Докл. Акад. Наук СССР
Том 281 (1985), № 4

Soviet Math. Dokl.
Vol. 31 (1985), No. 2

LOWER BOUNDS FOR THE MONOTONE COMPLEXITY OF SOME BOOLEAN FUNCTIONS

UDC 519.95

A. A. RAZBOROV

The *combinatorial complexity* L_f *of a Boolean function* $f(x_1, \ldots, x_n)$ is the least number of logical elements AND, OR and NOT necessary for its realization in the form of a functional scheme. It is well known (see, for example, [1]) that there are Boolean functions whose combinatorial complexity is an exponential function of the number of variables. In a recent article [2], a natural sequence of Boolean functions

(1) $$f_1(x_1, \ldots, x_{n_1}), f_2(x_1, \ldots, x_{n_2}), \ldots, f_m(x_1, \ldots, x_{n_m}), \ldots$$

was constructed, with $L_{f_m} \geq C^{n_m}$, where $C > 1$ is a universal constant.

In this note we will restrict ourselves to the consideration of sequences of the form (1) satisfying the following condition: the language $\{(\varepsilon_1 \cdots \varepsilon_{n_m}) | m \in \mathbf{N}, f_m(\varepsilon_1, \ldots, \varepsilon_{n_m}) = 1\}$ in the alphabet $\{0, 1\}$ can be recognized by a nondeterministic Turing machine in time which is polynomial in the length of the input n_m (i.e. it is an NP-language). Such sequences will be called *constructive.*

It is interesting to obtain lower bounds on the combinatorial complexity of functions from the constructive sequence (1), for example, in connection with the following remark (derivable from the results of [3]): if there is a constructive sequence of the form (1) such that

$$\varlimsup_{m \to \infty} \frac{\log L_{f_m}}{\log n_m} = \infty,$$

then $P \neq NP$. Apparently the strongest result obtained in this direction is found in [4], where an example of a constructive sequence (1) is constructed with $L_{f_m} \geq 2.5 n_m$.

The *monotone complexity* L_f^+ *of a monotone Boolean function* $f(x_1, \ldots, x_n)$ is the least number of functional elements OR and AND necessary for its realization in the form of a functional scheme (without the element NOT). Clearly $L_f^+ \geq L_f$, and therefore the problem of finding asymptotic lower bounds on L_f^+ for constructive sequences (1) of monotone Boolean functions is simpler. The best bound of this type known until now was obtained in [5]:

$$L_{f_m}^+ \geq C \frac{n_m^2}{\log n_m}, \qquad C > 0,$$

for a certain constructive sequence of the form (1).

In this note we shall construct two constructive sequences of monotone Boolean functions for which $L_{f_M}^+ \geq n_m^{(C \log n_m)}$, with $C > 0$. The general result from which these bounds may be obtained is stated in Theorem 1. Theorems 2 and 3 are devoted to bounds for the monotone complexity of functions from specific constructive sequences. In order to formulate the results, it is convenient to interpret a Boolean function as the set of inputs on which it takes the value 1.

More precisely, let $R = \{e_1, \ldots, e_n\}$ be a finite set, and $B_n = \mathcal{P}(R)$ its power set. We define a bijection $\chi: B_n \to \{0, 1\}^n$ in the following way: for $E \in B_n$ we set $\chi(E) = (\varepsilon_1, \ldots, \varepsilon_n)$, where $\varepsilon_i = 0$ if $e_i \notin E$, and $\varepsilon_i = 1$ if $e_i \in E$.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 65Q25.

To the Boolean function $f(x_1,\dots,x_n)$, of n variables we assign the set $A(f) \in \mathcal{P}(B_n)$ in the following way: $A(f) = \{E \in B_n | f(\chi(E)) = 1\}$. Clearly A gives a bijection between the set of all Boolean functions of n variables and $\mathcal{P}(B_n)$, for which $A(f_1 \& f_2) = A(f_1) \cap A(f_2)$ and $A(f_1 \vee f_2) = A(f_1) \cup A(f_2)$. We call the set $M \in \mathcal{P}(B_n)$ *monotone* if for all $E_1, E_2 \in B_n$, from $E_1 \in M$ and $E_1 \subseteq E_2$ it follows that $E_2 \in M$. We remark that a Boolean function f is monotone if and only if the set $A(f)$ is monotone. We denote by $\mathcal{P}^+(B_n)$ the family of all monotone subsets of B_n. Among the elements of $\mathcal{P}^+(B_n)$ there are, for example, the sets $A(0) = \varnothing$, $A(1) = B_n$, and $A(x_i) = \{E \in B_n | e_i \in E\}$.

