Theoretical Computer Science 57 (1988) 113-129
North-Holland

ENTROPY OF CONTACT CIRCUITS AND LOWER BOUNDS ON THEIR COMPLEXITY

Stasys P. JUKNA

Institute of Mathematics, Lithuanian Academy of Sciences, 232600 Vilnius, Lithuanian SSR, U.S.S.R.

Abstract. A method for obtaining lower bounds on the contact circuit complexity of explicitly defined Boolean functions is given. It appears as one of possible concretizations of a more general "convolutional" approach to the lower bounds problem worked out by the author in 1984 [12]. The method is based on an appropriate notion of "inner information" or "entropy" of finite objects (circuits, Boolean functions, etc.). Lower bounds on the complexity are obtained by means of entropy-preserving embeddings of circuits into the more restricted ones. This allows to prove in a uniform and easy way that contact circuits, which are local in a sense that the function computed by a subcircuit weakly depends on the whole circuit, require $2^{\Omega(\sqrt{n})}$ or even $2^{\Omega(n/\log n)}$ contacts to compute some explicitly defined n-argument Boolean functions from NP.

1. Introduction

Although it has long been known that "almost all" n-argument Boolean functions require exponential size to be computed by a contact circuit, the best lower bound proved to date for explicitly defined functions remains an[1] $\Omega(n^2(\log_2 n)^{-2})$ bound by Nechiporuk [16].

Thus, in order to gain more insight in the problem of proving nontrivial lower bounds, one has investigated more restricted models of Boolean networks. Moreover, the restrictions are usually chosen so as to achieve some "locality" in computations, i.e., to achieve the situation where the function computed by a subnetwork weakly depends (or does not depend at all) on the whole network.

Probably, the first nontrivial result in this direction was obtained by Tkachev [24]. He has proved that the unbounded fan-in combinatorial circuits of depth $\leqslant 3$ over the basis $\{\&, \vee\}$ require[2] $\exp(n^{1/4})$ gates to compute some concrete monotone Boolean function of n variables. Independently, and at about the same time, Furst, Saxe and Sipser [10] have proved (via nice probabilistic arguments) that even such simple Boolean functions as parity or majority require more than a polynomial number of gates to be computed by unbounded fan-in circuits over $\{\&, \vee, \neg\}$ of *any* constant depth. Later, Hastad [11] improved these bounds for depth $\leqslant k$ circuits to $\exp(n^{1/k})$. Recently, Razborov [22] has shown that the majority function requires superpolynomial size, constant-depth circuits even over the basis $\{\&, \text{parity}\}$. Thus depth restrictions are too strong to separate complex functions from simple ones.

[1] $f = \Omega(g)$ means that $(\exists c > 0)(\forall n)(\exists m > n)\ cf(m) \geqslant g(m)$.

[2] $\exp(n)$ stands for $2^{\Omega(n)}$.

0304-3975/88/$3.50

The second class of sufficiently "local" circuits is that of monotone ones. Until recently, the best known lower bound for this class of Boolean networks was an $\Omega(n^2/\log n)$ bound by Wegener [26]. Recently, via a major development of the standard approach of proving lower bounds—demonstrating that a certain amount of progress must be made, and that no step makes more than δ progress, for some small δ—Andreev [4] and Razborov [21] have proved superpolynomial lower bounds for monotone networks. These networks are interesting in a sense that for some monotone Boolean functions—so called "slice" functions—their monotone and nonmonotone complexity is almost the same. (This has been observed by Berkowitz (as cited in Valiant [25])). Unfortunately, for slice functions the Andreev-Razborov technique does not work. On the other hand, the nonmonotone network model is too "global" and there does not seem to be a way to define progress appropriately.

The third class of Boolean networks for which nonpolynomial lower bounds were obtained is that of contact circuits with bounds on various "resources" (width, multiplicity of reading). The first nearly-exponential lower bound for read-once-only π-schemes was proved by Pulatov in [20]. Later, analogous bounds for read-once-only branching programs (a special case of read-once-only contact circuits) were obtained by Pudlák and Žák [17], Žák [29], Wegener [27], Dunne [9] and Ajtai et al. [1]. Width-restricted branching programs have first been promoted by Borodin, Dolev, Fich and Paul [6]. Their main result, completed by Yao [28], is a superpolynomial lower bound for width-2 branching programs computing the majority function. For width $\geqslant 2$ programs the only nontrivial lower bounds remain a barely nonlinear bound by Chandra, Furst and Lipton [8] and an $\Omega(n \log_2 n/\log_2\log_2 n)$ bound by Pudlák [18] and Ajtai et al. [1] obtained by Ramsey-like arguments. The lack of progress in this direction is explained by Barington's recent result [5] that already width-5 branching programs are almost as powerful as (unrestricted) π-schemes or formulas over $\{\&, \vee, \neg\}$.

Thus, to prove nontrivial lower bounds (even for restricted models of Boolean networks), a new insight is needed. Our definition of "inner information" or "entropy" is motivated by the search for such a new technique. The basic idea (given also in [12, 13]) is quite simple: we suggest to define the lower bound on the complexity by means of "entropy-preserving" embeddings of networks into the more restricted ones. To be more specific, let some class of finite objects (Boolean networks, Boolean functions, etc.) be given. Then we choose an appropriate notion of "subobject" and some (binary) relation φ of their "similarity". Let A^* denote the set of all subobjects of an object A. A subset $\mathfrak{A} \subseteq A^*$ such that for any two distinct subobjects B and C from $\mathfrak{A}$ it holds that either $B\varphi C$ or $C\varphi B$ (or both), is called a *φ-interval* over A^*. Define the *φ-entropy* of A, entropy$(A:\varphi)$, to be the minimal number of φ-intervals (over A^*) covering A^*. Thus, for reflexive φ, we have that $1 \leqslant \text{entropy}(A:\varphi) \leqslant |A^*|$, where $|A^*|$ denotes the cardinality of A^*. We will say that an object A is *(φ, ψ)-epimorphic* to an object B if there exists a (possibly partial) surjection $\nu: A^* \to B^*$ such that, for all subobjects C and D from $\nu^{-1}(B^*)$,

$C\varphi D$ implies $\nu(C)\,\psi\,\nu(D)$. The following simple fact expresses the main idea of our approach.

Fact 1.1. *Suppose that φ and ψ are both reflexive and that A is (φ, ψ)-epimorphic to B. Then* $\text{entropy}(A:\varphi) \geqslant \text{entropy}(B:\psi)$ *(though it may be the case that* $\text{size}(A) \lessdot \text{size}(B)$).

Let us outline the way in which this fact will be used to derive lower bounds. Let $\mathfrak{B}$ denote the set of some initial representations of Boolean functions (truth-tables, disjunctive normal forms, etc.), and let $\mathfrak{M}$ be some class of Boolean networks. In order to define the lower bound for

$$L_{\mathfrak{M}}(f) = \min\{\text{size}(S) : S \in \mathfrak{M} \text{ and } S \text{ computes } f\}, \quad f \in \mathfrak{B},$$

choose some intermediate classes of (more restricted) networks $\mathfrak{M} = \mathfrak{M}_0 \supset \mathfrak{M}_1 \supset \cdots \supset \mathfrak{M}_k = \mathfrak{B}$ and appropriate relations $\varphi = \varphi_0, \varphi_1, \ldots, \varphi_k = \psi$ of their similarity so as to ensure the following two constraints:

(i) for any $S \in \mathfrak{M}$, $\text{size}(S) \geqslant \text{entropy}(S:\varphi)$, and

(ii) any network S from $\mathfrak{M}_i$ is $(\varphi_i, \varphi_{i+1})$-epimorphic to some equivalent (i.e., computing the same Boolean function) network S' in $\mathfrak{M}_{i+1}$. Then $L_{\mathfrak{M}}(f) \geqslant \text{entropy}(f:\psi)$.

