If the group G is finite the order $(A; \preccurlyeq)$ and the numbered set (A^*, β) will also be finite. Therefore, we have the following result which was proved earlier independently by the author Morozov.

COROLLARY 1. The class of all groups of automorphisms of finite numbered sets coincides up to isomorphism with the class of all finite groups.

It is natural to ask for a description of the automorphisms in the category of numbered sets where the morphisms are given by 1-morphisms [1, p. 165]. Let **A** be a numbered set and denote by $\mathrm{Aut}_1(\mathbf{A})$ the group of these automorphisms. It follows from [1, p. 104, Theorem 2], that $\varphi \in \mathrm{Aut}_1(\mathbf{A})$ exactly then when there exists a recursive permutation which represents φ on the α-numbers. Our results so far provide an easy answer to our question.

COROLLARY 2. The class of all groups of the form $\mathrm{Aut}_1(\mathbf{A})$ (**A** a numbered set) coincides up to isomorphism with the class of all at most countable groups.

Proof. We consider the numbered set (A^*, β) from the proof of Lemma 3. It follows from (3) that (A^*, β) is an n-subobject of the completely numbered set $(\Pi H, \pi H)$. Therefore, the numbering β is precomplete by [1, p. 158, Proposition 4]. If G is an at most countable group than it follows from the proof of the main theorem that G is isomorphic to $\mathrm{Aut}(A^*, \beta)$ for some such (A^*, β). It follows from the precompleteness of the numbered set (A^*, β) and the theorem of [1, p. 165] that $\mathrm{Aut}(A^*, \beta) = \mathrm{Aut}_1(A^*, \beta)$. The corollary is established.

In the opinion of the author it would be interesting to describe the automorphism groups $\mathrm{Aut}(\mathbf{A})$ for known classes of numbered sets **A**, for example of the positives, negatives, subobjects of Post numbers, etc.

LITERATURE CITED

1. Yu. L. Ershov, Theory of Numberings [in Russian], Nauka, Moscow (1977).

LOWER BOUNDS ON THE SIZE OF BOUNDED DEPTH CIRCUITS OVER A COMPLETE BASIS WITH LOGICAL ADDITION

A. A. Razborov

One of the major problems in computational complexity theory is obtaining good lower bounds on circuit complexity of Boolean functions of NP-sequences. Despite continued efforts, the progress in this area has been slight — the best known bound of this kind is 3n (where n is the number of variables), as derived by Blum [1].

Superpolynomial lower bounds on the size of circuits computing functions of NP-sequences were recently obtained under various restrictions on the circuits. In [2, 3] it was proved that the realization complexity of a mod-2 logical addition function by bounded depth circuits over the basis $\{\&, \vee\}$ increases superpolynomially with the number of variables. A better bound for the same problem was obtained independently in [4].

Exponential lower bounds on the size of monotone bounded depth circuits computing various functions are given in [5-7]. Exponential lower bounds on the realization of logical addition by bounded depth circuits over the same basis $\{\&, \vee\}$ were established in [8]. A simpler proof of similar bounds was presented in [9].

Another solved case is that of a monotone, circuit over $\{\&, \vee\}$ (with not necessarily bounded depth). Superpolynomial lower bounds on monotone complexity for functions of NP-sequences were derived by the present author in [10, 11]. Andreev [12] extended these bounds to other NP-sequences, while strengthening them to exponential. Alon and Boppana [13], independently of Andreev, also strengthened the bounds from [10, 11] to exponential.

V. A. Steklov Mathematical Institute, Academy of Sciences of the USSR. Translated from Matematicheskie Zametki, Vol. 41, No. 4, pp. 598-607, April, 1987. Original article submitted April 29, 1986.

0001-4346/87/4134-0333$12.50

We consider bounded depth circuits over the basis $\{\&, \vee, \ominus\}$. Since the function $x_1 \oplus x_2 \oplus \ldots \oplus x_n$ has superpolynomial realization complexity by bounded depth circuits over $\{\&, \vee\}$ (see [2-4, 8, 9]), the circuits considered in this paper are computationally stronger than circuits over $\{\&, \vee\}$. Our aim is to prove an exponential lower bound on the realization complexity of the voting function by bounded depth circuits over $\{\&, \vee, \ominus\}$. First we prove a similar bound over $\{\&, \oplus\}$, and then suggest how it can be extended to $\{\&, \vee, \ominus\}$ (see the remark at the end).

