BOUNDS FOR HODES - SPECKER THEOREM

Pavel Pudlák
Mathematical Institute ČSAV
115 67 Praha
Czechoslovakia

Abstract: In [2] Hodes and Specker proved a theorem which implies that certain Boolean functions have nonlinear formula size complexity. I shall prove that the asymptotic bound for the theorem is n.log log n.

§ 0. Introduction

Let f be a Boolean function, i.e. $f:\{0,1\}^n \to \{0,1\}$ for some positive integer n. The variables of f will be denoted usually by $x_1,\dots,x_n$. Given $1 \leq i_1 < i_2 < \dots < i_r \leq n$, then $f|x_{i_1} x_{i_2} \dots x_{i_r}$ denotes the function from $\{0,1\}^r$ into $\{0,1\}$ obtained by substituting 0's for all the variables of f different from $x_{i_1} \dots x_{i_r}$. In § 5 we shall need substitutions containing also 1's; in such a case we add a superscript to the bar. A base is an arbitrary finite set of Boolean functions Ω ; the elements of Ω are called connectives. The (formula size) complexity of f in base Ω is the number $L_\Omega(f)$ equal to the minimum of the total number of occurrences of variables in an expression over Ω equivalent to f , (or ∞ if such an expression does not exist).

The theorem of Hodes and Specker [2] can be expressed as follows:

If Ω is the base of all binary connectives, (or equivalently $\Omega = \{0,1,\wedge,\oplus\}$), then there exists a function S(r,n) such that for every r

$$\lim_{n \to \infty} S\ (r,n) \longrightarrow \infty \quad ,$$

and if

(1) $L_\Omega(f) \leq n.\ S(r,n)$, then there exist $1 \leq i_1 < \dots < i_r \leq n$ and a Boolean function b(x,y) of two arguments such that

$$f|x_{i_1} \dots x_{i_r} \equiv b(x_{i_1} \oplus \dots \oplus x_{i_r} , x_{i_1} \vee \dots \vee x_{i_r}).$$

($\oplus$ denotes addition modulo 2).

This form of the statement is convenient for the proof. For the proofs of lower bounds the theorem is used the other way around, namely, if f does not have a restriction of the form above, then it has complexity $n \cdot S(r,n)$, thus nonlinear. The function S constructed by Hodes and Specker grows for fixed r more slowly than $\log^{*} n$ (which is the inverse function to $2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$ m-times). The aim of this paper is to show that the theorem holds in an arbitrary base Ω with the estimate (1) replaced by

$$L_{\Omega}(f) \leq \varepsilon_{\Omega} . n(\log \log n - \log r)$$

for some $\varepsilon_{\Omega} > 0$. All the logarithms in this paper are of base 2. Further, I shall show that for $\Omega = \{\oplus, \wedge, \vee\}$ and $r \geq 3$ fixed, the bound is asymptotically best; this was done jointly with S. Poljak. Since Hodes-Specker theorem has a direct application to lower bounds on complexity of symmetric Boolean functions, the paper is also a contribution to this still open field.

My method of the proof is based on the Ramsey theorem. This is not surprising since the theorem (in the form above) resembles the Ramsey theorem. The Ramsey theorem has been used by Vilfan [11] for proving a generalization of Hodes-Specker theorem but in a different manner. The idea of my proof is very simple. Let $\alpha(x_1,\dots,x_n)$ be a formula of small complexity. For every i,j, $1 \leq i < j \leq n$, define the induced formula $\alpha\{x_i,x_j\}$ in a suitable way and so that the number of occurrences of x_i,x_j in the induced formula is the same as in the original one and it does not contain other variables. This concept is almost the same as the one used by Nečiporuk in [8]. Since the complexity of α is small, the number of occurrences of x_i in α is small for many i's, say for x_i, $i=1,\dots, m \geq n/2$. If I restrict myself to this set of variables then the number of nonisomorphic induced formulae is small. Now I colour the pairs (i,j) from $\{1,\dots,m\}$ by "the shape of $\alpha\{x_i,x_j\}$". Using the Ramsey theorem I get a subset $\{i_1,\dots,i_r\} \subseteq \{1,\dots,m\}$ such that for every $a<b$, $c<d$, $\alpha\{x_{i_a}, x_{i_b}\}$ is isomorphic to $\alpha\{x_{i_c}, x_{i_d}\}$. The same is true if I use the induced formula $\beta = \alpha\{x_{i_1},\dots, x_{i_r}\}$, (defined similarly) instead of α. Then it is shown that formulae with this property (it is natural to call them homogeneous formulae) have a very special shape which forces them to be equivalent to $b(x_{i_1} \oplus \dots \oplus x_{i_2}, x_{i_1} \vee \dots \vee x_{i_r})$. This is the longest part of the proof since (as it

is often the case in lower bound proofs) one has to consider many cases. The concept of inducing is, of course, chosen so that β is equivalent to the formula obtained from α by substituting 0's for every variable different from $x_{i_1},\dots,x_{i_r}$.

It seams that the method could be used for some other kinds of complexity, (e.g. number of arithmetic operations), therefore in § 1 I prove a theorem about general terms. In § 2 the theorem is applied to Boolean formulae in order to obtain the main result.

§ 1 Structure of homogenous terms

In this paragraph I shall use terms (denoted by α, β, ...) of the language consisting of a set of variables $V = \{x_1,\dots,x_n\}$, (denoted also by $x,y,z,u,v,\dots$) a set of at least binary operations Ω (denoted by a,b,d, ...) and a single constant c. The set of variables which occur in a term α will be denoted by $V(\alpha)$. We shall agree to write $\alpha(u_1,\dots,u_k)$ to indicate that $V(\alpha) \subseteq \{u_1,\dots,u_k\}$.

It is important to visualize terms as rooted trees in which the vertices are the leaves labelled by the elements of V c and junctions labelled by the elements of Ω of the corresponding arity; moreover the leaves are lineariily ordered, which induces a linear ordering of the successors of any junction. The tree structure determines an ordering of the vertices, namely, u is below v iff the shortest path from v to the root contains u iff the subterm determined by v is a subterm of the subterm determined by u. The isomorphism of terms will be defined by $\alpha(u_1,\dots,u_k) \cong \beta(v_1,\dots,v_k)$ iff

$$\alpha(u_1,\dots,u_k) = \beta(v_1/u_1,\dots,v_k/u_k),$$

where y/z denotes the substitution of z for every occurrence of y. From this point on I shall use the less precise notation without the substitution sign.

Definition

Let α be a term, $X \subseteq V$. The term induced by X will be denoted by X and defined inductively by

$cX = c$;

$x_iX = x_i$ if $x_i \in X$,

$\quad = c$ otherwise;

$b(\alpha_1,\dots,\alpha_k) = \alpha_iX$ if $\alpha_jX = c$ for all $j \neq i$,

$\quad = b(\alpha_1X,\dots,\alpha_kX)$ otherwise.

(hence $= c$ if $\alpha_j X = c$ for all j).

Less formally the induced term αX can be defined as follows. If $X \cap V(\alpha) = \emptyset$ then $\alpha X = c$. Otherwise

(i) omit from α all the junctions v such that the subformula determined by v is of the form $b(\beta_1,\dots,\beta_k)$, where $V(\beta_i) \cap X \neq \emptyset$ for at most one i;

(ii) omit all the leaves labelled by the elements of $V(\alpha) - X$;

(iii) at the junctions whose arity does not correspond to the number of predecessors, fill the remaining places by c; and preserve the labeling and the orderings. (The operation (iii) is never used if Ω contains only binary symbols.) Whence we have the following lemma.

Lemma 1.1 $X \subseteq Y \Rightarrow X = (\alpha Y)X$. □

If $X = \{x_{i_1},\dots,x_{i_k}\}$, $Y = \{x_{j_1},\dots,x_{j_k}\}$, $i_1 < \dots < i_k$, $j_1 < \dots < j_k$ then I shall write

$$\alpha X \cong \beta Y$$

instead of

$$\alpha X(x_{i_1},\dots,x_{i_k}) \cong \beta Y(x_{j_1},\dots,x_{j_k}).$$

Definition

A term α is called k-homogeneous over Z iff $\forall X,Y \subseteq Z, |X| = |Y| = k$,

$$\alpha X \cong \alpha Y.$$

I shall omit k and/or Z if $k = 2$, $Z = V$.