Note that the counting argument used by Nechiporuk in [16] is a special case of our approach with $\varphi = \psi = \text{identity}$ relation.

In this paper we apply such an approach for contact circuits. (For other kinds of Boolean networks this may be done in a similar manner.) This leads to a nearly-exponential lower bound for local circuits. Informally, a contact circuit computing a Boolean function of n variables $x_1, \ldots, x_n$ is (t, r)-local if for each of its nodes u of distance $\leqslant r$ (from the source) there is a subset $Y_u \subseteq \{x_1, \ldots, x_n\}$, with $|Y_u| \leqslant t$ such that, starting from the node u, the knowledge of all variables not tested on any path from the circuit's source to u and the knowledge of variables from Y_u is sufficient to determine the value of the function. A circuit is (k, t, r)-local if it has some (t, r)-local subcircuit, the source of which is at distance $\leqslant k$ from the source of the circuit. Thus, e.g., read-once-only contact circuits are $(0, 0, n)$-local. On the other hand, any circuit is $(0, t, n)$-local for some $t \leqslant n$. In Section 6 a uniform argument is given to generate concrete n-argument Boolean functions from NP (and even from P) which require $(\sqrt{n}, t, \sqrt{n})$-local circuits of size $\exp(\sqrt{n})$ or even of size $\exp(n/\log_2 n)$.

2. Preliminaries

A (directed) *contact circuit* (also called *contact gating scheme*) over the set of Boolean variables $X = \{x_1, \ldots, x_n\}$ is a labelled acyclic graph G with

(i) a distinguished node of indegree $= 0$ (the source of G),

(ii) *some* edges labelled by contacts x^a, where $x \in X$ and $a \in \{0,1\}$, i.e., by variables $x^1 = x$ or their negations $x^0 = \bar{x}$.

A *branching program* is a directed contact circuit with the following additional constraints:

(iii) every node has outdgree at most 2,

(iv) for every node v with outdegree 2, one of the edges leaving v is labelled by a variable $x \in X$ and the other is labelled by its complement $\bar{x}$.

A path starting in the source of the circuit is called *initial*. A *chain* is an initial path ending in some sink, i.e., in a node of outdegree 0. Every path P of G defines the monomial $\hat{P} = \hat{e}_1 \cdot \ldots \cdot \hat{e}_k$, where $\{e_1, \ldots, e_k\}$ is the set of all labelled edges in P and $\hat{e}$ denotes the label of e. (In what follows we shall also identify $\hat{P}$ with the set of contacts $\{\hat{e}_1, \ldots, \hat{e}_k\}$). A path P is a *null-path* iff $\hat{P} = 0$, i.e., if $\{x, \bar{x}\} \subseteq \hat{P}$ for some $x \in X$. A circuit G computes a Boolean function $f: \{0,1\}^n \to \{0,1\}$ iff $f = \hat{G}$, where $\hat{G}$ denotes the disjunction of the monomials defined by its chains. For a circuit G, let $V(G)$ denote the set of its nodes. Given a node v, let G^v denote the minimal subgraph of G containing all the initial paths to v, and let G_v denote the minimal subgraph of G containing all the paths from v to sinks of G. Thus v is a (unique) sink of G^v as well as a source of G_v. If G is a *contact tree* (i.e., if the underlying graph of G is a directed tree), then $|\hat{G}^v| = 1$ for any $v \in V(G)$.

A variable $x \in X$ is called *critical* for a node v of G iff for some $a \in \{0,1\}$ the following holds: there exist two non-null chains P_1 and P_2 of G^v and a non-null chain P_3 of G_v such that $x^a \in \hat{P}_1$, $\bar{x}^a \in \hat{P}_3$ and $\hat{P}_2\hat{P}_3 \neq 0$. Put $\operatorname{crit}(v, G) = \{x \in X: x$ is critical for v in $G\}$. The *height* of v in G is the minimal number of different contacts in an initial non-null path to v. So, $0 \leq \operatorname{height}(v) \leq n$. For an integer $r \geq 0$, put $V_r(G) = \{v \in V(G): \operatorname{height}(v) \leq r\}$.

Definition 2.1. Let $k, t, r \geq 0$ be integers such that $k + r \leq n$. A contact circuit G is (t, r)*-local* iff $|\operatorname{crit}(v, G)| \leq t$ for all nodes v of height $\leq r$; G is (k, t, r)-local if G contains some (t, r)-local subcircuit G_v with $v \in V_k(G)$; G is t-local if G is (t, r)-local with $r = n$.

Thus any contact circuit of n variables is t-local for some $0 \leq t \leq n$. *Read-once-only* circuits (i.e., contact circuits with no repeated occurrences of contacts in their chains), *monotone* circuits (i.e., contact circuits with no negated variables) and circuits *with no null-chains* are special cases of 0-local ones. (Note also that a 0-local circuit is not necessarily a read-once-only one.)

The *size* of a circuit G, size(G), is the number of nodes in G. The *circuit-size complexity* of a Boolean function f is defined by

$$\mathrm{C}^k_{t,r}(f) = \min\{\operatorname{size}(G): \hat{G} = f \text{ and } G \text{ is } (k, t, r)\text{-local}\}.$$

In the case of branching programs, the corresponding measure is denoted by $\mathrm{BP}^k_{t,r}(f)$. If f is a function of n variables, we shall omit the indices $k = 0$, $t = n$ and $r = n$. Thus, e.g., $\mathrm{C}_t(f) = \mathrm{C}^0_{t,n}(f)$.

Remark 2.2. In this paper we shall consider only directed contact circuits since this model is a most suitable one to explain the main idea of our approach. On the other hand, from the observations made by Pudlák in [17, 19] it follows that directed contact circuits and branching programs are quite powerful. Let UC(f) denote the undirected contact circuit complexity of f. Then

$$\mathrm{C}(\cdot) \leqslant \mathrm{UC}(\cdot)^2 \quad \text{and} \quad \mathrm{BP}(\cdot) \leqslant \mathrm{C}(\cdot)^{\mathrm{O}(1)}.$$

The idea for the first inequality is to split given undirected contact circuit G into a sequence of identical copies and replace each undirected edge by two directed edges which go from a given copy to the next one. We do not need more copies than the number of nodes of G. The proof of the second inequality is based on a probabilistic argument of Aleliunas et al. [2].

Remark 2.3. Local circuits are quite powerful. For example, one may easily verify that $\mathrm{BP}_0(f_n) \leqslant \mathrm{O}(n^2)$ for every symmetric Boolean function f_n of n variables. On the other hand, Brustmann and Wegener in [7] have proved that any sequence of symmetric functions f_n, $n = 1, 2, \ldots$, such that the length of shortest prime implicants or prime clauses of f_n grows faster than $(\log_2 n)^c$ for any constant $c > 0$ require super-polynomial constant-depth combinatorial circuits over $\{\&, \vee, \bar{\ }\}$.

Definition 2.4. Given an integer $r \geqslant 0$ and a binary relation $\varphi \subseteq V(G) \times V(G)$, we define an *entropy* $\mathrm{H}_r^\varphi(G)$ of a circuit G to be the φ-entropy of $V_r(G)$, i.e., $\mathrm{H}_r^\varphi(G)$ is the minimal number of φ-intervals (over $V(G)$) covering $V_r(G)$. For a Boolean function f, let $\mathrm{H}_r^\varphi(f) = \min\{\mathrm{H}_r^\varphi(T) \colon \hat{T} = f$ and T is read-once-only contact tree$\}$. In the case of branching trees, the corresponding entropy is denoted by $\mathrm{E}_r^\varphi(f)$. Put also $\mathrm{H}^\varphi(f) = \mathrm{H}_n^\varphi(f)$. (Observe that $\mathrm{E}(f)$ is actually the entropy of the truth-table $f^{-1}(1)$ of f, whereas $\mathrm{H}(f)$ is actually the entropy of its Disjunctive Normal Forms (DNF in short)). Note that $\mathrm{H}^\varphi(f) \geqslant \max\{\mathrm{H}_r^\varphi(f) \colon 0 \leqslant r \leqslant n\}$.