The method of proof used in this paper has many features in common with the method of [10-13]. In order to stress this similarity, we divide our paper into sections corresponding to those in [11]. In Sec. 1 we introduce the necessary definitions and prove a theorem which leads to lower bounds on the size of bounded depth circuits, using a general construction which I call regular model. In Sec. 2, a series of regular models are constructed from Boolean polynomials of bounded degree. Finally, in Sec. 3 these models are used in order to prove an exponential lower bound on the realization complexity of the voting function by bounded depth circuits over $\{\&, \ominus\}$. Those propositions which, in our opinion, will be helpful in estimating the complexity of other Boolean functions are presented in the form of theorems; the others are stated as lemmas.

1. Bounded Depth Circuits and Regular Models. We consider Boolean functions of n variables $x_1, x_2, \ldots, x_n$; the number n is regarded as fixed until Lemma 6 inclusive. Let $B_n \rightleftharpoons \{0, 1\}^n$; $G_n \rightleftharpoons \{0, 1\}^{B_n}$ be the family of all n-place Boolean functions. There exists a unique one-to-one correspondence between G_n and $\mathbf{F}_2[x_1, \ldots, x_n]$ (for polynomials over the field $\mathbf{F}_2$ we naturally assume that $x_i^2 = x_i$); the Boolean function is identified with its representing polynomial. Addition in the field $\mathbf{F}_2$ is denoted by $\oplus$.

In defining a circuit of depth k over $\{\&, \oplus\}$ (in what follows, simply a circuit of depth k), we follow [3] with some modifications. The definition is by induction on k.

A circuit of depth 0 is an element of the set $\{x_1, x_1 \oplus 1, x_2, x_2 \oplus 1, \ldots, x_n, x_n \oplus 1\}$. A circuit of depth k is a nonempty set of circuits of depth $(k-1)$. A circuit of depth k is called a $\oplus$-circuit if k is odd and a &-circuit if k is even.

For a circuit C of depth k, we now define the Boolean function $f_C \in G_n$ computed by the circuit. For a circuit of depth 0, let $f_C \rightleftharpoons C$. The function f_C computed by a $\oplus$-circuit (&-circuit) C of nonzero depth is $\oplus_{B \in C} f_B$ (respectively, $\&_{B \in C} f_B$).

The binary relation $\to$ for circuits is defined as reflexive and transitive closure of the membership relation. The size s(C) of the circuit C is $|\{B | \to C\}|$. Finally, for $f \in G_n$, let

$$L_k(f) \rightleftharpoons \min \{s(C) \mid C \text{ is a circuit of depth } k,\ k,\ f_C = f\}.$$

For $f \in G_n$, we denote $\|f\| \rightleftharpoons |\{\varepsilon \in B_n | f(\varepsilon) = 1\}|$. If $\mathfrak{A} \subseteq G_n$ is the family of Boolean functions and $f \in G_n$, then

$$\rho(f, \mathfrak{A}) \rightleftharpoons \min \{\|f \oplus g\| \mid g \in \mathfrak{A}\}. \tag{1}$$

A regular model $\mathfrak{M}$ of depth k is the tuple

$$\mathfrak{M} = \langle \mathfrak{M}_0, \mathfrak{M}_1, \ldots, \mathfrak{M}_k, \pi_1, \ldots, \pi_k \rangle, \tag{2}$$

where $\mathfrak{M}_i \subseteq G_n$ $(0 \leqslant i \leqslant k)$; $\{x_1, x_1 \ominus 1, x_2, x_2 \oplus 1, \ldots, x_n \oplus 1\} \subseteq \mathfrak{M}_0$; π_i is some mapping of the form $\pi_i: \mathcal{P}(\mathfrak{M}_{i-1}) \to \mathfrak{M}_i$. If $H \subseteq \mathfrak{M}_{i-1}$, then let

$$\delta(H, i) \rightleftharpoons \|\pi_i(H) \ominus \underset{f \in H}{*} f\|, \tag{3}$$

where * stands for $\oplus$ when i is odd and for & when i is even. The deficiency number $\delta(\mathfrak{M})$ of the model (2) is

$$\delta(\mathfrak{M}) \rightleftharpoons \max_{1 \leqslant i \leqslant k} \max_{H \subseteq \mathfrak{M}_{i-1}} \delta(H, i);$$

the top layer of the model $\mathfrak{M}$ is the family of Boolean functions $\mathfrak{M}_k$.