Now suppose some family $\mathfrak{M}$ of monotone subsets of the set B_n is given; that is, $\mathfrak{M} \subseteq \mathcal{P}^+(B_n)$. We call $\mathfrak{M}$ a *regular lattice* if the following two conditions are satisfied:

a) $\{A(0), A(1), A(x_1), \dots, A(x_n)\} \subseteq \mathfrak{M}$.

b) If $\mathfrak{M}$ is regarded as a partially ordered set under inclusion, them $\mathfrak{M}$ is a lattice with respect to this order.

The operations of taking greatest lower and least upper bounds will be denoted by $\sqcap$ and $\sqcup$ respectively. We introduce the notation

$$\delta_-(M_1, M_2) \rightleftharpoons (M_1 \sqcup M_2) \setminus (M_1 \cup M_2),$$
$$\delta_+(M_1, M_2) \rightleftharpoons (M_1 \cap M_2) \setminus (M_1 \sqcap M_2).$$

Suppose that we are given some monotone Boolean function $f(x_1,\dots,x_n)$ and a regular lattice $\mathfrak{M}$. The *distance* $\rho(f, \mathfrak{M})$ between f and $\mathfrak{M}$ is defined to be the least natural number t for which there are elements M, M_i and N_i of $\mathfrak{M}$, $i \le i \le t$, such that

$$M \subseteq A(f) \cup \bigcup_{i=1}^{t} \delta_-(M_i, N_i), \tag{2}$$

$$A(f) \subseteq M \cup \bigcup_{i=1}^{t} \delta_+(M_i, N_i). \tag{3}$$

It is relatively simple to prove the following

THEOREM 1. *For any monotone Boolean function $f(x_1,\dots,x_n)$ and any regular lattice $\mathfrak{M} \subseteq \mathcal{P}^+(B_n)$ the inequality $L_f^+ \ge \rho(f, \mathfrak{M})$ holds.*

We now turn to the construction of constructive sequences consisting of monotone Boolean functions of sufficiently great monotone complexity. The first example corresponds to finite fragments of the NP-complete problem CLIQUE.

Let m and s be natural numbers with $s < m$, and let $V = \{v_1, \dots, v_m\}$ be a finite set. We set $n = m(m-1)/2$ and $R = \{(v_i, v_j) | 1 \le i < j \le m\}$ (the order in which the elements of R are indexed is irrelevant). For every $W \subseteq V$ we define $E_W \in B_n$ ($B_n = \mathcal{P}(R)$) in the following way:

$$E_W \rightleftharpoons \{(v_i, v_j) \in R | v_i, v_j \in W\}.$$

Furthermore, we set

$$\mathfrak{Z}(m, s) = \{E \in B_n | \exists W\ (W \subseteq V\ \&\ \text{card}\, W = s\ \&\ E_W \subseteq E)\}.$$

$\mathfrak{Z}(m, s)$ consists of those E for which the graph (V, E) contains a clique of size at least s. It is clear that $\mathfrak{Z}(m, s)$ is monotone. Suppose that $F_{m,s}(x_1, \dots, x_n) = A^{-1}(\mathfrak{Z}(m, s))$ is the corresponding monotone Boolean function. A lower bound for $L^+_{f_{m,s}}$ is obtained on the basis of Theorem 1 using a certain regular lattice $\mathfrak{M}_{m,s}$. We will describe the construction of $\mathfrak{M}_{m,s}$ in general terms.

We introduce the following notation: $\mathfrak{A} = \{W | W \subseteq V$ and card $W \le s - 1\}$; $r = [2se^s \ln m]$. We define a binary relation $S \subseteq \mathfrak{A} \times \mathfrak{A}^r$ in the following way:

$$\langle W_0, (W_1, \dots, W_r)\rangle \in S \quad \text{if and only if} \quad \forall i, j\ (1 \le i < j \le r \Rightarrow W_i \cap W_j \subseteq W_0).$$

The fact that $\langle W_0, (W_1, \ldots, W_r)\rangle \in S$ will be more briefly expressed in the form $W_1, \ldots, W_r \vdash W_0$.