For monomials K and W, put $K \rhd W = \{x^a \colon x^a \in K$ and $x^a \in W\}$ and $K \ominus W = (K - (K \rhd W)$. For a DNF $D = K_1 \vee \cdots \vee K_p$ and a monomial W, let $D[W]$ denote the set of all DNFs $K_1 W_1 \vee \cdots \vee K_p W_p$ where $W_i \subseteq W$, $i = 1, 2, \ldots, p$. For a node v of a contact tree T, let $\hat{v}$ denote the (unique) monomial in T^v.

Convention: To avoid unwieldy expressions we shall write v, P, G instead of $\hat{v}$, $\hat{P}$, $\hat{G}$ if the meaning is clear from the context.

Let us now define some concrete relations of “similarity”. Given a contact tree T and two of its nodes u and v, let

- $u \backsim v$ iff T_u and T_v are isomorphic (as labelled graphs);
- $u \psi v$ iff $(u \ominus v) \cdot T_u = (v \ominus u) \cdot T_v$;
- $u \theta v$ iff $T_u[u \ominus v] \cap T_v[v \ominus u] \neq \emptyset$.

Note that $\backsim \subseteq \psi \subseteq \theta$. Therefore, $H^{\backsim} \geqslant H^{\psi} \geqslant H^{\theta}$.

To illustrate the definition, let us give a short example. Let $\hat{v} = x_1 x_2 x_5$, $\hat{u} = \bar{x}_2 \bar{x}_3 x_4$, $\hat{T}_v = x_4 \vee \bar{x}_3$ and $\hat{T}_u = x_1 \vee x_5$. Then $v \ominus u = x_1 x_5$ and $u \ominus v = \bar{x}_3 x_4$. The nodes v and

u are not ψ-similar, since the DNFs $(v\ominus u)\cdot T_v = x_1x_4x_5 \vee x_1\bar{x}_3x_5$ and $(u\ominus v)\cdot T_u = \bar{x}_3x_4x_5 \vee x_1\bar{x}_3x_4$ realize different Boolean functions. But these are φ-similar since the sets $T_v[v\ominus u]$ and $T_u[u\ominus v]$ both contain the DNF $x_4x_5 \vee x_1\bar{x}_3$.

3. Entropy and complexity

A Boolean function f is called *critical* if any two distinct vectors from $f^{-1}(1)$ differ in at least two coordinates.

Fact 3.1. *Let G be a contact circuit computing a critical Boolean function of n variables. Then for any non-null chain P of G it holds that $|\hat{P}| = n$.*

Proof. Straightforward. □

Theorem 3.2. *For any Boolean function f and integers t, $r \geqslant 0$, with $t \leqslant r$, the following bound holds*:

$$\mathrm{C}^0_{t,r}(f) \geqslant \mathrm{H}^{\varphi}_r(f)\cdot 3^{-t},$$

where $\varphi = \psi$ if f is critical, and $\varphi = \theta$ otherwise. The bound holds also with C *and* H *replaced by* BP *and* E.

Proof. Let G be some minimal $(0, t, r)$-local contact circuit computing f, i.e., $\hat{G} = f$ and $\mathrm{size}(G) = \mathrm{C}^0_{t,r}(f)$. Let T be an "unfoldment" of G, i.e., T is the contact tree obtained from G as the result of the following procedure of "unfolding": for a node v of G with indegree $\geqslant 2$, switch some edge leading to v to the root of some new circuit isomorphic to G_v. Thus, if $N(v)$ denotes the set of all the nodes of T corresponding to $v \in V(G)$, then all the subtrees of T, rooted in $N(v)$, are pairwise isomorphic. Put $N_r(T) = \{N(v){:}\ v \in V_r(G)\}$. Then, obviously, $\mathrm{size}(G) \geqslant |N_r(T)| \geqslant \mathrm{H}^{\backsim}_r(T)$.

Remove from T all the nodes v (together with the corresponding pendant edges) such that each chain of T_v contains a contact contrary to some contact from $\hat{v}$. Let T^0 denote the resulting tree. It computes f and has no null-chains.

Claim 3.3. $\mathrm{H}^{\backsim}_r(T^0) \leqslant |N_r(T)|\cdot 3^t$.

To prove the claim, let v be some node of G of height $\leqslant r$, and put $Y = \mathrm{crit}(v, G)$. Since G is $(0, t, r)$-local, $|Y| \leqslant t$. Set $Y^* = \{x^a{:}\ x \in Y \text{ and } a \in \{0, 1\}\}$ and let $M(Y)$ denote the set of all non-null monomials over Y^*. Thus, $|M(Y)| = 3^{|Y|} \leqslant 3^t$. By U denote the set of all nodes of T^0 corresponding to $N(v)$. For a monomial K, put $U(K) = \{u \in U{:}\ \hat{u} \cap Y^* = K\}$. It is clear that for any $K \in M(Y)$ all the subtrees of T^0, rooted in $U(K)$, are pairwise isomorphic. Therefore, $\mathrm{entropy}(U{:}\ \backsim) \leqslant |M(Y)|$, and the assertion of Claim 3.3 follows.

Next, let T^* denote the tree obtained from T^0 after all the repeated occurrences of contacts in its chains have been wiped out. Obviously, such a transformation does not change the function. Since T^* is read-once-only, $\mathrm{H}^{\varphi}_r(T^*) \geqslant \mathrm{H}^{\varphi}_r(f)$. So by Fact 1.1, it remains to prove the following claim.

Claim 3.4. *$V_r(T^0)$ is $(\backsim, \varphi)$-epimorphic to $V_r(T^*)$.*

The case $\varphi = \theta$ is obvious. To prove the claim for $\varphi = \psi$, suppose that f is critical. It is sufficient to show that, for any two nodes u and v of T^0 with $u \backsim v$, the following holds: if $x^a \in u \ominus v$, then either $x^a \in v \ominus u$ or $x^a \in K$ for any monomial K from T^0_v. Indeed, if $x^a \notin v \ominus u$, then by Fact 3.1, any monomial from T^0_v must contain some contact of x. Since $T^0_u = T^0_v$ and T^0 has no null-chains, it follows that any monomial from T^0_v contains x^a. This completes the proof of Claim 3.4, and thus the proof of Theorem 3.2. □

Let $X = \{x_1, \ldots, x_n\}$. An *assignment* is a function δ from X into $X \cup \{0, 1\}$ such that, for each $x \in X$, $\delta(x) \in \{0, 1, x\}$. The set $\mathrm{sign}(\delta) = \delta^{-1}(0) \cup \delta^{-1}(1)$ is a *signature* of δ; $|\delta| = |\mathrm{sign}(\delta)|$ is a *rank* of δ. Given a Boolean function $f(X)$, we shall denote by f^δ the function we obtain by composing f and δ, i.e., $f^\delta(X) = f(\delta(x_1), \ldots, \delta(x_n))$. Notice that f^δ is a function of $n - |\delta|$ variables.

The following obvious fact points out the "deterministic nature" of branching programs.

Fact 3.5. *Let P be an initial non-null path to a node v in a branching program G computing f. Then, for any assignment δ such that $(\hat{P})^\delta = 1$, we have $f^\delta = (\hat{G}_v)^\delta$.*

Hence we have the following useful fact.

Fact 3.6. *For any Boolean function f it holds that*

$$\mathrm{BP}^k_{t,r}(f) \geqslant \min_{|\delta|=k} \mathrm{BP}^0_{t,r}(f^\delta).$$

Theorem 3.7. *For any Boolean function f it holds that*

$$\mathrm{BP}^k_{t,r}(f) \geqslant \min_{|\delta|=k} \mathrm{E}^{\varphi}_r(f^\delta) \cdot 3^{-t},$$

where $\varphi = \psi$ if f is critical, and $\varphi = \theta$ otherwise.

