Electronic Colloquium on Computational Complexity, Report No. 130 (2011)

On a Modification of Lupanov's Method with More Uniform Distribution of Fan-out

Sergei A. Lozhkin, lozhkin@cs.msu.su
Alexander E. Shiganov, alexander.shiganov@gmail.com
Lomonosov Moscow State University[1]
MGU, Vorobjovy Gory, Moscow, 119899, Russia

Abstract

In this paper we suggest a modification of classical Lupanov's method [8] that allows building circuits over the basis $\{\&, \vee, \neg\}$ for Boolean functions of n variables with size at most

$$\frac{2^n}{n}\left(1+\frac{3\log n+O(1)}{n}\right),$$

and with more uniform distribution of outgoing arcs by circuit gates.

For almost all Boolean functions of n variables in the circuits for these functions, which are built using our method, the fraction of gates with fan-out 2 is asymptotically at least 1/32. This fact disproves upper bound [15] on the number of circuits with exact number of gates with fan-out at least 2.

1 Introduction

Boolean circuit model is one of the most studied computational models in complexity theory (see [14]). There are various families of Boolean circuits, such as: circuits and formulas over a finite complete basis, contact or relay-contact circuits, branching programs or binary-decision diagrams (BDD), etc. The (weighted) number of gates in a circuit is called its *complexity*. *The complexity of a Boolean function* f is the smallest (weighted) number of gates in a Boolean circuit computing f.

Asymptotic approach in studying circuit complexity is concerned with the complexity of almost all Boolean functions and the complexity of the hardest Boolean function of n variables, when n tends to infinity. Fundamental concepts of this approach have been introduced by Shannon [12], and the complexity of the hardest single-output n-variable Boolean function is usually called *Shannon function*. The main purpose of the asymptotic approach is to obtain and to improve lower and upper bounds on Shannon functions for different classes of Boolean circuits. Upper bounds for Shannon functions are usually based on constructive methods for circuit synthesis while the lower bounds are usually proved via Shannon's counting argument [12]. In [7] we reviewed the history of improvements of bounds on a Shannon function for several families of Boolean circuits including high accuracy asymptotic bounds [3–6]. The latter stand for such upper and lower bounds on a function, depending on natural n and having form $2^n/\psi(n)$, where[2] $\psi(n)=o(2^n)$ and $\psi^{-1}(n)=o(1)$, that differ by at most $O(2^n/\psi^2(n))$.

This article is devoted to the synthesis of the hardest Boolean functions by circuits with certain restrictions related to the uniformity of the distribution of outgoing arcs by circuit's gates. The degree of the uniformity of this distribution plays specific role in the model of circuit embedded into a lattice [2, 13]. We shall also review previous results for circuits with restrictions on the fan-out of gates.

[1]The research was supported by Russian Foundation for Basic Research, project 09-01-00817-a.

[2]We refer the reader to [14] for O, o and Ω notations.

ISSN 1433-8092

In this paper we consider the class $\mathbb{C}$ of circuits over the basis $\{\&, \vee, \neg\}$. The *complexity* or *size* of a circuit is the number of gates in it. Let $L(n)$ be the Shannon function for the studied class. In [11] via a counting argument and Lupanov's method [8] the following asymptotically equal bounds were proved[3]:

$$\frac{2^n}{n}\left(1+\frac{\log n - O(1)}{n}\right) \leqslant L(n) \leqslant \frac{2^n}{n}\left(1+\frac{3\log n + O(1)}{n}\right). \tag{1}$$

The upper and lower bounds (1) are also mentioned in [1], where a simplified proof of the lower bound is given. We shall also repeat the proof of the bounds (1) in Sections 2 and 3 of this paper. In [6] the upper bound on $L(n)$ was improved to:

$$L(n) \leqslant \frac{2^n}{n}\left(1+\frac{\log n + \log\log n + O(1)}{n}\right) \tag{2}$$

giving together with the lower bound (1) the bounds close to high accuracy asymptotic bounds on $L(n)$.

In several papers the subclasses of $\mathbb{C}$ with the restrictions on the fan-out of circuits' gates were considered. For $i = 1, 2, \ldots$ let $\mathbb{C}^{(i)}$ be the class of circuits whose gates have fan-out at most i and $L^{(i)}(n)$ be Shannon function for $\mathbb{C}^{(i)}$. Note that $\mathbb{C}^{(1)}$ is the class of formulae over the basis $\{\&, \vee, \neg\}$. The asymptotically equal bounds on $L^{(1)}(n)$ were obtained in [9]:

$$\frac{2^n}{\log n}\left(1-O\left(\frac{1}{\log n}\right)\right) \leqslant L^{(1)}(n) \leqslant \frac{2^n}{\log n}\left(1+\frac{2\log\log n + O(1)}{\log n}\right). \tag{3}$$

The upper bound on $L^{(1)}(n)$ was improved in [4, 5]:

$$L^{(1)}(n) \leqslant \frac{2^n}{\log n}\left(1+O\left(\frac{1}{\log n}\right)\right), \tag{4}$$

thus giving together with the lower bound (3) high accuracy asymptotic bounds on $L^{(1)}(n)$.

