LOWER BOUNDS ON THE COMPLEXITY OF LOCAL CIRCUITS

(Preliminary Report)

S.P.Jukna

Institute of Mathematics and Cybernetics
Lithuanian Academy of Sciences
232021 Vilnius, USSR

A method is proposed for obtaining lower bounds on the complexity of logical networks. It allows one to prove in a uniform and easy way that sufficiently local circuits (including monotone circuits, bounded depth circuits, circuits with no null chains, etc.) require nearly-exponential size to compute naturally arising Boolean functions. Our best lower bound for an NP function of n variables is $\exp(\Omega(\sqrt{n}\log n))$.

1. Introduction. Although most of the Boolean functions (BFs in short) have exponential complexity the largest known lower bound for effectively defined functions (or ELB for Effective Lower Bound) remains an $\Omega(n^2/\log^2)$ bound by Nechiporuk [N 66] . The principality of such a situation was foreseen already in 1959 by Jablonskij [Jab59].

Thus in order to gain more insight to the problem of proving non-trivial lower bounds, one has investigated more restricted models. While introducing the restrictions, an attempt is usually made to achieve the situation where the function, computed by a subcircuit, weakly depends (or does not depend at all) on the whole circuit, i.e. to achieve a certain locality in computations. This has been done at first by Tkachev [T 80] who investigated the realization of BFs by circuits of depth ≤ 3 over the complete basis $\{\&, \vee, {}^-\}$ and proved nearly exponential ELB of size $\exp(\Omega(n^{1/4}))$. Independently and at about the same time Furst/Saxe/Sipser [FSS 81] obtained super-polynomial ELBs for the circuits of any constant depth. Considering a different restriction of the circuits, namely the circuits with no null chains, Pulatov [P 79] and Kuznetsov [K 81] obtained ELBs of size $\exp(\Omega(n))$ for some special BFs. Investigating one-time-only branching programs Pudlák/Žák [PŽ 83, Ž 84] ,Wegener [W 84] and Dunne [D 85] obtained an ELBs of size $\exp(\Omega(n^{1/2}))$. For monotone circuits, i.e. the circuits over the incomplete basis $\{\&, \vee, 0, 1\}$, Andreev [A 85] has recently proved nearly-exponential ELBs of size $\exp(\Omega(n^{1/8-o(1)}))$. Independently for the same class of circuits (but for other BFs) Razborov [R 85] obtains ELBs of size $\exp(\Omega(\log^2 n))$. Subsequently, modifying Razborov's arguments Alon/Boppana [AB 85] improved these bounds to $\exp(\Omega(n^{1/4}(\log n)^{1/2}))$.

In this paper we propose some initial ideas of a new method for

obtaining non-trivial ELBs. In the case of local circuits it allows us to obtain in a uniform and easy way nearly-exponential ELBs of size $\exp(\Omega(n^{1/2}\log n))$.

Our method represents an appropriate concretization of an entropic approach to the lower bounds problem we propose in [Juk 84]. Basic idea is quite simple: we offer to define the lower bound on the complexity by means of "entropy preserving" imbeddings of circuits into the more restricted ones. In [Juk 84], to define the entropy of machines, we use Janov's [Jan 75] notion of convolution of their computation trees, and apply this to bound the complexity of Turing machine computations. Here we apply such an approach to Boolean networks. To be more specific, let there be given some encoding $F: X \to Y$ of the objects from Y (Boolean functions) by the objects from X(networks) together with some measure $m: X \to N$ of their complexity. A goal is to define the lower bounds for the induced measure $L(y) = \min\{m(x) : F(x) = y\}$ on Y without any use of the encoding F. Doing this we propose to act as follows. Choose some intermediate classes (of more restricted circuits) $X = X_0 \supset X_1 \supset \ldots \supset X_k = Y$. Further, identify any object $x \in X$ with an appropriate set x^* of its "sub-objects" and choose some binary relation $\varphi \subseteq x^* \times x^*$ of their "similarity". Define φ-entropy $H^{\varphi}(x)$ of x to be the minimal number of φ-intervals, covering x^* ; $A \subseteq x^*$ is a φ-interval over x^* iff $a\varphi b$ for all $a,b \in A$. An object x_1 is said to be (φ,ψ)-epimorphic to x_2 iff there is a(possibly partial) surjection $\nu: x_1^* \to x_2^*$ such that for any a,b from $\nu^{-1}(x_2^*)$, $a\varphi b$ implies $\nu(a)\psi\nu(b)$. Then $H^{\varphi}(x_1) \geqslant H^{\psi}(x_2)$, though it may be the case that $m(x_1) < m(x_2)$. Thus, if the relations $\varphi = \varphi_0, \ldots, \varphi_k = \psi$ are chosen so that $H^{\varphi} = m$ and for any $y \in Y$ and $x \in X_i \cap F^{-1}(y)$, x is $(\varphi_i, \varphi_{i+1})$-epimorphic to some $x' \in X_{i+1} \cap F^{-1}(y)$, then $L(y) \geqslant H^{\psi}(y)$.

