TWO LOWER BOUNDS FOR CIRCUITS OVER THE BASIS (&, V, ¬)

(Preliminary Report)

Stasys P. Jukna

Institute of Mathematics and Cybernetics
Lithuanian Academy of Sciences
232600 Vilnius, Akademijos, 4
Lithuanian SSR, U.S.S.R.

ABSTRACT *A general approximation technique to get lower bounds for the complexity of combinational circuits over an arbitrary algebras of operations is presented. The technique generalizes recent methods for monotone circuits and yields some new results. This report contains an* $\exp(\Omega(\log^2 n))$ *lower bound for the complexity of realization of non-monotone Boolean functions by circuits over the basis* (&,V,¬) *computing sufficiently many prime implicants , and of three-valued functions by circuits over some incomplete three-valued extensions of* (&,V,¬).

INTRODUCTION

The general idea of approximation technique in the theory of lower bounds for Boolean circuits is to approximate the circuits by more restricted ones. Various refinements of such an approach have already been used in a great many of lower bounds proofs. At present we have three main refinements. These are :

- *probabilistic approximations*, by Furst,Saxe and Sipser [5], Ajtai [1], Hastad [7], Yao [17], Hajnal et al. [6] , etc.
- *functional approximations*, by Andreev [3,4], Razborov [13-15], Alon and Boppana [2], Paterson [12], Smolensky [16], Ugol'nikov [19], etc. ;
- *topological approximations*, [8-10].

The aim of this report is to develope the functional approximation technique in order to obtain lower bounds for circuits over an arbitrary algebras of operations. The technique generalizes the methods of [2-4,12-16] and yields some new results.

The first result concerns Boolean circuits over the basis (&,V,¬) with ¬ -gates on the top of circuit. Any such circuit S computes some Boolean function f_S and also some disjunctive normal form (DNF for short) D_S of f_S (see Section 3 for details). A circuit S is called to be a *δ-circuit* $(0 \le \delta \le 1)$ iff

$$| D_S \cap \mathrm{Imp}(f_S) | \ge | \mathrm{Imp}(f_S) |^{\delta} - 1 ,$$

where Imp(f) denotes the set of all prime implicants of f of minimal length ; S is *∗-circuit* if $D_S = \mathrm{Imp}(f_S)$. For $\delta \in [0,1] \cup \{*\}$ and a Boolean function f , let $C_\delta(f)$ denote the minimum number of gates in a δ-circuit computing f ; in case of monotone basis $\{\&,\vee\}$ we will write $C_\delta^+(f)$. Notice that $C_\delta(f) \le C_\gamma(f) \le C_*(f)$ for any $0 \le \delta \le \gamma \le 1$, and that $C_0(f) = C(f)$ is the usual combinational complexity of f . Moreover, if f is monotone then $C_\delta^+(f) = C_\gamma^+(f) = C^+(f)$ since $Imp(f_S) \subseteq D_S$ for any monotone S .

These functionals have been considered by many authors. Probably, the first non-trivial result in this direction is an exponential trade-off between $*$-circuits and (monotone) 1-circuits proved by Okol'nishnikova in [11]. Namelly, she proved the bound $C_*(f_n) \ge exp(\Omega(n^{1/4}))$ for a single sequence of monotone canonical functions f_n such that $C_1^+(f_n) \le 2n$. (A function f is *canonical* if $Imp(f)$ coincides with the set $PI(f)$ of all prime implicants of f). Latter, Andreev [3,4], Razborov [13,14] and Alon and Boppana [2] have considered the functional $C^+(f)$ and obtained super-polynomial (up to $exp(\Omega(n^{1/3-o(1)}))$ in [4]) lower bounds for some sequences of monotone canonical functions f_n with $\cup f_n^{-1}(1) \in NP$. These bounds hold also for $C_1(f_n)$. This is becouse any minimal circuit over $\{\&,\vee,\neg\}$ computing a *positive* DNF (i.e. a DNF without *negations*) has no *null-chains*. However, it is known [8-10,13,14] that the presence of null-chains may substantialy reduce the circuit size. For example, in [13] a sequence of montone canonical functions f_n is given such that $C^+(f_n) \ge n^{\Omega(\log n)}$ and $C_\delta(f_n) \le n^{O(1)}$ for some $0 \le \delta < 1$. Thus we need a technique to prove lower bounds for *non-positive* DNFs, and, in particular, for $C_\delta(f)$ with a *non-monotone* f .

Such a technique is described in Section 1. In Section 2 the technique is demonstrated by a general lower bound on the complexity of realization of sets by circuits over basises consisting of so-called $\exists$-operations. This general bound yield all the known bounds [2,3,13,14] and some new lower bounds. In Section 3 a sequence of non-monotone Boolean functions π_n is given and it is proved that for any constant $\delta \in (0,1]$ it holds that

$$n^{\Omega(\ln n)} \le C_\delta(\pi_n) \le n^{\ln n} .$$

In section 4 we prove that circuits over some three-valued extensions of $\{\&,\vee,\neg\}$ require super-polynomial number of gates to compute a single sequence of three-valued functions.