Lupanov [10] proved the following upper bound on $L^{(2)}(n)$:

$$L^{(2)}(n) \leqslant \frac{2^n}{n}\left(1+O\left(\frac{1}{\sqrt{n}}\right)\right). \tag{5}$$

A subclass $\mathbb{C}^{(1)}_{\&,\vee}$ of $\mathbb{C}$ was introduced in [5]. Class $\mathbb{C}^{(1)}_{\&,\vee}$ consists of circuits where only inputs and the inverter gates, i.e., gates labelled "$\neg$", can have more than 1 outgoing arc. For the corresponding Shannon function $L^{(1)}_{\&,\vee}(n)$ high accuracy asymptotic bounds were obtained [5]:

$$L^{(1)}_{\&,\vee}(n) = \frac{2^n}{n}\left(1+\frac{2\log n \pm O(1)}{n}\right). \tag{6}$$

The set of circuits $\tilde{\mathbb{C}} \subseteq \mathbb{C}$ is called an *asymptotically optimal family* if for any function f it contains the only circuit which implements f, and $\tilde{L}(n) = \frac{2^n}{n}(1+o(1))$, where $\tilde{L}(n)$ is Shannon function with respect to $\tilde{\mathbb{C}}$. Via a counting argument it follows that almost all n-input circuits from an asymptotically optimal family have complexity at least $\frac{2^n}{n}(1+o(1))$, while the number of outgoing arcs from circuit's

[3]We use the abbreviation log for $\log_2$.

inputs and inverters is $o(2^n/n)$ (see Section 2 of this paper). Note that the synthesis methods, which give upper bounds (1), (2) and (5), (6), produce asymptotically optimal families contained in the corresponding classes $\mathbb{C}$ and $\mathbb{C}^{(2)}$, $\mathbb{C}^{(1)}_{\&,\vee}$. We analyze these families in terms of uniformity of the distribution of outgoing arcs by circuit's gates.

One can easily see that the total number of arcs in a circuit $\mathcal{S}$ of size L with L' inverters equals $2L-L'-1$, thus the average fan-out in $\mathcal{S}$, i.e., the average number of arcs, outgoing from the gates, is $(2L-L'-R'-1)/L \leqslant 2$, where R' is the number of arcs outgoing from the inputs of $\mathcal{S}$. Note that the expression for the average degree tends to 2 if $(L'+R')/L$ tends to 0, and this condition is fulfilled for almost all n-input circuits from any asymptotically optimal family. Therefore, the greater number of gates with fan-out 2, the more uniform the distribution of outgoing arcs by all gates.

Note that the circuits built by Lupanov's method [8] as well as the circuits from $\mathbb{C}^{(1)}_{\&,\vee}$ built by method [5] with size fulfilling the upper bound (1) and (6) respectively, have rather nonuniform distribution of outgoing arcs by gates. Indeed, in these n-input circuits only $O(2^n/n^2)$ gates have "branching" output (i.e., fan-out at least 2) and average fan-out of these gates is $\Omega(n)$. As concerns the n-input circuits built by method [6] with size satisfying the bound (2), they have $O\left(\frac{2^n}{n\log n}\right)$ gates with branching output while average degree of their fan-out is $\Omega(\log n)$. The synthesis method [10] produces a family of circuits with more uniform distribution of outgoing arcs. In these circuits there are $o(2^n/n)$ gates with fan-out 1 while the rest of the gates have fan-out 2. However [10] gives a higher bound (5) on the corresponding Shannon function as compared to the previously mentioned methods.

In this paper we describe a rather simple modification of Lupanov's method [8], which produces a family of circuits with size satisfying the upper bound (1) and which at the same time have more uniform distribution of outgoing arcs by circuit's gates. In particular, for almost all n-input circuits in this family the fraction of gates with fan-out 2 is asymptotically at least 1/32.

Note that our results as well as [6,10] disprove the bounds [15]. Indeed, Lemma 3.1 in [15] states

$$|\hat{\mathbb{C}}(n,L,T)| \leqslant \frac{2^{L\log(T+n)+O(L)}}{T!}, \tag{7}$$

where $\hat{\mathbb{C}}(n,L,T)$ is the set of circuits with fan-in of gates at most two, which have n inputs, size L and exactly T gates of fan-out at least 2. Based on (7) in [15] the lower bound obtained

$$L(n) \geqslant \frac{2^n}{n}\left(1+\frac{2\log n - O(1)}{n}\right),$$

which contradicts the upper bound (2).

On the other hand, via a counting argument and (7) it follows (see Section 2 of this paper) that for any $\delta \in (0,1)$ the class of circuits having fraction of gates with branching output at least δ cannot contain asymptotically optimal family. This contradicts (5) and the results of the present paper giving one more disproof of claims [15].

2 Basic definitions and supplementary results

By B_n we denote the set of all Boolean functions $f : \{0,1\}^n \to \{0,1\}$ of the variables $x_1,\ldots,x_n$. We use the lexicographical order on $\{0,1\}^n$ and the corresponding

numeration $\nu : \{0,1\}^n \to [0, 2^n)$, where

$$\nu(\alpha_1, \ldots, \alpha_n) = \alpha_1 2^{n-1} + \alpha_2 2^{n-2} + \cdots + \alpha_n 2^0.$$

A circuit $\mathcal{S}$ over the basis $\{\&, \vee, \neg\}$ with input variables $(x_1, \ldots, x_n)$ and output variables $(y_1, \ldots, y_m)$ is a directed acyclic graph, which has n sources labeled by distinct input variables, other nodes (gates) have fan-in either 1 or 2 and are labeled either by "$\neg$" (fan-in 1) or by "&" or "$\vee$" (fan-in 2). For $i = 1, \ldots, m$ the output variable y_i is assigned to one of the vertices of $\mathcal{S}$.

Let v be a vertex of $\mathcal{S}$. *The function f_v implemented (computed) in v* is defined inductively by the depth of v. If v has depth 0 and label x_i, then $f_v = x_i$. Next, if v has incoming arcs from vertices $v_1, \ldots, v_k$ implementing $f_{v_1}, \ldots, f_{v_k}$, then $f_v = \neg f_{v_1}$ if $k = 1$ and $f_v = f_{v_1} \circ f_{v_2}$ if $k = 2$, where "$\circ$" is a label of v.

The circuit $\mathcal{S}$ with m outputs *implements (computes)* vector $(f_1, \ldots, f_m)$ where f_i is a function implemented at i-th output, $i = 1, \ldots, m$.