Here we apply such an approach for contact circuits. For other kinds of logical networks this may be done in a similar manner.

2. Terminology. A contact circuit (or simply a circuit) is a finite undirected graph, the edges of which are labeled by contacts, i.e. by variables and their negations $x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n$, or by constant 1, with distinguished node-root and some nodes-terminals. For an edge e, $\hat{e}$ denotes its label. A chain is a path with no cycles. A chain, starting in a circuit's root is initial. A branch is an initial chain ending in some terminal. A chain $C = v_0 e_1 v_1 e_2 \ldots e_h v_h$ defines the minterm $\hat{C} = \hat{e}_1 \hat{e}_2 \ldots \hat{e}_h$. If C is an initial chain of a contact tree we shall write $\hat{v}_h$ instead of $\hat{C}$, and call the number of contacts in C a height of v_h. A chain C is null chain iff $\hat{C} \equiv 0$.

A circuit is primitive (or one-time-only) iff any of its branches contains no repeated occurrences of variables. Given a circuit S, a vicinity of a node $v \in S$ consists of all the variables x such that for some $a \in \{0,1\}$ the following is valid: there exist an initial non-null chains C_0, C_1 to v and a non-null chain C_2 from v to a terminal of S such that $x^a \in C_2$, $\bar{x}^a \in C_0$ and $\bar{x}^a \notin C_1$. A circuit is t-local ($t \geq 0$) iff the vicinity of any of its node contains no more than t variables. Thus one-time-only circuits, monotone circuits (i.e. the circuits with no negated variables) and circuits with no null chains are special instances of t-local circuits with t=0. On the other hand any circuit of n variables is t-local for some $t \leq n$.

A circuit S is q-circuit ($1 \leq q \leq \infty$) if any Boolean vector realizes no more than q distinct branches of S. Thus any circuit is ∞-circuit. A branching program (BP) is a special case of the 1-circuit: it is a directed contact circuit, where each node has an outdegree ≤ 2, and the edges leaving a node with an outdegree =2 are labeled by contrary contacts. For the sake of uniformity we shall refer to BP as to 0-circuit.

The size L(S) of circuit S is the number of nodes in S. The complexity of a Boolean function f is defined by $L_{t,q}(f) = \min L(S)$ where min is over all the t-local q-circuits S, computing f. Put $C_t = L_{t,\infty}$, $DC_t = L_{t,1}$ ("D" for Deterministic) and $BP_t = L_{t,0}$. Then clearly, $C_t(f) \leq DC_t(f) \leq BP_t(f)$. Onthe other hand it is known (see, e.g. [PŽ 83]) that C_∞ and BP_∞ are polynomially related.

For a contact tree T let T^* denote the set of all its (complete) subtrees. Given $\varphi \subseteq T^* \times T^*$, let $H^\varphi(T)$ denote φ-entropy of T, i.e. $H^\varphi(T) = H^\varphi(T^*)$. The entropy of a Boolean function f is defined by $H_q^\varphi(f) = \min\{H^\varphi(T) : T \text{ is a primitive q-tree and } \hat{T} = f\}$. Here and in what follows $\hat{T}$ stands for the disjunction of all branches in T.