Furthermore, if $\mathfrak{A}_1 \subseteq \mathfrak{A}_2$ and $W \in \mathfrak{A}$, then the expression $\mathfrak{A}_1 \vdash W$ signifies that there are $W_1, \ldots, W_r \in \mathfrak{A}_1$ with $W_1, \ldots, W_r \vdash W$. A set $\mathfrak{A}_1 \subseteq \mathfrak{A}$ will be called *closed* if $\forall W \in \mathfrak{A}$ $(\mathfrak{A}_1 \vdash W \Rightarrow W \in \mathfrak{A}_1)$. Since the intersection of closed sets is closed, there is a smallest closed subset $\mathfrak{A}_1^* \subseteq \mathfrak{A}$ containing $\mathfrak{A}_1$, for any $\mathfrak{A}_1 \subseteq \mathfrak{A}$.

For a closed $\mathfrak{A}_1 \subseteq \mathfrak{A}$ we define the element $\ulcorner\mathfrak{A}_1\urcorner \in \mathcal{P}^+(B_n)$ in the following way:

$$\ulcorner\mathfrak{A}_1\urcorner = \{E \in B_n | \exists W \in \mathfrak{A}_1(E_W \subseteq E)\}.$$

Finally, we set $\mathfrak{M}_{m,s} = \{\ulcorner\mathfrak{A}_1\urcorner | \mathfrak{A}_1 \text{closed}\}$.

LEMMA 1. a) *$\mathfrak{M}_{m,s}$ is a regular lattice.*

b) *The lattice operations in $\mathfrak{M}_{m,s}$ have the following form:*

$$\ulcorner\mathfrak{A}_1\urcorner \sqcap \ulcorner\mathfrak{A}_2\urcorner = \ulcorner\mathfrak{A}_1 \cap \mathfrak{A}_2\urcorner; \qquad \ulcorner\mathfrak{A}_1\urcorner \sqcup \ulcorner\mathfrak{A}_2\urcorner = \ulcorner(\mathfrak{A}_1 \cup \mathfrak{A}_2)^*\urcorner.$$

The desired lattice $\mathfrak{M}_{m,s}$ has been constructed. In estimating the quantity $\rho(f_{m,s}, \mathfrak{M}_{m,s})$ from below, a key role is played by two lemmas stated below, which we give without proof.

For an arbitrary $\mathfrak{A}_1 \subseteq \mathfrak{A}$ we denote by $\mathfrak{A}_1^\flat$ the subset of the minimal elements of $\mathfrak{A}_1$, i.e.

$$\mathfrak{A}_1^\flat = \{W \in \mathfrak{A}_1 | \forall W'(W' \subset W \Rightarrow W' \notin \mathfrak{A}_1)\}.$$

LEMMA 2. *If $\mathfrak{A}_1$ is closed then* $\operatorname{card} \mathfrak{A}_1^\flat \leq (s-1)! r^{s-1}$.

Suppose that $H = [s-1]^V$ is the set of functions from V into $\{1, \ldots, s-1\}$. For each function $h \in H$, we define the ($(s-1)$-partite) graph $E_h \in B_n$ by the equality

$$E_h = \{(v_i, v_j) | h(v_i) \neq h(v_j)\}.$$

LEMMA 3. *Let $W_0, W_1, \ldots, W_r \in \mathfrak{A}$ and $W_1, \ldots, W_r \vdash W_0$. Then*

$$\operatorname{card}\{h \in H | E_{w_0} \not\subseteq E_h \ \& \ E_{W_1} \not\subseteq E_h \ \& \ \cdots \ \& \ E_{W_r} \not\subseteq E_h\} \leq (1 - e^{-s})^r \cdot \operatorname{card} H.$$

From Lemmas 2 and 3 we obtain the following lower bound on the distance.

LEMMA 4. $\rho(f_{m,s}, \mathfrak{M}_{m,s}) \geq m^s (s^3 e^s \ln m)^{-2s}$.