Lemma 1.2 If $|V| \geqslant 3$ and α is homogeneous then α is 1-homogeneous.

Proof: easily from Lemma 1.1. □

I shall use also the following notation:

$$\alpha[y_1,\dots,y_k]$$

means that *every* y_i *occurs in* α *exacitly once* and α *does not contain other variables*;

$$\alpha(u,v]$$

means that $V(\alpha) = \{u,v\}$ and v *occurs in* α *exactly once*.

If α can be expressed in the form $\varphi(u,\psi]$, where ψ is not a single variable, then u is uniquely determined; if moreover ψ is minimal, then also φ and ψ are uniquely determined.

Examples.

1. $a(b(d(y,z), e(x,x)),x) = \varphi(x,\psi]$ where
   $\varphi(u,v] = a(v,u)$, $\psi = b(d(y,z), e(x,x))$,

or

$\varphi(u,v] = a(b(v,e(u,u)),u)$, $\psi = d(y,z)$.

2. $a(b(x,y), d(x,e(z,x)))$ cannot be decomposed.

Theorem 1.3 (Structure of homogeneous terms.) Let α be a homogeneous term, $V = \{x_1,\dots,x_n\}$, $n \geqslant 3$, and suppose α does not contain constant subterms other then c. Then at least one of the following conditions holds:

1) $\alpha = c$;

2) $\alpha = b(\beta_1,\dots,\beta_k)$ and $\beta_1,\dots, \beta_k$ are homogeneous;

3) $\alpha = \varphi(x_1, \varphi(x_2,\dots,\varphi(x_n, \delta] \dots]]$ or
   $\alpha = \varphi(x_n, \varphi(x_{n-1},\dots \varphi(x_1, \delta] \dots]]$ and δ is homogeneous;

4) $\alpha = \varphi(x_1, \varphi(x_2,\dots \varphi(x_{n-1}, \psi(x_n)] \dots]]$,
   or the same with the reverse order of variables;

5) $\alpha = \varphi[\delta(x_1),\dots,\delta(x_n)]$ where, for some $b \in \Omega$ and $i < j$, every nontrivial subformula of $\varphi[y_1,\dots,y_n]$ is of the form
$$b(c,\dots,c,\mu,c,\dots,c, \nu ,c,\dots,c).$$
   where μ , ν are on the i-th and j-th places.

If moreover α is 3-homogeneous, then at least one of the conditions 1)-4) holds.

An example of a homogeneous term is shown on Fig.1.

Proof:

(i) First I prove the theorem for Ω consisting of binary operations only. The binary operations will be denoted by an infix o , thus different occurrences of o may denote different operations. Let α be a homogeneous term. I omit the trivial case when α is a variable or the constant, and assume $\alpha = \beta \circ \gamma$. Consider the following three main cases (with several subcases):

1. $V(\beta) \cap V(\gamma) = \emptyset$.

1.1. If $V(\beta) = \emptyset$, then $\alpha X = \gamma X$, thus β and γ are homogeneous, which is condition 2) of the theorem. If $V(\gamma) = \emptyset$, then we get the same.

1.2. Let $u \in V(\beta)$, $v \in V(\gamma)$. Then

(1) $\alpha\{u,v\} = \beta\{u\} \circ \gamma\{v\}$.

Let $w \in V$ be an arbitrary element, and let δ be the smallest subterm of α containing all the occurrences of w . If there were an occurrence of z in δ , $z \neq w$, then $\alpha\{w,z\}$ could not be isomorphic to (1). Thus I have proved that
$$\alpha = \varphi[\delta_1(x_1),\dots, \delta_n(x_n)] .$$
1-homogeneity of α , (Lemma 1.2), implies
$$\delta_1(t) = \dots = \delta_n(t),$$
and homogeneity implies that all the operations in

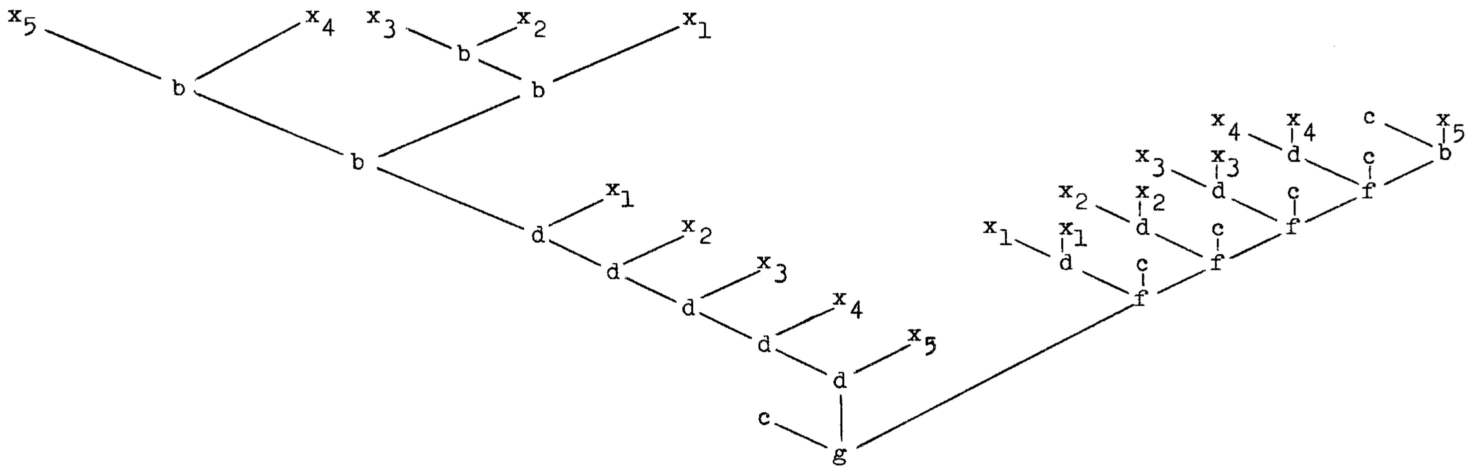


Fig.1. An example of a homogeneous term;
n = 5, b,d binary, f,g ternary.

$\varphi[y_1,\dots,y_n]$ are equal, thus we get 5).

2. $V(\beta) = V(\gamma) = V$. Then

$$\alpha X = \beta X \circ \gamma X,$$

thus β , γ are homogeneous - condition 2).

3. $V(\beta) \cap V(\gamma) \neq \emptyset$ and $V(\beta) \subsetneqq V$. (The case $V(\gamma) \subsetneqq V$ is symmetric).

3.1. Claim: $|V(\beta)| = 1$.

If not, then we have $u \in V(\beta)$, $v \in V(\beta) \cap V(\gamma)$, $w \in V(\beta)$, $w \neq v$. Then

$$\alpha\{u,v\} = \beta\{v\} \circ \gamma\{u,v\},$$
$$\alpha\{w,v\} = \beta\{w,v\} \circ \gamma\{w,v\}.$$

(w may not occur in $\gamma\{w,v\}$). This two terms cannot be isomorphic, since $\beta\{v\}$ contains only one variable, while $\beta\{w,v\}$ contains two.

3.2. Claim: $V(\beta) = \{x_1\}$ or $V(\beta) = \{x_n\}$.

If $V(\beta) = \{x_i\}$, $1 < i < n$, then the first occurrence of a variable bóth in $\alpha\{x_1,x_i\}$ and $\alpha\{x_i x_n\}$ is x_i, thus they would not be isomorphic.

Henceforth assume $V(\beta) = \{x_1\}$ ($=\{x_n\}$ being symmetric). By the assumption of this case $x_1 \in V(\gamma)$, hence $V(\gamma) = V(\alpha) = V$.

3.3 Claim: $\alpha = \varphi_1(x_1, \varphi_2(x_2,\dots \varphi_{n-1}(x_{n-1}, \psi] \dots]]$.

I shall prove by induction for $i = 1,\dots,n-1$,

(2) $\alpha = \varphi_1(x_1,(\varphi_2(x_2,\dots \varphi_i(x_i, \psi_i] \dots]]$.

For $i = 1$ this is just the assumption $V(\beta) = \{x_1\}$.

Suppose (2) for $i < n-1$ and chose ψ_i minimal. Then $\psi_i = \mu \circ \nu$ where $V(\mu)$, $V(\nu)$ are not subsets of $\{x_i\}$.