For a minterm K and a disjunctive normal form (DNF in short) $D = K_1 \vee \ldots \vee K_r$, let $D\{K\}$ denote the set of all DNFs $K_1K_1' \vee \ldots \vee K_rK_r'$ where $K_i' \subseteq K$ $(1 \leq i \leq r)$. For minterms K_1 and K_2, put $K_1 \rhd K_2 = \{x^a : x^a \in K_1 \text{ and } \bar{x}^a \in K_2\}$ and $K_1 \dot{-} K_2 = K_1 - (K_1 \rhd K_2)$.

Define two special relations ψ and θ on T^* as follows. For subtrees T_v and T_u with the roots v and u, let:

$T_v \psi T_u$ iff $(\hat{v} \dot{-} \hat{u})\hat{T}_v = (\hat{u} \dot{-} \hat{v})\hat{T}_u$, and

$T_v \theta T_u$ iff $\hat{T}_v\{\hat{v} \dot{-} \hat{u}\} \cap \hat{T}_u\{\hat{u} \dot{-} \hat{v}\} \neq \emptyset$.

Notice that $H^\psi(T) \geq H^\theta(T)$, since $\psi \subseteq \theta$.

3. Complexity and Entropy. Let E denote the set of all Boolean functions f such that any two distinct Boolean vectors from $f^{-1}(1)$ differ in at least two coordinates.

Theorem 1. For any Boolean function f, any $t \geq 0$ and $0 \leq q \leq \infty$, we have

$$L_{t,q}(f) \geq H_q^{\varphi}(f) \cdot 3^{-t},$$

where $\varphi = \psi$ if $f \in E$, and $\varphi = \theta$ otherwise.

Proof. Consider an unfoldnment T of some minimal t-local q-circuit S, computing f, i.e. T is a contact q-tree such that $\hat{T} = f$ and $H^I(T) = L_{t,q}(f)$, where I stands for the isomorphism relation. Remove from T all the edges e (together with their successors) such that an initial chain to e contains a contact contrary to $\hat{e}$. Let T^o denote the resulting contact tree. Hence, T^o has no null chains and $\hat{T}^o = f$. Moreover, from the locality of S it follows that $H^I(T^o) \leq H^I(T) \cdot 3^t$. Indeed, let $\{T_v : v \in V\}$ be an I-interval over T^*. As S is minimal, all the nodes of T from V correspond to a single node v_o of S. Let X be the vicinity of v_o in S. Then $|X| \leq t$ (here and in what follows $|X|$ stands for the cardinality of X). Put $mt(X) = \{x^a : x \in X \text{ and } a \in \{0,1\}\}$, and let M denote the set of all non-null minterms over $mt(X)$. Clearly, $|M| = 3^{|X|} \leq 3^t$. Let U be the set of nodes in T^o, corresponding to V, and let A denote the set of all subtrees of T^o rooted in U, i.e. $A = \{T_u^o : u \in U\}$. For a minterm K from M, put $U(K) = \{u \in U : \hat{u} \cap mt(X) = K\}$. It is seen that for any minterm K all the subtrees from A rooted in $U(K)$ are pairwise isomorphic. Hence A contains no more than $|M| \leq 3^t$ pairwise non-isomorphic subtrees. Therefore, $H^I(T^o) \leq H^I(T) \cdot 3^t$. Next, replace all the repeated occurrences of contacts in any of T^o's branch by 1. Clearly, such a relabeling does not change the function. It is also seen that T^o is (I, φ)-epimorphic to the resulting q-tree T^1, where $\varphi = \psi$ if $f \in E$, and $\varphi = \theta$ otherwise. So $H^I(T^o) \geq H^{\varphi}(T^1)$ where by definition, $H^{\varphi}(T^1) \geq H_q^{\varphi}(f)$. □

Taking into account the structure of coverings one may investigate more meaningful notions of entropy and improve Theorem 1 for less restrictive notions of locality. In particular, one may relax the condition "$\bar{x}^a \notin C_1$" in the definition of vicinity to "$\bar{x}^a \notin C_1/C_0$" where C_1/C_0 denotes the maximal tail of C_1 which has no edge in common with C_0. However, this is not in the scope (nor the aim) of the present report and will be published elsewhere.

