ISSN 0027-1322, Moscow University Mathematics Bulletin, 2022, Vol. 77, No. 3, pp. 144–153. © Allerton Press, Inc., 2022.
Russian Text © The Author(s), 2022, published in Vestnik Moskovskogo Universiteta, Seriya 1: Matematika, Mekhanika, 2022, No. 3, pp. 32–40.

Refined Bounds on Shannon's Function for Complexity of Circuits of Functional Elements

S. A. Lozhkin*

Chair of Mathematical Cybernetics, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University, Moscow, Russia

Received February 10, 2022

Abstract—Earlier, the author proposed rather general approaches and methods for obtaining high accuracy and close to high accuracy asymptotic bounds on Shannon's function for complexity in various classes of circuits. Most of the results obtained with their aid were published in a number of papers, except perhaps for the close to the high accuracy asymptotic bounds on Shannon's function for the complexity of circuits without restrictions on their structure. This paper fills this gap and presents a modified and simplified version of one of the above-mentioned methods, which, nevertheless, allows obtaining the bounds with the required accuracy.

DOI: 10.3103/S002713222203007X

Keywords: *Boolean function, circuits of the functional elements, complexity, high accuracy asymptotic bounds*

1. BASIC DEFINITIONS AND DENOTATIONS, FORMULATIONS OF RESULTS

Suppose that $B = \{0, 1\}$, B^n (where $n = 1, 2, \dots$) is the unit n-dimensional cube,[1] that is, the set of collections of lengths n of zeros and units, with the ith digit of which the Boolean variable x_i, $i = 1, \dots, n$, is related and $P_2(n)$ is the set of functions of the algebra of logic, in other words, of Boolean functions depending on these variables and mapping B^n to B. Below, by default, under the function we understand the function of algebra of logic, and under the variable we understand the Boolean variable.

We consider the formulas and circuits of functional elements over an arbitrary complete basis $\mathrm{B} = \{\mathcal{E}_1, \dots, \mathcal{E}_b\}$, where an element $\mathcal{E}_i$, $i = 1, \dots, b$, implements the function $\phi_i(x_1, \dots, x_{k_i})$, which in the case $k_i \geqslant 2$ significantly depends on all its variables and whose complexity is characterized by a positive real number L_i, which is called the *weight* of the element $\mathcal{E}_i$. For an element $\mathcal{E}_i$, $i \in [1, b]$, such that $k_i \geqslant 2$, we also define its *reduced weight* ρ_i, equal to the relation $\dfrac{L_i}{k_i - 1}$, and introduce the value $\rho_{\mathrm{B}} = \min\limits_{k_i \geqslant 2} \rho_i$, which is considered the *reduced weight* of the basis B. By default, the circuit is the circuit of functional elements in the basis B, and, as usual, the formulas are considered the special case of circuits. In the standard way we determine the complexity $L(\Sigma)$ of the circuit (formula) Σ as the sum of its elements.

Without loss in generality, we assume that in the basis B there exists at least one so called *amplifying* element $\mathcal{E}_i$, for which $k_i = 1$ and $\phi_i = x_1$. Here, under the *amplifying* circuit we understand the circuit in which the outputs of the elements with the reduced weight ρ_{B} are not branched, that is, the circuit with zeroth depth of branching. Note that a formula is an amplifying circuit.

*E-mail: lozhkin@cs.msu.ru

[1] The concepts that are not defined in this work can be found, e.g., in [1–3].

Consider the classes U_{B}^{Φ}, $U_{\mathrm{B}}^{\mathrm{C}}$, and $U_{\mathrm{B}}^{\mathrm{AC}}$, which consist, respectively, of formulas, circuits, and amplifying circuits in the basis B and are complete in the sense that we can implement any function in each of them. Moreover, it is clear that $U_{\mathrm{B}}^{\Phi} \subset U_{\mathrm{B}}^{\mathrm{AC}} \subset U_{\mathrm{B}}^{\mathrm{C}}$. For any of these classes of the form $U_{\mathrm{B}}^{\mathrm{A}}$ and an arbitrary function f, in the common way we determin its complexity $L_{\mathrm{B}}^{\mathrm{A}}(f)$ as the minimal complexity of circuits of $U_{\mathrm{B}}^{\mathrm{A}}$ implementing f, and, then, for a natural number n, $n = 1, 2, \ldots$, we introduce the corresponding Shannon function

$$L_{\mathrm{B}}^{\mathrm{A}}(n) = \max_{f \in P_2(n)} L_{\mathrm{B}}^{\mathrm{A}}(f).$$

We recall that the asymptotic behavior of Shannon's functions $L_{\mathrm{B}}^{\Phi}(n)$ and $L_{\mathrm{B}}^{C}(n)$ was established by Lupanov (see [4, 5] and also [2]); moreover, from the results obtained by him it follows that[2]

$$L_{\mathrm{B}}^{\mathrm{C}}(n) \sim L_{\mathrm{B}}^{\mathrm{AC}}(n) \sim \rho_{\mathrm{B}} \frac{2^n}{n}, \quad L_{\mathrm{B}}^{\Phi}(n) \sim \rho_{\mathrm{B}} \frac{2^n}{\log n}. \tag{1}$$

In this case it appeared that the relative error of bounds of Shannon's functions in (1) equal to the ratio of the difference between the upper and lower bounds of Shannon's function $L_{\mathrm{B}}^{\mathrm{A}}(n)$ to itself is $O\left(\frac{L_{\mathrm{B}}^{\mathrm{A}}(n)}{2^n} \log\left(\frac{2^n}{L_{\mathrm{B}}^{\mathrm{A}}(n)}\right)\right)$, that is, is $O\left(\frac{\log\log n}{\log n}\right)$ for the class U_{B}^{Φ} and $O\left(\frac{\log n}{n}\right)$ for the classes $U_{\mathrm{B}}^{\mathrm{C}}$, $U_{\mathrm{B}}^{\mathrm{AC}}$.