Thus in order to bound the complexity of a given Boolean function, it is enough to bound the entropy of its read-once-only contact trees. In a number of cases this is an easy exercise. Let us demonstrate this for some natural classes of Boolean functions.

4. Entropy of mixed and stable Boolean functions

A Boolean function $f(X)$ is (*weakly*) *m-mixed* iff, for any $Y \subseteq X$ with $|Y| \leq m$, and any two distinct assignments δ, γ of signature Y it holds that (either $f^\delta = f^\gamma = 0$ or) $f^\delta \neq f^\gamma$. Let BF_n (respectively BF_n^m) denote the class of all (m-mixed) Boolean functions. The class of mixed functions is sufficiently rich.

Theorem 4.1 (Mamatov [15]). *For arbitrary small $c > 0$, the following holds:*
(i) *If $m \leq n-(1+c)\log_2 n$, then $|\mathrm{BF}_n^m|/|\mathrm{BF}_n| \to 1$ as $n \to \infty$,*
(ii) *If $m \geq n-(1-c)\log_2 n$, then $\mathrm{BF}_n^m = \emptyset$ for every sufficiently large n.*

For a Boolean function f and an integer $m \geq 1$, let $Q_m(f)$ denote the minimal number p of monomials $K_1, \dots, K_p$ such that $f \leq K_1 \vee \cdots \vee K_p$ and $|K_1| = \cdots = |K_p| = m$.

The following lemma and Theorem 4.1 assert that the θ-entropy of almost all Boolean functions of n variables is $\geq \exp(n)$.

Lemma 4.2. *If f is $2m$-mixed ($m \geq 1$), then $\mathrm{E}_m^\theta(f) \geq 2^{m+1}-1$. If f is weakly $2m$-mixed ($m \geq 1$), then $\mathrm{E}_m^\theta(f) \geq Q_m(f)$.*

Proof. To prove the first bound, let T be some read-once-only branching tree computing a $2m$-mixed Boolean function f. Put $U_m = \{u \in V(T) : \mathrm{height}(u) = m\}$. It is sufficient to prove the following two claims.

Claim 4.3. $|U_m| \geq 2^m$.

Claim 4.4. *Any θ-interval over U_m contains exactly one node.*

To prove Claim 4.3, assume that $|U_m| \leq 2^m - 1$. Then there is a node u of height $\leq m-1$ and of outdegree $=1$ such that the unique edge, (u, v) say, is labelled by some contact x^a. Let δ be the assignment of rank $|\bar{v}| \leq m$ such that $\hat{u}^\delta = 1$ and $\delta(x) = a + 1 (\mathrm{mod}\, 2)$. Then, obviously, $\hat{T}^\delta = 0$, and by Fact 3.5, $f^\delta = 0$, contradicting thc assumption that f is m-mixed.

To prove Claim 4.4, assume that $u \,\theta\, v$ for some distinct nodes u, v from U_m. For a monomial K, let $\mathrm{var}(K)$ denote the set of variables in K. Consider assignments δ and γ of signature $\mathrm{var}(u(v \ominus u))$ such that $\hat{u}^\delta = 1$ and $\hat{v}^\gamma = 1$. Since $u \,\theta\, v$ and T has no null-chains, $\hat{T}^\delta = \hat{T}^\gamma$. By Fact 3.5, $f^\delta = f^\gamma$. But $\delta \neq \gamma$ and $|\delta| = |\gamma| < 2m$. This contradiction completes the proof of Claim 4.4.

The proof of the second bound is analogous to that of the previous one with Claim 4.3 replaced by the following obvious Claim 4.3: $|U_m| \geq Q_m(f)$. □

A Boolean function $f(X)$ is *m-stable* iff, for any $x \in X$ and $Y \subseteq X - \{x\}$ with $|Y| \leq m$, there exists an assignment δ of signature $X - Y - \{x\}$ such that f^δ depends merely on x, i.e., either $f^\delta(x, Y) \equiv x$ of $f^\delta(x, Y) \equiv \bar{x}$.

Note: If f is critical, then f is m-stable for no $m \geq 1$.

Using an argument originally employed by Wegener [27], Dunne in [9] has proved that a special case of 0-local branching program require $\exp(m)$ size to compute m-stable functions. Lemma 4.2 yields a more general bound.

Lemma 4.5. *If f is $2m$-stable for some $m \geqslant 1$, then* $\mathrm{E}_m^\theta(f) \geqslant 2^{m+1} - 1$.

Proof. By Lemma 4.2, it is sufficient to prove the following claim.

Claim 4.6. *If f is m-stable, then f is $(m+1)$-mixed.*

To prove the claim, suppose that $f(X)$ is not $(m+1)$-mixed. This means that, for some $Y \subseteq X$ with $|Y| \leqslant m+1$, there are at least two distinct assignments δ, γ of signature Y such that $f^\delta = f^\gamma$. Choose a variable $x \in Y$ for which $\delta(x) \neq \gamma(x)$. Then, for any $a \in \{0, 1\}$ and any assignment ρ of signature $X - Y$, $f^\rho(x, Y - \{x\})$ does not equal x^a. But $|Y - \{x\}| \leqslant m$. Therefore, f is not m-stable. □

Theorem 4.7. *Let m, k, t, r be integers such that $2 \leqslant k + 2r \leqslant m$ and $t \geqslant 0$. If f is m-stable or m-mixed Boolean function, then* $\mathrm{BP}_{t,r}^k(f) \geqslant 2^r \cdot 3^{-t}$. *If f is weakly m-mixed, then*

$$\mathrm{BP}_{t,r}^k(f) \geqslant \min\{Q_r(f^\delta): |\delta| = k\} \cdot 3^{-t}.$$

Proof. Let δ be an assignment of rank k such that

$$\mathrm{E}_r^\theta(f^\delta) = \min\{\mathrm{E}_r^\theta(f^\delta): |\delta| = k\}.$$

If f is m-stable (m-mixed or weakly m-mixed), then f^δ is $2r$-stable (respectively $2r$-mixed or weakly $2r$-mixed) since $|\delta| + 2r \leqslant m$. So it remains to apply Theorem 3.7 and Lemmas 4.2 and 4.5. □

For monotone Boolean functions there is a quite simple criterion of their stability in terms of their (unique) shortest DNFs. For a Boolean function $f(X)$, let $\mathrm{Imp}(f)$ denote the set of all its prime implicants. For a variable $x \in X$, put $\mathrm{Imp}(f, x) = \{K \in \mathrm{Imp}(f): x \in K\}$.

Fact 4.8. *A monotone Boolean function $f(X)$ is m-stable for some $m \geqslant 1$ if and only if, for any $x \in X$ and $Y \subseteq X - \{x\}$ with $|Y| \leqslant m$, the following holds:*

(i) *$K_0 \cap Y = \emptyset$ for some $K_0 \in \mathrm{Imp}(f, x)$,*

(ii) *$W - (K_0 \cup Y) \neq \emptyset$ for any $W \in \mathrm{Imp}(f) - \mathrm{Imp}(f, x)$.*

5. Entropy of disjoint Boolean functions

For a Boolean vector $\tilde{a} = (a_1, \ldots, a_n)$, with $a_i \in \{0, 1\}$, put $\mathrm{Ind}(\tilde{a}) = \{i: a_i = 1\}$ and $\|\tilde{a}\| = |\mathrm{Ind}(\tilde{a})|$. For a Boolean function f, set $M_f = \{\tilde{a} \in f^{-1}(1): f(\tilde{b}) = 0$ for any $\tilde{b} \leqslant \tilde{a}$, $\tilde{b} \neq \tilde{a}\}$, where $\tilde{b} \leqslant \tilde{a}$ iff $a_i \geqslant b_i$, $i = 1, \ldots, n$, and put $\mathrm{wh}(f) = \min\{\|\tilde{a}\|: \tilde{a} \in M_f\}$. Let also M_f^* denote the set of minimal elements of M_f, i.e., $M_f^* = \{\tilde{a} \in M_f: \|\tilde{a}\| = \mathrm{wh}(f)\}$.

