ISSN 0965-5425, Computational Mathematics and Mathematical Physics, 2015, Vol. 55, No. 4, pp. 724–730. © Pleiades Publishing, Ltd., 2015.
Original Russian Text © S.N. Selezneva, 2015, published in Zhurnal Vychislitel'noi Matematiki i Matematicheskoi Fiziki, 2015, Vol. 55, No. 4, pp. 730–736.

On the Multiplicative Complexity of Some Boolean Functions[1]

S. N. Selezneva

Moscow State University, Moscow, 119992 Russia

e-mail: selezn@cs.msu.su

Received March 5, 2014

Abstract—In this paper, we study the multiplicative complexity of Boolean functions. The multiplicative complexity of a Boolean function f is the smallest number of &-gates in circuits in the basis $\{x \,\&\, y, x \oplus y, 1\}$ such that each such circuit computes the function f. We consider Boolean functions which are represented in the form $x_1, x_2 \ldots x_n \oplus q(x_1, \ldots, x_n)$, where the degree of the function $q(x_1, \ldots, x_n)$ is 2. We prove that the multiplicative complexity of each such function is equal to $(n-1)$. We also prove that the multiplicative complexity of Boolean functions which are represented in the form $x_1 \ldots x_n \oplus r(x_1, \ldots, x_n)$, where $r(x_1, \ldots, x_n)$ is a multi-affine function, is, in some cases, equal to $(n-1)$.

DOI: 10.1134/S0965542515040119

Keywords: Boolean function, circuit, complexity, multiplicative complexity, upper bound.

1. INTRODUCTION

In this paper, we study the multiplicative complexity of Boolean functions. The multiplicative complexity of a Boolean function f is the smallest number of &-gates (binary multiplications) in circuits in the basis $\{x \,\&\, y, x \oplus y, 1\}$ such that each such circuit computes the function f. The multiplicative complexity of a function f is denoted by $\mu(f)$.

The multiplicative complexity of Boolean functions in the worst case was considered in [1, 2]. In [1], it was obtained that $\mu(n) = (1 + o(1)) \cdot 2^{n/2}$ for $\mu(n) = \max\limits_{f} \mu(f)$, where the index f runs over all functions of n variables. The multiplicative complexity of explicitly defined Boolean functions is studied [2–7]. In [2], an important class of symmetric functions was considered, and it was proved that the multiplicative complexity of each symmetric function of n variables is no more than $n + O(\sqrt{n})$. In [3], it was proved that $\mu(f) \geq n - 1$ holds for each function of the degree n, for example, for $x_1 \ldots x_n$. This is the best lower bound of the multiplicative complexity which is proved for explicitly defined functions of n variables. In [3], it was also shown that the multiplicative complexity of each multi-affine Boolean function of n variables is no more than $(n-1)$. In [3, 4], quadratic functions were studied. It was shown that the multiplicative complexity of each quadratic function of n variables is no more than $\lfloor n/2 \rfloor$, where $\lfloor a \rfloor$ is the greatest integer which is not more than a. Moreover, all quadratic functions f of n variables with $\mu(f) = \lfloor n/2 \rfloor$ were described. The multiplicative complexity of the threshold function of n variables with the thresholf of 2 was obtained in [5]. In [6, 7], the multiplicative complexity of some other functions was obtained.

In [8], a relation between the multiplicative complexity and the other circuit complexity of functions was studied. It was shown how to obtain a lower bound for the circuit complexity of a function in the basis of all functions of two variables, if the multiplicative complexity of this function is known. By some functions for which multiplicative complexity is no less than $(n-1)$, a $(7/3)n$ lower bound of the circuit complexity was obtained for the same functions. In [9], a relation between the multiplicative complexity and the additive complexity of functions was shown.

In this paper, we consider functions which are represented in the form $x_1 x_2 \ldots x_n \oplus q(x_1, \ldots, x_n)$, where $q(x_1, \ldots, x_n)$ is a quadratic function. We study the multiplicative complexity of such functions. There exist quadratic functions of n variables whose multiplicative complexity is equal to $\lfloor n/2 \rfloor$. We examine how the multiplicative complexity is changed if we add the term $x_1 \ldots \cdot x_n$ to such functions. We prove that the multiplicative complexity of each obtaining function of n variables becomes equal to $(n-1)$. Then we consider

[1] The article was translated by the author.

functions which are represented as a sum modulo 2 of two multi-affine functions. We prove that the multiplicative complexity of functions of the form $x_1 \ldots x_n \oplus r(x_1, \ldots, x_n)$, where $r(x_1, \ldots, x_n)$ is a multi-affine function, is, in some cases, equal to $(n - 1)$. To obtain our bounds of the multiplicative complexity, we apply similar approaches.