In work [6], for Shannon's functions U_{B}^{Φ} and $U_{\mathrm{B}}^{\mathrm{AC}}$ the high accuracy asymptotic bounds were first obtained, that is, the bounds with the relative error $O\left(\frac{1}{\log n}\right) = O\left(\frac{L_{\mathrm{B}}^{\Phi}(n)}{2^n}\right)$ and $O\left(\frac{1}{n}\right) = O\left(\frac{L_{\mathrm{B}}^{\mathrm{AC}}(n)}{2^n}\right)$, respectively. It was proved that following equalities are true[3]

$$L_{\mathrm{B}}^{\Phi}(n) = \rho_{\mathrm{B}} \frac{2^n}{\log n}\left(1 + \frac{æ_{\mathrm{B}} \log\log n \pm O(1)}{\log n}\right), \tag{2}$$

$$L_{\mathrm{B}}^{\mathrm{AC}}(n) = \rho_{\mathrm{B}} \frac{2^n}{n}\left(1 + \frac{(2 + æ_{\mathrm{B}}) \log n \pm O(1)}{n}\right), \tag{3}$$

where $æ_{\mathrm{B}} = 1$ if all elements of the basis B with the reduced weight ρ_{B} implements either only disjunctions of variables, or conjunctions of variables, or linear functions, and $æ_{\mathrm{B}} = 0$ in other cases.

In work [6–10] the authors considered another examples of classes of circuits in which for the corresponding complexity Shannon's functions it was succeeded to obtaining the high accuracy asymptotic bounds.

Recall that in [6] the following upper bound is given without proof

$$L_{\mathrm{B}}^{\mathrm{C}}(n) \leqslant \rho_{\mathrm{B}} \frac{2^n}{n}\left(1 + \frac{(1 + æ_{\mathrm{B}}) \log n + \log\log n + O(1)}{n}\right), \tag{4}$$

which was proved in [7, Theorem 8]. Note that the upper bounds (4) are achieved on schemes with the branching depth 1, that is, on schemes admitting the branching of output of the elements of the reduced weight ρ_{B}, but not admitting the chains of length 2 of elements of the indicated form with branching outputs. Here, it appeared (see [7, Lemma 22]) that bound (4) is the high accuracy bound for the complexity of circuits of the given type.

[2] All logarithms are taken to base 2 and the asymptotic equality $a(n) \sim d(n)$ of two functions of natural argument n, $n = 1, 2, \ldots$, occurs iff $a(n) = (1 + o(1))d(n)$.

[3] The presence in the right-hand side of equalities (2) and (3) of the term of the form $\pm a(n)$ means that for the left-hand side of the corresponding equality the upper and lower bounds take place that are obtained from its right-hand side by replacing the given term by the term $|a(n)|$ and $-|a(n)|$, respectively.

Note also, that the upper bound (4) in the case $æ_{\rm B} = 0$ and (see, e.g., [6]) the lower bound

$$L_{\rm B}^{\rm C}(n) \geqslant \rho_{\rm B}\frac{2^n}{n}\left(1+\frac{\log n - O(1)}{n}\right) \tag{5}$$

can be considered the bounds of Shannon's functions $L_{\rm B}^{\rm C}(n)$ close to the high accuracy asymptotic bounds taking into account that their relative error is

$$o\left(\frac{\log n}{n}\right) = o\left(\frac{L_{\rm B}^{\rm C}(n)}{2^n}\log\left(\frac{2^n}{L_{\rm B}^{\rm C}(n)}\right)\right), \tag{6}$$

which is substantially lower than the relative error of the corresponding bounds (1).

Below in this work, we consider the circuits in the standard basis $\rm B_0$, which consists of elements $\mathcal{E}_{\&}$, $\mathcal{E}_{\vee}$, $\mathcal{E}_{\neg}$, $\mathcal{E}_{\rm AC}$, having the weight 1 and implementing the functions $x_1 \cdot x_2$, $x_1 \vee x_2$, $\overline{x}_1$, x_1, respectively. Here, it is clear that the complexity functional $L(\Sigma)$ of the circuit Σ is simply equal to the number of its elements. The index of the basis $\rm B_0$ in the denotations of the above introduced complexity functionals and the corresponding Shannon functions will be omitted.

The main result of the current work is a proof of the upper bound (4) for the basis $\rm B_0$ simpler than in [7], that is, the proof of the next statement

Theorem. *For all natural n, $n = 1, 2, \ldots$, for Shannon's function $L^{\rm C}(n)$ the inequality*

$$L^{\rm C}(n) \leqslant \frac{2^n}{n}\left(1+\frac{\log n + \log\log n + O(1)}{n}\right) \tag{7}$$

is satisfied.

Note that the upper bound (7) and lower bound (5) have the relative error of form (6), that is, are the bounds of Shannon's function $L_{\rm B}^{\rm C}(n)$ close to the high accuracy asymptotic bounds.

2. UNIVERSAL SETS OF FUNCTIONS AND SELECTIVE PARTITIONS OF VARIABLES. REPETITION-FREE FORMULAS WITH OPTIMAL COMPLEXITY AND BOUNDED SELECTIVE ENTROPY

Recall that the main concepts and some results of [3, 6] related with the sets of functions universal for a given function and their construction on the basis of special partitions of variables of this function.