Definition 5.1. A Boolean function f is (k, r)-*disjoint* iff $\mathrm{wh}(f) \geqslant 2r$ and for any k pairwise distinct vectors $\tilde{a}_1, \ldots, \tilde{a}_k$ from M_f^* it holds that $|\mathrm{Ind}(\tilde{a}_1) \cap \cdots \cap \mathrm{Ind}(\tilde{a}_k)| \leqslant r-1$; f is k-*disjoint* if f is (k, r)-disjoint for some $r \geqslant 1$.

Theorem 5.2. (i) *If f is 2-disjoint, then* $\mathrm{H}^{\psi}(f) \geqslant |M_f^*|$.

(ii) *If f is k-disjoint for some $k \geqslant 3$ and $f^{-1}(1) = M_f^*$, then*

$$\mathrm{E}^{\psi}(f) \geqslant |M_f^*| \cdot (k-1)^{-2} \quad \textit{and} \quad \mathrm{H}^{\psi}(f) \geqslant \tfrac{1}{2}|M_f^*| \cdot (k-1)^{-3}.$$

Proof. Let f be (k, r)-disjoint for some $k \geqslant 2$ and $r \geqslant 1$, and let T be a read-once-only contact tree computing f. For a node v of T, let $A(v)$ denote the set of all the vectors $\tilde{a}$ from M_f^* such that $\tilde{a}$ realizes some chain of T containing v. Put $U = \{v \in V(T) \colon |\hat{v}|_+ = r\}$, where, for a monomial K, $|K|_+$ stands for the number of unnegated variables in K. Choose some subset $V \subseteq U$ which is minimal in a sense that $A(V) = \bigcup\{A(v) \colon v \in V\} = M_f^*$ but $M_f^* - A(V - \{v\}) \neq \emptyset$ for each $v \in V$. Put

$$\chi = \max\{|V_0| \colon V_0 \text{ is a } \psi\text{-interval over } V\}.$$

Claim 5.3. $\mathrm{H}_r^{\psi}(T) \geqslant |M_f^*|/(k-1) \cdot \chi$.

To prove the claim, observe that $\mathrm{H}_r^{\psi}(T) \geqslant |V| \cdot \chi^{-1}$. Moreover, $|V| \geqslant |M_f^*| \cdot (k-1)^{-1}$. Indeed, otherwise there must be a node $v \in V$ such that $|A(v)| \geqslant k$. But

$$\left|\bigcap\{\mathrm{Ind}(\tilde{a}) \colon \tilde{a} \in A(v)\}\right| \geqslant |\hat{v}|_+ = r,$$

a contradiction. So it remains to bound χ.

(i): Suppose that f is (k, r)-disjoint with $k = 2$. Then $\chi = 1$. Assume that $u \,\psi\, v$ for some nodes $u \neq v$ from V. Since $k = 2$, $|A(u)| = |A(v)| = 1$. Moreover $A(u) \neq A(v)$ as V is minimal. Let $A(u) = \{\tilde{a}\}$, and let P be a chain of T such that $u \in P$ and $\hat{P}(\tilde{a}) = 1$. Let K denote the monomial such that $P = \hat{u} \cdot K$. Without loss of generality,

$$|u \rhd v|_+ \geqslant |v \rhd u|_+ . \tag{1}$$

Since $u \,\psi\, v$, there is a monomial W in T_v such that

$$(u \ominus v) \cdot K = (v \ominus u) \cdot W. \tag{2}$$

Let $\tilde{b}$ be a Boolean vector with the minimal number of ones for which $\hat{v} \cdot W(\tilde{b}) = 1$. By (1) and (2), $\|\tilde{b}\| = |\hat{v} \cdot W|_+ \leqslant |\hat{P}|_+ = \|\tilde{a}\|$. Hence, $\tilde{b} \in M_f^*$ and $\tilde{b} \neq \tilde{a}$. But by (2),

$$|\mathrm{Ind}(\tilde{a}) \cap \mathrm{Ind}(\tilde{b})| \geqslant |K|_+ \geqslant \|\tilde{a}\| - |\hat{u}|_+ = \mathrm{wh}(f) - r \geqslant r,$$

a contradiction.

(ii): Suppose that f is (k, r)-disjoint with $k \geqslant 3$. To prove the theorem in this case, it is sufficient to prove that $\chi \leqslant k-1$ if T is a branching tree, and $\chi \leqslant (k-1)^2 + 1$ otherwise.

Let $\{v_1, \ldots, v_\chi\}$ be some ψ-interval over V.

Case 1: T is a branching tree. Choose some $\tilde{a}_1 \in A(v_1)$. Let P be a chain of T such that $\hat{P}(\tilde{a}_1) = 1$ and v_1 is in P. Let K_1 denote a monomial such that $\hat{P} = \hat{v}_1 K_1$.

Since any node v_i, $i=2,\dots,\chi$, is ψ-similar to v_1, it follows that $\hat{T}_{v_i}$ contains a monomial K_i such that

$$(v_1 \ominus v_i)\cdot K_1=(v_i \ominus v_1)\cdot K_i. \tag{3}$$

Since T has no null-chains, there exist vectors $\{\tilde{a}_2,\dots,\tilde{a}_\chi\}$ such that $\hat{v}_i\cdot K_i(\tilde{a}_i)=1$. As $f^{-1}(1)=M_f^*$, all these vectors are in M_f^*. Moreover, all these vectors are pairwise distinct since T is a branching tree. But by (3),

$$|\bigcap\{\mathrm{Ind}(\tilde{a}_i)\colon i\leqslant\chi\}|\geqslant|K_1|_+\geqslant \mathrm{wh}(f)-r\geqslant r.$$

Therefore, $\chi\leqslant k-1$.

Case 2: T is not a branching tree. Since V is minimal for any i, $1\leqslant i\leqslant\chi$, there is some $\tilde{a}_i$ in $A(v_i)-A(V-\{v_i\})$. Let K_i denote a monomial from $\hat{T}_{v_i}$ such that $\hat{v}_i\cdot K_i(\tilde{a}_i)=1$. Since any node v_j, $2\leqslant j\leqslant\chi$, is ψ-similar to v_1, it follows that $\hat{T}_{v_1}$ contains a monomial K_i' such that

$$(v_i \ominus v_1)\cdot K_i=(v_1 \ominus v_i)\cdot K_i'. \tag{4}$$

Since $|A(v_1)|\leqslant k-1$ and $f^{-1}(1)=M_f^*$, by (4), there exists some set $J\subseteq\{2,\dots,\chi\}$ such that $|J|\geqslant(\chi-1)/(k-1)$ and $K_i'=K_j'$ for all $i, j\in J$. Let $j_0\in J$. Then

$$|\bigcap\{\mathrm{Ind}(a_j)\colon j\in J\}|\geqslant|K_{j_0}'|_+\geqslant \mathrm{wh}(f)-r\geqslant r,$$

and from the k-disjointness of f it follows that $|J|\leqslant k-1$. Thus, $\chi\leqslant(k-1)^2+1$. This completes the proof of Case 2, and thus the proof of Theorem 5.2. □

6. Applications

The results of the previous sections provide a uniform way to obtain nearly-exponential lower bounds on the complexity of local contact circuits. In a number of cases this leads to an improvement of lower bounds recently obtained by quite strong (but special) techniques. Since it would be tedious to attempt to indicate all such bounds, we restrict ourselves to some typical examples.