From Lemma 4 and Theorem 1 the analogous bound for $L^+_{f_{m,s}}$ follows directly. In the next theorem some asymptotic properties of the bounds are established.

THEOREM 2. *Suppose that $f_{m,s}(x_1, \ldots, x_{n_m})$, with $n_m = m(m-1)/2$, is the monotone Boolean function defined above, corresponding to the set of those graphs on m vertices which contain a clique of size at least s. Then:*

a) *for $s = \text{const}$ and $m \to \infty$*

$$L^+_{f_{m,s}} \geq O(m^s / (\log m)^{2s});$$

b) *for $s = [\frac{1}{4} \ln m]$ and $m \to \infty$*

$$L^+_{f_{m,s}} \geq O(m^{C \log m}), \qquad C > 0.$$

REMARK 1. For comparison we mention the obvious upper bound

$$L^+_{f_{m,s}} \leq \frac{s^2}{2} \cdot \binom{m}{s}.$$

The corresponding functional scheme in the elements AND and OR is easily constructed on the basis of complete item-by-item examination of all elements of the set $\{W | \operatorname{card} W = s\}$.

REMARK 2. Both of the sequences of Boolean functions considered in Theorem 2 are constructive.

Our second example of a constructive sequence with the lower bound $n_m^{(C \log n_m)}$ on its monotone complexity is a sequence of functions computing the logical permanent of a Boolean matrix. We specify a Boolean function $f_m(x_{1,1}, \ldots, x_{i,j}, \ldots, x_{m,m})$ of $n_m = m^2$ variables by the formula

$$f_m(x_{1,1}, \ldots, x_{i,j}, \ldots, x_{m,m}) = \bigvee_{\sigma \in S_m} \mathop{\&}_{i=1}^{m} x_{i,\sigma(i)}.$$

We will consider the graph-theoretical interpretation of this function.

We choose two disjoint sets of vertices $V = \{v_1, \ldots, v_m\}$ and $W = \{w_1, \ldots, w_m\}$. Suppose that $e_{i,j} = (v_i, w_j)$ and $R = \{e_{i,j} | 1 \leq i, j \leq m\}$. then $B_n = \mathcal{P}(R)$ turns out to be exactly the set of all bipartite graphs with parts V and W, and $A(f_m)$ coincides with the set of all bipartite graphs containing a perfect matching (a *perfect matching* in a graph $E \subseteq V \times W$ is a set of m edges having no vertices in common pairwise).

From the result of [6] the bound $L_{f_m} \leq O(m^5)$ follows for the combinatorial complexity. On the other hand, we have

THEOREM 3. *Suppose that $f_m(x_{1,1}, \ldots, x_{i,j}, \ldots, x_{m,m})$ is the logical permanent of an $m \times m$ Boolean matrix. Then $L^+_{f_m} \geq m^{C \log m}$, with $C > 0$.*

The proof is similar in outline to the proof of Theorem 2 (the full proof of Theorems 1 and 3 will be published in an article in Mathematicheskie Zametki **37** (1985)).

Theorem 3 gives an affirmative answer to Pratt's question [7] as to whether the gap between the combinatorial and the monotone complexity of Boolean function can be suprapolynomial in the number of variables.

In conclusion I would like to thank A. L. Semenov, who interested me in the subject considered here, and S. I. Adyan, for his invaluable help in preparing this work for publication.

Moscow State University

Received 14/JAN/85

BIBLIOGRAPHY

1. Michael S. Paterson, Journées Algorithmiques (Paris, 1975), Astérisque No. 38–39, Soc. Mat. France, Paris, 1976, pp. 183–201.
2. N. K. Kosovskiĭ, Seventh All-Union Conf. Math. Logic, Abstracts of Reports, Novosibirsk, 1984, p. 77. (Russian)
3. J. E. Savage, J. Assoc. Comput. Mach. **19** (1972), 660–674.
4. Wolfgang J. Paul, SIAM J. Computing **6** (1977), 427–433.
5. Ingo Wegener, Theoret. Comput. Sci. **21** (1982), 213–224.
6. John E. Hopcroft and Richard M. Karp, SIAM J. Computing **2** (1973), 225–231.
7. Vaughan R. Pratt, SIAM J. Computing **4** (1975), 326–330.

Translated by G. L. CHERLIN