For the collection $\sigma = (\sigma_1, \ldots, \sigma_n)$ from B^n the number $\nu(\sigma) = \sum\limits_{i=1}^{n} \sigma_i 2^{n-i}$ prescribes its so called lexicographic number. Under *segment* of the cube B^n we understand, as usual, such set of its collections whose ν-numbers form the segment of integer numbers. The segment of even length (power), which begins from the collection having an even number, we call *even*.

Following [3, 6], we say that the set of functions $G \subseteq P_2(m)$ is *universal for the function* $\phi(y_1, \ldots, y_p)$, or *ϕ-universal set of order m* if for any function $g \in P_2(m)$ there exist functions $g_1, \ldots, g_p$ from G such that

$$\phi(g_1, \ldots, g_p) = g. \tag{8}$$

In the case when equality (8) for an arbitrary function g from $P_2(m)$ and some functions $g_1, \ldots, g_p$ from G is satisfied on some set of collections $\delta, \delta \subseteq B^m$, we say that the set G is *ϕ-universal set (of functions) of order m* for *sets of collections δ*.

Note that the latter notion corresponds to the notion of ϕ-universal matrix of height $|\delta|$ from [6, Sect. 4] if the rows of this matrix are in the one-to-one correspondence to the sets of the cube B^m from the set δ and its columns are considered the columns of values of the functions from the set G on the set of collections from δ.

Suppose that a function ϕ is considerably dependent on all its variables $Y = \{y_1, \ldots, y_p\}$ and $D = (Y_1, \ldots, Y_d)$ is the partition of the set Y into nonempty pairwise nonintersecting subsets $Y_1, \ldots, Y_d$. The partition D is called the *selective* partition of the variables of the function ϕ [6, Sect. 3] if for each $i, 1 \leqslant i \leqslant d$ and for any variable $y_j \in Y_i$ there exist Boolean constants $\alpha_1^{(j)}, \ldots, \alpha_{i-1}^{(j)}, \alpha_{i+1}^{(j)}, \ldots, \alpha_d^{(j)}$, at the substitution of which instead of all variables from $Y_1, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_d$, respectively, the function ϕ turns into the function of the form $y_j \oplus \beta_j$, where β_j is another constant. Note that the trivial partition of variables of the function ϕ into p components is selective.

The *entropy* of a partition D of a set Y into the components $Y_1, \ldots, Y_d$ is understood as the value

$$H(D) = -\frac{1}{|Y|}\sum_{i=1}^{d} |Y_i| \log \frac{|Y_i|}{Y}.$$

It appeared (see [6, Sect. 3]) that, using the selective partition D of the indicated type for the set of variables Y of a function $\phi(y_1, \ldots, y_p)$ having a "small" entropy $H(D)$, we can construct a "good" set of functions ϕ-universal for the given set of collections δ, $\delta \subseteq B^m$. For this purpose, we need to take the partition $\Delta = (\delta_1, \ldots, \delta_p)$ of the set δ related with the partition D of the set of variables Y of the function ϕ as follows: the variable y_i, $i = 1, \ldots, p$, corresponds to the component δ_i, and for any k, $k \in [1, d]$, for any i such that $y_i \in Y_k$, the equality $|\delta_i| = s_k$ is satisfied. Note that, in this case $p_1 s_1 + \ldots + p_d s_d = |\delta|$, where $p_k = |Y_k|$ for all k, $k = 1, \ldots, d$.

On the basis of partitions D and Δ we can construct the so called *standard* set of functions $\mathcal{G}$, $\mathcal{G} \subseteq P_2(m)$, ϕ-universal for the set of collections δ such that

$$\mathcal{G} = \mathcal{G}_1 \cup \ldots \cup \mathcal{G}_d, \quad |\mathcal{G}| = 2^{s_1} + \ldots + 2^{s_d}, \tag{9}$$

where the set $\mathcal{G}_k$ consists of 2^{s_k} functions.

The matrix $\mathcal{M}$ corresponding to the set $\mathcal{G}$ consists of d vertical "bands" $\pi_1, \ldots, \pi_d$ having the lengths $2^{s_1}, \ldots, 2^{s_d}$ and related with the components $Y_1, \ldots, Y_d$ and with the sets $\mathcal{G}_1, \ldots, \mathcal{G}_d$, respectively. On the other side, the matrix $\mathcal{M}$ includes d "large" horizontal bands $\Pi_1, \ldots, \Pi_d$, having the heights $p_1 s_1, \ldots, p_d s_d$ and related with the components $Y_1, \ldots, Y_d$, respectively. In this case the band Π_i, $i = 1, \ldots, d$, is divided into p_i main horizontal bands of local height s_i, related, as we have said above, with the different variables from Y_i and with the components of partition Δ corresponding to them and giving the matrix in the intersection with the band π_i whose columns are all collections of the cube B^{s_i} arranged by their increasing ν-numbers in the assumption that the top digits of the ν-numbers are located at the top. Each of the remaining blocks of the matrix $\mathcal{M}$ lying at the intersection between one vertical and one of the main horizontal bands is filled with the same constant of form $\alpha_j^{(i)}$ related with the selectivity of partition D. We assume that all functions from $\mathcal{G}$ outside δ are 0. We call the number $s = \max\limits_{1 \leqslant i \leqslant d} s_i$ the *maximal local height* of the matrix $\mathcal{M}$ and set $\mathcal{G}$.