Nevertheless, even such a naive definition of entropy leads to rather strong lower bounds. By Theorem 1, in order to bound the complexity of a given BF it sufficies to bound the entropy of its primitive trees. Let us demonstrate this for three natural classes of BFs.

Let $X = \{x_1,\dots,x_n\}$. An assignment is a function $\varrho: X \to X \cup \{0,1\}$ such that for any $x \in X$, either $\varrho(x) \in \{0,1\}$ or $\varrho(x) = x$; $D\varrho = \varrho^{-1}(0) \cup \varrho^{-1}(1)$ is a signature of ϱ; $|D\varrho|$ is a rank of ϱ. For a Boolean function $f(X)$, f^{ϱ} denotes the subfunction $f(\varrho(x_1), \dots, \varrho(x_n))$. A Boolean function $f(X)$ is m-mixed ($0 < m \leq n$) if for any $Y \subseteq X$, with $|Y| \leq m$, and any two assignments $\varrho \neq \gamma$ of the signature Y, either $f^{\varrho} = f^{\gamma} \equiv 0$ or $f^{\varrho} \neq f^{\gamma}$; it is strongly m-mixed if $f^{\varrho} \neq f^{\gamma}$ for all such assignments. The class of mixed BFs is sufficiently rich: for any $m \leq n - (1+\varepsilon)\log n$, with $\varepsilon > 0$ arbitrary small almost all BFs of n variables are strongly m-mixed. For an assignment ϱ, put $K(\varrho) = \{x^{\varrho(x)}: x \in D\varrho\}$. For a BF $f(X)$, let $Q_f(m)$ denote the least number r of assignments $\varrho_1,\dots,\varrho_r$ of rank = m, possessing the representation: $f = \bigvee_{i=1}^{r} K(\varrho_i)\cdot f^{\varrho_i}$.

Theorem 2. If $f(X)$ is a 2m-mixed Boolean function then $H_1^{\theta}(f) \geq Q_f(m)$. If, in addition, f is strongly m-mixed then $H_1^{\theta}(f) \geq \exp(m)$.

Proof. Consider a primitive 1-tree T, computing f, and let V denote the set of its nodes of height m. Then clearly, $|V| \geq Q_f(m)$. If f is strongly m-mixed then $|V| \geq \exp(m)$, since T is a 1-tree. So it remains to show that any θ-interval over T^* contains no more than one subtree rooted in V. Indeed, let (on the contrary) that $T_v \,\theta\, T_u$ for some $v \neq u$ from V. Put $K = \hat{v}(\hat{u} \dot{-} \hat{v})$, and let var(K) denote the set of variables in K. Consider an assignment ϱ of signature var(K) such that $K^{\varrho} = 1$, and let γ be an assignment (of the same signature) such that $\gamma(x) \neq \varrho(x)$ if $x \in \mathrm{var}(\hat{u} \rhd \hat{v})$, and $\gamma(x) = \varrho(x)$ otherwise. Since $T_v \,\theta\, T_u$ and T has no null chains, it follows that $(\hat{T}_v)^{\varrho} = (\hat{T}_u)^{\gamma}$. Thus $f^{\varrho} = f^{\gamma}$, since $(\hat{v})^{\varrho} = (\hat{u})^{\gamma} = 1$ and T is a 1-tree. Moreover, $\varrho \neq \gamma$, since otherwise some Boolean vector $\tilde{a}$, with $\tilde{a}_i = \varrho(x_i)$ for $x_i \in D\varrho$, realizes ≥ 2 branches of T. But $|D\varrho| = |D\gamma| < 2m$. □

A Boolean function $f(X)$ is m-stable if for any $x \in X$ and any $Y \subseteq X - \{x\}$, with $|Y| \leq m$, there is an assignment γ of signature $X - Y - \{x\}$ such that f^{γ} depends merely on x, i.e. either $f^{\gamma}(x,Y) = x$ or $f^{\gamma}(x,Y) = \bar{x}$. Following the proof of Theorem 2 one can easily prove

Theorem 3. If f is a 2m-stable Boolean function then $H_1^{\theta}(f) \geq \exp(m)$.