1. Circuits and Metric Criterions of Their Complexity

Fix some $n \ge 1$ and let F be a collection of n-ary operations $f : \mathfrak{A}^n \dashrightarrow \mathfrak{A}$ over some set $\mathfrak{A}$. A *circuit over the algebra* $(\mathfrak{A}; F)$ *with input* $\mathfrak{B} \subseteq \mathfrak{A}$ is an ordered sequence $S = \{s_1,\dots,s_t\} \subseteq \mathfrak{A}$ such that $\forall\ i = 1,\dots,t$ $s_i = f(b_1,\dots,b_n)$ for some $f \in F$ and $b_1,\dots,b_n$

$\in \mathfrak{H} \cup \{s_1,\dots,s_{i-1}\}$. The number t of elements in S is the *size* of S. We say S *computes* a vector $A \in \mathfrak{A}^k$ iff $A \subseteq \mathfrak{H} \cup S$. (Here and in what follows we shall often identify a vector with the set of its elements). The *circuit-size complexity* of $A \in \mathfrak{A}^k$ *over an algebra* $(\mathfrak{A};F)$ *with respect to* $\mathfrak{H} \subseteq \mathfrak{A}$, denoted by $L_F(A,\mathfrak{H})$, is the size of a minimal circuit over $(\mathfrak{A};F)$ with input $\mathfrak{H}$, computing A. Notice that $L_F(A,\mathfrak{H}) = 0$ for any $A \subseteq \mathfrak{H}$.

We say an algebra $(\mathfrak{B};G)$ is a *Q-image* of an algebra $(\mathfrak{A};F)$, where $Q \subseteq \mathfrak{A}\times\mathfrak{B}$, iff for each $f \in F$ there is some $g \in G$ such that for all vectors $A = (a_1,\dots,a_n) \in \mathfrak{A}^n$ and $B = (b_1,\dots,b_n) \in \mathfrak{B}^n$ we have that $\{(a_i,b_i) : i=1,\dots,n\} \subseteq Q$ implies $(f(A),g(B)) \in Q$. For $\mathfrak{H} \subseteq \mathfrak{A}$, put $Q(\mathfrak{H}) = \{ b\in\mathfrak{B} : (a,b)\in Q$ for some $a\in\mathfrak{H} \}$.

THEOREM 1. *If* $(\mathfrak{B};G)$ *is a Q-image of* $(\mathfrak{A};F)$ *then for any* $a\in\mathfrak{A}$ *and* $\mathfrak{H} \subseteq \mathfrak{A}$ *we have :*

$$L_F(a,\mathfrak{H}) \geq \inf_{b\in Q(a)} L_G(b,Q(\mathfrak{H})) .$$

Proof : straightforward. ∎

For numbers $k,m \geq 1$, let $\mathfrak{A}_{k,m}$ denote the set of all $k\times m$-matrices over $\mathfrak{A}$. Thus, e.g., $\mathfrak{A}_{k,1} = \mathfrak{A}^k$, the k-th cartesian degree of $\mathfrak{A}$. A *semimetric* over $\mathfrak{A}$ is a functional

$$\rho : \bigcup_{k\geq 1} (\mathfrak{A}^k\times\mathfrak{A}^k) \longrightarrow R_+$$

satisfying the usual "triangle rule": $\rho(x,y) \leq \rho(x,z) + \rho(z,y)$. For $A \in \mathfrak{A}^k$ and a subset $\mathfrak{B} \subseteq \mathfrak{A}$, put $\rho(A,\mathfrak{B}) = \inf\{\rho(A,B): B\in\mathfrak{B}^k \}$. For a $k\times m$-matrix A, let $\underline{A}$ denote the vector $(A_1,\dots,A_k) \in \mathfrak{A}^{km}$, where A_i stands for the i-th row of A. Given a vector of operations $\underline{f} = (f_1,\dots,f_k) \in F^k$ and a matrix $A \in \mathfrak{A}_{k,m}$, we denote by $\underline{f}(A)$ the vector $(f_1(A_1),\dots,f_k(A_k)) \in \mathfrak{A}^k$. Put $\underline{f}(\mathfrak{B}) = \{ \underline{f}(B) : B \in \mathfrak{B}_{k,n} \}$ and define the "one-step-closure" $F(\mathfrak{B})$ of $\mathfrak{B} \subseteq \mathfrak{A}$ by $F(\mathfrak{B}) = \bigcup \{ f(\mathfrak{B}) : f \in F \}$. A semimetric ρ is called to be *F-contractible on* $\mathfrak{B} \subseteq \mathfrak{A}$ iff for any $A\in\mathfrak{A}_{k,n}$ and $\underline{f} \in F^k$ it holds

$$\rho(\underline{f}(A),\underline{f}(\mathfrak{B})) \leq \rho(\underline{A},\mathfrak{B}).$$

The following theorem generalizes the standard approach of proving circuit-size lower bound - demonstrating that a certain amount of progress must be made, and that no step makes more than δ progress, for some small δ.