The set of functions G and matrix M that are obtained from $\mathcal{G}$ and $\mathcal{M}$ when removing a part of collections from the set δ and eliminating the corresponding rows of the matrix $\mathcal{M}$ and still are ϕ-universal for the set of remaining collections (rows) are considered the result of applying the *reduction* operation to $\mathcal{G}$ and $\mathcal{M}$. We speak of *evenness* of the matrix M (set G) if the heights of all main horizontal bands of M are even numbers (respectively, the components of the partition of Δ related with G are even segments).

The results of [6, Sect. 4] imply the validity of the following statement.

Lemma 1. *Suppose that δ is an even segment of a cube B^m and $D = (Y_1, \ldots, Y_d)$ is the selective partition of a set of variables $Y = \{y_1, \ldots, y_p\}$ of a function $\phi(y_1, \ldots, y_p)$. Then for any even s such that $s > \log p$ and $|\delta| \leqslant p(s - H(D))$, there exists an even (reduced) standard set of functions G ϕ-universal for the set δ with the maximal local height s for which*[4]

$$|G| \leqslant 2^{s+2}, \quad L(\mathbf{G}) \leqslant 3|G| + O(d2^{m+\frac{s}{2}}). \tag{10}$$

[4] For a set of functions G, $G \subseteq P_2(m)$, by $\mathbf{G}$ we denote the system of functions of the form $(g_1, \ldots, g_\lambda)$, where $\lambda = |G|$, composed of all distinct functions of the set G.

Remark. The set $G = G_1 \cup \ldots \cup G_d$ is obtained as a result of reduction of the original set $\mathcal{G}$ of form (9) for which, due to the lemma hypothesis, in choosing the even local height s_i, $i = 1, \ldots, d$, from the real segment of length 2 with the center $\left(s - \log \frac{p}{p_i} + 1\right)$, where $p_i = |Y_i|$, the relations are satsfied:

$$p_1 s_1 + \ldots + p_d s_d \leqslant |\delta| + 2p,\ p_i 2^{s+2} \geqslant p|\mathcal{G}_i| = p 2^{s_i}. \tag{11}$$

Moreover, due to (11) the indicated reduction comes to the possible decrease by 2 of a part of local heights and possible removal of 2 rows from some main horizontal bands of the matrix $\mathcal{M}$ related with the set $\mathcal{G}$.

It follows from [6, Sect. 3] that in the basis $\{\mathcal{E}_{\&}, \mathcal{E}_{\vee}\}$ we can construct a sequence of repetition-free formulas with increasing number of varaibles and bounded selective entropy of the functions they implement.

Lemma 2. *For any natural p in the basis $\{\mathcal{E}_{\&}, \mathcal{E}_{\vee}\}$ there exists a repetition-free formula Φ_p that implements the function $\phi_p(y_1, \ldots, y_p)$ having the selective partition D_p of the set of all its variables; moreover,* [5]

$$L(\Phi_p) = p - 1,\ H(D_p) \leqslant e_1.$$

3. SYNTHESIS OF AMPLIFYING CIRCUITS AND HIGH ACCURACY ASYMPTOTIC UPPER BOUNDS ON SHANNON'S FUNCTION FOR THEIR COMPLEXITY

Using Lemmas 1 and 2, we can prove the following statement that provides (see [6]) the high accuracy upper asymptotic bound on Shannon's function $L^{\text{AC}}(n)$.

Lemma 3. *For an arbitrary function f, $f \in P_2(n)$, there exists a circuit Σ_f, $\Sigma_f \in U^{AC}$, implementing it such that*

$$L(\Sigma_f) \leqslant \frac{2^n}{n}\left(1 + \frac{2\log n + O(1)}{n}\right). \tag{12}$$

Proof. For constructing the circuit Σ_f, we select the natural parameters m, s, and p so that s is even and

$$m < n, \quad m + e_1 \leqslant s \leqslant 2^m, \quad p = \left\lceil \frac{2^m}{s - e_1} \right\rceil. \tag{13}$$

By Lemma 2 we construct the formula $\Phi = \Phi_p$ implementing the function $\phi = \phi_p$ for which there exists a selective partition of variables D such that $H(D) \leqslant e_1$. Note that, due to (13) for a partition D of the function ϕ the conditions of Lemma 1 are satisfied, that is, there exists a set G that is ϕ-universal for the entire cube B^m and satisfies (10).

Let us divide the collection of variables $(x_1, \ldots, x_n)$ into the subcollections

$$x = (x_1, \ldots, x_m), z = (z_1, \ldots, z_{n-m}) = (x_{m+1}, \ldots, x_n)$$

and consider the Shannon decomposition of the function f by the variables z

$$f(x, z) = \bigvee_{\sigma \in B^{n-m}} K_\sigma(z) f_\sigma(x), \tag{14}$$

where for the collection $\sigma = (\sigma_{m+1}, \ldots, \sigma_n)$ the elementary conjunction $K_\sigma(z)$ has the form $x_{m+1}^{\sigma_{m+1}} \cdot \ldots \cdot x_n^{\sigma_n}$ and $f_\sigma(x) = f(x, \sigma)$ is the so called remainding function of the function f.

Note that, representation (14) can be transformed using the so called standard multiplexor function μ_q of order q of address variables $x_1, \ldots, x_q$ and informative variables $y_0, \ldots, y_{2^q-1}$ that can be defined by the equation

$$\mu_q(x_1, \ldots, x_q, y_0, \ldots, y_{2^q-1}) = \bigvee_{\sigma \in B^q} K_\sigma(x_1, \ldots, x_q) y_{\nu(\sigma)}.$$

[5] The letter e with different subscripts denotes some positive constants.