Using an argument originally employed by Wegener in [W 84], Dunne in [D 85] shows that computing any m-stable BF requires primitive BP of size exp(m). Theorems 1,3 yield more general bound.

Corollary 1. If f is a 2m-stable Boolean function then for any $t \geq 0$, we have: $DC_t(f) = \Omega(\exp(m - t))$.

The weight $\mathrm{wh}(\tilde{a})$ of $\tilde{a} \in \{0,1\}^n$ is the number of 1's in $\tilde{a}$. We call $\tilde{a}$ a lower one (LWO) of a BF f iff $f(\tilde{a}) = 1$ and $f(\tilde{b}) = 0$ for

any $\tilde{b} \in \{0,1\}^n$ such that $\tilde{b} \leq \tilde{a}$ and $wh(\tilde{b}) = wh(\tilde{a}) - 1$. For a monotone BFs this notion of LWO coincides with the usual one . Let N_f (M_f) denote the set of all LWOs of f (of minimal weight). Thus, $wh(\tilde{a}) = wh(\tilde{b})$ for all $\tilde{a},\tilde{b} \in M_f$. For $\tilde{a} \in \{0,1\}^n$, put $Z(\tilde{a}) = \{i : \tilde{a}_i = 1\}$. A Boolean function f is (k,r)-uniform ($k \geq 2$, $r \geq 1$) iff $wh(\tilde{a}) \geq 2r$ for all $\tilde{a} \in M_f$, and for any k pairwise distinct LWOs $\tilde{a}_1,\ldots,\tilde{a}_k$ from M_f it holds: $|Z(\tilde{a}_1) \cap \ldots \cap Z(\tilde{a}_k)| \leq r$; f is k-uniform if it is (k,r)-uniform for some $r \geq 1$; f is strongly k-uniform if,in this connection, $M_f = N_f$. Thus, the uniformity of f corresponds to a certain "uniformity of distribution" of symbols in its shortest DNFs.

Theorem 4.If f is a 2-uniform Boolean function then $H^{\Psi}_{\infty}(f) \geq |M_f|$. If f is strongly k-uniform for some $k \geq 2$ and $f \in E$ then for any q, $0 \leq q \leq \infty$, it holds: $H^{\Psi}_q(f) \geq |M_f| \cdot (k-1)^{-2} \max(1/k, 1/(q+1))$.

4. Applications. Theorems 1-4 permit us to obtain in a uniform and easy way nearly-exponential lower bounds on the complexity of local circuits. In a number of cases it leads us to the improvement of ELBs recently obtained by quite strong (but special) methods. Whilst it would be tedious to attempt to indicate all such ELBs we restrict ourselves to some typical samples.

A great deal of examples may be defined by means of transversals in (0,1)-matrices. For $k \geq 2$, let W_k denote the set of all functions $w: \underline{k} \to \underline{k}$, where $\underline{k} = \{0,1,\ldots,k-1\}$. For an (0,1)-matrix $X = \{x_{i,j} : i,j \in \underline{k}\}$, let $Tr(X)$ denote the set of all transversals of X, i.e. $Tr(X) = \{w \in W_k : x_{i,w(i)} = 1 \text{ for all } i \in \underline{k}\}$.For $F \subseteq W_k$, let $tr_F(X)$ denote the number of transversals of X in F, i.e. $tr_F(X) = |F \cap Tr(X)|$. Any subset of k-valued functions $F \subseteq W_k$ induces the following two Boolean functions $\underline{F}^0(X)$ and $\underline{F}^1(X)$ of $n = k^2$ variables: $\underline{F}^0(X) = 1$ iff $tr_F(X) > 0$, and $\underline{F}^1(X) = tr_F(X) \pmod 2$. For such a BFs there is quite a simple criterion of their stability. Let gr(w) denote the graph of w. We say that $F \subseteq W_k$ is m-dense if for any $y \in \underline{k}^2$ and any $Y \subseteq \underline{k}^2 - \{y\}$, with $|Y| \leq m$, there is $w_o \in F$ such that: $y \in gr(w_o)$, $Y \cap gr(w_o) = \emptyset$ and $gr(w) - (Y \cup gr(w_o)) \neq \emptyset$ for any other w from $F - \{w_o\}$.