THEOREM 1. Assume that there exists a regular model of depth k with deficiency number δ and top layer $\mathfrak{A}$. Then for any Boolean function f,

$$L_k(f) \geqslant \rho(f, \mathfrak{A}) \cdot \delta^{-1}.$$

Proof. Let $\mathfrak{M} = \langle \mathfrak{M}_0, \mathfrak{M}_1, \ldots, \mathfrak{M}_k, \pi_1, \ldots, \pi_k \rangle$ be the model whose existence is assumed by the theorem. For any circuit C of depth $i \leq k$ define the Boolean function $f_C^{\mathfrak{M}} \in \mathfrak{M}_i$ by induction on i.

If the circuit C is of depth 0, then $f_C \in \mathfrak{M}_0$ by definition of regular model, and we set $f_C^{\mathfrak{M}} = f_C$. If the circuit C is of depth $i > 0$, then we set

$$f_C^{\mathfrak{M}} = \pi_i(\{f_B^{\mathfrak{M}} \mid B \in C\}), \tag{4}$$

since $f_B^{\mathfrak{M}}$ already has been defined. Simple induction on depth shows that

$$f_C^{\mathfrak{M}} \ominus f_C \leqslant \bigvee \{\pi_j(\{f_B^{\mathfrak{M}} \mid B \in D\}) \oplus \underset{B \in D}{*} f_B^{\mathfrak{M}} \mid D \to C\}, \tag{5}$$

where * stands for $\oplus$ when the depth j of the circuit D is odd and for & when it is even. Using (5), the definition of deficiency number and (3), we obtain

$$\| f_C^{\mathfrak{M}} \ominus f_C \| \leqslant \delta(\mathfrak{M}) \cdot s(C). \tag{6}$$

If a circuit C of depth k computes the function f_C, then from (6) and (1), noting that $f_C^{\mathfrak{M}} \in \mathfrak{A}$ we obtain $\rho(f_C, \mathfrak{A}) \leq \delta \cdot s(C)$.

2. Construction of a Regular Model. By P(d) we denote the linear subspace in G_n formed by all polynomials of degree not higher than d. Take a natural ℓ and let

$$\mathfrak{M}_{2j} = \mathfrak{M}_{2j+1} = P(l^j) \quad (j \geqslant 0). \tag{7}$$

Our immediate objective is to define the mapping $\pi_i: \mathcal{P}(\mathfrak{M}_{i-1}) \to \mathfrak{M}_i$ so that the tuple $\langle \mathfrak{M}_0, \mathfrak{M}_1, \ldots, \mathfrak{M}_k, \pi_1, \ldots, \pi_k \rangle$ reduces to a regular model with deficiency number not exceeding $2^{n-\ell}$.

If i is odd, then, noting that $\mathfrak{M}_{i-1} = \mathfrak{M}_i$ is a linear subspace in G_n, we simply set $\pi_i(H) = \ominus_{f \in H} f$ and obtain

$$\delta(H, i) = 0 \quad \text{(i is odd)} \tag{8}$$

For even i, the possibility of choosing π_i so that $\delta(H, i) \leq 2^{n-\ell}$ for all H is suggested by the following lemma (which is a key element of the proof).

LEMMA 1. If $H \subseteq P(d)$, then there exists $g \in P(d\ell)$ such that $\|(\&_{f \in H} f) \oplus g\| \leq 2^{n-\ell}$.

Proof. Let $h = \&_{f \in H} f$. Set $\mathrm{Ann}(h) = \{f \in P(d) \mid f \& h = 0\}$. The Ann(h) is a linear subspace in P(d). We will show how to choose a sequence

$$f_1, f_2, \ldots, f_t, \ldots \tag{9}$$

of elements from Ann(h) such that $\|h \oplus (\&_{i=1}^{t}(f_i \oplus 1))\| \leq 2^{n-t}$. The sequence (9) is constructed by induction on t.