The paper is organized as follows. In Section 2, we introduce basic definitions and notation. In Section 3, we consider some properties of quadratic functions and prove bounds of the multiplicative complexity for some functions. In Section 4, we consider multi-affine functions and their properties and prove bounds of the multiplicative complexity for some sums modulo 2 of two multi-affine functions.

2. BASIC DEFINITIONS AND NOTATION

Boolean functions and their polynomial representations. Let $B = \{0, 1\}$. If $\alpha = (a_1, \ldots, a_n) \in B^n$ and $\beta = (b_1, \ldots, b_n) \in B^n$ then we say that $\alpha \le \beta$ iff $a_1 \le b_1, \ldots, a_n \le b_n$ $(n \ge 1)$. *The weight* $|\alpha|$ of n-tuple $\alpha = (a_1, \ldots, a_n) \in B^n$ is $\sum_{i=1}^{n} a_i$ (this sum is on integer numbers). If $\alpha = (a_1, \ldots, a_n) \in B^n$ then the monomial $m_\alpha = \prod_{a_i = 1} x_i$ *corresponds to* the tuple α. We assume that $m_{(0, \ldots, 0)} = 1$.

A Boolean function f of n variables is a mapping $f: B^n \longrightarrow B$, $n = 0, 1, \ldots$. Each Boolean function $f(x_1, \ldots, x_n)$ can be represented by an expression in the form

$$\bigoplus_{\alpha \in B^n : c_f(\alpha) = 1} m_\alpha,$$

where $c_f(\alpha) = \bigoplus_{\beta \le \alpha} f(\beta) \in B$ are coefficients, $\alpha \in B^n$, and $\oplus$ denotes addition modulo 2 (EXOR sum). This representation of Boolean functions is called *Zhegalkin polynomial*. It's known, that each Boolean function can uniquely be represented by a Zhegalkin polynomial. The degree $\deg(f)$ of a Boolean function $f(x_1, \ldots, x_n)$ is $\max_{\alpha \in B^n : c_f(\alpha) = 1} |\alpha|$.

Circuits and multiplicative complexity. *A circuit* in the basis $\{x \,\&\, y, x \oplus y, 1\}$ is a directed acyclic graph with nodes whose in-degree is 0 or 2. Nodes with the zero in-degree are marked by a variable from the set $\{x_1, \ldots, x_n\}$ or by the constant 1. Such nodes are called *inputs*. Nodes whose in-degree is 2 are marked by & or by $(\oplus)$. Such nodes are called *gates*. For each node v of a circuit there is a Boolean function such that this function is computed in this node. If v is an input with a variable x_i (or with the constant 1) then the Boolean function x_i (the constant 1) is computed in v. If edges from a node v_1 and from a node v_2 enter a node v, and Boolean functions f_1 and f_2 are computed in the nodes v_1 and v_2 respectively, and the node v has the mark & $(\oplus)$ then $f_1 \,\&\, f_2$ $(f_1 \oplus f_2)$ is computed in the node v. A circuit C *computes* a Boolean function f, if there exists a node in C in which f is computed.

The multiplicative complexity of a Boolean function f is the smallest number of &-gates in circuits in the basis $\{x \,\&\, y, x \oplus y, 1\}$ such that each such circuit computes the Boolean function $f(x_1, \ldots, x_n)$. The multiplicative complexity of a Boolean function f is denoted by $\mu(f)$.

3. THE MULTIPLICATIVE COMPLEXITY OF SOME BOOLEAN FUNCTIONS

A Boolean function f is called *quadratic*, if $\deg(f) = 2$. In [4], it is proved that $\mu(f) \le \lfloor n/2 \rfloor$ for an arbitrary quadratic function of n variables, and quadratic functions f of n variables for which $\mu(f) = \lfloor n/2 \rfloor$ holds are described. In this paper, we need the structure of some circuits for quadratic functions. Therefore, in this section, we formulate some results (Lemma 3.1) from [4]. Notice that we formulate this results in the form that is convenient for our purposes.