For an integer $q\geqslant 2$, put $\bar{q}=\{1,\dots,q\}$ and $\bar{n}=\bar{q}\times\bar{q}$. Subsets of $\bar{n}$ will be called *points* over $\bar{n}$ and subsets of points will be called *point-sets* over $\bar{n}$. For a (0, 1)-matrix $X=\{x_a\colon a\in\bar{n}\}$, let PS($X$) denote the set of all points A over $\bar{n}$ such that, for any $a\in\bar{n}$, $a\in A$ implies $x_a=1$.

Definition 6.1. A point-set F over $\bar{n}$ is *m-dense* if, for any $a\in\bar{n}$ and $A\subseteq\bar{n}-\{a\}$ with $|A|\leqslant m$, there is a point $B\in F$ such that the following holds:

(i) $a\in B$,

(ii) $A\cap B=\emptyset$,

(iii) $C-(A\cup B)\neq\emptyset$ for any point $C\in F-\{B\}$ with $a\notin C$.

Given a point-set F over $\bar{n}$, we associate with F the following two Boolean functions $\xi(F)$ and $\eta\{F\}$ of $n=q^2$ variables:

$$\xi\{F\}(X)=1 \text{ iff } |F\cap \mathrm{PS}(X)|=1 (\mathrm{mod}\, 2)$$

and

$$\eta\{F\}(X)=1 \text{ iff } |F\cap \mathrm{PS}(X)|>0.$$

Note that η is monotone but ξ is not, in general.

Lemma 6.2. *If F is an m-dense point-set, then $\xi\{F\}$ and $\eta\{F\}$ are both m-stable (and hence, $m+1$-mixed). Moreover, $\eta\{F\}$ is m-stable only if F is m-dense.*

Proof. The second claim follows directly from Fact 4.8. To prove the first claim, let F be an m-dense point-set and fix some $x_a\in X$ and $Y\subseteq X-\{x_a\}$ with $|Y|\leqslant m$. Let $A\subseteq \bar{n}$ denote the set of indices of variables from Y, i.e., $Y=\{x_b\colon b\in A\}$. Let δ be an assignment such that $\delta(x_b)=1$ if $b\in B-\{a\}$, and $\delta(x_b)=0$ if $b\in \bar{n}-(A\cup B)$, where B is from Definition 6.1. Since $A\cap B=\emptyset$, δ is well-defined and $\mathrm{sign}(\delta)=X-Y-\{x_a\}$. Since $C-(A\cup B)\neq\emptyset$ for any point $C\in F-\{B\}$ (with $a\notin C$), it follows that for any assignment γ of signature Y, $\mathrm{PS}(X^{\delta,\gamma})=\emptyset$ if $x_a=0$, and $|\mathrm{PS}(X^{\delta,\gamma})|=1$ if $x_a=1$. Therefore, $\xi^{\delta}\{F\}(X)=\eta^{\delta}\{F\}\equiv x_a$. □

Let us give some typical examples of dense point-sets.

Convention: To avoid unwieldy expressions we shall identify any set F of q-valued functions $\sigma\colon\bar{q}\to\bar{q}$ with the corresponding point-set $\{\lceil\sigma\rceil\colon \sigma\in F\}$ of their graphs $\lceil\sigma\rceil=\{(i,j)\colon \sigma(i)=j\}$.

Example 6.3. For $q\geqslant 2$, let $\mathrm{Tw}(q)$ denote the set of all total functions $\sigma\colon\bar{q}\to\bar{q}$ such that, for each $j\in\bar{q}$, either $\sigma^{-1}(j)=\emptyset$ or $|\sigma^{-1}(j)|\geqslant 2$.

Fact 6.4. *For an even integer $q\geqslant 2$, the point-set $\mathrm{Tw}(q)$ is $\frac{1}{2}q$-dense.*

Proof. Put $m=\frac{1}{2}q$ and fix some $a=(i_0,j_0)\in\bar{n}$ and $A\subseteq\bar{n}-\{a\}$ with $|A|\leqslant m$. Without loss of generality, $A\subseteq\bar{m}^2$ and $a\in\bar{m}^2$. (The case $a\notin\bar{m}^2$ is analogous). Define $\delta\colon\bar{q}\to\bar{q}$ as follows: $\delta(i_0)=\delta(i_0+m)=j_0$ and, for $i\in\bar{q}-\{i_0,i_0+m\}$, $\delta(i)=m+i$ if $i\leqslant m$ and $\delta(i)=i$ if $i\geqslant m+1$. Then, obviously, $\delta\in\mathrm{Tw}(q)$, $a\in\lceil\delta\rceil$ and $A\cap\lceil\delta\rceil=\emptyset$. So it remains to show that $\lceil\sigma\rceil-(A\cup\lceil\delta\rceil)\neq\emptyset$ for any $\sigma\in\mathrm{Tw}(q)$ such that $\sigma(i_0)\neq\delta(i_0)$. Assume that $\lceil\sigma\rceil\subseteq A\cup\lceil\delta\rceil$. Since $\sigma(i_0)\neq\delta(i_0)$, it follows that $\sigma(i_0)=j_1$ for some $j_1\neq j_0$ and $j_1\leqslant m$. Since σ is in $\mathrm{Tw}(q)$ and $\sigma(i)=\delta(i)$ for all $i\geqslant m+1$, there must be some $i_1\leqslant m$, $i_1\neq i_0$, such that $\sigma(i_1)=\sigma(i_0)=j_1$. Hence, $|\sigma^{-1}(j_2)|=1$ for $j_2=\delta(i_1)$, a contradiction. □

Example 6.5. For $q\geqslant 2$, let $\mathrm{Per}(q)$ denote the set of all bijections $\sigma\colon\bar{q}\to\bar{q}$.

Comment: $\mathrm{Per}(q)$ is actually the collection of perfect matchings. Thus, for example, $\xi\{\mathrm{Per}(q)\}(X)=1$ iff the q-vertex digraph, specified by a $(0,1)$-matrix X, contains an odd number of perfect matchings.

Fact 6.6. *For an even integer $q \geq 2$, the point-set* $\mathrm{Per}(q)$ *is* $\frac{1}{2}q$*-dense.*

Proof. The proof of this fact is analogous to that of Fact 6.4. □

Example 6.7. For a prime number $q \geq 5$ and an integer $d \geq 1$, let $\mathrm{Pol}(q, d)$ denote the set of all polynomials of degree at most d over the Galois field $\mathrm{GF}(q)$ of order q. (Here we identify the set of elements of $\mathrm{GF}(q)$ with $\bar{q}$.) Put $\mathrm{Pol}(q) = \mathrm{Pol}(q, \frac{1}{2}q)$.

Fact 6.8. *For each d, with $1 \leq d \leq \frac{1}{2}q$, the point-set* $\mathrm{Pol}(q, d)$ *is* $(d-1)$*-dense.*

Proof. Fix some $a \in \bar{n}$ and $A \subseteq \bar{n} - \{a\}$ with $|A| \leq d-1$. For $i \in \bar{q}$, let I_i denote the ith column of $\bar{n}$, i.e., $I_i = \{(i, j) : j \in \bar{q}\}$. Put

$$J = \{i \in \bar{q} : I_i \cap A \neq \emptyset \text{ and } a \notin I_i\}.$$

Then, obviously, $|J| \leq d-1$. Since $|A| \leq d-1 < q$, it follows that $I_i - A \neq \emptyset$ for each $i \in \bar{q}$. Hence, for each $i \in J$ we may choose some $b_i \in I_i - A$. Put

$$D = \{b_i : i \in J\} \cup \{a\}.$$

Since $|D| = |J| + 1 \leq d$, there is a polynomial δ in $\mathrm{Pol}(q, d)$ such that $D \subseteq \lceil \delta \rceil$. It is clear that $a \in \lceil \delta \rceil$ and $A \cap \lceil \delta \rceil = \emptyset$. So it remains to show that $\lceil \delta \rceil - (A \cup \lceil \delta \rceil) \neq \emptyset$ for any other polynomial σ from $\mathrm{Pol}(q, d)$.