THEOREM 2. *Let* $(\mathfrak{A};F)$ *be an algebra,* $A\in\mathfrak{A}^k$ *be a vector and* $\mathfrak{H} \subseteq \mathfrak{A}$. *Then for any subset* $\mathfrak{B} \subseteq \mathfrak{A}$ *and any F-contractible on* $\mathfrak{B}$ *semimetric* ρ *we have that*

$$L_F(A,\mathfrak{H}) \geq \rho(A,\mathfrak{B})\,\delta^{-1} - 1 ,$$

where $\delta = \sup \{ \rho(C,\mathfrak{B}) : C \in (\mathfrak{H} \cup F(\mathfrak{B}))^m, m\geq 1 \}$.

Proof: We proceed by induction on $t = L_F(A,\mathfrak{H})$. If $t = 0$ then $A \le \mathfrak{H}$, and hence $\rho(A,\mathfrak{B}) \le \delta$. For the induction step assume that $A = \underline{f}(C)$ for some $\underline{f} \in F^k$ and $C \in \mathfrak{A}_{k,n}$ with $L_F(\underline{C},\mathfrak{H}) \le t-1$. By the triangle rule we have, for any $B \in \mathfrak{A}_{k,n}$, that

$$\rho(A,\mathfrak{B}) = \rho(\underline{f}(C),\mathfrak{B}) \le \rho(\underline{f}(C),\underline{f}(B)) + \rho(\underline{f}(B),\mathfrak{B}) .$$

Since ρ is F-contractible on $\mathfrak{B}$, we have by the induction hypothesis that for *some* $B \in \mathfrak{B}_{k,n}$ $\rho(\underline{f}(C),\underline{f}(B)) \le \rho(\underline{C},\mathfrak{B}) \le t\delta$. Therefore, $\rho(A,\mathfrak{B}) \le t\delta + \rho(\underline{f}(B),\mathfrak{B}) \le t\delta + \delta = (t+1)\delta$. ■

Let us now introduce an algebraic definition of contractible semimetrics, generalizing the methods of [2-4,12-16].

Let $(\mathfrak{A};\oplus)$ be a semigroup with a unit element $\mathbf{1}$, and let $\ll \subseteq \mathfrak{A}^2$ be some reflexive and transitive relation. A triple $\mathfrak{S} = (\mathfrak{C},\oplus,\ll)$, is an *approximation structure* iff $\oplus$ is monotone with respect to $\ll$ and $\mathbf{1} \in \mathfrak{C} \subseteq \mathfrak{A}$. Define "linear covers" $\mathrm{Cov}_t(\mathfrak{C})$ of $\mathfrak{C}$ by :
$\mathrm{Cov}_{t+1}(\mathfrak{C}) = \{ a\oplus b :\ a \in \mathrm{Cov}_t(\mathfrak{C})$ and $b \in \mathfrak{C} \}$ where $\mathrm{Cov}_0(\mathfrak{C}) = \{\mathbf{1}\}$.

A structure induces the following natural *measure of accurancy* $\rho(A,B)$ (with which a vector A is approximated by a vector B) : $\rho(A,B)$ is the minimum number $m \ge 0$ for which $\mathrm{Cov}_m(\mathfrak{C})$ contains an element e such that $(\forall i)$ $a_i \ll b_i\oplus e$. Notice that $\rho(x,x) = 0$, since $\ll$ is reflexive, but $\rho(x,y) \ne \rho(y,x)$ on the whole.

A structure $\mathfrak{S} = (\mathfrak{C},\oplus,\ll)$ is *compatible with an algebra* $(\mathfrak{A};F)$ iff each operation $f \in F$ is both "$\ll$*-monotone*" and "$(\oplus,\ll)$*-idempotent*", i.e. if for any $A,B \in \mathfrak{A}^n$ and $c \in \mathfrak{A}$: $a_1 \ll b_1,\dots, a_n \ll b_n$ implies $f(A) \ll f(B)$, and $f(A\oplus c) \ll f(A)\oplus c$, where $A\oplus c = (a_1\oplus c,\dots,a_n\oplus c)$.

LEMMA 1. *Let $\mathfrak{S}$ be an approximation structure and let ρ be the induced measure of accurancy. If $\mathfrak{S}$ is compatible with an algebra $(\mathfrak{A};F)$ then ρ is a semimetric F-contractible on any subset $\mathfrak{B} \subseteq \mathfrak{A}$.*

Proof : Since $\ll$ is transitive and reflexive and $\oplus$ is monotone with respect to $\ll$, we have that ρ is a semimetric. To show that ρ is F-contractive on a subset $\mathfrak{B} \subseteq \mathfrak{A}$, let $f \in F$ and $A \in \mathfrak{A}_{k,n}$ with $\rho(\underline{A},\mathfrak{B}) = \rho(\underline{A},\underline{B}) = m$ for some $B \in \mathfrak{B}_{k,n}$, i.e. $a_i \ll b_i\oplus e$ for some $e \in \mathrm{Cov}_m(\mathfrak{C})$ and all $i = 1,\dots,nk$. Since $\mathfrak{S}$ is compatible with $(\mathfrak{A};F)$, we have :

$$\forall j=1,\dots k \qquad f_j(A_j) \ll f_j(B_j\oplus e) \ll f_j(B_j) \oplus e .$$

Therefore, $\rho(\underline{f}(A),\underline{f}(\mathfrak{B})) \le m = \rho(\underline{A},\mathfrak{B})$. ■

Given a subsets $\mathfrak{B},\mathfrak{C} \subseteq \mathfrak{A}$ and a pair of semimetrics ρ_0 and ρ_1, we shall write $[\rho_0,\rho_1](\mathfrak{C},\mathfrak{B}) \le d$ if for any $c \in \mathfrak{C}$ there exists an $b \in \mathfrak{B}$ such that $\rho_0(c,b) \le d$ and $\rho_1(b,c) \le d$.