Indeed, representation (14) is equivalent to the representation

$$f(x,z) = \mu_{n-m}(z, f_{(0,\dots,0)}(x), \dots, f_\sigma(x), \dots, f_{(1,\dots,1)}(x)). \tag{15}$$

On the basis of representation (15) for the function f and representation (8), for each of its remainder functions of type f_σ, $\sigma \in B^{n-m}$, in the basis $\widetilde{\mathrm{B}_0} = \{\mathcal{E}_{\&}, \mathcal{E}_{\vee}, \mathcal{E}_{\neg}\}$ we construct the circuit $\widetilde{\Sigma_f}$ that implements f. We compose it of the following subcircuits:

(1) the subcircuit Σ_G of variables x implementing the system of functions $\mathbf{G}$;

(2) the subcircuit $\widehat{\Sigma}$ for each collection σ from B^{n-m} impelmenting the function $f_\sigma(x)$ presented in the form (8), by means of the formula Φ whose input variables are connected to the outputs Σ_G according to this representation;

(3) the subcircuit $\check{\Sigma}$ implementing the function $\mu_{n-m}(z, y_0, \dots, y_{2^{n-m}-1})$, the information input y_σ, $\sigma \in B^{n-m}$, which is connected, according to (14) and (15), to the output $\widehat{\Sigma}$, where the function $f_\sigma(x)$ is implemented.

Inequalities (10), Lemma 2, and the known (see, e.g., [3]) bounds on the complexity of multiplexor functions imply that

$$L(\Sigma_G) \leqslant 3|G| + O(p \cdot 2^{m+\frac{s}{2}}), \quad L(\widehat{\Sigma}) = 2^{n-m}(p-1), \quad L(\check{\Sigma}) \leqslant 3 \cdot 2^{n-m}, \tag{16}$$

$$L(\widetilde{\Sigma_f}) \leqslant 2^{n-m}(p-1) + O(p \cdot 2^{m+\frac{s}{2}} + 2^s + 2^{n-m}). \tag{17}$$

To obtain the sought amplifying circuit Σ_f from the circuit $\widetilde{\Sigma_f}$, we need to pass through the amplifying elements $\mathcal{E}_{\mathrm{AC}}$ both the "branching" outputs of hte "internal" elements of its subcircuits Σ_G, $\check{\Sigma}$, and the outputs of its subcircuit Σ_G "branching" in $\widetilde{\Sigma_f}$. Here, for the complexity of a circuit $\widetilde{\Sigma_f}$ bound (17) still holds.

Choosing the parameter values so that

$$m = \lceil 2\log n \rceil, \quad s = 2\left\lceil \frac{n - 2\log n}{2} \right\rceil, \quad p = \left\lceil \frac{2^m}{s - e_1} \right\rceil$$

and proving that in this case for some n_0 and any n, $n \geqslant n_0$, conditions (13) are met, by substituting the indicated values into (17), we obtain (12).

The lemma is proved.

4. METHOD FOR SYNTHESIS OF CIRCUITS THAT ALLOWS OBTAINING CLOSE TO HIGH ACCURACY ASYMPTOTIC BOUNDS OF SHANNON'S FUNCTION FOR THEIR COMPLEXITY

Before we proceed to the proof of the theorem, we outline the approach to synthesizing the circuits in the class U^{C} that allows obtaining the upper bound (7) instead of the upper bound (12).

This approach consists in perofrming the decomposition of functions and construction of the circuits Σ_G, $\widehat{\Sigma}$, similarly to the way it was done in proving Lemma 3, but not for all collections σ from B^{n-m}, but for those of them for which $\nu(\sigma) < N = O\left(\dfrac{2^{n-m}}{\log n}\right)$. The goal of this "partial" implementation of the function f consists in the following: to implement the functions from the new "wider" universal set that can be applied in implementation of remainder functions $f_\sigma(x)$ for the case $\nu(\sigma) \geqslant N$ at the outputs of the certain part of elements used in the formulas of type $\mathcal{F} = \mathcal{F}_p$.

The validity of the theorem is implied by the following statement.

Lemma 4. *For an arbitrary function f, $f \in P_2(n)$, there exists a scheme Σ_f, $\Sigma_f \in U^{\mathrm{C}}$, implementing it such that*

$$L(\Sigma_f) \leqslant \frac{2^n}{n}\left(1 + \frac{\log n + \log\log n + O(1)}{n}\right). \tag{18}$$

Proof. Similarly to the proof of Lemma 3, for each p, $p = 1, 2, \ldots$, by Lemma 2 we construct the formula $\Phi_p(y_1, \ldots, y_p) = \Phi$ of complexity $(p-1)$ implementing the function $\phi_p(y_1, \ldots, y_p) = \phi$ which has such a selective partition $D = (Y_1, \ldots, Y_d)$ of the set of its variables $Y = \{y_1, \ldots, y_p\}$ for which $|Y_i| = p_i$ for all i, $i = 1, \ldots, d$, and $H(D) = H(\phi) \leqslant e_1$. Suppose that $Y' = \{y'_1, \ldots, y'_p\}$, $Y'' = \{y''_1, \ldots, y''_p\}$, and the partitions $D' = (Y'_1, \ldots, Y'_d)$ and $D'' = (Y''_1, \ldots, Y''_d)$ are the result of applying D to the sets of variables Y' and Y'', respectively.