The complexity or *size* $L(\mathcal{S})$ of the circuit $\mathcal{S}$ is the number of gates in $\mathcal{S}$. For a Boolean function f (a set of Boolean functions G) $L(f)$ (resp. $L(G)$) is the smallest size of a circuit $\mathcal{S}$ over the basis $\{\&, \vee, \neg\}$ computing f (resp. computing the vector of all functions from G). Shannon function $L(n)$ is defined as usual:

$$L(n) = \max_{f \in B_n} L(f).$$

We denote $x^0 = \overline{x}$, $x^1 = x$. By $\mu_n(x_1, \ldots, x_n, y_0, \ldots, y_{2^n-1})$ we denote the storage access function, i.e.,

$$\mu_n = \bigvee_{(\sigma_1, \ldots, \sigma_n) \in \{0,1\}^n} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} y_{\nu(\sigma_1, \ldots, \sigma_n)},$$

where $x_1, \ldots, x_n$ are called the *address variables* and $y_0, \ldots, y_{2^n-1}$ are called the *information variables*.

Lemma 1. *For $n = 1, 2, \ldots$ there exists a circuit S_n implementing μ_n, such that*

$$L(S_n) \leqslant 2^{n+2}. \tag{8}$$

Proof. The following formula $\mathcal{F}_n(x_1, \ldots, x_n, y_0, \ldots, y_{2^n-1})$ implements μ_n:

$$\mathcal{F}_n = \bigvee_{\sigma_1 \in \{0,1\}} x_1^{\sigma_1} \left(\bigvee_{\sigma_2 \in \{0,1\}} x_2^{\sigma_2} \left(\cdots \left(\bigvee_{\sigma_n \in \{0,1\}} x_n^{\sigma_n} y_{\nu(\sigma_1, \ldots, \sigma_n)} \right) \cdots \right) \right).$$

It is easy to see that $\mathcal{F}_n$ has $(2^n - 1)$ symbols "$\vee$", $(2^n - 1)$ symbols "$\neg$" and $2(2^n - 1)$ symbols "&". The circuit S_n implements the formula $\mathcal{F}_n$ and has size at most 2^{n+2}. □

Using Shannon's expansion for Boolean function $f(x_1, \ldots, x_n)$ with respect to the variables $x'' = (x_{m+1}, \ldots, x_n)$, where $0 < m < n$, one can obtain the following representation for f:

$$f(x', x'') = \mu_n(x'', f_{\tilde{0}}(x'), \ldots, f_{\tilde{1}}(x')), \tag{9}$$

where $x' = (x_1, \ldots, x_m)$ and $f_{\sigma''}(x') = f(x', \sigma'')$, $\sigma'' \in \{0,1\}^{n-m}$.

Lemma 2. *For any Boolean function $f \in B_n$ there exists a circuit $\mathcal{S}_f$ of size at most $3(2^n - 1)$ implementing f.*

Proof. If $f \equiv 0$ then for the circuit $\mathcal{S}_f$ we take the formula $x_1 \cdot \overline{x}_1$. If $f \not\equiv 0$, the following equality holds

$$f = \mu_n(x_1, \ldots, x_n, f(\tilde{0}), \ldots, f(\tilde{1})).$$

For the circuit $\mathcal{S}_f$ we take the circuit implementing the formula $\mathcal{F}'_n$ which is obtained from the formula $\mathcal{F}_n$ (see Lemma 1) after substituting 0 and 1 in place of information variables of μ_n and appropriate reduction of the expression. Note that $\mathcal{F}'_n$ has at most $(2^n - 1)$ symbols "$\vee$", at most $(2^n - 1)$ symbols "$\neg$" and at most $(2^n - 2)$ symbols "&", therefore, $L(\mathcal{S}_f) \leqslant 3(2^n - 1)$. □

Lemma 3. *For natural numbers s and r, $2 \leqslant s \leqslant (r-2)$, the fraction δ of Boolean matrices M with s rows and 2^r columns, such that there exists a set $V \subseteq \{0,1\}^s$, $|V| \geqslant 2^{s-2}$, and each tuple from V occurs as a column of M at least once and at most 2^{r-s-2} times, satisfies the inequality*

$$\delta \leqslant 2^{r+2^s+\gamma 2^r},$$

where $\gamma = \log 3 - \frac{7}{4} < 0$.

Proof. In order to specify the matrix M, it suffices to

1. choose a set $\hat{V}$ of 2^{s-2} tuples from $\{0,1\}^s$;
2. choose $i \in [2^{s-2}, 2^{r-4}]$ and a set I of i elements from $[1, 2^r]$, that will specify the numbers of columns in M, which are picked from $\hat{V}$;
3. for every $j = 1, \ldots, 2^r$ choose the tuple from $\{0,1\}^s$ as the j-th column of M which belongs to $\hat{V}$ ($\{0,1\}^s \backslash \hat{V}$) if $j \in I$ (resp. $j \notin I$).

Note that the set $\hat{V}$ can be chosen in $\binom{2^s}{2^{s-2}}$ different ways. For any i from $[2^{s-2}, 2^{r-4}]$ set I with i elements can be chosen in $\binom{2^r}{i}$ different ways. Columns of M indexed with the elements from I can be chosen in $(2^{s-2})^i$ different ways and the rest of the columns can be chosen in $(2^s - 2^{s-2})^{2^r - i}$ different ways. Therefore, the fraction δ satisfies the inequality:

$$\delta 2^{s2^r} \leqslant \binom{2^s}{2^{s-2}} \sum_{i=2^{s-2}}^{2^{r-4}} \binom{2^r}{i} (2^{s-2})^i (2^s - 2^{s-2})^{2^r - i},$$

$$\delta \leqslant \binom{2^s}{2^{s-2}} 2^{-2^{r+1}} 3^{2^r} \sum_{i=2^{s-2}}^{2^{r-4}} \binom{2^r}{i} 3^{-i}.$$

Since the product under the sum sign increases with i on the segment $[2^{s-2}, 2^{r-4}]$,

$$\delta \leqslant \binom{2^s}{2^{s-2}} 2^{-2^{r+1}} 3^{2^r} 2^{r-4} \binom{2^r}{2^{r-4}} 3^{-2^{r-4}}.$$

From the last inequality and taking into account that $\binom{v}{u} \leqslant 2^v$ and $\binom{v}{u} \leqslant (3v/u)^u$ we obtain the desired bound:

$$\delta \leqslant 2^{2^s - 2^{r+1} + 2^r \log 3 + r} (3 \cdot 16)^{2^{r-4}} 3^{-2^{r-4}} \leqslant 2^{r + 2^s + \left(\log 3 - \frac{7}{4}\right) 2^r}.$$

□

In this section we shall also prove the properties of asymptotically optimal families of circuits, which were mentioned in the Introduction.