A Boolean function f is called *affine*, if $\deg(f) < 1$. Denote by A^n the set of all affine functions of the variables $x_1, \ldots, x_n$. An affine Boolean function f is called *linear*, if $c_f(0, \ldots, 0) = 0$. Denote by L^n the set of all linear functions of the variables $x_1, \ldots, x_n$. Linear (affine) functions of n variables $g_1, \ldots, g_m$ are called *linearly independent*, if

$$c_1 g_1 \oplus \ldots \oplus c_m g_m = 0,$$

where $c_1, ..., c_m \in B$, implies $c_1 = ... = c_m = 0$. Otherwise, the linear (affine) functions $g_1, ..., g_m$ are called *linearly dependent*. It's known that the set L^n is a linear space of dimension n.

An expression in the form

$$t \oplus \bigoplus_{i=1}^{l} g_i \cdot h_i,$$

where $g_1, ..., g_l, h_1, ..., h_l \in L^n$, and $h \in A^n$, is called *a quadratic pseudopolynomial expression* (for short, a QPP expression) of length l. It's easy to see, that each quadratic function is represented by a QPP expression, e.g., by its Zhegalkin polynomial. *The length* $l_2(f)$ of a quadratic function f in the class of QPPs is the minimal length among all QPP expressions that represent f. It's clear that $l_2(f) \le n(n-1)/2$ for an arbitrary quadratic function f of n variables. But a more stronger fact holds, namely $l_2(f) \le \lfloor n/2 \rfloor$ for an arbitrary quadratic function f of n variables [4].

If P is a QPP expression such that P represents a function f, and the length of P is equal to $l_2(f)$, then we say that P is *a minimal* QPP expression for f.

Lemma 3.1 ([4, 3]). *Let P be a minimal QPP expression for a quadratic Boolean function $f(x_1, ..., x_n)$, and P has the form $t \oplus \prod_{i=1}^{l} g_i \cdot h_i$, where $g_1, ..., g_l, h_1, ..., h_l \in L^n$, $t \in A^n$. Then the linear functions $g_1, ..., g_l, h_1, ..., h_l$ are linearly independent.*

Now we prove that the multiplicative complexity of an arbitrary function $f(x_1, ..., x_n)$ that is represented in the form $x_1 ... x_n \oplus q(x_1, ..., x_n)$, where q is a quadratic function, is equal to $(n-1)$.

Theorem 3.2. *If $n \ge 3$, and $f(x_1, ..., x_n)$ is a Boolean function that is represented in the form $x_1 ... x_n \oplus q(x_1, ..., x_n)$, where q is a quadratic Boolean function, then $\mu(f) = n - 1$.*

Proof. 1. *Upper bound.* Represent a quadratic function $q(x_1, ..., x_n)$ by its minimal QPP expression P. Let the QPP expression P be in the form $t \oplus \bigoplus_{i=1}^{l} g_i h_i$, where $g_i, h_i \in L^n$, $i = 1, ..., l$, $t \in A^n$. By Lemma 3.1, the linear functions $g_1,..., gl, h_1, ..., h_l$ are linearly independent. We obtain that $2l \le n$, because the dimension of the linear space L^n is n. Add linear functions $g_{2l+1}, ..., g_n \in L^n$ to the linear functions $g_1, ..., g_l, h_1, ..., h_l$ such that the linear functions $g_1, ..., g_l, h_1, ..., h_l, g_{2l+1}, ..., g_n$ are linearly independent. We can always do it, because the dimension of the linear space L^n is n.

Consider the product

$$\left(\prod_{i=1}^{l} g_i h_i\right) \cdot \left(\prod_{j=2l+1}^{n} g_i\right).$$

This product represents a certain Boolean function. Denote this function by $f_1(x_1, ..., x_n)$. Prove that the function $f_1(x_1, ..., x_n)$ is equal to $\prod_{i=1}^{n} (x_i \oplus a_i)$ for some $a_1,..., a_n \in B$. For this, we write the system of linear equations

$$\begin{gathered}
g_1(x_1, \ldots, x_n) = 1, \\
\ldots, \\
g_l(x_1, \ldots, x_n) = 1, \\
h_1(x_1, \ldots, x_n) = 1, \\
\ldots, \\
h_l(x_1, \ldots, x_n) = 1, \\
g_{2l+1}(x_1, \ldots, x_n) = 1, \\
\ldots, \\
g_n(x_1, \ldots, x_n) = 1.
\end{gathered} \tag{1}$$