3.3.1. First I show

$$x_{i+1} \in V(\mu) \cap V(\nu).$$

Suppose not, say $x_{i+1} \in V(\mu) - V(\nu)$. Then $x_j \in V(\nu)$ for some $j \neq i,i+1$. If $i+1 < j$, then

$$\alpha\{x_{i+1},x_j\} = \mu\{x_{i+1},x_j\} \circ \nu\{x_j\} \ncong$$
$$\alpha\{x_1,x_2\} = \beta\{x_1\} \circ \gamma\{x_1,x_2\},$$

since $x_2 \in V(\gamma)$, - contradiction. If $j < i$, then

$\alpha\{x_j,x_{i+1}\} = \varphi_j(x_j, \mu\{x_j,x_{i+1}\} \circ \nu\{x_j\}] = \varphi'(x_j, \mu\{x_j,x_{i+1}\}]$;

$\alpha\{x_j,x_i\} = \varphi_j(x_j, \varphi_i(x_i, \psi_i\{x_i,x_j\}]]$.

This two terms cannot be isomorphic, since there are more occurrences of u in $\varphi'(u,v]$ than in $\varphi_j(u,v]$, - contradiction.

3.3.2. Now I show

(3) $V(\mu) = \{x_{i+1}\}$.

For $j > i+1$, x_j cannot belong to $V(\mu)$ since
$\alpha\{x_{i+1}, x_j\} = \mu\{x_{i+1},x_j\} \circ \mu\{x_{i+1},x_j\} \cong$
$\cong \alpha\{x_1,x_2\} = \beta\{x_1\} \circ \gamma\{x_1,x_2\}$.
If $x_j \in V(\mu)$ for some $j < i+1$, then the following two terms could not be isomorphic
$\alpha\{x_j,x_{i+1}\} = \varphi_j(x_j, \mu\{x_j,x_{i+1}\} \circ \nu\{x_j,x_{i+1}\}]$;
$\alpha\{x_j,x_n\} = \varphi_j(x_j, \mu\{x_j\} \circ \nu\{x_j,x_n\}]$.
Thus, by (3), ψ_i can be expressed in the form

$\psi_i = \varphi_{i+1}(x_{i+1}, \psi_{i+1}]$,
which ends the proof of the claim.

3.4. Claim: If ψ is minimal in 3.3, then
(4) $\varphi_1(u,v = \dots = \varphi_{n-1}(u,v]$.
Let ψ be minimal.If $V(\psi) = \{x_n\}$, then, for $i < n$,

$$\alpha\{x_i,x_n\} = \varphi_i(x_i, \psi\{x_n\}],$$

and the claim follows easily from homogeneity. Otherwise ψ contains at least two variables, hence $\psi = \mu \circ \nu$ for some μ, ν. Using the same argument as in 3.3.1 one can show that $x_n \in V(\mu) \cap V(\nu)$. Thus for $i < n$
(5) $\alpha\{x_i,x_n\} = \varphi_i(x_i, \mu\{x_i,x_n\} \circ \nu\{x_i,x_n\}]$,
whence the claim follows easily.

If $V(\psi) = \{x_n\}$, then α is of the form 4). Therefore it remains to consider the case when $V(\psi)$ is larger. Then $V(\psi) = V$, since α must contain the same number of occurrences of every variable and by 3.3 and 3.4.

3.5. Claim: $\psi = \varphi_n(x_n, \chi]$, for some φ_n and χ. In the proof of 3.4 I have shown (5) (for every $i < n$). This term must be isomorphic to

$\alpha\{x_1,x_2\} = \varphi_1(x_1, \varphi_2(x_2, \psi_2\{x_1,x_2\}]]$.
Moreover we know that $\varphi_1(u,v] = \varphi_2(u,v]$, thus for some term f ,
$\varphi_2(x_2, \psi_2\{x_1,x_2\}] = \beta(x_2) \circ f \cong \mu\{x_i,x_n\} \circ \nu\{x_i,x_n\}$.
Hence $V(\mu) = \{x_n\}$, which proves the claim.

Further I shall assume that χ in 3.5 is minimal.

3.6. Claim: $\varphi(u,v] =_{df} \varphi_1(u,v] = \dots = \varphi_{n-1}(u,v]$ does not contain more occurrences of u then $\varphi_n(u,v]$.

3.6.1. First assume $x_n \in V(\chi)$. Then
(6) $\alpha\{x_1,x_2\} = \varphi(x_1, \varphi(x_2, \chi\{x_1,x_2\}]] \cong \alpha\{x_1,x_n\} = \varphi(x_1, \varphi_n(x_n, \chi\{x_1\}]]$,
whence the claim follows. In the rest of the proof of the claim I assume $x_n \in V(\chi)$ and $\chi = \mu \circ \nu$, for some $\mu \circ \nu$.

3.6.2. If $x_j \in V(\mu) \cap V(\nu)$, $j < n$, then $\chi\{x_j,x_n\}$ is the minimal term such that $\alpha\{x_j,x_n\}$ can be expressed as

$\varphi(x_j, \varphi_n(x_n, \chi\{x_j,x_n\}]]$.

Comparing this decomposition with the decomposition of $\alpha\{x_1,x_2\}$ in (6) the claim follows.

3.6.3. I shall show that $V(\mu) \cap V(\nu) \neq \{x_n\}$. If not, then there are $x_i \in V(\mu) - V(\nu)$, $x_j \in V(\nu) - V(\mu)$, $i,j \neq n$, since χ is minimal. Then

$\alpha\{x_i,x_n\} = \varphi(x_i, \varphi_n(x_n, \mu\{x_i,x_n\} \circ \nu\{x_n\}]] \ncong$
$\ncong \alpha\{x_j,x_n\} = \varphi(x_j, \varphi_n(x_n, \mu\{x_n\} \circ \nu\{x_j,x_n\}]]$,

a contradiction.

3.6.4. It remains to consider $V(\mu) \cap V(\nu) = \emptyset$. Suppose it is so and $x_n \in V(\mu)$. (The proof would be similar if $x_n \in V(\nu)$). Choose x_i,x_j as in 3.6.3. If $i < j$, then

(7) $\alpha\{x_i,x_j\} \cong \alpha\{x_i,x_n\}$,
hence

$\varphi(x_j, \mu\{x_j\} \circ \nu\{x_i\}] \cong \varphi_n(x_n, \mu\{x_n\} \circ \nu\{x_i\}]$.

This isomorphism maps $\nu\{x_i\}$ onto itself, hence $\mu\{x_j\} \circ \nu\{x_i\}$ onto $\mu\{x_n\} \circ \nu\{x_i\}$, thus $\varphi(u,v] = \varphi_n(u,v]$, which is even more than I wanted to prove. If $j < i$ then in (7) $\mu\{x_j\}$ must be mapped onto $\nu\{x_i\}$, by the uniqueness of the decomposition, and then $\mu\{x_j\} \circ \nu\{x_i\}$ onto $\mu\{x_n\} \circ \nu\{x_i\}$ which is impossible. Thus 3.6 is proved.

Now I can end Case 3. Since

$\alpha\{x_1\} = \varphi(x_1, \chi\{x_1\}] \cong \alpha\{x_n\} = \varphi_n(x_n, \chi\{x_n\}]$, and by 3.6, either
$\varphi_n(u,v] = \varphi(u,v]$,
or there is some φ' such that
$\varphi_n(u,v] = \varphi(u,\varphi'(u,v]]$.
Thus for some term δ,
$\alpha = \varphi(x_1, \varphi(x_2, \ldots \varphi(x_n, \delta] \ldots]]$.

Since for $i<j$,

$$\alpha\{x_i,x_j\} = \varphi(x_i, \varphi(x_j, \delta\{x_i,x_j\}]] ,$$

δ is homogeneous, i.e., condition 3).

(ii) Now let α be a homogeneous term over a general base Ω . For every operation $b \in \Omega$ of arity $k \geqslant 3$, choose $k-1$ new binary operations $b_1,\dots,b_{k-1}$. Let α' be the term resulting from α by applying all the possible substitutions of the form

$$b(\beta_1,\dots,\beta_k) \longmapsto b_1(\beta_1,b_2(\beta_2,\dots b_{k-1}(\beta_{k-1},\beta_k)\dots)).$$

Claim: α' is homogeneous. This is because similar operations produce $\alpha' X$ from αX, namely, the operations of the form

$$b(c,\dots,c,\alpha_{i_1},c,\dots,c,\alpha_{i_2},c,\dots\ \dots,c,\alpha_{i_j},c,\dots,c) \longmapsto$$
$$\longmapsto b_{i_1}(\alpha_{i_1},b_{i_2}(\alpha_{i_2},\dots b_{i_{j-1}}(\alpha_{i_{j-1}},\alpha_{i_j})\dots)).$$

By (i) I know that at least one of the five conditions of the theorem holds for α'. Accordingly I shall consider four cases.