THEOREM 3. *Let $(\mathfrak{A};F)$ be an algebra, $a \in \mathfrak{A}$ and $\mathfrak{B},\mathfrak{H} \subseteq \mathfrak{A}$. Let also*

ρ_0 and ρ_1 be a pair of accurancy measures induced by a pair of approximation structures $\mathfrak{S}_0$ and $\mathfrak{S}_1$. If these structures both are compatible with $(\mathfrak{U};F)$ and $[\rho_0,\rho_1](\mathfrak{H} \cup F(\mathfrak{B}),\mathfrak{B}) \le d$ $(d>0)$ then

$$L_F(a,\mathfrak{H}) \ge d^{-1} \inf_{b\in\mathfrak{B}} \max \{ \rho_0(a,b), \rho_1(b,a) \} .$$

Proof : Follows directly from Theorem 2 and Lemma 1 . ∎

2. THE GENERAL LOWER BOUND

Let E be some finite set, $|E| \ge 2$ and $n \ge 1$. *Points* are elements of E^n and *figures* are elements of the power set $P(E^n)$ of E^n. Fix some element $* \in E$ and define the *weight* $N(x)$ of a point x by $N(x) = |\{i : x(i) \ne *\}|$, where $x(i)$ is the i-th coordinate of x. We say x *covers* y ($x \angle_* y$ for short) if $\forall i$ $y(i) \in \{x(i),*\}$. Hence, if $x \angle_* y$ then $N(x)\ge N(y)$. Thus, for any distinguished point $*\in E$, $(E^n, \angle_*)$ is an upper semilattice with the maximal element $\underline{*} = (*,\ldots,*)$ and the *join* $\sup(x,y)$ defined as the (unique) point z of minimal weight such that $\{x,y\} \angle_* z$. For a point x and figures X,Y we shall write $x \angle_* Y$ if $x \angle_* y$ for some $y\in Y$, and $X \angle_* Y$ if $x \angle_* Y$ for all $x\in X$. For a figure X, set $X^\nabla = \{ x\in E^n : x \angle_* X \}$ and $\lfloor X \rfloor = \{ x\in X : \forall y\in X \ (x \angle_* y \Rightarrow y = x) \}$

An operation $f : P(E^n)^m \longrightarrow P(E^n)$ is an $\exists$-*operation* if there is a system $\Omega_f \subseteq P(\{1,\ldots,m\})$ such that for any point x and figures $X_1,\ldots,X_m$ it holds that

$$x \angle_* f(X_1,\ldots,X_n) \ \text{ iff } \ (\exists\omega \in\Omega_f)(\forall i \in\omega) \quad x \angle_* X_i .$$

Let $\mathfrak{F}$ denote the set of all $\exists$-operations. Notice that, for example, the union $\cup$ and the *concatenation* $\odot$, given by

$$X\odot Y = \lfloor \{ x\in E^n : x \angle_* X \text{ and } x \angle_* Y \} \rfloor ,$$

both are $\exists$-operations with $\Omega_\cup = \{\{1\},\{2\}\}$ and $\Omega_\odot = \{\{1,2\}\}$.

LEMMA 2. *For any $F \subseteq \mathfrak{F}$ and $\mathfrak{U} \subseteq P(E^n)$ containing E^n, the structure $(\mathfrak{U},\cup,\angle_*)$ is an approximation structure compatible with the algebra of figures $(P(E^n);F)$.*

To apply Theorem 3, we shall make use of the concept of closed figure similar to that of closed system of sets introducd in [2,13]. Let $p\ge1$ and $r\ge2$ be numbers to be choosen later, and let E^n_p denote the set of all points of weight at most p. The *closure* of a figure $X\subseteq E^n_p$, denoted by $X^{\circledcirc}$, is the smallest figure $Y\supseteq X$ such that for any r (not necessarily distinct) points $x_1,\ldots,x_r$ of Y, the figure Y contains all the points $y\in E^n_p$ such that $y \angle_* \sup(x_i,x_j)$ for all $1\le i<j\le r$. A figure X is *closed* if $X^{\circledcirc} = X$. Let $\mathfrak{B}_{p,r}$ denote the set of all closed figures.

LEMMA 3. *For any figure* $X \subseteq E^n_p$ *it holds that*

(i) $\left| \lfloor X^{\circledcirc} \rfloor - X^{\nabla} \right| \le 2r^p$ *and*

(ii) if X *is closed then* $\left| \lfloor X \rfloor \cap E^n_k \right| \le (r-1)^k$ *for any* $0 \le k \le p$.