Assume that $\lceil \sigma \rceil \subseteq (A \cup \lceil \sigma \rceil)$ for some polynomial $\sigma \neq \delta$. This means that

$$|\{i \in \bar{q} : \sigma(i) \neq \delta(i)\}| \leq |A| \leq d - 1,$$

and hence, $|\lceil \sigma \rceil \cap \lceil \delta \rceil| \geq q - (d-1) \geq d+1$. But σ and δ are both of degree at most d. Therefore, $\sigma = \delta$, a contradiction. □

Example 6.9. For integers $q \geq 2$ and $s \geq 1$, let $\mathrm{BCl}(q, s)$ denote the set of all points A over $\bar{n} - \Delta$, where $\Delta = \{(i, i) : i \in \bar{q}\}$, such that $A = I \times J$ for some $I, J \subseteq \bar{q}$ with $I \cap J = \emptyset$ and $|I| = |J| = s$. Let also $\mathrm{Cl}(q, s)$ denote the set of all points A over $\bar{n} - \Delta$ such that, for some $I \subseteq \bar{q}$ with $|I| = s$, it holds that $A \subseteq I \times I$ and, for all $i \neq j$ from I, either $(i, j) \in A$ or $(j, i) \in A$ (or both).

Comment: $\mathrm{BCl}(q, s)$ is actually the collection of s-bicliques, i.e., of complete bipartite $2s$-vertex digraphs, and $\mathrm{Cl}(q, s)$ is the collection of (directed) s-cliques.

Fact 6.10. *Let $q \geq s \geq 3$. Then*

(i) $\mathrm{BCl}(q, s)$ *is m-dense with* $m = \min\{s^2, q - 2s\} - 1$,

(ii) $\mathrm{Cl}(q, s)$ *is m-dense with* $m = \min\{\binom{s}{2}, q - s\} - 1$.

Proof. To prove the first claim, fix some $a = (i_0, j_0) \in \bar{n} - \Delta$ and $A \subseteq \bar{n} - \{a\}$ with $|A| \leq m$. Without loss of generality, $A \subseteq \bar{m}^2$ and $a \in \bar{m}^2$. Put

$$I = \{m+1, \ldots, m+s-1\}, \qquad J = \{q-s+1, \ldots, q\},$$

$$I_1 = I \cup \{i_0\} \quad \text{and} \quad J_1 = J \cup \{j_0\}.$$

Let $B = I_1 \times J_1$. Then $I_1 \cap J_1 = \emptyset$ since $m < q - 2s$ and $i_0 \neq j_0$. Hence, B is in BCl(q, s), $a \in B$ and $A \cap B = \emptyset$. So it remains to show that $C - (A \cup B) \neq \emptyset$ for any point C from BCl(q, s) with $a \notin C$. Assume that $C \subseteq A \cup B$ for some such point C. Then $C \cap (I \times J) = \emptyset$ since $|I| = |J| = s - 1$ and $a \notin C$. But $|A| \leqslant m \leqslant s^2 - 1$. Hence, C must contain some b from $(\{i_0\} \times J) \cup (I \times \{j_0\})$. Let, for example, $b \in \{i_0\} \times J$. Then $b = (i_0, j)$ for some $j \in J$. Since $s \geqslant 3$, there must be an integer $i_1 \leqslant m$ such that $i_1 \neq i_0$ and $(i_1, j) \in B$, which contradicts the definition of B. This completes the proof of (i). The proof of the second claim is analogous. □

Corollary 6.11. *For $q \geqslant 2$, let F_q stand for any of the following point-sets*: Pol(q), Per(q), Tw(q), BCl$(q, \frac{1}{4}q)$ *and* Cl$(q, \frac{1}{2}q)$. *Let also f_n stand for a Boolean function $\xi\{F_q\}$ or $\eta\{F_q\}$ (of $n \leqslant q^2$ variables). Then, for all integer-valued functions $k(q)$, $r(q)$ and $t(q)$ such that $k + 2r \leqslant \frac{1}{2}q$ and $t \leqslant (1 - \varepsilon)r$ for some constant $\varepsilon > 0$, it holds that*

$$\mathrm{BP}^k_{t,r}(f_n) \geqslant \exp(\sqrt{n}).$$

Proof. This immediately follows from Theorem 4.7 and Facts 6.4, 6.6, 6.8 and 6.10. □

Comment: An $\exp(\sqrt{n})$ lower bound for the complexity of $\eta\{\mathrm{Per}\}$ and clique functions in the class of once-time-only branching programs (a special case of 0-local branching programs) have already been proved in [17, 27, 9]. For an important case of 0-local contact circuits, namely the monotone ones, the results of [4, 21, 3] yield an $\exp(n^{1/4 - o(1)})$ lower bound for $\eta\{\mathrm{Pol}\}$ and an $\exp((\log_2 n)^2)$ lower bound for $\eta\{\mathrm{Per}\}$. Though the contact circuit complexity and the (unrestricted) branching program complexity are polynomially related (see Remark 2.2), it is not yet known if this also holds for monotone contact circuits and local branching programs. So, Corollary 6.11 does not directly imply the bounds for monotone circuits. Notice, however, that Andreev–Razborov's argument [4, 21] essentially uses the monotonicity of circuits, so it does not work for such close (to $\eta\{\mathrm{Per}\}$ and $\eta\{\mathrm{Pol}\}$) Boolean functions as $\xi\{\mathrm{Per}\}$ and $\xi\{\mathrm{Pol}\}$.

Example 6.12. For a Boolean function f, let f^* denote the characteristic function of M_f^*. (Note that f^* is critical for any f). In most cases not only f itself but also f^* and $f \cdot g$, where g is a critical Boolean function, are hard to compute by local circuits. Consider, for example, the following three Boolean functions of $n = q^2$ variables:

$$g_n^* = \eta^*\{\mathrm{Per}(q)\}, \qquad h_n^* = \eta^*\{\mathrm{Pol}(q)\},$$

$$h_n = \eta\{\mathrm{Pol}(q)\} \cdot \mathrm{parity}_n, \quad \text{where } \mathrm{parity}_n(\tilde{a}) = 1 \text{ iff } \|\tilde{a}\| = 1 (\mathrm{mod}\ 2).$$

One may easily verify that g_n^* is $((\frac{1}{2}q)!, \frac{1}{2}q)$-disjoint, and that h_n and h_n^* are both $(2, \frac{1}{2}q)$-disjoint. Theorems 3.2 and 5.2 directly yield the following bounds.

Corollary 6.13. *Let $t = t(n)$ be such that $t \leqslant (1-\varepsilon)\sqrt{n}$ for some integer $\varepsilon > 0$, and let $f_n \in \{h_n, h_n^*\}$. Then*

$$\mathrm{BP}_t(g_n^*) \geqslant \exp(\sqrt{n})$$

and

$$\log_2 \mathrm{C}_t(f_n) \geqslant \tfrac{1}{4}\sqrt{n} \cdot \log_2 n - 1.6 \cdot t \quad \textit{for any } t \geqslant 0.$$

Note. $\log_2 \mathrm{C}_0(h_n^*) \leqslant \frac{1}{3}\sqrt{n} \cdot \log_2 n$.

Comment: Concerning the circuits with no null-chains Pulatov [20] and Kuznetsov [14] have proved that for any Boolean function f it holds that $\mathrm{C}_0(f) \geqslant |f^{-1}(1)|^{d/n}$, where d stands for the Hamming distance between any two distinct vectors from $f^{-1}(1)$. This allows to obtain nearly-exponential lower bounds for some critical Boolean functions. However, if d is too small with respect to $|f^{-1}(1)|$, this argument does not work. For example, if $f = h_n^*$, then $d \leqslant \sqrt{n}$, and so $|f^{-1}(1)|^{d/n} = \mathrm{O}(n)$ (cf. Corollary 6.13).