1. $\alpha' = c$, then $\alpha = c$.

$\alpha' = \beta \circ \gamma$, and β , γ are homogeneous, then

$\alpha = b(\beta,\beta_2,\dots,\beta_k)$, $k \geqslant 2$,

where $V(\beta) = V = V(\gamma) = \bigcup_{i=2}^{k} V(\beta_i)$. Whence

$$\alpha X = b(\beta X, \beta_2 X,\dots,\beta_k X),$$

thus $\beta,\beta_2,\dots,\beta_k$ are homogeneous - condition 2).

3. If 3) or 4) holds for α' then

$\alpha' = \varphi'(x_1,\varphi'(x_2,\psi_2]]$,

(or with x_n,x_{n-1} instead of x_1,x_2).

3.1. Claim: φ' corresponds to a part of the original term α . Suppose not, then for some operation b of α , $i<j$ and terms $\xi'(x_1),\mu',\nu'$,

(8) $\alpha' = b_i(\xi'(x_1),b_j(\mu',\nu'))$,

or for some term ψ ,

$\alpha' = \psi(x_1,b_i(\xi'(x_1),b_j(\mu',\nu')))$,

where

(9) $b_j(\mu',\nu') = \varphi'(x_2,\psi_2]$.

Without loss of generality I shall consider only (8). Then α is of the following form

$b(\dots\ \xi(x_1)\ \dots\ \mu\ \dots\ \nu_1\ \dots\ \nu_2\ \dots\ \dots\ \nu_m\ \dots)$, where only f ,μ, $\nu_1,\dots,\nu_m$ are different from c , and

$V(\mu) = V(\mu')$, $\bigcup_{i=1}^{m} V(\nu_i) = V(\nu')$.

By (9), $V(\mu') = \{x_2\}$ or $V(\nu') = \{x_2\}$. In the first case

$\alpha\{x_1,x_2\} = b(\dots f(x_1)\dots \mu(x_2) \dots \nu_1\{x_1,x_2\} \dots \nu_m\{x_1,x_2\} \dots)$,

while a term corresponding to $\mu(x_2)$ in $\alpha\{x_1,x_3\}$ is missing - contradiction. The second case is ruled out by a similar argument, thus the claim is proved.

Now the condition 3) or 4) follows easily from the claim. If e.g.

$\alpha' = \varphi'(x_1, \varphi'(x_2,\dots \varphi'(x_n, \delta']\dots]]$,

then

$= \alpha(x_1, \varphi(x_2,\dots \varphi(x_n, \delta]\dots]]$,

where φ is the term corresponding to φ'. Homogeneity of δ can be proved in the same way as in (i).

4. $\alpha' = \varphi'[\delta'(x_1),\dots,\delta'(x_n)]$, and all the operations in $\varphi'[y_1,\dots,y_n]$ are the same. If this is an operation of Ω then, clearly, $\alpha = \varphi'[\delta_1(x_1),\dots,\delta_n(x_n)]$. If it is b_i, for some $b \in \Omega$, then different occurrences of b_i in α must correspond to different occurrences of b in α , (since they have the same index i). Thus again $\alpha = \varphi[\delta_1(x_1),\dots,\delta_n(x_n)]$. The rest is the same as in (i), 1.2.

(iii) Let α be 2- and 3-homogeneous. Suppose 5) holds. Then because of 3-homogeneity also 4) holds.□

Remarks.

1. An easy corollary of the theorem is that if α is 1,2,3-homogeneous, then it is k-homogeneous for every $k \leq n$. It would be more appropriate to reserve the word "homogeneous" for this concept.

2. The theorem can be inverted if the relation of ψ to φ in 4) is specified.

§ 2 The lower bound theorem

In this paragraph I shall apply Theorem 1.3 to Boolean formulae. For sake of convenience I consider only bases which contain nullary connectives (constants) 0,1, unary connectives $\neg(x)$, $\underline{0}(x)$, $\underline{1}(x)$, and do not contain the identity unary connective. The letters will be used in a similar way as in § 1, i.e. α, β , ..., are formulae,

$x,y,z,u,v,\dots$ variables, $a,b,d,\dots$ at least unary connectives, c, c_i for $0,1$, etc. Also I shall assume that the formulae do not contain parts of the form $a_1(a_2(\beta)),(a_1,a_2$ unary connectives), or $(b(c_1,\dots,c_k)$, (b a k-ary connective and $c_i \in \{0,1\}$).

Definition

Let α be a Boolean formula, X a set of variables. Then αX_B - the formula B-induced by X is the formula produced from α by the following rules:

1) substitute 0 for the variables of X;
2) replace every part $b(c_1,\dots,c_k)$ by the corresponding constant;
3) replace every part $b(\alpha_1,\dots \alpha_k)$, where only α_i is a nonconstant, by α_i or $a(\alpha_i)$, where a is the corresponding unary connective;
4) replace every part $a_1(a_2(\beta))$ by β or $a(\beta)$, where a is the corresponding unary connective $(a(x) = a_1(a_2(x)))$.

k-B-homogeneous and B-homogeneous formulae are defined analogically as in § 1.

For a formula α denote by $F(\alpha)$ the term which results from α by omitting the unary connectives of α and replacing 0's and 1's by the symbol c. (Clearly, if α is a formula in the sense of this paragraph then $F(\alpha)$ is a term in the sense of § 1.)

Lemma 2.1

1) $X \subseteq Y \Longrightarrow \alpha X_B = (\alpha Y_B)\ Y_B$;
2) α is B-homogeneous over $Z \Rightarrow \alpha Z_B$ is B homogeneous over Z, (α may contain other variables than those in Z);
3) $F(\alpha X_B) = (F(\alpha))X$;
4) α is B-homogeneous over $Z \Rightarrow F(\alpha)$ is homogeneous over Z;
5) α is B-homogeneous over Z, $|Z| \geqslant 3 \Rightarrow \alpha$ is 1-B-homogeneous.

Proof:

If $V(\alpha) \cap X \neq \emptyset$, then αX_B can be constructed as follows:

1. construct $(F(\alpha))X$,
2. add the corresponding unary connectives and replace the symbol c by the corresponding constants.

Whence we obtain 3). Then using Lemma 1.1 we get 1). The implications 1) $\Rightarrow$ 2), 1) $\Rightarrow$ 5), 3) $\Rightarrow$ 4) are trivial. □

Lemma 2.2 (Structure of B-homogeneous formulae). Let $\alpha(x_1,\dots,x_n)$ be B-homogeneous over $V = \{x_1,\dots,x_n\}$, $n \geq 3$. Then at least one of the following conditions holds:

1) $\alpha \equiv$ constant;

2) $\alpha = b(\beta_1,\dots,\beta_k)$, $b \in \Omega$, $k \geq 1$, and $\beta_1,\dots,\beta_k$ are B-homogeneous;

3) $\alpha = \varphi(x_1, \varphi(x_2, \dots \varphi(x_{n-1}, \psi(x_n, \delta]] \dots]]$, or with the reverse order of variables, where δ is B-homogeneous, $\varphi(u,v] = \psi(u,v]$ or $\varphi(u,v] = \psi(u, \neg v]$, and $\varphi(u,v]$ is equivalent either to $u \oplus v$ or $u \vee v$ or $\neg u \wedge v$ or v;

4) $\alpha = \varphi(x_1, \varphi(x_2, \dots \varphi(x_{n-1}, \psi(x_n)] \dots]]$, or with the reverse order of variables, where
   (i) either $\varphi(u,v] \equiv u \oplus v$ and ($\psi(u) \equiv u$ or $\psi(u) \equiv \neg u$),
   (ii) or $\varphi(u,v] \equiv u \vee v$ and $\psi(u) \equiv u$,
   (iii) or $\varphi(u,v] \equiv \neg u \wedge v$ and $\psi(u) \equiv \neg u$;

5) $\alpha = \varphi[\delta(x_1), \dots, \delta(x_n)]$, where for some $c \in \{0,1\}$,
   (i) either $\varphi[y_1,\dots,y_n] \equiv c \oplus y_1 \oplus \dots \oplus y_n$,
   (ii) or $\varphi[y_1,\dots,y_n] \equiv c \oplus (y_1 \vee \dots \vee y_n)$ and $\delta(y) \equiv y$,
   (iii) or $\varphi[y_1,\dots,y_n] \equiv c \oplus (y_1 \wedge \dots \wedge y_n)$ and $\delta(y) \equiv \neg y$.