Lemma. Let $F \subseteq W_k$ and $a \in \{0,1\}$. Then $\underline{F}^a$ is m-stable iff F is m-dense.
Corollary 2.For any m-dense subset $F \subseteq W_k$, any $a \in \{0,1\}$ and $t \geq 0$, we have: $DC_t(\underline{F}^a) = \Omega(\exp(m/2 - t))$.

To illustrate this, let us consider the following three classes of k-valued functions: (1) Pr, the set of all permutations of $\underline{k}$; (2) Rd, the set of all residue functions $w_1(w_2(x) \bmod p)$, where p =

$= \lfloor k/2 \rfloor$ and $w_1, w_2 \in Pr$; (3) Pl, the set of all polynomials of degree at most p over the Galois field GF(k), where k is a prime power. It is easily seen that all these classes are m-dense for any $m \leq p-2$.

Corollary 3. Let $F \in \{Pr, Rd, Pl\}$ and $a \in \{0,1\}$. If $t = t(n) \leq n^{1/2-o(1)}$ then $DC_t(F^a) = \exp(\Omega(\sqrt{n}))$.

Recently, concerning an important case of 0-local ∞-circuits, namely the monotone ones, Andreev [A 85] obtained an $\exp(\Omega(n^{1/8-o(1)}))$ lower bound for $\underline{Pl}^0$. Razborov [R 85] obtained an $\exp(\Omega(\log^2 n))$ bound for $\underline{Pr}^0$. Modifying Razborov's arguments, Alon/Boppana [AB 85] improved the lower bound for $\underline{Pl}^0$ to $\exp(\Omega(n^{1/4}(\log n)^{1/2}))$. These arguments use essentially the monotonicity of circuits, so they do not work for such "close" functions as, e.g. $\underline{Pl}^1$ and $\underline{Pr}^1$.

For a Boolean function f, let f_* denote the characteristic function of N_f. If f is monotone then, clearly, $f_* \in E$. In many cases not only f itself but also f_* is hard to compute by a local circuit. For example, $\underline{Pl}^0_*$ is (2,p)-uniform and $\underline{Pr}^0_*$ is ((k-i)!,i)-uniform for any $1 \leq i \leq p$, so Theorems 1 and 4 yield

Corollary 4. For any $t \geq 0$ and $0 \leq q \leq \infty$, we have:

$$L_{t,q}(\underline{Pr}^0_*) = \exp(\Omega(\sqrt{n} - t)), \text{ and}$$

$$\exp(\Omega(\sqrt{n \log n} - t)) \leq C_t(\underline{Pl}^0_*) \leq \exp(O(\sqrt{n \log n})).$$

Concerning the circuits with no null chains Pulatov/Kuznetsov [P 79, K 81] have proved that for any BF f, $C_0(f) \geq |f^{-1}(1)|^{d/n}$, where d stands for the minimal Hamming's distance between any two distinct vectors from $f^{-1}(1) \subseteq \{0,1\}^n$. It enables them to obtain nearly-exponential lower bounds for some special functions. However, if d is too small with respect to $|f^{-1}(1)|$, their arguments do not work. For example, if $f = \underline{Pl}^0_*$ then $d \leq \sqrt{n}$, whereas $|f^{-1}(1)| = \exp(1/4 \sqrt{n} \log n)$, and hence, $|f^{-1}(1)|^{d/n} = O(n)$ (cf. corollary 4).

For $1 \leq s \leq n$, let f^s_n be the function of $r = \binom{n}{2}$ Boolean variables representing the edges of an undirected graph G on n nodes, whose value is 1 iff G contains an s-clique. Razborov in [R 85] shows that f^s_n, with $s = \lfloor 1/4 \ln n \rfloor$, requires monotone circuit of size $\exp(\Omega(\log^2 n))$. Subsequently, Alon/Boppana [AB 85] improved this bound to $\exp(\Omega(n/\log n)^{1/3})$. Wegener in [W 84] proves that f^s_n, with $s = \lceil (2n/3)^{1/3} \rceil$ requires 0-local BP of size $\Omega(\exp(n/3 - o(n)))$. As f^s_n is m-stable for any $m \leq \min\{\binom{s}{2}, n-s\} - 1$, Theorems 1 and 3 directly yield