For the set $\tilde{\mathbb{C}} \subseteq \mathbb{C}$ and natural number n let $\tilde{\mathbb{C}}(n)$ denote the set of circuits $\mathcal{S} \in \tilde{\mathbb{C}}$ which have the single output and n inputs $x_1, \ldots, x_n$. For the circuit $\mathcal{S} \in \mathbb{C}$ we define

- $l(\mathcal{S})$ – the number of circuit's inverters;
- $R(\mathcal{S})$ – the number of the arcs outgoing from circuit's inputs;
- $T(\mathcal{S})$ – the number of circuit's gates with branching output;
- $t(\mathcal{S})$ – the number of the circuit's gates with fan-out 2.

Note that

$$l(\mathcal{S}) \leqslant L(\mathcal{S}), \quad t(\mathcal{S}) \leqslant T(\mathcal{S}) \leqslant L(\mathcal{S}),$$

and via induction on $L(\mathcal{S})$ one can show that

$$R(\mathcal{S}) + l(\mathcal{S}) - 1 \leqslant L(\mathcal{S}). \tag{10}$$

In the Appendix A we prove that for any positive real numbers a, b, n, u such that

$$a \geqslant b, \ n \geqslant 1, \ u \leqslant \frac{2^n}{b\left(n - \log n + \log\left(\frac{2a}{b}\right)\right)}, \tag{11}$$

the inequality holds

$$\log((au)^{bu}) \leqslant 2^n \left(1 - \frac{1}{12\left(n + \log\left(\frac{a}{b}\right)\right)}\right). \tag{12}$$

Two circuits are *equivalent* if they implement equal vectors of functions. The following statement is proved in the Appendix B.

Lemma 4. *The number of non-equivalent circuits $\mathcal{S} \in \mathbb{C}(n)$ such that $L(\mathcal{S}) \leqslant L$, $R(\mathcal{S}) \geqslant R$ and $l(\mathcal{S}) \geqslant l$, where $R+l \leqslant L+1$, is not greater than $(16n)^{R+l}(16(L+n))^{L-R-l+1}$.*

It follows from Lemma 4 for $R = l = 0$ and inequalities (11) and (12) for $a = 16$, $b = 1$, $u = \lambda(n) + n$, where

$$\lambda(n) = \frac{2^n}{n - \log n + 5} - n = \frac{2^n}{n}\left(1 + \frac{\log n - 5 + o(1)}{n}\right),$$

that the number of circuits $\mathcal{S} \in \tilde{\mathbb{C}}(n)$ such that $L(\mathcal{S}) \leqslant \lambda(n)$ is at most $o(2^{2^n})$. Therefore,

$$L(n) \geqslant \lambda(n) \text{ and } L(f) \geqslant \lambda(n)$$

for almost all functions $f \in B_n$.

Lemma 5. *For any asymptotically optimal family $\tilde{\mathbb{C}} \subseteq \mathbb{C}$ its Shannon function $\tilde{L}(n)$ can be represented as*

$$\tilde{L}(n) = \frac{2^n}{n+10}(1 + \varepsilon(n)) - n, \tag{13}$$

where $\varepsilon(n) > 0$ and $\varepsilon(n)$ tends to 0 when n tends to infinity, and the inequality

$$R(\mathcal{S}) + l(\mathcal{S}) \leqslant \varepsilon(n)\tilde{L}(n)$$

is fulfilled for almost all circuits $\mathcal{S} \in \tilde{\mathbb{C}}(n)$.

Proof. It follows from asymptotic optimality of $\tilde{\mathbb{C}}$ that (13) holds for some sequence $\varepsilon(n)$ which tends to 0 when n tends to infinity. For any natural number n

$$\tilde{L}(n) \geqslant L(n) \geqslant \lambda(n) > \frac{2^n}{n+10} - n,$$

therefore $\varepsilon(n) > 0$.

For real $\delta \in \left(0, \frac{1}{2}\right]$ consider the set $\tilde{\mathbb{C}}_\delta(n)$ which consists of the circuits $\mathcal{S} \in \tilde{\mathbb{C}}(n)$ such that $R(\mathcal{S}) + l(\mathcal{S}) \geqslant \delta\tilde{L}(n)$. From (10) and Lemma 4 we obtain the inequality

$$\begin{aligned}\left|\tilde{\mathbb{C}}_\delta(n)\right| &\leqslant \tilde{L}^2(n) \max_{\delta\tilde{L}(n)\leqslant R+l\leqslant\tilde{L}(n)+1} (16n)^{R+l}(16(\tilde{L}(n)+n))^{\tilde{L}(n)-R-l+1} \\ &\leqslant \tilde{L}^2(n)(16n)^{\delta\tilde{L}(n)}\left(16(\tilde{L}(n)+n)\right)^{(1-\delta)\tilde{L}(n)} \leqslant \left(256n(\tilde{L}(n)+n)\right)^{(1-\delta)(\tilde{L}(n)+4)}.\end{aligned}$$

Note that if

$$a = 256n,\ b = (1-\delta),\ u = \tilde{L}(n)+n,\ \delta = \delta(n) = \min\left\{\varepsilon(n), \tfrac{1}{2}\right\},$$

the conditions (11) are satisfied for sufficiently large n. Therefore, via (12) we obtain $\left|\tilde{\mathbb{C}}_{\delta(n)}(n)\right| = o(2^{2^n})$, i.e., for almost all circuits $\mathcal{S} \in \tilde{\mathbb{C}}(n)$

$$R(\mathcal{S}) + l(\mathcal{S}) \leqslant \varepsilon(n)\tilde{L}(n).$$

The lemma is proved. □

Note that in the conditions of Lemma 5 it follows from the bound (7) that $T(\mathcal{S}) \leqslant \varepsilon(n)\tilde{L}(n)$ for almost all circuits $\mathcal{S} \in \tilde{\mathbb{C}}(n)$. This fact contradicts with the results [10] and Theorem 1 from Section 3 of this paper.