Induction base, $t = 0$ is obvious: $\|h\| \leq 2^n$.

Induction Step. Assume that the polynomials $f_1, f_2, \ldots, f_t$ have already been constructed: $\Delta_t = \{\varepsilon \mid h(\varepsilon) \neq (\&_{i=1}^{t}(f_i \oplus 1))(\varepsilon)\}$; $|\Delta_t| \leq 2^{n-t}$. Since $f_i \in \mathrm{Ann}(h)$ $(1 \leq i \leq t)$, then $h \leq f_i \oplus 1$ and so $h \leq \&_{i=1}^{t}(f_i \oplus 1)$. Therefore, if $\varepsilon \in \Delta_t$, then $h(\varepsilon) = 0$; $(\&_{i=1}^{t}(f_i \oplus 1))(\varepsilon) = 1$. Since $h = \&_{f \in H} f$, then $\exists (f_0 \in H)(h \leqslant f_0;\ f_0(\varepsilon) = 0)$. The element $1 \oplus f_0$ is in Ann(h) and $(1 \oplus f_0)(\varepsilon) = 1$.

For each $\varepsilon \in \Delta_t$ introduce the linear functional p_ε from Ann(h) defined by the rule $p_\varepsilon = f(\varepsilon)$. The preceding argument shows that for any $\varepsilon \in \Delta_t$ the functional p_ε is nondegenerate. Let f be a random variable uniformly distributed on Ann(h). Then for any $\varepsilon \in \Delta_t$ we obtain $P[f(\varepsilon) = 1] = 1/2$ and so $M[|\{\varepsilon \in \Delta_t \mid f(\varepsilon) = 1\}|] = 1/2|\Delta_t|$. As f_{t+1} take an element of Ann(h) such that $|\{\varepsilon \in \Delta_t \mid f_{t+1}(\varepsilon) = 1\}| \geq 1/2|\Delta_t|$. Then we get $|\Delta_{t+1}| \leqslant 1/2\,|\Delta_t| \leqslant 2^{n-t-1}$, which completes the induction step.

We have thus constructed the sequence (9). Setting $g = \&_{i=1}^{\ell}(f_i \oplus 1)$, we obtain an element with the properties required in Lemma 1.

We have thus proved that for any natural ℓ there exists a regular model of depth with top layer $P(\ell^{[k/2]})$ and deficiency number not exceeding $2^{n-\ell}$. Theorem 1 leads to

THEOREM 2. $L_k(f) \geq \rho(f, P(\ell^{[k/2]})) \cdot 2^{\ell - n}$.

3. Lower Bounds for the Voting Function. The voting function is defined as the following Boolean function from G_n: $MAJ(n)(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) = 1 \Leftrightarrow$ there are $\geq n/2$ ones among $\varepsilon_1, \ldots, \varepsilon_n$.

Instead of estimating (MAJ(n), P(d)) (for some d), we will first try to solve the same problem for some symmetric function f. This proof will rely on an idea which has occurred in the literature at least once (see [14, Sec. 11]). In our opinion, this method deserves a completely general formulation.

Assume for the time being that k is a field; V a finite-dimensional vector space over k; $X \subseteq V$ the set which generates V as a vector space. Then $L^X(v) \rightleftharpoons \min\{|X_0| \mid X_0 \subseteq X$ and v is contained in the linear hull of the set $X_0\}$ is defined for any $v \in V$. The proposed method establishes a lower bound on $L^X(v)$ in the following way. Let $A: V \to M$ be a linear operator (M is the space of matrices of a certain dimension over the field k). Let $r = \max\{rg(A \cdot (x)) \mid x \in X\}$. Then for any $v \in V$ we have the bound $L^X(v) \geq r^{-1} \cdot rg(A(v))$.