Corollary 5. If $s = \lfloor (2n)^{1/2} \rfloor$ then for any $t \geq 0$, we have:

$$DC_t(f^s_n) = \Omega(\exp(n/2 - \sqrt{n} - t)).$$

Considering $g_n = (f_n^{n/2})_*$, known also as an "exactly-half clique function", Pudlák/Žák [PŽ 83, Ž 84] proved that g_n requires primitive BP of size $\exp(\Omega(n))$. As far as g_n is m-mixed for any $m \leq \lfloor r/2 \rfloor$, Theorems 1 and 2 directly yield

Corollary 6. For any $t = t(n) \leq n^{1-o(1)}$, we have:

$$DC_t(g_n) = \exp(\Omega(n)).$$

Finally, notice that the non-local branching program complexity of Boolean functions $\underline{Pr}^0$, $\underline{Pr}^1$, $\underline{Pl}^0_*$ and g_n is actually polynomial. Thus, if $t \leq n^{1/2-o(1)}$ then some functions of n variables require nearly-exponential t-local circuits, whereas their n-local circuit complexity is polynomial, i.e. the locality of circuits may force an exponential rise of their complexity.

Acknowledgment - I wish to thank Professor J.I.Janov for his support and many helpful discussions.

References:

[AB 85] N.Alon and R.B.Boppana: The monotone circuit complexity of Boolean functions,manuscript (1985)- to appear in Combinatorica.

[A 85] A.E.Andreev: On one method of obtaining lower bounds of individual monotone function complexity, Dokl. Akad. Nauk SSSR, 282 (1985), pp. 1033-1037.

[D 85] P.E.Dunne: Lower bounds on the complexity of 1-time-only branching programs,Lecture Notes in Comput.Sci.,199(1985),pp.90-99.

[FSS 81] M.Furst, J.B.Saxe and M.Sipser: Parity, circuits and polynomial-time hierarchy, 22ND Symp. on the Foundations of Computer Science,(1981),pp. 260-270.

[Jab 59] S.V.Jablonskij: On algorithmic obstacles in synthesis of minimal contact schemes, Problemy Kibernetiki, 2 (1959),pp.75-121.

[Jan 75] J.I.Janov: On some semantic characteristics of Turing machines, Dokl. Akad. Nauk SSSR, 224 (1975), pp.301-304.

[Juk 84] S.P.Jukna: Convolutional characterization of computability and complexity of computations, Colloquia Mathematica Societatis János Bolyai, 44 (1984), pp. 251-270.

[K 81] S.E.Kuznetsov: Combinatorial circuits with no null chains over basis $\{\&, \vee, \bar{}\}$, Izvestija VUZ, Matematika, 5 (1981), pp. 56 - 63.

[N 66] E.I.Nechiporuk: A Boolean function, Doklady Akad. Nauk SSSR, 169 (1966), pp. 765 - 766.

[PŽ 83] P.Pudlák and S.Žák: Space complexity of computations, Preprint Univ. Prague (1983), 30p.

[P 79] A.K.Pulatov: Lower bounds on the complexity of implementation of characteristic functions of group codes by Π-networks, Combinatorial-Algebraic Methods in Applied Mathematics, Gorki (1979), pp. 81 - 95.

[R 85] A.A.Razborov: Lower bounds on the monotone complexity of some Boolean functions, Doklady Akad. Nauk SSSR, 281 (1985), pp. 798 - 801.

[T 80] G.A.Tkachev: On the complexity of a sequence of Boolean functions by implementing in terms of circuits and Π-circuits under additional restrictions on the circuits structure, Combinatorial-Algebraic Methods in Applied Mathematics, Gorki (1980), pp. 261 - 207.

[W 84] I.Wegener: On the complexity of branching programs and decision trees for clique functions, Univ. Frankfurt, Interner Bericht , 5 (1984), 32p.

[Ž 84] S.Žak: An exponential lower bounds for one-time-only branching programs, Lecture Notes in Computer Science, 176 (1984), pp. 562 - 566.