Indeed, for $\delta \in \left(0, \frac{1}{2}\right]$ let the set $\tilde{\mathbb{C}}'_\delta(n)$ consist of the circuits $\mathcal{S} \in \tilde{\mathbb{C}}(n)$ such that $T(\mathcal{S}) \geqslant \delta\tilde{L}(n)$. Via (7) and $u! \geqslant \left(\frac{u}{3}\right)^u$, $\left(\frac{1}{\delta}\right)^\delta \leqslant 3$, $\tilde{L}(n) \geqslant n$ we obtain

$$\begin{aligned}\left|\tilde{\mathbb{C}}'_\delta(n)\right| &\leqslant \left|\bigcup_{\delta\tilde{L}(n)\leqslant T\leqslant L\leqslant\tilde{L}(n)} \hat{\mathbb{C}}(n, L, T)\right| \leqslant \frac{\tilde{L}^2(n)\left(c(\tilde{L}(n)+n)\right)^{\tilde{L}(n)}}{\left(\delta\tilde{L}(n)\right)!} \\ &\leqslant \tilde{L}^2(n)\left(\frac{3c(\tilde{L}(n)+n)}{\delta\tilde{L}(n)}\right)^{\delta\tilde{L}(n)}\left(c(\tilde{L}(n)+n)\right)^{(1-\delta)\tilde{L}(n)} \\ &\leqslant \left(\left(\frac{6c}{\delta}\right)^{\frac{\delta}{1-\delta}} c(\tilde{L}(n)+n)\right)^{(1-\delta)(\tilde{L}(n)+4)} \leqslant \left(c'(\tilde{L}(n)+n)\right)^{(1-\delta)(\tilde{L}(n)+4)},\end{aligned}$$

where c and c' are some constants. Next, by setting $\delta = \delta(n) = \min\left\{\varepsilon(n), \frac{1}{2}\right\}$ and by repeating the reasoning used in the proof of Lemma 5, we obtain $\left|\tilde{\mathbb{C}}'_{\delta(n)}(n)\right| = o(2^{2^n})$. Thus, $T(\mathcal{S}) \leqslant \varepsilon(n)\tilde{L}(n)$ for almost all circuits $\mathcal{S} \in \tilde{\mathbb{C}}(n)$.

3 Modification of Lupanov's method and estimation of the number of gates with fan-out 2

Let m and s be natural numbers, $s \leqslant 2^m$ and $p = \lceil 2^m/s \rceil$. A partition $\mathcal{I} = (I_1, \ldots, I_p)$ of $\{0,1\}^m$ is called a *standard partition of height* s, if $|I_1| = \ldots = |I_{p-1}| = s$, $|I_p| \leqslant s$ and[4] $\nu^{-1}(I_1), \ldots, \nu^{-1}(I_p)$ are consecutive segments.

[4]For $A \subseteq \{0,1\}^m$, $\nu^{-1}(A) = \bigcup_{\alpha\in A} \nu^{-1}(\alpha)$.

A set of Boolean functions $G \subseteq B_m$ is called *a universal set of order m and rank p*, if for each $g \in B_m$ there exist such $g_1, \ldots, g_p$ from G that

$$g = g_1 \vee \ldots \vee g_p. \tag{14}$$

Let s and m be natural numbers, $s \leqslant 2^m$, $p = \lceil 2^m/s \rceil$ and $\mathcal{I} = (I_1, \ldots, I_p)$ be a standard partition of height s of $\{0,1\}^m$. A universal set G of order m and rank p is called a *standard universal set of order m and height s* if it can be represented in the form:

$$G = G^{(1)} \cup \cdots \cup G^{(p)},$$

where for $i = 1, \ldots, p$ the set $G^{(i)}$ consists of all functions which equal 0 on any tuple lying outside I_i.

Lemma 6. *Let G be a standard universal set of order m and height $s \leqslant 2^m$. Then there exists a circuit $\mathcal{S}_G$ implementing G such that*

$$L(\mathcal{S}_G) \leqslant 6\lceil 2^m/s \rceil (2^s + 2^{m+s/2}). \tag{15}$$

Proof. Let $p = \lceil 2^m/s \rceil$ and $\mathcal{I} = (I_1, \ldots, I_p)$ be a standard partition of height s of $\{0,1\}^m$. By definition, G is represented in the form

$$G = G^{(1)} \cup \cdots \cup G^{(p)},$$

where for $i = 1, \ldots, p$ the functions in $G^{(i)}$ equal 0 on any tuple lying outside I_i. For $\sigma \in \{0,1\}$ and $i \in [1,p]$ let $G^{(i)}_\sigma$ contain all non-constant functions $g(x_1, \ldots, x_{m-1}, \sigma)$, where $g \in G^{(i)}$. It easy to see that for $i = 1, \ldots, p$:

$$|G^{(i)}| \leqslant 2^s, \quad |G^{(i)}_0 \cup G^{(i)}_1| \leqslant 2^{(s+3)/2}.$$