Proof: Similar to that of lemmas 2.3 and 2.5 in [2]. ∎

For an m-ary $\exists$-operation f and a sequence of figures $\underline{X} = (X_1, \ldots X_m)$, set

$$f[\underline{X}] = \bigcup_{\omega \in \Omega_f} \bigcap_{i \in \omega} X_i .$$

Notice that $f[\underline{X}] \subseteq f(\underline{X})$ but $f[\underline{X}] \ne f(\underline{X})$ in general. For example, $\cup[X,Y] = X \cup Y$ but $\odot[X,Y] = X \cap Y \ne X \odot Y$ on the whole. Moreover, if $f \in \mathfrak{F}$ and all $X_i \subseteq E^n_p$ then $f[\underline{X}] \subseteq E^n_p$ whereas $\neg (f(\underline{X}) \subseteq E^n_p)$ in general.

Given a collection of $\exists$-operations F, let $\mathfrak{C}^0_{p,r}$ and $\mathfrak{C}^1_{p,r}$ denote the sets of all figures of the form $f(\underline{X})^{\nabla} - (f[\underline{X}]^{\circledcirc})^{\nabla}$ and, respectively, of the form $(f[\underline{X}]^{\circledcirc})^{\nabla} - f(\underline{X})^{\nabla}$, where $f \in F$ and $X_i \in \mathfrak{B}_{p,r}$. Let ρ_0 and ρ_1 be the measures of accurancy induced by the structures $(\mathfrak{C}^0_{p,r}, \cup, \angle_*)$ and $(\mathfrak{C}^1_{p,r}, \cup, \angle_*)$. Fix the following collection of "singular" figures

$$\mathfrak{S}_0 = \{\emptyset\} \cup \{ \{x\} : x \in E^n \text{ and } N(x) \le 1 \}$$

It is easy to see that then for any $p \ge 1$ and $r \ge 2$, it holds that

$$[\rho_0, \rho_1](\mathfrak{S}_0 \cup F(\mathfrak{B}_{p,r}), \mathfrak{B}_{p,r}) \le 1 .$$

Therefore, by Theorem 3 and Lemma 2 we have, for any figure X, that

$$L_F(X, \mathfrak{S}_0) \ge \inf_{Y \in \mathfrak{B}_{p,r}} \max \{ \rho_0(X,Y), \rho_1(Y,X) \} \tag{1}$$

To bound ρ_0 and ρ_1, let us introduce some auxiliary parameters. For figures X and Y, set $R(X) = \min \{ N(x) : x \in X \}$, $\gamma_X(Y) = |\{ x \in \lfloor X \rfloor : x \angle_* Y \}|$, and for $k \ge 0$, put $\gamma_X(k) = \max \{ \gamma_X(\{y\}) : y \in E^n$ and $N(y) = k \}$. A figure X is *r-disjoint* if $\gamma_X(t) \le \gamma_X(s)(3r-3)^{s-t}$ for all $0 \le s \le t$.

THEOREM 4. *Let* X *be a figure,* $\mathfrak{S}$ *be a collection of figures,* $1 \le p \le R(X)$, $r \ge 2$ *and* $0 \le \varepsilon \le (|E|-1)^{-1}$. *Let also* F *be a collection of* $\exists$*-operations of arity at most* m *and let* $\ell = \lceil (p+1)/m \rceil$. *Then for any r-disjoint figure* Y *and for any figure* Z *such that* $Y \angle_* X \angle_* Z$, *it holds that*

$$L_F(X, \mathfrak{S}) \ge \min \left\{ \frac{\gamma_Y(0)}{2m(r-1)^{\ell} \gamma_Y(\ell)} , \frac{1 - \gamma_Z(0)\, \varepsilon^{R(Z)}}{2r^p (1 - \varepsilon^p)^r} \right\} - \delta_F(\mathfrak{S})$$

where

$$\delta_F(\mathfrak{S}) = \sum_{W \in \mathfrak{S}} L_F(W, \mathfrak{S}_0).$$

Proof : By (1) it is sufficient to prove that for any closed figure B

$\in \mathfrak{B}$, it holds that $\rho_0(X,B) \ge u$ or $\rho_1(B,X) \ge v$ (or both), where u and v stand for the first and second expression in $\min(\ldots)$. There are two possible cases, depending on B.

Case 1 : $\underline{*} \notin B$. Then $\rho_0(X,B) \ge \rho_0(Y,B) \ge u$.

The first inequality holds for any $Y \angle_* X$. The idea of proof of the second one is analogous to that of Theorem 4.3 in [2]. By the definition of ρ_0, there exist $t \le \rho_0(Y,B)$ figures $U_1,\ldots,U_t$ in $\mathfrak{C}^0_{p,r}$ such that $\lfloor Y \rfloor \subseteq (B \cup U_1 \cup \ldots \cup U_t)^\nabla$. Hence, $\rho_0(Y,B) \ge (\gamma_Y(0) - \gamma_Y(B))/\max \gamma_Y(U_i)$. Since $\underline{*} \notin B$, we have that $N(x) \ge 1$ for all $x \in B$, and since Y is r-disjoint, we have by Lemma 3(ii) that

$$\gamma_Y(B) \le \sum_{k=1}^{p} (r-1)^k \gamma_Y(k) \le \frac{1}{2} \gamma_Y(0)$$