In the following, we consider the formula $\Psi(y', y'') = \Psi$, where y' and y'' are collections of variables $y' = (y'_1, \ldots, y'_p)$ and $y'' = (y''_1, \ldots, y''_p)$, respectively, and the formula $\Psi(y', y'')$ is obtained from the formula $\Phi_p(y_1, \ldots, y_p)$ by replacement of y_i, $i = 1, \ldots, p$, by the disjunction $y'_i \vee y''_i$ and implements the function $\psi_p(y', y'') = \psi(y', y'') = \phi(y'_1 \vee y''_1, \ldots, y'_p \vee y''_p)$ of variables $\mathcal{Y} = Y' \cup Y''$.

Following the proof of Lemma 3, we set

$$x = (x_1, \ldots, x_m), \quad z = (z_1, \ldots, z_{n-m}) = (x_{m+1}, \ldots, x_n),$$

and, then, to construct the circuit Σ_f implementing the function $f(x, z)$ from $P_2(n)$, similarly to (13), we choose the natural parameters m, s', s'', and p so that s' and $s''$are even numbers and, moreover,

$$m < n, \quad s' + s'' \leqslant 2^m, \quad \min\{s', s''\} \geqslant m + e_1 + 2, \quad p = \left\lceil \frac{2^m}{s' + s'' - 2e_1} \right\rceil. \tag{19}$$

Note that, due to (19), for the function ϕ, partition D', and maximal local height s' (respectively, D'' and s''), the conditions of Lemma 1 are met. According to Remark, we construct the even standard nonreduced matrix M' to it that is $\phi(y')$-universal for the segment $\delta' = [0, t')$ of the cube B^m and has local heights $s'_1, \ldots, s'_d$, where $t' = p_1 s'_1 + \ldots + p_d s'_d$ and the analogous set G' of variables x related with it, together with its representation $G' = G'_1 \cup \ldots \cup G'_d$ of form (9). We set $t'' = 2^m - t'$ and, by Lemma 1 and Remark, construct the standard (reduced) matrix M'' that is $\phi(y'')$-universal for the segment $\delta'' = [t', 2^m)$ of the cube B^m of length t'' and the set of functions G'' of variables x related with it, together with its representation $G'' = G''_1 \cup \ldots \cup G''_d$ of form (9).

Here, to construct the sets G' and G'', we use the partitions Δ' and Δ'' into even sequential segments of segments δ' and δ'', respectively, and the sets G' and G'' themselves by their construction consist of functions taking 0 on the sets of collections δ'' and δ', respectively. Hence, the set $G' \cup G''$ is a ψ-universal set of functions of order m, and, in addition to that, due to (10)

$$t' \leqslant p(s' - e_1), \quad t'' \leqslant p(s'' - e_1), \quad |G'| \leqslant 2^{s'+2}, \quad |G''| \leqslant 2^{s''+2} \tag{20}$$

and

$$L^{\mathrm{C}}(\mathbf{G}') \leqslant 3|G'| + O\left(p \cdot 2^{m + \frac{s'}{2}}\right), \quad L^{\mathrm{C}}(\mathbf{G}'') \leqslant 3|G''| + O\left(p \cdot 2^{m + \frac{s''}{2}}\right). \tag{21}$$

Similarly to (14) and (15), for the function $f(x, z)$ we consider its Shannon expansion in variables z

$$f(x, z) = \bigvee_{\sigma \in B^{n-m}} K_\sigma(z) f_\sigma(x) = \mu_{n-m}(z, f_{(0,\ldots,0)}(x), \ldots, f_\sigma(x), \ldots, f_{(1,\ldots,1)}(x)), \tag{22}$$

where $f_\sigma(x) = f(x, \sigma)$. Here, due the above said, for any remainder function $f_\sigma(x)$, from decomposition (22) for certain functions $g'_{1,\sigma}, \ldots, g'_{p,\sigma}$ from G' and certain functions $g''_{1,\sigma}, \ldots, g''_{p,\sigma}$ from G'', the equality is satisfied

$$f_\sigma(x) = \psi(g'_{1,\sigma}, \ldots, g'_{p,\sigma}, g''_{1,\sigma}, \ldots, g''_{p,\sigma}). \tag{23}$$

Consider representation (23) for all collections σ from the initial segment I of length N of the cube B^{n-m} of variables z. In this case, for any function g' from G' we define its *multiplicity* as the number of enterings of this function to representations (23) for $\sigma \in I$ at the place of any of the first p variables of the function ψ. Note that, the average value of the indicated multiplicity over the entire set G' is $\dfrac{Np}{|G'|}$

and, dut to (10) is not less than $S' = \dfrac{Np}{2^{s'+2}}$, and its average value over the set G'_i for any i, $1 \leqslant i \leqslant d$, is $\dfrac{Np_i}{|G'_i|}$, and, consequently, according to (11), not less than S'.

Below, we introduce an auxiliary unit cube B^{m+1} of variables (x_0, x) consisting of m-dimensional subcubes $B^{m+1}(0,x)$ and $B^{m+1}(1,x)$, the first of which is "identified" with the cube $B^m(x)$. At the outputs of the "upper" elements of disjunction of formulas Ψ, used in implementation of representations (23) for $\sigma \in I$, we attempt at obtaining all the functions from the standard set of functions G that is ϕ-universal for some initial segment δ of the subcube $B^{m+1}(1,x)$ of the above introduced cube $B^{m+1}(x_0,x)$, has maximal local height s, where $s = h + s'$, and is related with the partition D so that the representation $G = G_1 \cup \ldots \cup G_d$ of form (9) is true.

Let us first consider the case when the above introduced multiplicities of the functions from G' are "almost" identical, that is, not less than 2^h, where h is an even number and $h = 2\left\lfloor \dfrac{1}{2}\log S' \right\rfloor$. In this case we continue the functions from G' to the subcube $B^{m+1}(1,x)$ so that the variable x_0 is fictituous for them and increase all local heights s'' of the set G'' by h.