Note that any function g from $G^{(i)}$ can be represented by one of the formulae:

$$g = \overline{x}_m g_0 \vee x_m g_1 \text{ or } g = x^\sigma_m g_\sigma \text{ or } g = x_m \& \overline{x}_m,$$

where $g_\sigma \in G^{(i)}_\sigma$. By Lemma 2 each function in $G^{(i)}_0 \cup G^{(i)}_1$ can be implemented by a circuit with at most $3(2^{m-1} - 1)$ gates. Each function $g \in G^{(i)}$ we implement using at most 3 gates whose inputs are connected to the input node x_m or to the output of the circuit implementing $\overline{x}_m$ or to the output of the circuit for g_σ. We use this approach for $i = 1, \ldots, p$ and finally obtain the circuit $\mathcal{S}_G$ implementing G such that

$$L(\mathcal{S}_G) \leqslant 3p\,2^s + 3p(2^{m-1} - 1)2^{(s+3)/2} + 1 \leqslant 6p(2^s + 2^{m+s/2}).$$

The lemma is proved. □

We remind that in order to build circuit $\mathcal{S}_f$ implementing a Boolean function $f(x_1, \ldots, x_n)$ by Lupanov's method [8] one should choose natural numbers m and s, such that $m < n$, $s \leqslant 2^m$, and then use the representation (9) in which every $f_{\sigma''}(x')$, $\sigma'' \in \{0,1\}^{n-m}$, is implemented via (14) for a standard universal set G of order m and height s. By choosing m and s such that

$$m = \lceil 2 \log n \rceil \text{ and } s = \lceil n - 3 \log n \rceil,$$

and using Lemmas 1 and 6 we obtain the following statement.

Lemma 7. *For any Boolean function $f(x_1,\dots,x_n)$ there exists a circuit $\mathcal{S}_f$ implementing f such that*

$$L(\mathcal{S}_f) \leqslant \frac{2^n}{n}\left(1+\frac{3\log n+O(1)}{n}\right), \quad T(\mathcal{S}_f)=O\left(\frac{2^n}{n^2}\right).$$

The next theorem is the main result of the present paper.

Theorem 1. *For any Boolean function $f(x_1,\dots,x_n)$ there exists a circuit $\mathcal{S}_f$ implementing f such that*

$$L(\mathcal{S}_f) \leqslant \frac{2^n}{n}\left(1+\frac{3\log n+O(1)}{n}\right),$$

and for sufficiently large n, for almost all f from B_n,

$$t(\mathcal{S}_f) \geqslant 2^{n-5}/n.$$

Proof. As in Lupanov's method [8] we choose natural numbers m and s, such that $m<n$ and $s\leqslant 2^m$. Then we split the variables $x=(x_1,\dots,x_n)$ into two groups: $x'=(x_1,\dots,x_m)$ and $x''=(x_{m+1},\dots,x_n)$. Next, we denote $p=\lceil 2^m/s\rceil$ and take a standard universal set $G=G^{(1)}\cup\dots\cup G^{(p)}$ of order m and height s. Let the functions in G depend on x'. Recall that for $i=1,\dots,p$ the functions in $G^{(i)}$ equal 0 on the tuples lying outside I_i, where $(I_1,\dots,I_p)$ is a standard partition of $\{0,1\}^m$ of height s. For convenience we assume that for $i=1,\dots,p$ set $G^{(i)}$ contains the constant function 0.

Based on (14) and (9) we represent $f(x',x'')$ in the following way:

$$f(x',x'')=\bigvee_{\sigma''=(\sigma_{m+1},\dots,\sigma_n)\in\{0,1\}^{n-m}} x_{m+1}^{\sigma_{m+1}}\cdots x_n^{\sigma_n}(g^{(1)}_{\sigma''}\vee\dots\vee g^{(p)}_{\sigma''}), \tag{16}$$

where for each $\sigma''\in\{0,1\}^{n-m}$ and $i=1,\dots,p$ the function $g^{(i)}_{\sigma''}$ belongs to $G^{(i)}$ and coincides with $f_{\sigma''}(x')$ on the tuples from I_i.

Let A^n_α denote the set $\{(\alpha,\alpha_2,\dots,\alpha_n)\in\{0,1\}^n\}$. For $\alpha=0,1$ and $g\in G^{(i)}$ let $D_\alpha(g)$ be the set of tuples σ'' from A^{n-m}_α for which $g=g^{(i)}_{\sigma''}$. Let $d=\lfloor p/2\rfloor$. For each $\sigma''\in\{0,1\}^{n-m}$ and $i=1,\dots,d$ we introduce the function $h^{(i)}_{\sigma''}(x',x_{m+1})$ which equals

1. function $g^{(i)}_{\sigma''}\vee\overline{x}_{m+1}g^{(i+d)}_{\sigma''}$ if $\sigma''\in A^{n-m}_0$;
2. function $g^{(i)}_{\sigma''}\vee g^{(i+d)}_{\sigma''}$ if $\sigma''\in A^{n-m}_1$ and the number[5] of the tuple σ'' in the set $D_1(g^{(i)}_{\sigma''})$ is greater than $|D_0(g^{(i)}_{\sigma''})|$;
3. function $h^{(i)}_{\beta_{\sigma''}}\vee g^{(i+d)}_{\sigma''}$, in all other cases, where $\beta_{\sigma''}\in D_0(g^{(i)}_{\sigma''})$ and its number in this set equals the number of the tuple σ'' in the set $D_1(g^{(i)}_{\sigma''})$.

Note that for any $\sigma''=(\sigma''_{m+1},\dots,\sigma''_n)\in\{0,1\}^{n-m}$ and $i\in[1,d]$:

$$h^{(i)}_{\sigma''}(x',\sigma''_{m+1})=g^{(i)}_{\sigma''}(x')\vee g^{(i+d)}_{\sigma''}(x'). \tag{17}$$

Let $i\in[1,d]$. It follows from the definition that for $\beta\in A^{n-m}_0$ the function $h^{(i)}_\beta$ occurs in item 3 in at most one definition of some $h^{(i)}_{\sigma''}$, $\sigma''\in\{0,1\}^{n-m}$. Let $q^{(i)}$ be the number of tuples $\beta\in A^{n-m}_0$ for which that happens. Note that

$$q^{(i)}=\sum_{g\in G^{(i)}}\min\{|D_0(g)|,|D_1(g)|\}. \tag{18}$$

[5]We assume that tuples from the set $S\subseteq\{0,1\}^n$ are numbered in it from 1 to $|S|$ according to lexicographical ordering.