Proof:
Let α be B-homogeneous over V. By Lemma 2.1, $F(\alpha)$ is homogeneous. If $F(\alpha) = c$, then α is constant. Now assume that α is not constant. Then by Theorem 1.3 at least one of the conditions 2)-5) holds for $F(\alpha)$. I shall consider five cases.

1. $\alpha = a(\beta)$, where a is a unary connective. Since α is not constant, $a = \neg$, and $V(\beta) = V$. Let $\emptyset \neq X \subseteq V$, $|X| = 2$, then αX_B is either a variable or a more complicated formula. If αX_B is a variable, or if the main connective of it is at least binary, then $\alpha X_B = \neg \beta X_B$. If $\alpha X_B = b(\gamma)$, $b(x) = \neg(x)$, $\underline{0}(x)$, $\underline{1}(x)$ resp. then $\beta X_B = \gamma$, $\underline{1}(\gamma)$, $\underline{0}(\gamma)$ resp. Thus

$$\alpha X_B \cong \alpha Y_B \Rightarrow \beta X_B \cong \beta Y_B,$$

hence β is homogeneous. This proves condition 2) of the lemma.

Henceforth I shall assume that the main connective of α is at least binary.

2. $F(\alpha) = b(\beta_1,\dots,\beta_k)$, $\beta_1,\dots,\beta_k$ homogeneous. Then $\alpha = b(\gamma_1,\dots,\gamma_k)$ and $V(\gamma_i) = V(\beta_i) = V$ for $i = 1,\dots,k$. Thus
$\alpha X_B = b(\gamma_1 X_B,\dots,\gamma_k X_B)$,

whence $\gamma_1,\dots,\gamma_k$ are B-homogeneous - condition 2).

3. $F(\alpha) = \varphi'(x_1, \varphi'(x_2,\dots, \varphi'(x_n,\delta']]$where δ' is homogeneous. (I shall not consider the symmetric case where the variables are in the reverse order.) Then α can be decomposed as follows

(1) $\alpha = \varphi_1(x_1, \varphi_2(x_2,\dots \varphi_n(x_{n-1},\delta]\dots]]$.

The decomposition might not be unique because of unary connectives. Therefore I postulate that the unary connective which is possible to include either in φ_i or φ_{i+1}, $i<n$ be included in φ_i. The unary connective between φ_n and δ will be included in φ_n if and only if there is the same connective between φ_1 and φ_2. Now $\varphi_2,\dots,\varphi_n$ have the main connective at least binary; the same is true about φ_1, since this is the assumption above. The formula $\alpha\{x_1\}$, hence any $\alpha\{x_i\}$ too, has the main connective at least binary. This proves that

(2) $\varphi_1(0,v]\equiv \dots \equiv\varphi_{n-1}(0,v]\equiv v$.

Hence, for $i<n$,

$\alpha\{x_i,x_n\} = \varphi_i(x_i, \varphi_n(x_n, \delta]\{x_i,x_n\}]$,

therefore $\varphi_1 = \varphi_2 = \dots = \varphi_{n-1}$. I shall denote these by φ and φ_n by ψ. Since

$F(\varphi(u,v]) = \varphi'(u,v] = F(\psi(u,v])$

and since

$\alpha\{x_1\} \cong \alpha\{x_n\}$,

the only difference between $\varphi(u,v]$ and $\psi(u,v]$ might be the unary connective at v. Recall that the decomposition (1) is chosen so that if there is a unary connective at v in $\psi(u,v]$ then the same is at v in $\varphi(u,v]$. By (2) the connective can be only the negation. Thus

(3) $\varphi(u,v] = \psi(u,v]$ or $\varphi(u,v] = \psi(u,\neg v]$.

Then, by (2),

(4) $\psi(0,v] = v$ or $\psi(0,v] = \neg v$ respectively.

Since $\delta' = F(\delta)$ is homogeneous and α is B-homogeneous, the only difference between δX_B and δY_B, $|X|=|Y|= 2$, might be the main unary connective. Using (2), (3) and (4), one can easily compute that the parity of the number of negations before the last junction of δ is always the same. Hence δX_B and δY_B are isomorphic, which proves that δ is B-homogeneous. The rest of condition 3) follows from $\varphi(0,v]\equiv v$.

4. Suppose condition 4) of Theorem 1.3 holds for $F(\alpha)$. Then , using quite a similar argument, one can prove condition 4) of the lemma. The relation between φ and ψ follows easily from B-homogeneity and the assumption that α is nonconstant.

5. Suppose condition 5) of Theorem 3.1 holds for $F(\alpha)$. Then $\alpha = \varphi[\delta_1(x_1),\ldots, \delta_n(x_n)]$. This decomposition is not unique again. If I choose $\delta_1,\ldots,\delta_n$ so that their main connectives are not unary, then, by 1-B-homogeneity, $\delta_1 = \delta_2 = \ldots = \delta_n$. Thus I can drop out the subscripts at δ. Since α is nonconstant, $\delta(x) \equiv x$ or $\equiv \neg x$. The assumption about $F(\alpha)$ implies that there are occurrences of only one connective b of arity $k \geq 2$ in φ, and they are always in a contex

$$(5) \qquad \ldots\ b(c_1,\ldots,c_i, \mu, c_{i+2},\ldots,c_j, \nu, c_{j+2},\ldots,c_k)\ \ldots\ .$$

Every Boolean formula of two arguments is equivalent to a formula

$$(6) \qquad d(e_1(x) \mathrm{o}\ e_2(y)),$$

where any of the unary connectives $d, e_1 e_2$ may be missing and $\mathrm{o} \in \{\oplus , \vee\}$. Choose such a formula for

$$b(c_1,\ldots,c_i,x,c_{i+2}\ldots c_j,y,c_{j+2},\ldots,c_k),$$

replace every occurrence of (5) in φ by this formula, and collect consecutive unary connectives. Denote by ψ the resulting formula. ψ contains only binary and unary connectives. Denote by $\beta = \psi\ [\delta(x_1),\ldots, \delta(x_n)]$.
Since $\psi \equiv \varphi$,
$\beta\{x_i\} = \alpha\{x_i\}$.

A similar argument shows that $\beta\{x_i,x_j\}$, $1 \leq i < j \leq n$ can be constructed from $\alpha\{x_i,x_j\}$ using the same procedure by which I constructed β from α . Thus β is B-homogeneous.

Now I shall consider three cases.

5.1. The binary connectives of φ are $\oplus$. If there occurs a constant unary connective in ψ , then some, hence by 1-B-homogeneity every, $\beta\{x_i\}$ must be constant. Since the binary connectives are $\oplus$, this is possible only if there is a constant unary connective on every path from a variable to the root. Then ψ , hence also α , is constant - contradiction. If there is no constant unary connective in ψ , then $\psi(y_1,\ldots,y_n)$, hence $\varphi(y_1,\ldots,y_n)$, is equivalent to $t \oplus y_1 \oplus \ldots \oplus y_n$, $t \in \{0,1\}$, i.e. condition 5), (i) of the lemma.

5.2. The binary connectives of γ are $\vee$ and $\delta(x) \equiv x$. Then $\gamma[x_1,\ldots,x_n]$ is B-homogeneous, as it is equivalent to β . Let, for $1 \leq i < j \leq n$,

(7) $\gamma\{x_i,x_j\} = f(g_1(x_i) \vee g_2(x_j))$,

where any of the unary connectives f, g_1,g_2 may be missing. If f is not missing, then it is also the main connective of γ (consider $\gamma\{x_1,x_n\}$). It was shown in part 1 of the proof that in such a case after removing the main connective I get a B-homogeneous formula again. Thus without loss of generality I can assume that f is missing.

Claim: The unary connectives may occur only at the variables of γ .

