
a_{i_1, 1} W_{i_1} + \cdots + a_{i_M, 1} W_{i_M} = 0 \\
\vdots \\
a_{k, i} W_{i_1} + \cdots + a_{k, i_M} W_{i_M} = 0
\end{cases}
\end{align*}
\]

where \(a_{i, j} = i \in I_1\).

By virtue of the \(\Delta\)-independence of \(\{I_1, \ldots, I_K\}\) 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:

\[
\begin{align*}
W_{p_1} + b_{1, k} W_{p_2} + \cdots + b_{1, k} W_{p_k} + \cdots = 0 \\
W_{p_2} + b_{2, k} W_{p_3} + \cdots + b_{2, k} W_{p_k} + \cdots = 0 \\
\vdots \\
W_{p_k} + \cdots = 0
\end{align*}
\]

The variables \(W_{p_{k+1}}, \ldots, W_{p_M}\) can be chosen arbitrarily, after which \(W_{p_1}, \ldots, W_{p_k}\) 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 \( \Delta \)-independent.

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

\[ A_i \Delta \ldots \Delta A_j \text{ (4)} \]

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 \( \Delta \)-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 \( G_p \) \( (1 \leq p \leq d(A)) \). 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 \( \{G_p\}_{1 \leq p \leq d(A)} \) \( k \) subsets which are \( \Delta \)-independent. Then, by Lemma 4, \( |A| \cdot d(A) \leq 2M \). We now use Lemma 3 and find that \( z \cdot 2^M \cdot \sum_{(A) \in G} |A| \cdot d(A) \cdot (2^M - 1) \cdot (M - 1) \), where \( z \) is the number of elements of the s.f.c. which is being examined. Whence \( z \geq (2M - 1 - 1/2)(M - 1) \). The theorem is proved.

LITERATURE CITED


PROBLEM OF PATH CONNECTIONS IN GRAPHS

D. Yu. Grigor'ev

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]).