From (16) and (17) we obtain:

$$f(x',x'') = \bigvee_{\sigma''=(\sigma_{m+1},\ldots,\sigma_n)\in\{0,1\}^{n-m}} x_{m+1}^{\sigma_{m+1}}\cdots x_n^{\sigma_n}(h^{(1)}_{\sigma''}\vee\cdots\vee h^{(d)}_{\sigma''}\vee h^{(0)}_{\sigma''}), \tag{19}$$

where $h^{(0)}_{\sigma''} = g^{(p)}_{\sigma''}$ if p is odd and $h^{(0)}_{\sigma''}\equiv 0$ otherwise.

The circuit $\mathcal{S}_f$ is built according to (19). It consists of subcircuits $\mathcal{S}_1,\ldots,\mathcal{S}_5$ of the following structure:

1. $\mathcal{S}_1$ has inputs x' and implements functions from G by Lemma 6;
2. $\mathcal{S}_2$ implements functions $\overline{x}_{m+1}g$, where $g\in G^{(d+1)}\cup\cdots\cup G^{(2d)}$, using the outputs of $\mathcal{S}_1$;
3. $\mathcal{S}_3$ implements for each $\sigma''\in\{0,1\}^{n-m}$ and for each $i\in[1,d]$ the functions $h^{(i)}_{\sigma''}$ according to their definitions using the outputs of $\mathcal{S}_1$ and $\mathcal{S}_2$;
4. $\mathcal{S}_4$ implements for each $\sigma''\in\{0,1\}^{n-m}$ the "internal" disjunction

   $$h^{(1)}_{\sigma''}\vee\cdots\vee h^{(d)}_{\sigma''}\vee h^{(0)}_{\sigma''}$$

   from (19) using the outputs of $\mathcal{S}_3$ (and also $\mathcal{S}_1$ in case when p is odd);
5. $\mathcal{S}_5$ is built by Lemma 1 and implements the storage access function μ_{n-m} of the address variables x'' and the information variables, connected to the corresponding outputs of $\mathcal{S}_4$ according to (19).

The output of $\mathcal{S}_5$ is the output of the circuit $\mathcal{S}_f$.

From the construction of $\mathcal{S}_f$ and Lemmas 1, 6 we obtain:

$$L(\mathcal{S}_f) = L(\mathcal{S}_1)+\ldots+L(\mathcal{S}_5),$$

$$L(\mathcal{S}_1)\leqslant 6p(2^s+2^{m+s/2}),\quad L(\mathcal{S}_2)\leqslant p\,2^s+1,$$

$$L(\mathcal{S}_3)\leqslant d\,2^{n-m},\quad L(\mathcal{S}_4)\leqslant d\,2^{n-m},\quad L(\mathcal{S}_5)\leqslant 2^{n-m+2}.$$

Setting

$$m=\lceil 2\log n\rceil \text{ and } s=\lceil n-3\log n\rceil, \tag{20}$$

we obtain the claimed upper bound on the size of the circuit $\mathcal{S}_f$:

$$L(\mathcal{S}_f)\leqslant\frac{2^n}{n}\left(1+\frac{3\log n+O(1)}{n}\right).$$

In order to get the lower bound on $t(\mathcal{S}_f)$ note that according to (18)

$$t(\mathcal{S}_f)\geqslant\sum_{i=1}^{d}q^{(i)}=\sum_{i=1}^{d}\sum_{g\in G^{(i)}}\min\{|D_0(g)|,|D_1(g)|\} \tag{21}$$

Consider for every $i\in[1,d]$ and for every $\alpha\in\{0,1\}$ the matrix $M^{(i)}_\alpha$ with s rows and 2^{n-m-1} columns, whose j-th column is the column of values of $g^{(i)}_{\sigma''}$ on the tuples of I_i, where $\nu(\sigma'')=j+\alpha 2^{n-m-1}$.

Note that by (20) for sufficiently large n the values of s and $r=n-m-1$ satisfy the conditions of Lemma 3. Let $Q^{(i)}_\alpha$ be the set of functions f, such that the inequality

$$|D_\alpha(g)|\leqslant 2^{n-m-s-3} \tag{22}$$

is fulfilled for at least 2^{s-2} functions $g \in G^{(i)}$. Applying Lemma 3 to matrices $M_\alpha^{(i)}$ we obtain

$$|Q_\alpha^{(i)}| \leqslant 2^{2^n+2^s+(n-m)+\gamma 2^{n-m-1}}. \tag{23}$$

Consider the set $\hat{B}_n$ which is the union of the sets $Q_\alpha^{(i)}$ for all $i \in [1,d]$ and $\alpha \in \{0,1\}$. Let $\breve{B}_n = B_n \backslash \hat{B}_n$. From the definitions and (22) it follows that for any $f \in \breve{B}_n$ and for any $i \in [1,d]$ there exist at least 2^{s-1} functions $g \in G^{(i)}$, such that

$$\min\{|D_0(g)|, |D_1(g)|\} \geqslant 2^{n-m-s-3}.$$

Therefore, taking into account (20) and (21), for sufficiently large n,

$$t(\mathcal{S}_f) \geqslant d\, 2^{s-1} 2^{n-m-s-3} = d\, 2^{n-m-4} \geqslant 2^{n-5}/n.$$

Note that from (23) and (20) we have

$$|\hat{B}_n| \leqslant 2d\, 2^{2^n+2^s+(n-m)+\gamma 2^{n-m-1}} = o(2^{2^n}).$$

Hence the set $\breve{B}_n$ contains almost all functions from B_n. □

Acknowledgements We thank Alexey Pospelov for detailed and helpful comments on an earlier draft of the paper.

References

[1] Frandsen, G. S., Miltersen, P. B.: Reviewing bounds on the circuit size of the hardest functions. *Information Processing Letters*, Volume 95, Issue 2, 2005, 354–357.