Let us now return to our problem. For any d', d'' such that $d' + d'' \leq n$, construct the linear operator $A_{d',d''}: G_n \to M\left(\binom{n}{d'} \times \binom{n}{d''}\right)$ [by M(p × q) we denote here and in what follows the space of p × q matrices over F_2]. We assume that the rows of the matrices from $M\left(\binom{n}{d'} \times \binom{n}{d''}\right)$ are indexed by d'-element subsets I of the set {1, 2, ..., n}, and the columns are indexed by d''-element subsets J. For any $K \subseteq \{1, 2, \ldots, n\}$, let

$$B_n(K) \rightleftharpoons \{\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in B_n \mid \forall\, (i \in K)(\varepsilon_i = 0)\}.$$

Note that

$$B_n(K_1 \cup K_2) = B_n(K_1) \cap B_n(K_2). \tag{10}$$

In this notation, the operator Ad',d'' is defined by the formula

$$A_{d',d''}: f \mapsto A, \text{ where } a_{IJ} \rightleftharpoons \bigoplus_{\varepsilon \in B_n(I \cup J)} f(\varepsilon). \tag{11}$$

LEMMA 2. a) If d' + d'' + d < n and $f \in P(d)$, then $A_{d',d''}(f) = 0$; b) if $\|f\| = 1$, then $rg(A_{d',d''}(f)) \leq 1$.

Proof. a) By linearity, it suffices to consider the case when f is a monomial. Let $f = \&_{i \in K} x_i$; $|K| \leq d$; $A_{d',d''}(f) = A$. Then $a_{IJ} = \bigoplus_{\varepsilon \in B_n(I \cup J)} \&_{i \in K} \varepsilon_i$. Since $|I \cup J \cup K| < n$, then a_{IJ} is the sum of an even number of 1s (in particular, if $K \cap (I \cup J) \neq \emptyset$, then this number of 1s is zero) and is therefore equal to 0 in the field F_2; b) from (10) and (11) we obtain the quality $A_{d',d''}(f) = A_{d'_0}(f) \cdot A_{0,d''}(f)$, which is true when $\|f\| = 1$. This directly implies b).

LEMMA 3. If d' + d'' + d < n, then $\rho(f, P(d)) \geq rg(A_{d',d''}(f))$.

Proof. Use (1) to choose a polynomial $g \in P(d)$ such that $\|f \oplus g\| = \rho(f, P(d))$. Then $rg(A_{d',d''}(f)) \leq rg(A_{d',d''}(f \oplus g)) + rg(A_{d',d''}(g))$. The first term does not exceed $\|f \oplus g\|$ by Lemma 2b; the second is zero by Lemma 2a.

THEOREM 3. For any d', d'' such that d' + d'' < n, we have $L_k(f) \geq \exp_2((n - d' - d'' - 1)^{2/k} - n)\, rg(A_{d',d''}(f))$.

Proof. The theorem follows directly from Theorem 2 and Lemma 3 if we set $\ell = (n - d' - d'' - 1)^{2/k}$; $d = n - d' - d'' - 1$.

We now introduce special intersection matrices $P_{d',d''}$ of size $\binom{n}{d'} \times \binom{n}{d''}$, which are defined as follows:

$$p_{IJ} = \begin{cases} 0, & \text{if } I \cap J \neq \emptyset, \\ 1, & \text{if } I \cap J = \emptyset. \end{cases} \tag{12}$$

LEMMA 4. Let $d < n/2$. Consider the matrix $P_d = (P_{d,0}; P_{d,1}; \ldots; P_{d,d})$, obtained by writing the intersection matrices in a single row (observing the row indexing). Then $rg(P_d) = \binom{n}{d}$.

Proof. We have to show that the rows of matrix P_d are linearly independent, i.e., for any nonzero matrix $H \in M\left(1 \times \binom{n}{d}\right)$ $HP_d \neq 0$. To this end, consider the polynomial $f_H = \oplus_{|I|=d} h_I \& _{i \in I} x_i$. Take I_0 so that $h_{I_0} \neq 0$ and in the polynomial f_H make the substitution $\{x_i \to 1 \mid i \notin I_0\}$. After this substitution, we obtain a nonzero polynomial in the variables $\{x_i \mid i \in I_0\}$, since the term $\&_{i \in I} x_i$ remains untouched. Therefore, the polynomial obtained after the substitution is equal to 1 on some distribution of the variables $\{\varepsilon_i \mid i \in I_0\}$. Setting all the other places equal to 1, we obtain in the end $\varepsilon \in B_n$, with at most d zeros and such that $f_H(\varepsilon) = 1$.