Suppose not. Take some junction such that there is exactly one unary connective below it. Let i,j be such that the paths from x_i and x_j to the root meet at it for the first time. Then f must occur in (7) - contradiction.

$\underline{1}$ cannot occur in γ since γ is not constant. Suppose γ contains $\neg$. Then by 1-B-homogeneity it must contain at least two occurences of $\neg$. By B-homogeneity it must contain three such occurrences. But then f must occur in (7) again - contradiction. Now we know that only $\underline{0}$ may occur in γ . But if $\underline{0}$ was at one variable then it must be at every one. This would be a contradiction since γ is not constant. Thus I have proved that γ may contain a unary connective only as the main connective. Hence we have 5), (ii) of the lemma.

5.3. The binary connectives of γ are $\vee$ and $\delta(x) \equiv \neg x$. This is dual to 5.2, hence

$$\gamma[y_1,\ldots,y_n] \equiv c \oplus (x_1 \wedge \ldots \wedge x_n), \quad c \in \{0,1\},$$

and 5) (iii) follows.□

Corollary 2.3 Let α be B-homogeneous over V, $V(\alpha) \subseteq V = \{x_1,\ldots,x_n\}$ $n \geq 3$. Then, for some Boolean function of two arguments b ,

$$\alpha(x_1,\ldots,x_n) \equiv b(x_1 \oplus \ldots \oplus x_n, x_1 \vee \ldots \vee x_n).$$

Proof:

Use induction and Lemma 2.2. For example let

$$\alpha = \varphi(x_1, \varphi(x_2,\ldots\varphi(x_n, \delta]\ldots]],$$

where δ is B-homogeneous and $\varphi(u,v] \equiv \neg u \wedge v$.

Then by the induction assumption

$\delta \equiv b(x_1 \oplus \dots \oplus x_n, x_1 \vee \dots \vee x_n)$.

Hence

$$\alpha \equiv \neg x_1 \wedge \neg x_2 \wedge \dots \wedge \neg x_n \wedge b(x_1 \oplus \dots \oplus x_n, x_1 \vee \dots \vee x_n) \equiv$$
$$\equiv (x_1 \vee x_2 \vee \dots \vee x_n) \wedge b(x_1 \oplus \dots \oplus x_n, x_1 \vee \dots \vee x_n).$$

Theorem 2.4 (Main Theorem.) For every base Ω , there exists a positive constant $\mathcal{E}_\Omega$ such that, for every $f : \{0,1\}^n \to \{0,1\}$, $r \geq 3$, if

$L_\Omega(f) \leq \mathcal{E}_\Omega n(\log \log n - \log r)$,

then there exist $1 \leq i_1 < \dots < i_r \leq n$ and a Boolean function b of two arguments such that

$$f | x_{i_1} \dots x_{i_r} \equiv b(x_{i_1} \oplus \dots \oplus x_{i_r}, x_{i_1} \vee \dots \vee x_{i_r}) .$$

Proof:

1. Let Ω and $r \geq 3$ be given. Let $\beta(x_1,\dots,x_m)$ be a k-formula, which means that no variable occurs in β more than k-times. Then every B-induced formula βX_B is again a k-formula. There exists a constant $C > 0$ such that the number of k-formulae with two variables is at most $\ell = 2^{C.k}$. Thus ℓ is an upper bound to the number of non-isomorphic formulae βX_B, where $|X| = 2$.

By the Ramsey theorem (see e.g. [7]), if

(1) $m \geq \ell^{r\ell}$

then there exists $Z = \{x_{i_1},\dots,x_{i_r}\}$, $1 \leq i_1 < \dots < i_r \leq n$, such that the formulae B-induced by two element subsets of Z are isomorphic, i.e. β is B-homogeneous over Z . By Lemma 2.1, βZ_B is B-homogeneous over Z and, by Corollary 2.3,

$$f | x_{i_1} \dots x_{i_r} \equiv \beta Z_B \equiv b(x_{i_1} \oplus \dots \oplus x_{i_r}, x_{i_1} \vee \dots \vee x_{i_r}).$$

If

(2) $$k \leq \frac{\log \log m - \log r - \log C}{C+1}$$

then

$$C.k + \log k + \log C + \log r \leq (C+1).k + \log C + \log r \leq \log \log m,$$
$$\Rightarrow 2^{C.k} . C.k.r \leq \log m \Rightarrow \ell^{r\ell} \leq m.$$

Hence (2) $\Rightarrow$ (1).

3. Let $f: \{0,1\}^n \to \{0,1\}$, $N = L_\Omega(f)$. Then there exists a formula $\alpha(x_1,\dots,x_n) \equiv f$ such that the total number of occurrences of va-

riables in α is N. Thus there are $m \geq n/2$ variables which have at most $2N/n$ occurrences each. Let X be the set of these variables. Denote by $\beta = \alpha X_B$. Then β is a k-formula, where $k = \lfloor 2N/n \rfloor$.By 1 and 2, in order to find the required restriction of f, it is enough to have (2), i.e. solving the inequalities,

$$N \leq \frac{1}{2(C+1)} \cdot n \cdot (\log(\log n-1) - \log r - \log C).$$

If $\varepsilon > 0$ is sufficiently small, then the last inequality is implied by

$$N \leq \varepsilon \cdot n \cdot (\log \log n - \log r),$$

for every N and r. □

Remarks.

1. The theorem is true also for $r = 2$, but it is trivial, since, instead of the bound for $L_\Omega(f)$, it is enough to have $n \geq 3$. (Find x_i, x_j, $i \neq j$, such that $f(0^{i-1} 1\, 0^{n-i}) = f(0^{j-1}\, 1\, 0^{n-j})$.) On the other hand $r = 3$ suffices for most applications.

2. For more precise estimates it is better to preserve the constant term $- \log C$ in (2). A direct computation gives for the base Ω of all at most binary connectives the following bound

$$L_\Omega(f) \leq \frac{1}{34} \cdot n \cdot (\log \log n - \log r - 17).$$

3. In the same manner as Hodes and Specker did, I can show that the condition of the theorem can be strengthened to

$$f \mid x_{i_1} \ldots x_{i_r} \equiv b(x_{i_1} \vee \ldots \vee x_{i_r})$$

for some unary Boolean function b , if $\Omega = \{0,1,\underline{0},\underline{1}, \neg, \vee, \wedge\}$. In the light of the results of Khrapčenko [3],[4] and Kričevskij [6], see also [10], this is uninteresting however.

§ 3 Some applications

Corollary 3.1 For every base Ω there is a constant $\delta_\Omega > 0$ such that, for every function $f:\{0,1\}^n \longrightarrow \{0,1\}$ and $1 < k < n-3$, if for every vector $\vec{c} \in \{0,1\}^n$

$$\sum c_i = k \Rightarrow f(c) = 0, \text{ (resp. 1)},$$

$$\sum c_i = k + 2 \Rightarrow f(c) = 1, \text{ (resp. 0)},$$

then

$L_{\Omega}(f) \geq \delta_{\Omega} \cdot n \cdot \log \log n \cdot \square$

The proof is almost identical with the proof of Symmetric Function Lower Bound Theorem of [1]. Hence I give only a hint: if $k \leq n/2$, consider a function obtained from f by substituting $k-1$ one's in f; if $k > n/2$, do the same with the dual function. (See also the proof of Theorem 4.2 below.)

A function $f : \{0,1\}^n \rightarrow \{0,1\}$ is called symmetric, if $f(\vec{c})$ depends only on $\sum c_i$. The symmetric threshould functions T_k^n, defined by

$$T_k^n (\vec{c}) = 1 \quad \text{iff} \quad \sum_{i=1}^{n} c_i \geq k,$$

are examples of symmetric functions. Corollary 3.1 can be applied to T_k^n if $1 < k < n-1$, however a more general theorem holds.