[2] Hromkovich, J., Lozhkin, S. A., Rybko, A. I., Sapozhenko, A. A., Shkalikova, N. A.: Lower bounds on the area complexity of Boolean circuits, *Theoretical Computer Science*, 97, 1992, 285–300.

[3] Lozhkin, S. A.: On the synthesis of oriented switching circuits, *Moscow Univ. Comput. Math. Cybernet.*, 1995, N. 2, 32–37.

[4] Lozhkin, S. A.: On the synthesis of certain types of circuits based on translation partitions generated by universal matrices, *Moscow Univ. Comput. Math Cybernet.*, 1996, N. 1, 57–63.

[5] Lozhkin, S. A.: High accuracy bounds on the complexity of circuits of some types, *Mat. Probl. Kibern.*, 6, 1996, 189–214.

[6] Lozhkin, S. A.: *Asymptotic bounds of high accuracy on the complexity of control systems*, Doctor thesis, Moscow State University, 1997.

[7] Lozhkin, S. A., Shiganov, A. E.: High Accuracy Asymptotic Bounds on the BDD Size and Weight of the Hardest Functions, *Fundamenta Informaticae*, Vol. 104, Issue 3, 2010, 239–253.

[8] Lupanov, O. B.: A method of circuit synthesis, *Izv. VUZ Radiofiz.*, 1, 1958, 120–140.

[9] Lupanov, O. B.: Complexity of formula realization of functions of logical algebra, *Problems of Cybernetics*, 3, Pergamon Press, 1962, 782–811.

[10] Lupanov, O. B.: On one class of circuits of functional elements (formulae with finite memory), *Problems of Cybernetics*, 7, 1962, 61–114. [In Russian] (Original Russian Text – Lupanov, O. B.: Ob odnov klasse skhem iz funktsionalnyh elementov (formuli s konechnoi pamyat'u), *Problemy Kibernetiki*, 7, 1962, 61–114.)

[11] Lozhkin, S. A.: *Lectures on Basics of Cybernetics*, Moscow University Press, 2004. [In Russian] (Original Russion Text – Lozhkin, S. A.: *Lekcii po Osnovam Kibernetiki*, Izdatel'stvo Moskovskogo Universiteta, 2004.)

[12] Shannon, C. E.: The synthesis of two-terminal switching circuits, *Bell Syst. Techn. J.*, 1949, v.28, N-l, 59–98.

[13] Ullman, J. D.: *Computational aspects of VLSI*, Computer Science Press, 1984.

[14] Wegener, I.: *The complexity of Boolean functions*, Teubner (Stuttgart)/Wiley (Chichester), 1987.

[15] Yamamoto, M.: A tighter lower bound on the circuit size of the hardest Boolean functions. Electronic Colloquium on Computational Complexity, Report No. 86, 2011.

Appendix A

We shall prove that (12) follows from (11).

In case $a = b = 1$

$$\begin{aligned}\log(u^u) &\leqslant \frac{2^n}{n - \log n + 1}\left((n - \log n + 1) + \log\left(\frac{n}{n - \log n + 1}\right) - 1\right)\\ &\leqslant 2^n\left(1 - \frac{\log\left(2 - \frac{\log(n/2)}{n/2}\right)}{n - \log n + 1}\right)\\ &\leqslant 2^n\left(1 - \frac{\log(2 - e_1)}{2n}\right),\end{aligned}$$

where $e_1 = \max\limits_{v>0} \frac{\log v}{v} = \frac{\log e}{e} < \frac{4}{5}$. Therefore

$$-\log(2 - e_1) < -\log\left(\frac{6}{5}\right) = \log\left(1 - \frac{1}{6}\right) < \ln\left(1 - \frac{1}{6}\right) < -\frac{1}{6},$$

hence

$$\log(u^u) \leqslant 2^n\left(1 - \frac{1}{12n}\right).$$

The general case when $a \geqslant b$ reduces to the previous case by replacing u with au and n with $n + \log\left(\frac{a}{b}\right)$.

Appendix B

We assume that a spanning tree of the circuit $\mathcal{S} \in \mathbb{C}$ preserves the labels of the inner vertices. A *supertree* $\mathcal{D}$ of the circuit $\mathcal{S} \in \mathbb{C}$ is a tree obtained from some spanning tree of $\mathcal{S}$ by connecting all arcs absent in the spanning tree to their end vertices. There exist at most 8^L different supertrees of the circuits from $\mathbb{C}$ of the size

at most L. Indeed, to specify a supertree of the circuit $\mathcal{S} \in \mathbb{C}$, for each inner vertex v of $\mathcal{S}$ starting at the output of $\mathcal{S}$ it suffices to choose one of 8 possibilities for the label and the predecessors of v:

("&", inner node, inner node), ("&", leaf, inner node), ("&", leaf, leaf),
("$\vee$", inner node, inner node), ("$\vee$", leaf, inner node), ("$\vee$", leaf, leaf),
("$\neg$", inner node), ("$\neg$", leaf).

Now we shall prove Lemma 4.

Proof. In order to specify the circuit $\mathcal{S}$ which satisfies the conditions of the lemma, it suffices to

1. choose a supertree $\mathcal{D}$ of the circuit $\mathcal{S}$ such that $\mathcal{D}$ contains at most L inner vertices and at most $L - l + 1$ leaves;
2. choose R leaves of $\mathcal{D}$ and connect them to the inputs $x_1, \ldots, x_n$;
3. connect the remaining leaves to the inputs $x_1, \ldots, x_n$ or to the inner vertices of $\mathcal{D}$.

Therefore, the sought number of the circuits is not greater than

$$8^L 2^{L-l+1} n^R (L+n)^{L-R-l+1} \leqslant (16n)^{R+l} (16(L+n))^{L-R-l+1}.$$

The lemma is proved. □

ECCC ISSN 1433-8092
http://eccc.hpi-web.de