To bound $\gamma_Y(U_i)$, recall that $U_i = f(\underline{W})^\nabla - (f[\underline{W}]^{\circledcirc})^\nabla$ for some $f \in F$ and some sequence of closed figures $\underline{W} = (W_1,\ldots,W_m)$. If $x \in U_i^\nabla$ then there is some $\omega \in \Omega_f$ so that, for any $j \in \omega$, the point x covers some point y_j of $\lfloor W_j \rfloor$. Moreover, as no point of $f[\underline{W}]^{\circledcirc}$ is covered by x, we have that $x \angle_* \bigcap_{k\in\omega'} W_k$ for *no* $\omega' \in \Omega_f$. Let z be the point of minimal weight which covers all the points y_j, $j \in \omega$. If $N(z) \le p$ then, since figures W_j are closed, the point z is in $\bigcap_{k\in\omega} W_k$, which is impossible since $x \angle_* z$. Thus $N(z) \ge p+1$ and so $N(y_j) \ge \lceil N(z)/|\omega| \rceil \ge \ell$ for some $j \in \omega$. Therefore, if $x \in U_i^\nabla$ then x covers some point of $\lfloor W_1 \rfloor \cup \ldots \cup \lfloor W_m \rfloor$ of weight at least ℓ. Hence, by Lemma 3(ii) we have that

$$\gamma_Y(U_i) \le \sum_{k=\ell}^{p} m(r-1)^k \gamma_Y(k) \le m(r-1)^\ell \gamma_Y(\ell).$$

Case 2 : $\underline{*} \in B$. Then $\rho_1(B,X) \ge v$.

Indeed, by the definition of ρ_1, there exist $t \le \rho_1(B,X)$ figures $D_1,\ldots,D_t \in \mathfrak{C}^1_{p,r}$ such that $B^\nabla \subseteq (X \cup D_1 \cup \ldots \cup D_t)^\nabla$. Let $x \in (E-\{*\})^n$ be a random point in which each $x(i) \in E-\{*\}$ appears independently with probability ε $(0 \le \varepsilon \le (|E|-1)^{-1})$. Then $\mathrm{Prob}\{ x \angle_* B \} = 1$, since $\underline{*} \in B$, and $\xi_0 = \mathrm{Prob}\{ x \angle_* X \} \le \mathrm{Prob}\{ x \angle_* Z \} \le \gamma_Z(0)\, \varepsilon^{R(C)}$. Hence $t \ge (1 - \xi_0)/\xi$ where $\xi = \max \mathrm{Prob}\{ x \angle_* D_i \}$. By Lemma 3(i), $\xi \le 2r^p\eta^r$ where $\eta = \max\{ \mathrm{Prob}(\neg(x \angle_* y)) : y \in E^n_p\}$. It remains to observe that $\eta \le 1 - \varepsilon^p$. ∎

3. The Complexity of Disjunctive Normal Forms

Fix some alphabet of Boolean variables $\{u_1,\ldots,u_n\}$, and let $E^n = \{*,0,1\}$. We identify a monomial $\&_{i\in I} u_i^{\sigma_i}$ with the point $x \in E^n$ such that $\forall j=1,\ldots,n$, $x(j)=\sigma_j$ if $j \in I$ and $x(j)=*$ otherwise. So, *DNFs are figures over* E^n. A DNF $X \subseteq E^n$ *realizes* a Boolean function $f(u_1,\dots,u_n)$ iff $f^{-1}(1) = X^{\nabla} \cap \{0,1\}^n$. Let $Imp(f)$ denote the set of all prime implicants of minimal length of f, i.e. $x \in Imp(f)$ iff x is a prime implicant of f and $N(x) \le N(y)$ for any other prime implicant y of f.

For $\delta \in [0,1]$ and a Boolean function f, let $D(f,\delta)$ denote the set of all DNFs X realizing f and such that $|X \cap Imp(f)| \ge |Imp(f)|^{\delta} - 1$.

LEMMA 4. *For any Boolean function* f *and* $\delta \in [0,1]$ *it holds that*

$$C_{\delta}(f) \ge \min_{A \in D(f,\delta)} L_{\{\cup,\odot\}}(X,\mathfrak{F}_0) .$$

Proof: Take $Q = \{ (f,X) : X \text{ realizes } f \}$ and apply Theorem 1. ∎

EXAMPLE 1. Let q be a prime number such that $s = [\frac{1}{12} \ln q] \ge 1$, and let $GF(q)$ be the Galois field of order q with the addition $+$. Fix an element $e \ne 0$ of $GF(q)$ and consider the following Boolean function $\pi_n(U)$ of $n = q^2$ variables $U = \{u_{a,b} : a,b \in GF(q) \}$. Given a quadratic $q \times q$-matrix $\mathcal{A} = (\alpha_{a,b})$ with $\alpha_{a,b} \in \{0,1\}$, let $\pi_n(\mathcal{A}) = 1$ iff there is a polynomial p of degree at most $s-1$ over $GF(q)$ such that for all $a \in GF(q)$, $\alpha_{a,p(a)} = 1$ and $\alpha_{a,p(a)+e} = 0$. Notice that π_n is non-monotone: $\pi_n(\mathcal{A}) = 0$ if $\mathcal{A}$ contains more than $n-q$ or less than q ones. Set $Y_n = Imp(\pi_n)$, and let $Z_n = \{ K^+_{p_1} \& K^-_{p_2}$: p_1 and p_2 are polynomials of degree atmost $s-1$ }, where a monomial K^+_p (K^-_p) consists of all the literals $u_{a,p(a)}$ (resp., $\bar{u}_{a,p(a)\oplus e}$), $a \in GF(q)$. Notice that $Y_n \subseteq Z_n$ and $X_n \angle_{*} Z_n$ for any DNF X_n realizing π_n. Moreover $R(Y_n) = R(Z_n) = 2q$, $\gamma_{Y_n}(0) = |Y_n| = q^s$, $\gamma_{Z_n}(0) = q^{2s}$ and $\gamma_{Y_n}(k) \le q^{s-[(k+1)/2]}$ for all $k \ge 1$. Since $\cup$ and $\odot$ both are $\exists$-operations, Theorem 4 implies the following