Corollary 3.2 For all but sixteen symmetric functions $f : \{0,1\}^n \longrightarrow \{0,1\}$,

$L_{\Omega}(f) \geq \delta_{\Omega} \cdot n \cdot \log \log n \cdot \square$

Such a corollary (but with the old bound) was derived by Khrapčenko [5]. The sixteen functions are

$$c_1 \oplus (c_2 \wedge (x_1 \oplus \dots \oplus x_n)) \oplus (c_3 \wedge x_1 \wedge \dots \wedge x_n) \oplus$$
$$\oplus (c_4 \wedge (x_1 \vee \dots \vee x_n)), \; c_1, c_2, c_3, c_4 \in \{0,1\}.$$

I shall show a less direct application of Theorem 2.4. Let $n = m.k$ and let $\underline{C}$ denote a $m \times k$ matrix of 0's and 1's. Define

$g^{m,k}(C) = 1$ iff there are at least two rows with odd numbers of 1, or equivalently,

$$g^{m,k}(A) = T_2^m (c_{11} \oplus \dots \oplus c_{1k}, c_{21} \oplus \dots + \oplus c_{2k}, \dots, c_{m1} \oplus \dots$$
$$\dots \oplus c_{mk}).$$

Proposition 3.3 For any base Ω, $L_{\Omega}(g^{m,k}) \geq \delta_{\Omega} \cdot m \cdot k \cdot \log \log m.$

Proof:

Let $\alpha (x_{11}, \dots, x_{mk}) \equiv g^{m,k}$ be a formula over Ω. Let $1 \leq j \leq k$, and consider the j-th column. Then

$$\alpha \{x_{1j}, x_{2j}, \dots, x_{mj}\} \equiv T_2^m (x_{1j}, \dots, x_{mj}),$$

thus it is of complexity at least

$\delta_{\Omega} \cdot m \cdot \log \log m$.

Hence there are at least so many occurrences of variables of the j-th column in α . Summing over all the columns I get the bound. □

Notice that I get a nonlinear bound even if k is "large" (say $k = n^{1-\varepsilon}$), when the theorem cannot be used directly. (The same bound can be proved for the function $f^{k,m}$ considered in [1], but they have a better bound for it).

§ 4 Asymptotical optimality of the bound

The following example arose during a discussion with S. Poljak.

I shall use↑for exponentiation, i.e. $m{\uparrow}n$ is m^n; following the usual convention I shall omit brackets in expressions like $m{\uparrow}(n{\uparrow}k)$.

Define by induction for $m,k \geq 1$:

$$\alpha_{1,m}(x_1,x_2,\dots,x_{m\uparrow 2}) = (\bigvee_{1}^{m} x_i) \oplus (\bigvee_{m+1}^{2m} x_i) \oplus \dots \oplus (\bigvee_{(m-1)m+1}^{m\uparrow 2} x_i);$$

$$\alpha_{k+1,m}(x_1,x_2,\dots,x_{m\uparrow 2\uparrow(k+1)}) = \alpha_{k,m}(\beta_1,\beta_2 \dots \beta_{m\uparrow 2\uparrow k}),$$

where for $i = 1,\dots, m{\uparrow}2{\uparrow}k$

$$\beta_i = \alpha_{k,m}(x_{(i-1).m\uparrow 2\uparrow k+1},\ x_{(i-1).m\uparrow 2\uparrow k\,+\,2} \dots x_{i.m\uparrow 2\uparrow k}).$$

Thus every variable x_i, $i \leq m{\uparrow}2{\uparrow}k$ occurs in $\alpha_{k,m}$ exactly once.
Define, for $n = 2{\uparrow}2{\uparrow}r$

$$\alpha_n = \bigwedge_{i=1}^{r} \alpha_{i,2\uparrow 2\uparrow(r-i)} .$$

Hence α_n has n variables, every variable occurs in it $r = \log \log n$ times. Therefore the complexity of α_n is $n.\log \log n$. The reader is recommended to try to visualize α_n as a labeled tree, see Fig. 2.

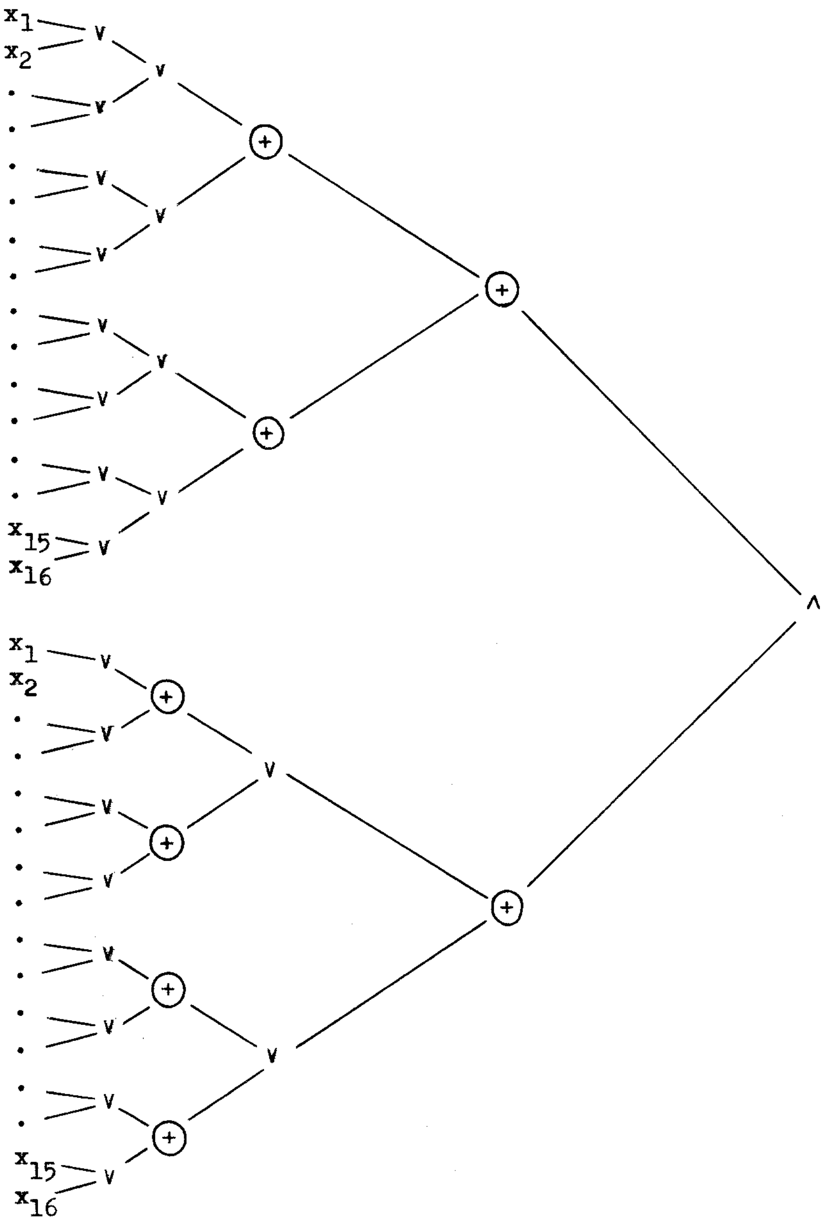
Lemma 4.1 For every $\vec{c} \in \{0,1\}^n$

$$\sum c_i = 1 \Rightarrow \alpha_n(\vec{c}) = 1,$$

$$\sum c_i = 3 \Rightarrow \alpha_n(\vec{c}) = 0.$$

Proof:

First it is easy to show using induction



<u>**Fig.2.**</u> α_{16}

(1) $\sum c_i = 0 \Rightarrow \alpha_{k,m}(\vec{c}) = 0;$

(2) $\sum c_i = 1 \Rightarrow \alpha_{k,m}(\vec{c}) = 1.$

The first implication of the lemma follows from (2). The second one will be proved by induction over $r = \log\log n$. If $r = 1$, then $n = 4$ and

$$\alpha_4 = \alpha_{1,2} = (x_1 \vee x_2) \oplus (x_3 \vee x_4).$$

Thus the implication can be verified easily. Let $r > 1$ and suppose that the implication holds for α_ℓ, $\ell = 2\uparrow 2\uparrow(r-1)$.
Let $\vec{c} \in \{0,1\}^n$ be given, where

$c_{i_1} = c_{i_2} = c_{i_3} = 1,\ i_1 < i_2 < i_3$,

$c_i = 0$ otherwise.

Divide c into ℓ blocks of length ℓ , where the j-th block is

$$\vec{c}^j = (c_{j\ell+1}, c_{j\ell+2}, \dots, c_{(j+1)\ell}).$$

Now I shall consider three cases.