It follows from the above described peculiarities of the standard universal sets of functions and matrices related with them that the matrix M'' related with the set G'' transforms to the matrix M''_+ with $l = |G''|2^h$ columns and $t'' + ph$ rows in this case. In each of the main horizontal bands of the matrix M''_+, we separate a subband composed of its h lower rows, join all these subbands into a matrix $\lfloor M''_+ \rfloor$ of the same length l and height ph, and relate its rows with the segment $\widetilde{\delta}''$ of length ph of the subcube $B^{m+1}(1,x)$ starting from the collection with the index $2^m + t' - 1$ and divided into p sequential segments of length h by the partition $\widetilde{\Delta}''$. We leave the remaining rows of the matrix M''_+ generating its submatrix $\lceil M''_+ \rceil$ at the same positions that are related with the segment δ'' of the cube $B^m(x)$ and have been occupied by the rows of the matrix M''.

Note that, the matrix $\lceil M''_+ \rceil$ is obtained by 2^h-multiple duplication of each column of the matrix M'' and that the matrix $\lfloor M''_+ \rfloor$, in its turn, also is a result of a certain duplication of columns in the standard $\phi(y'')$-universal matrix M^* constructed based on the partition D'' with local heights h. Here, all 2^h duplicates of the same column of the submatrix $\lceil M''_+ \rceil$ of the matrix M''_+ located in the ith vertical band of M'' in the intersection with any main horizontal band of the matrix $\lfloor M''_+ \rfloor$, which is related with the variable from Y''_i, yield the submatrix consisting of all 2^h columns of height h.

Now, we consider the so constructed sets of functions G' and G''_+ of variables (x_0, x) and then set $x_0 = \chi_I(z)$, where $\chi_I(z)$ is the characteristics function of the segment I of the cube B^{n-m}. We prove that at the outputs of the upper elements of disjunction of formulas Ψ used in implementation of representations (23) for $\sigma \in I$, where the functions g''_i are taken from the set G''_+, in the case $\sigma \notin I$ we obtain the standard set of functions G that is ϕ-universal for the segment $\delta = [0, t' + ph)$ of the cube $B^m = B^{m+1}(1,x)$ and related with the partition D and also with the partition Δ of the segment δ whose jth component, $j = 1, \ldots, p$, is obtained as a result of joining jth components of partitions Δ' and $\widetilde{\Delta}''$.

Indeed, suppose that $G^* = G^*_1 \cup \ldots \cup G^*_d$ is a set of functions of variables x the columns of whose values correspond to the columns of the matrix M^* under the assumption that the rows of this matrix are related to the segment $\widetilde{\delta}''$ and that are equal to 0 outside $\widetilde{\delta}''$. Then, each function g from G can be represented as $g = g' \vee g^*$, where $g' \in G'_i$, $g^* \in G^*_i$, and $g \in G_i$ for some i, $1 \leqslant i \leqslant d$. Suppose that in this case the function g^* corresponds to such a column y from the ith vertical band of the matrix M^* related with Y''_i, which, in the intersection with any main horizontal band related with the variable from Y''_i yields the collection γ from B^h.

We consider the occurrence with the index q, $q \in [1, 2^h]$, of the function g' into one of representations (23), where $\sigma \in I$, instead of the variable y'_j from Y'_i of the function $\psi(y', y'')$ and in the same representation find the occurrence of the function g'' from G''_i instead of the variable y''_j from Y''_i. In implementation of this representation, instead of the function g'' we take its "continuation" to the cube

$B^{m+1}(1, x)$ such that its column of values in any of the main bands of the partition $\widetilde{\Delta}''$ related with Y_i'' is γ.

Note that, in the case $\sigma \notin I$ the mentioned representation provides the implementation of the function $g' \vee g^*$ at the output of the disjunction element connecting the variables y_j' and y_j'' in the formula Ψ, that is used to implement representation (23) at consideration.

In the case when the multiplicities of the functions from G' can "strongly" differ from each other, instead of the matrix M' related with the system of functions G', we use the matrix M_+' that is obtained from M' by t times duplicating the column related with the function $g', g' \in G'$, if the multiplicity g' is not less than $(t-1)\dfrac{pN}{|G'|}$, but less than $t\dfrac{pN}{|G'|}$.

We can easily see that the number of columns in the matrix M_+' is not larger than $2|G'|$ and that, by replacing the multiple occurrences of the columns of the matrix M' (more acucrately, the functions from G' corresonponding to them) in decomposition (23) at $\sigma \in I$ in the appropriate manner by the occurrences of the columns of the matrix M_+', we can achieve the reduction in the maximal multiplicity to the level not greater than S'. Hence, not less than $\dfrac{1}{4}$ of columns of the matrix M_+' have a multiplicity not less than $\dfrac{1}{4}S'$. It is these columns of the matrix M_+' that are continued to the subcube $B^{m+1}(1, m)$ so that, in the rows related with its initial segment $\widetilde{\delta}'$ of length $\widetilde{t}'$, we place the canonical $\phi(y')$-universal matrix $\widetilde{M}_+'$ of maximal local height $\widetilde{s}'$, $\widetilde{s}' = s' - 3$, corresponding to the even standard set $\widetilde{G}_+'$ ϕ'-universal for the segment $\widetilde{\delta}'$. Using the reasoning similar to the above given one, this allows proving that in the case at consideration it is possible to implement the functions from the set G of maximal local height s, $s = \widetilde{s}' + \widetilde{h}$, where $\widetilde{h} = h - 2$, at the outputs of the upper elements of the disjunction of formulas Ψ used in (23) for $\sigma \in I$.