Let $J = \{i \mid \varepsilon_i = 0\}$; $|J| \leq d$. Then $1 = f_H(\varepsilon) = \oplus_{|I|=d} h_I \&_{i \in I} \varepsilon_i$. Note that $\&_{i \in I} \varepsilon_i = p_{IJ}$. Hence $\oplus_{|I|=d} h_I p_{IJ} = 1$ and therefore $HP_d \neq 0$.

COROLLARY. $\forall \left(d' < \frac{n}{2}\right) \exists (d'' \leqslant d') \left(\operatorname{rg}(P_{d',d''}) \geqslant \frac{1}{n}\binom{n}{d'}\right)$.

Proof is obvious.

We will now show that $P_{d',d''} = A_{d',d''}(f)$ for some symmetric Boolean function f.

LEMMA 5. Let $d' + d'' < n$. Then there exists a symmetric function f such that $A_{d',d''}(f) = P_{d',d''}$.

Proof. We write the sought function f in the form

$$f = \oplus_{d=0}^{d'+d''} \lambda_d T_{n-d,n},$$

where $T_{s,n} = \oplus_{|I|=s} \&_{i \in I} x_i$ is a homogeneous symmetric polynomial of degree s, and $\lambda_d \in F_2$ are unknown coefficients. Let $A = A_{d',d''}(f)$; $|I| = d'$; $|J| = d''$; $K = I \cup J$; $|K| = u$; then $a_{IJ} = \oplus_{\varepsilon \in B_n(K)} \oplus_{d=0}^{d'+d''} \lambda_d T_{n-d,n}(\varepsilon) = \oplus_{d=0}^{d'+d''} \lambda_d \left(\oplus_{\varepsilon \in B_n(K)} T_{n-d,n}(\varepsilon)\right)$. Denote $\oplus_{\varepsilon \in B_n(K)} T_{n-d,n}(\varepsilon)$ by $\varphi(n, d, u)$; then $\varphi(n, d, u) = \oplus_{\varepsilon \in B_n(K)} T_{n-d,n}(\varepsilon) = \oplus_{i=0}^{n-u} \binom{n-u}{i}\binom{i}{n-d}$ (where $\binom{p}{q}$ is by definition zero if $p < q$). Hence, it directly follows that $\varphi(n, u, u) = 1$; $\varphi(n, d, u) = 0$ if $u > d$.

The sought condition $A = P_{d',d''}$ by (12) is equivalent to the system

$$\{\oplus_{d=0}^{d'+d''} \lambda_d \varphi(n, d, u) = \delta_{u, d'+d''}\}_{u=\max(d', d'')}^{d'+d''},$$

where δ is the Kronecker symbol. In view of the above, this system is triangular, and therefore its solution $\lambda_0, \lambda_1, \ldots, \lambda_{d'+d''}$ exists, supplying the sought symmetric function f.

We are now able to estimate $L_k(f)$ for some symmetric function f.

LEMMA 6. For any k, there exists a symmetric function f such that $L_k(f) \geqslant \frac{1}{70n^2} \exp_2(n^{1/k})$.

Proof. Let $d' = [n/2 - \sqrt{n}]$ and apply the corollary of Lemma 4. Find $d'' \leq d'$ such that $\operatorname{rg}(P_{d',d''}) \geqslant \frac{1}{n}\binom{n}{n/2-\sqrt{n}} \geqslant \frac{2^n}{70n^2}$. By Lemma 5, we have $A_{d',d''}(f) = P_{d',d''}$ for some symmetric function f. Lemma 6 for this function f follows directly from Theorem 3.

Finally, let us prove our main result.

THEOREM 4. For any fixed k,

$$L_k^{\&, \oplus}(\mathrm{MAJ}(n)) = \exp(\Omega(n^{1/k+1})),$$

where $L_k^{\&, \oplus}$ is the realization complexity by circuits of depth k over the basis $\{\&, \oplus\}$.

Proof. Any symmetric function $f(x_1, \ldots, x_n)$ is representable in the form $f(x_1, \ldots, x_n) = \oplus_{i=0}^{n} \lambda_i \mathrm{MAJ}(2n)(x_1, \ldots, x_n, 1^i, 0^{n-i})$, where $\lambda_i \in F_2$. Hence, $L_{k+1}(f) \leq nL_k(\mathrm{MAJ}(2n))$ for any symmetric function $f(x_1, \ldots, x_n)$. Choosing f as the function whose existence is asserted by Lemma 6, we obtain

$$L_k(\mathrm{MAJ}(2n)) \geqslant \frac{1}{70n^3} \exp_2(n^{1/k+1}). \tag{13}$$

Theorem 4 follows from (13).