Example 6.14. Let $n \geqslant 1$ be such that $k = \log_2 n$ and $b = n/k$ are integers. For a (0, 1)-matrix $X = \{x_{i,j} : i \in \bar{k}, j \in \bar{b}\}$, put

$$\mathrm{num}(X) = a_1 + a_2 2 + \cdots + a_k 2^{k-1},$$

where $a_i \in \{0, 1\}$ and $a_i = 1$ iff $x_{i,1} + \cdots + x_{i,b} \geqslant \frac{1}{2}(b-1)$. Let $\hat{f}_n$ denote a Boolean function, defined by $\hat{f}_n(X) = x_{i,j}$, where i, j are such that $(i-1)b + j = \mathrm{num}(X)$. A similar function has been introduced by Meyer and Paterson (as cited in Savage [23]).

Since $\hat{f}_n$ is m-mixed with $m = \frac{1}{2}(b-1)$ see, e.g., [23, p. 44]), we have the following corollary.

Corollary 6.15. *If* $t = \mathrm{o}(n/\log_2 n)$, *then* $\mathrm{BP}_t(\hat{f}_n) \geqslant \exp(n/\log_2 n)$.

Finally, notice that all the functions $\eta\{\mathrm{Per}\}$, $\xi\{\mathrm{Per}\}$, g_n^*, h_n^*, and $\hat{f}_n$ are computable by polynomial-size combinatorial circuits. Moreover, the (unrestricted) branching program complexity of g_n^*, h_n^*, and $\hat{f}_n$ is also polynomial. Therefore, some n-variable Boolean functions require nearly-exponential $n^{1-\varepsilon}$-local circuits (for an arbitrary small constant $\varepsilon > 0$) whereas their n-local circuit complexity is actually polynomial.

Hence, such restrictions as the locality (as well as the monotonicity, the absence of null-chains, constant-depth, etc.) of circuits are too rough to separate complex functions from the simple ones. To achieve this goal, a new insight into the circuit's structure is needed. One of the possible ways is to investigate more subtle notions of "subcircuit" and "similarity" so as to express the specifics of synthesis. We conjecture that (when suitably defined) the number of "highly unsimilar subfunctions" is a lower bound on the standard Boolean circuit complexity.

Acknowledgment

I am greatly indebted to Ju.I. Janov for stimulating discussions about the subject of this paper. I also express sincere appreciations to anonymous referees for their suggestions about the clarity of presentation.

References

[1] M. Ajtai, L. Babai, P. Hajnal, J. Komlós, P. Pudlák, V. Rödl, E. Szemerédi and G. Turán, Two lower bounds for branching programs, in: *Proc. 18th ACM STOC* (1986) 30-38.

[2] R. Aleliunas, R.M. Karp, R. Lipton, L. Lovász and C. Rackoff, Random walks, universal sequences and the complexity of maze problems, in: *Proc. 20th IEEE Symp. on FOCS* (1979) 218-223.

[3] N. Alon and R. Boppana, The monotone circuit complexity of Boolean functions, *Combinatorica*, to appear.

[4] A.E. Andreev, On a method of obtaining lower bounds for the complexity of individual monotone functions, *Dokl. Akad. Nauk SSSR* **282** (1985) 1033-1037 (in Russian).

[5] D.A. Barrington, Bounded-width polynomial size branching programs recognize exactly those languages in NC^1, in: *Proc. 18th ACM STOC* (1986) 1-6.

[6] A. Borodin, D. Dolev, F.E. Fich and W. Paul, Bounds for width two branching programs, *SIAM J. Comput.* **15** (1986) 549-560.

[7] B. Brustmann and I. Wegener, The complexity of symmetric functions in bounded-depth circuits, Internal Rept. 3186, FB Informatik, Univ. of Frankfurt, 1986.

[8] A.K. Chandra, M.L. Furst and R.J. Lipton, Multiparty protocols, in: *Proc. 15th ACM STOC* (1983) 94-99.

[9] P.E. Dunne, Lower bounds on the complexity of 1-time-only branching programs, in: L. Budach, ed., Lecture Notes in Computer Science **199** (Springer, Berlin, 1985) 90-99.

[10] M. Furst, J. Saxe and M. Sipser, Parity, circuits and the polynomial-time hierarchy, in: *Proc. 22nd IEEE Symp. on FOCS* (1981) 260-270.

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

[12] S.P. Jukna, Convolutional characterization of computability and complexity of computations, in: L. Lovász and E. Szemerédi, eds., *Theory of Algorithms* (Pécs, Hungary, 1984), Colloquia Mathematica Societatis Janos Bolyai **44** (North-Holland, Amsterdam, 1985) 251-270.

[13] S.P. Jukna, Lower bounds on the complexity of local circuits, in: J. Gruska, R. Rovan and J. Wiedermann, eds., Lecture Notes in Computer Science **233** (Springer, Berlin, 1986) 440-448.

[14] S.E. Kuznetsov, Combinatorial circuits with no null-chains over the basis {&, v, ¬}, *Izvestija VUZ, Matematika* **5** (1981) 56-63 (in Russian).

[15] J.A. Mamatov, On a principle of obtaining lower bounds on the complexity of formulas, *Dokl. Akad. Nauk SSSR* **245** (1979) 782-784 (in Russian).

[16] E.I. Nechiporuk, On a Boolean function, *Dokl. Akad. Nauk SSSR* **169** (1966) 765-766 (in Russian).

[17] P. Pudlák and S. Žák, Space complexity of computations, Tech. Rept., Univ. of Prague, 1983.

[18] P. Pudlák, A lower bound on the complexity of branching programs, in: M.P. Chytil and V. Koubek, eds., Lecture Notes in Computer Science **176** (Springer, Berlin, 1984) 480-489.

[19] P. Pudlák, The hierarchy of Boolean circuits, Preprint No. 20, Institute of Mathematics, Prague, 1986.

[20] A.K. Pulatov, Lower bounds on the complexity of implementation of characteristic functions of group codes by π-schemes, in: A.A. Markov, ed., *Combinatorial-Algebraic Methods in Applied Mathematics* (Gorki, 1979) 81-95 (in Russian).

[21] A.A. Razborov, A lower bound on the monotone network complexity of the logical permanent, *Mat. Zametki* **37** (1985) 887-900 (in Russian).

[22] A.A. Razborov, Lower bounds on the complexity of bounded-depth circuits in the basis {&, ⊕}, *Uspekhi Mat. Nauk* **41** (1986) 211-220 (in Russian).

[23] J.E. Savage, *The Complexity of Computing* (Wiley, New York, 1976).

[24] G.A. Tkachev, On the complexity of a sequence of Boolean functions by implementing in terms of circuits and π-schemes under additional restrictions on the circuits structure, in: *Combinatorial-Algebraic Methods in Applied Mathematics* (Gorki, 1980) 161-207 (in Russian).

[25] L.G. Valiant, Exponential lower bounds for restricted monotone circuits, in: *Proc. 15th ACM STOC* (1983) 110-117.

[26] I. Wegener, Boolean functions whose monotone complexity is of size $n^2/\log n$, *Theoret. Comput. Sci.* 21 (1982) 213-224.

[27] I. Wegener, On the complexity of branching programs and decision trees for clique functions, Internal Rept. 5/84, FB Informatik, Univ. of Frankfurt, 1984.

[28] A.C. Yao, Lower bounds by probabilistic arguments, in: *Proc. 24th IEEE Symp. on FOCS* (1983) 420-428.

[29] S. Žák, An exponential lower bound for one-time-only branching programs, in: M.P. Chytil and V. Koubek, eds., Lecture Notes in Computer Science 176 (Springer, Berlin, 1984) 562-566.