COROLLARY 1. *For any DNF* X_n *with* $\lfloor X_n \rfloor = Y_n$ *we have that*

$$L_{\{\cup,\odot\}}(X_n,\mathfrak{F}_0) \ge n^{\Omega(\ln n)}.$$

Proof : Take $r = [q^{1/3}]$, $p = [\frac{1}{2} \ln r]$ and $\varepsilon = ((\ln r)^2/r)^{1/p}$ and apply Theorem 4 ∎

Since Y_n realizes π_n, Lemma 4 and Corollary 1 yield

COROLLARY 2. *For any constant* $\delta \in (0,1]$ *it holds that*

$$n^{\Omega(\ln n)} \le C_{\delta}(\pi_n) \le n^{\varepsilon \ln n} \quad , \qquad \varepsilon \le 1/47.$$

Therefore, we have that either $C(\pi_n) \ge n^{\Omega(\ln n)}$ or *all* the minimal circuits for π_n compute DNFs X_n such that $|X_n \cap Y_n| \le |Y_n|^{o(1)}$.

4. THE COMPLEXITY OF THREE-VALUED FUNCTIONS

Let $E_3 = \{0,1,2\}$ and let $\mathbb{P}^n_3$ denote the set of all n-ary three-valued predicates $f : E^n_3 \longrightarrow \{0,1\}$.

Probably, the first non-trivial lower bound for circuits over an incomplete three-valued basises has been proved by Tkachev in [18]. He considers circuits over the algebra $(\mathfrak{P}_3^n;\ \wedge\ ,\ \otimes\ )$ with input $H_0=\{\nu_1,\dots,\nu_n\}$, where $\mathfrak{P}_3^n$ is the set of all three-valued functions $f\colon E_3^n \longrightarrow E_3$, $x\wedge y = \min(x,y)$, $x\otimes y = xy(\mathrm{mod}\ 2)$ and $\nu_i : E_3^n \longrightarrow E_3$ is the i-th projection, i.e. for $\sigma\in E_3^n$, $\nu_i(\sigma) = \sigma(i)$, the i-th coordinate of σ. In [18] the bound

$$L_{\{\wedge,\otimes\}}(t_n,H_0) \ \ge\ 2\binom{n}{n/2} - 1$$

is proved for the sequence of three-valued predicates $t_n \in \mathfrak{B}_3^n$ given by : $t_n(\sigma) = 1$ iff $\sigma\in\{1,2\}^n$ and $|\{i : \sigma(i)=1\}| \ge n/2 +1$.
Set $x\vee y = \max(x,y)$ and $H = \{\iota_1,\dots,\iota_n,\eta_1,\dots,\eta_n\}$ where for $\sigma\in E_3^n$

$$\iota_i(\sigma) = \begin{cases} 1 & \text{if } \sigma(i)=1,\\ 0 & \text{otherwise,}\end{cases} \quad\text{and}\quad \eta_i(\sigma) = \begin{cases} 1 & \text{if } \sigma(i)=2,\\ 0 & \text{otherwise.}\end{cases}$$

Notice that the predicate t_n has polynomial-size circuits over the algebra $(\mathfrak{B}_3^n\ ;\ \vee\ ,\ \otimes\ )$ even with input H :

$$L_{\{\vee,\otimes\}}(t_n,H) \ \le\ O(n^{5.3}) .$$

This follows from the representation

$$t_n(\sigma) = \xi_1(\sigma)\otimes\xi_2(\sigma)\otimes \dots \otimes\xi_n\otimes \mathrm{MAJ}_n(\iota_1(\sigma),\dots,\iota_n(\sigma)),$$

where $\xi_i(\sigma) = \iota_i(\sigma) \vee \eta_i(\sigma)$, and from the result of Valiant [20] that the monotone Boolean formula-size complexity of Boolean majority function MAJ_n is $O(n^{5.3})$.

In this section we demonstrate Theorem 4 by a super-polynomial lower bound for $L_{\{\vee,\otimes\}}(\circ,H)$. To do this, let $0\in E_3$ be the distinguished element of E_3 (i.e. 0 plays a role of $*$), and let $\angle_0$ be the corresponding order relation on E_3^n. Identify a predicate $f\in\mathfrak{B}_3^n$ with the figure $X_f = f^{-1}(1) \subseteq E_3^n$.