In a way similar to that we done it in Lemma 3, we first construct the circuit $\check{\Sigma}$ implementing, on the basis of representations (22) and (23), the function $\check{f} = f(x, z) \cdot \chi_I(z)$. Here, instead of the functions from G' and G'', we use the functions from G_+' and G_+'', respectively, so that, at the outputs of some upper elements of disjunctions of formulas Ψ, we provide the implementation of the functions which at $\chi_I(z) = 1$ coincide with the required functions from the set G ϕ-universal for the segment δ.

Consider a binary collection τ of length $Q = 2^m(2^{n-m} - N)$ which consists of $(2^{n-m} - N)$ columns of values of remainder functions $f_\sigma = f(x, \sigma)$, written in increasing order of indices $\nu(\sigma)$, $\sigma \in B^{n-m} \setminus I$, and partitioned into $T = \left\lceil \dfrac{Q}{l} \right\rceil$ sequential segments of length $l = t' + ph$. We construct the circuit $\widetilde{\Sigma}$ of input variables (x, z) that, using the collection of their values (β, σ), computes the collection (γ, θ) of values of its output variables (u, v), where $u = (u_1, \ldots, u_k)$, $v = (v_1, \ldots, v_m)$, and $k = \lceil \log T \rceil$, so that the numbers $\nu(\gamma) + 1$ and $\nu(\theta) + 1$ prescribe the number of the segment of the collection τ which contains the value $f(\beta, \sigma)$ and the number of the position in it in which this value is written, respectively.

The circuit Σ_f contains the circuits $\check{\Sigma}$, $\widetilde{\Sigma}$ as subcircuits, implements the feeding of the collection of variables x to the first m inputs of the subcircuit $\check{\Sigma}$ if $\chi_I(z) = 0$ and the collection of variables v of the subcircuit $\widetilde{\Sigma}$ if $\chi_I(z) = 1$. In the latter case it also implements the function $\hat{f}(x, z) = f(x, z) \cdot \chi_I(z)$ on the basis of decomposition

$$\hat{f}(x, z) = \bigvee_{i=1}^{T} \chi_i(x, z)\phi(g_1^{(i)}, \ldots, g_p^{(i)}),$$

where $\chi_i(x, z)$ is the characteristic function of the ith segment in the partition of the collection τ and the functions $g_j^{(i)}$, $j = 1, \ldots, p$, are taken from the set G. Here, to implement each internal superposition, we take one formula Φ whose inputs are connected to those outputs of the upper elements of disjunction of formulas Ψ of the scheme $\widehat{\Sigma}$ where the corresponding functions from G are implemented.

Construction of the circuit Σ_f is terminated by disjunction of the outputs of its subcircuits $\widehat{\Sigma}$ and $\check{\Sigma}$, because $f = \widehat{f} \vee \check{f}$.

Putting

$$m = \lfloor 2\log n \rfloor\,, \; s'' = 2\left\lceil \frac{n - 3\log n}{2} \right\rceil, \quad N = \left\lceil \frac{2^{n-m}}{\log n} \right\rceil$$

and choosing the parameter $s' = s$ in the same manner as in Lemma 3 and the parameter p according to (19), by (16), (20), and (21) we obtain the upper bound (18).

The lemma is proved.

FUNDING

The work is supported by the Ministry of Education and Science of Russia within the program of realization of the Moscow Center of Fundamental and Applied Mathematics, agreement no. 075-15-2019-1621.

CONFLICT OF INTEREST

The author declares that he has no conflicts of interest.

REFERENCES

1. S. V. Yablonskii, *Introduction to Discrete Mathematics* (Nauka, Moscow, 1986).
2. O. B. Lupanov, *Asymptotic Estimates of Complexity of Control Circuits* (Izd-vo Mosk. Univ., Moscow, 1984).
3. S. A. Lozhkin, *Lectures on Foundations of Cybernetics* (Izd. Otd. Fakul'teta Vychislit. Mat. Mosk. Gos. Univ., Moscow, 2004).
4. O. B. Lupanov, "On a method for circuit synthesis," Izv. Vyssh. Uchebn. Zaved., Radiofiz. **1**, 120–140 (1958).
5. O. B. Lupanov, "On the complexity of realization of Boolean algebra functions by formulas," Probl. Kibern. **3**, 61–80 (1960).
6. S. A. Lozhkin, "High accuracy asymptotic bounds on the complexity of circuits of different types," Mat. Vopr. Kibern. **6**, 189–214 (1996).
7. S. A. Lozhkin, "High-accuracy asymptotic estimates for complexity of control systems," Doctoral Dissertation in Mathematics and Physics (Lomonosov Moscow State Univ., Moscow, 1997).
8. S. A. Lozhkin, "Synthesis of formulas whose complexity and depth do not exceed the asymptotically best estimates of high degree of accuracy," Moscow Univ. Math. Bull. **62**, 101–107 (2007). https://doi.org/10.3103/S0027132207030047
9. S. A. Lozhkin and A. E. Shiganov, "High accuracy asymptotic bounds on the BDD size and weight of the hardest functions," Fundam. Informaticae **104**, 239–253 (2010). https://doi.org/10.3233/FI-2010-347
10. S. A. Lozhkin and V. A. Konovodov, "On the synthesis and complexity of formulae with bounded depth of alternation," Moscow Univ. Comput. Math. Cybern. **36**, 81–91 (2012). https://doi.org/10.3103/S0278641912020021

Translated by E. Oborin