1. $c_{i_1}, c_{i_2}, c_{i_3}$ belong to the same block, say the j-th block. By (1), (2), for every $1 < i \le r$, $m = 2\uparrow 2\uparrow(r-i)$,

$$\alpha_{i,m}(\vec{c}) = \alpha_{i-1,m}(\alpha_{i-1,m}(\vec{c}^1), \alpha_{i-1,m}(\vec{c}^2), \dots \alpha_{i-1,m}(\vec{c}^\ell)) \equiv$$

$$\equiv \alpha_{i-1,m}(0,\dots,0, \alpha_{i-1,m}(\vec{c}^j),0,\dots,0) \equiv \alpha_{i-1,m}(\vec{c}^j).$$

Hence

$$\alpha_n(\vec{c}) \equiv \alpha_{1,\ell}(\vec{c}) \wedge \alpha_\ell(\vec{c}^j),$$

which is equal to 0 by the induction assumption.

2. $c_{i_1}, c_{i_2}, c_{i_3}$ belong to different blocks, say to j_1-th, j_2-th, j_3-th ; $j_1 < j_2 < j_3$. By (1), (2), for every $1 < i \le r$, $m = 2\uparrow 2\uparrow(r-i)$,

$$\alpha_{i,m}(\vec{c}) \equiv \alpha_{i-1,m}(0,\dots,0, \alpha_{i-1,m}(\vec{c}^{j_1}), 0,\dots,0, \alpha_{i-1,m}(\vec{c}^{j_2}),$$

$$0,\dots,0, \alpha_{i-1,m}(\vec{c}^{j_3}),0,\dots,0) \equiv \alpha_{i-1,m}(\vec{d}),$$

where

$d_{j_1} = d_{j_2} = d_{j_3} = 1;\ d_j = 0$ otherwise.

Hence

$\alpha_n(\vec{c}\,) = \alpha_{1,\ell}(\vec{c}\,) \wedge \alpha_\ell(\vec{d}\,)$,

which is equal to 0 by the induction hypothesis.

3. Exactly two of $c_{i_1}, c_{i_2}, c_{i_3}$ belong to the same block. Then $\alpha_{1,\ell}(\vec{c}\,) \equiv 0$, hence $\alpha_n(\vec{c}\,) \equiv 0$. □

Theorem 4.2 Let $\Omega = \{\oplus, \vee, \wedge\}$, then for every $m \geqslant 1$, there exists $f: \{0,1\}^m \to \{0,1\}$ such that

$L_\Omega(f) \leqslant m.\lceil \log \log m \rceil$

and for no $1 \leqslant i < j < k \leqslant m$ and no b ,

(3) $f|x_ix_jx_k \equiv b(x_i \oplus x_j \oplus x_k, x_i \vee x_j \vee x_k)$.

Proof:

Let m be given, let $r = \lceil \log \log m \rceil$, $n = 2\uparrow 2\uparrow r$, and let α_n be the formula above. Let

$f \equiv \alpha_n\{x_1, \ldots, x_m\}$.

Then the complexity of f is $\leqslant m.r.$ The righthand side of (3) gives the same value for (1,0,0) and (1,1,1), hence by Lemma 4.1 (3) cannot hold. □

In fact I have proved a little bit more: the bound in Corollary 3.1 is asymptotically best.

§ 5 Related results

1. A generalization of Hodes-Specker theorem to d-ary logic, $d \geqslant 2$, was considered by Vilfan [11] . Let $D = \{0,1,\ldots, d-1\}$ be the set of logical values. A proper chain $C(x_1,\ldots,x_n,c)$ is, in my notation, every expression

$\varphi(x_1, \varphi(x_2, \ldots \varphi(x_n, c] \ldots]]$,

or with the reverse order of variables, where $c \in D$ and

$\varphi(0, \varphi(x,y]] \equiv \varphi(x,y]$.

(For $d = 2$ the last condition is equivalent to " $\varphi(0,x] \equiv x$ or $\varphi(0,x]$ is constant".) The generalization says, roughly speaking, this: If the complexity of $f: D^n \to D$ is "small", then there exist

$x_{i_1},\ldots,x_{i_r}$ such that

$$f \mid x_{i_1} \ldots x_{i_r} \equiv b(C_1(x_{i_1},\ldots,x_{i_r},c_1),\ldots,C_\ell(x_{i_1},\ldots,x_{i_r},c_\ell)),$$

where C_i are some proper chains. The actual bound, which is instead of "small", is again worse than $n \,.\, \log^* n$. Vilfan derives Hodes-Specker theorem from his generalization only for the base of all at most binary connectives, but this restriction is unessential. Because of the similarity with Theorem 1.3, I believe that Vilfan's theorem can be derived from it with a bound assymptotically equal to $n.\log \log \log n$ for fixed r and d .

3. A related theorem was proved by Fischer, Meyer and Paterson [1]. Their theorem can be expressed as follows: There exists a constant $\eta > 0$ such that if the complexity of $f:\{0,1\}^n \longrightarrow \{0,1\}$ over the base of all binary connectives is

(1) $\eta \,.n.(\log n - \log r)$,

then there exists a central restriction $f|^A x_{i_1} \ldots x_{i_r}$ (i.e. the number of substituted 1's equals to the number of substituted 0's possibly $+ 1$), such that

$$f|^A \; x_{i_1} \ldots x_{i_r} \equiv b(x_{i_1} \oplus \ldots \oplus x_{i_r}),$$

for some unary Boolean function b. If we replaced (1) by a bound $\varepsilon \,.\, n\,(\log \log n - \log r)$, then such a theorem would be a consequence of Theorem 2.4. For comparison consider the symmetric threshould functions. The theorem of Fischer et al. gives better bounds for T^n_k , where $\log n \ll k \ll n - \log n$, for $k \approx \log n$ or $k \approx n - \log n$ both theorems give assymptitically the same bound, and for the other values my theorem is better.

4. Still it is an open problem what is the complexity in a general base of such a simple function as T^n_2 . By the results of Kričevskij and others the complexity of T^n_2 is asymptotically $n.\log n$ for the base $\Omega = \{0,1,\neg,\wedge,\vee\}$, see also [10]. This is also the lowest known upper bound for any base. In this paper I have approached to this bound from below. However observe that formula α_n of § 4 can be easily transformed into a formula β_n such that for every $\vec{c}$, if $\sum c_i \leq 4$, then

$$\beta_n(\vec{c}\,) = T^n_2\,(\vec{c}\,),$$

and the complexity of β_n is assymptotically n.log log n. This can be generalized further, namely 4 can be replaced by an arbitrary constant.

References

[1] M.J. Fischer, A.R. Meyer, M.S. Paterson: Ω(n log n) lower bounds on length of Boolean formulas, SIAM J. Comput. Vol. 11, No.3, 1982, 416-427.

[2] L. Hodes, E. Specker: Lengths of formulas and elimination of quantifiers I, in Contributions to Mathematical Logic, H.A. Schmidt, K. Schütte, H.-J.Thiele, eds., North-Holland, (1968), 175-188.

[3] V.M. Khrapčenko: On the complexity of the realization of the linear function in class of π-cirquits, Mat. Zametki 9,1 (1971), 35-40, (Russian).

[4] V.M. Khrapčenko: The complexity of realization of symmetrical functions by formulae, Mat. Zametki 11,1 (1972), 109-120, (Russian), English translation in Math. Notes of the Academy of Sciences of the USSR 11, (1972), 70-76.

[5] V.M. Khrapčenko: Complexity of realization of symmetric Boolean functions on finite basis, Problemy Kibernetiki 31, (1976), 231-234, (Russian).

[6] R.E. Kričevskij: A bound for the formula size complexity of a Boolean function, Diskretnyj Analiz I, (1963), 13-23, also in Dokl. Akad. Nauk SSSR, Vol. 151, No. 4, 803-806, (Russian), English translation in Sov. Phys.-Dokl., Vol. 8, No. 8, (1964), 770-772.

[7] L. Lovász: Combinatorial Problems and Exercises, Akadémiai Kiadó and North-Holland, 1979.

[8] E.I. Nečiporuk: A Boolean function, Dokl. Akad. Nauk SSSR, Vol. 169, No. 4, 765-766, (Russian), English translation in Sov. Math. -Dokl. Vol. 7, No. 4, (1966), 999-1000.

[9] P. Pudlák: Boolean complexity and Ramsey theorems, manuscript.

[10] J.E. Savage: The Complexity of Computing, John Wiley and Sons, (1976).

[11] B. Vilfan: Lower bounds for the size of expressions for certain functions in d-ary logic, Theoretical Comp. Sci. 2, (1976), 249-269.