Lemma 5. *For any predicate* $f \in \mathfrak{B}_3^n$ *it holds that*

$$L_{\{\vee,\otimes\}}(f,H) \ \ge\ L_{\{\cup,\odot\}}(X_f,\mathfrak{H}_0).$$

Proof. Define $Q \subseteq \mathfrak{B}_3^n \times P(E_3^n)$ by $Q = \{(f,Y) : X_f= \{x\in E_3^n : x \angle_0 Y \}\}$. Then $Q(H) \subseteq \mathfrak{H}_0$ and the algebra of figures $(P(E_3^n);\ \cup,\ \odot)$ is Q-image of $(\mathfrak{B}_3^n;\ \vee,\ \otimes)$. It remains to apply Theorem 1. ∎

Example 2. Let us consider the following three-valued extention $\Pi_n\in\mathfrak{B}_3^n$ of π_n (see Example 1).For a quadratic $q\times q$-matrix $M = (m_{a,b})$ with $m_{a,b}\in E_3$, let $\Pi_n(M) = 1$ iff there is a polynomial p of degree at most s-1 over GF(q) such that $\forall a\in GF(q)$ $m_{a,p(a)}=1$ and $m_{a,p(a)+e}=2$.
Lemma 5 and Corollary 1 directly yield the following bound.

Corollary 3: $n^{\Omega(\ln n)} \le L_{\{\vee,\otimes\}}(\Pi_n,H) \le n^{C\ln n}$, $C\le 1/47$.

Obviously we are just begining to understand the power of functional (as well as probabilistic and topological) approximations in lower bounds proofs. The two examples given in this note, as well as examples is [2-4,13,14], all concern the standard algebra of DNFs. Of course, Theorems 1-3 admit further applications. For example, one may consider more subtle representations of Boolean functions such as the algebra of prime implicants, etc. Besides, a suitable combination of functional, probabilistic and topological approximation techniques may help.

REFERENCES

[1] M. Ajtai, Σ^1-formulae on finite structures. *Ann.of Pure and Appl.logic*, 24 (1984), pp. 1-48.

[2] N. Alon and R.B. Boppana, The monotone circuit complexity of Boolean functions, *Combinatorica*, 7, N.1 (1987), pp. 1-22.

[3] A.E. Andreev, On one method of obtaining lower bounds of individual monotone function complexity, *Doklady Akad. Nauk SSSR*, 282 (1985), pp. 1033-1037.

[4] A.E. Andreev, On one method of obtaining effective lower bounds of monotone complexity, *Algebra i Logika*, 26,N.1(1987),pp. 3-21.

[5] M. Furst, J.B. Saxe and M. Sipser, Parity, circuits and the polynomial time hierarchy , *Proc. 22nd FOCS* (1981),pp.260-270.

[6] A. Hajnal, W. Maass, P. Pudlak, M. Szegedy and G. Turan, Threshold circuits of bounded depth, *Proc. 28th FOCS* (1987), 99-110.

[7] J. Hastad, Almost optimal lower bounds for small depth circuits, *Proc. 18th STOC* (1986), pp. 6-20.

[8] S.P. Jukna, Lower bounds on the complexity of local circuits, *Lect. Notes in Comput. Sci.* 233 (Springer-Berlin, 1986),440-448.

[9] S.P. Jukna, Entropy of contact circuits and lower bounds on their complexity, *Theoret. Comput.Sci.*, 57, N.1 (1988).

[10] S.P. Jukna, On one entropic method of obtaining lower bounds on the complexity of Boolean functions, *Doklady Akad. Nauk SSSR*, 298, N.3 (1988), pp. 556-559.

[11] E.A. Okol'nishnikova, On the influence of one type of restrictions to the complexity of combinational circuits, *Discrete Analysis* , 36 (Novosibirsk, 1981), pp. 46-58.

[12] M.S. Paterson, Bonded-depth circuits over {⊕,&}, Preprint, 1986.

[13] A.A. Razbororov, Lower bounds for the monotone complexity of some Boolean functions, *Doklady Akad. Nauk SSSR*, 281 (1985), pp. 798-801.

[14] A.A. Razborov, A lower bound on the monotone network complexity of the logical permanent, *Mat. Zametki*, 37, N.6 (1985)

[15] A.A.Razborov, Lower bounds for the size of bounded-depth circuits over the basis { ⊕ ,&}, Preprint (Moscow, 1986).

[16] R. Smolensky, Algebraic methods in the theory of lower bounds for Boolean circuit complexity, *Proc. 19th STOC* (1987), pp.77-87.

[17] A. Yao, Lower bounds by probabilistic arguments, *Proc. 24th FOCS* (1983), pp. 420-428.

[18] G.A. Tkachev, On the complexity of one sequence of functions of k-valued logic, *Vestnik MGU*, *Ser.2*, N.1 (1977), pp. 45-57.

[19] A.B. Ugol'nikov, On the complexity of realization of Boolean functions by circuits over the basis with median and implication *Vestnik MGU*, *Ser.1*, N.4 (1987), pp. 76-78.

[20] L.G. Valiant, Short monotone formulae for the majority function, *Journal of Algorithms*, v. 5 (1984), pp. 363-366.