Remark 1. Since $\vee_{i=1}^{t} f_i = 1 \oplus \&_{i=1}^{t}(f_i \oplus 1)$, then $L_k^{\&, \oplus, \vee} = \Omega(L_{2k}^{\&, \oplus})$, where $L_k^{\&, \oplus, \vee}$ is the realization complexity by circuits of depth k over $\{\&, \vee, \oplus\}$ (the sequence of the operations is arbitrary). Hence we obtain the bound announced in [15],

$$L_k^{\&,\oplus,\vee}(\mathrm{MAJ}(n)) = \exp(\Omega(n^{1/2k+2})). \tag{14}$$

(14), in its turn, implies the conjecture of [3] that $\leq_{cp}$ parity is not true (for all the necessary definitions, see [3]).

Remark 2. After the paper had been submitted, I became aware of new results in this area [16, 17]. In particular, Smolensky [16] proved a generalization of Theorem 4, replacing $\oplus$ with Mod-q, where q is a power of a prime number. Paterson [17] simplified the analysis of Sec. 3 and strengthened the bound of Theorem 4.

LITERATURE CITED

1. N. Blum, "Boolean functions requiring 3n network size," Theor. Comput. Sci., 28, 337-345 (1984).
2. M. Furst, J. B. Saxe, and M. Sipser, "Parity, circuits, and the polynomial time hierarchy," Proc. 22nd Ann. IEEE Symp. on Foundations of Computer Sci. (1981), pp. 260-270.
3. M. Furst, J. B. Saxe, and M. Sipser, "Parity, circuits, and the polynomial time hierarchy," Math. Syst. Theory, 17, 13-27 (1984).
4. M. Ajtai, "Σ_1^1 formulas on finite structures," Ann. Pure Appl. Logic, 24, 1-48 (1983).
5. L. G. Valiant, "Exponential lower bounds for restricted monotone circuits," Proc. 15th Ann. ACM Symp. on Theory of Comp. (1983), pp. 110-187.
6. R. Boppana, "Threshold functions and bounded depth monotone circuits," Proc. 16th Ann. ACM Symp. on Theory of Comp. (1984), pp. 475-479.
7. M. Klaw, W. Paul, N. Pippenger, and M. Yannakakis, "On monotone formulas with restricted depth," Proc. 16th Ann. ACM Symp. on Theory of Comp. (1984), pp. 475-479.
8. A. Yao, "Separating the polynomial-time hierarchy by oracles," Proc. 26th Ann. IEEE Symp. on Foundations of Computer Science (1985), pp. 1-10.
9. J. Hastad, "Almost-optimal lower bounds for small depth circuits," Preprint (1985).
10. A. A. Razborov, "Lower bounds on monotone complexity of some Boolean functions," Dokl. Akad. Nauk SSSR, 281, No. 4, 789-801 (1985).
11. A. A. Razborov, "Lower bounds on monotone complexity of a logical permanent," Mat. Zametki, 37, No. 6, 887-900 (1985).
12. A. E. Andreev, "On a method of obtaining lower complexity bounds of individual monotone functions," Dokl. Akad. Nauk SSSR, 282, No. 5, 1033-1037 (1985).
13. N. Alon and R. B. Boppana, "The monotone circuit complexity of Boolean functions," Preprint (1985).
14. D. Yu. Grigor'ev, "Lower bounds for algebraic complexity of computations," Computational Complexity Theory, I [in Russian], Zapiski LOMI, Vol. 188, Nauka, Leningrad (1982).
15. A. A. Razborov, "Lower bounds on the size of bounded depth circuits over the basis $\{\&, \vee, \oplus\}$," Usp. Math. Nauk, 41, No. 4, 219-220 (1986).
16. R. Smolensky, "Algebraic methods in the theory of lower bounds for Boolean circuit complexity," Preprint, Univ. of California, Berkeley (1986).
17. M. Paterson, "Bounded depth circuits over $\{\oplus, 1\}$," Preprint, Univ. of Warwick (1986).