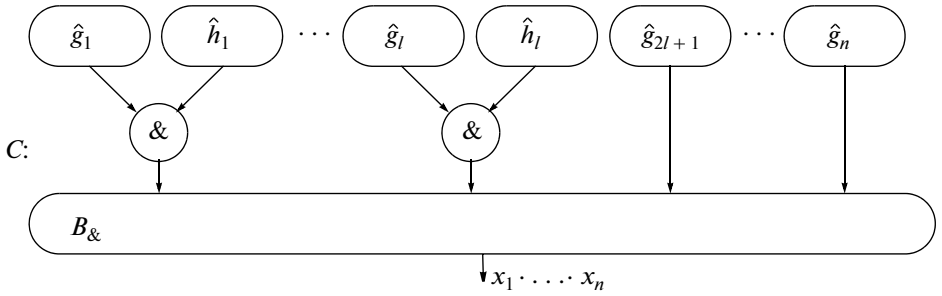

Fig. 1.

Notice, that if $x_1 = c_1, ..., x_n = c_n$ is a solution of the system (1), then the function $f_1(x_1, ..., x_n)$ is equal to 1 on the tuple $(c_1, ..., c_n) \in B^n$. And if the function $f_1(x_1, ..., x_n)$ is equal to 1 on the tuple $(d_1, ..., d_n) \in B^n$, then $x_1 = d_1, ..., x_n = d_n$ is a solution of the system (1).

The linear functions $g_1, ..., g_n, h_1, ..., h_l, g_{2l+1}, ..., g_n$ are linearly independent, therefore, by results of linear algebra, the system (1) has a unique solution $x_1 = b_1, ..., x_n = b_n$, where $b_1, ..., b_n \in B$. The Boolean function $\prod_{i=1}^{n}(x_i \oplus b_i \oplus 1)$ is equal to 1 on the single tuple $(b_1, ..., b_n) \in B^n$. Therefore, the expressions

$$\left(\prod_{i=1}^{l} g_i h_i\right) \cdot \left(\prod_{j=2l+1}^{n} g_i\right) \quad \text{and} \quad \prod_{i=1}^{n}(x_i \oplus b_i \oplus 1)$$

represent the same function $f_1(x_1, ..., x_n)$.

Denote $b_i \oplus 1$ by a_i, $i = 1, ..., n$. It's easy to see, that $f_1(x_1 \oplus a_1, ..., x_n \oplus a_n) = x_1 \ldots x_n$. Denote $g_i(x_1 \oplus a_1, ..., x_n \oplus a_n)$ by $\hat{g}_i(x_1, ..., x_n)$, $i = 1, ..., l, 2l+1, ..., n$. Denote $h_i(x_1 \oplus a_1, ..., x_n \oplus a_n)$ by $\hat{h}_i(x_1, ..., x_n)$, $i = 1, ..., l$. Then

$$x_1 \cdot \ldots \cdot x_n = \left(\prod_{i=1}^{l} \hat{g}_i \hat{h}_i\right) \cdot \left(\prod_{j=2l+1}^{n} \hat{g}_i\right).$$

Therefore, we can construct a circuit that computes the product $x_1 \ldots x_n$ by the following way (see Fig. 1).

The block $B_\&$ computes the conjunction of its $(n-1)$ inputs by $(n-1-l)$ &-gates. Therefore, this circuit C has $(n-1)$ &-gates.

Notice, that $g_i(x_1, ..., x_n)h_i(x_1, ..., x_n) = \hat{g}_i(x_1, ..., x_n)\hat{h}_i(x_1, ..., x_n) \oplus \hat{t}_i(x_1, ..., x_n)$ for some $\hat{t}_1, ..., \hat{t}_l \in A^n$. Therefore,

$$q(x_1, \ldots, x_n) = \hat{t}(x_1, \ldots, x_n) \oplus \bigoplus_{i=1}^{l} \hat{g}_i(x_1, \ldots, x_n)\hat{h}_i(x_1, \ldots, x_n),$$

where $\hat{t}(x_1, ..., x_n) = \bigoplus_{i=1}^{l} \hat{t}_i(x_1, \ldots, x_n) \in A^n$.

Hence, we can construct a circuit that computes f by the following way (see Fig. 2).

The block C is in Fig. 1. This block has $(n-1)$ &-gates. To compute the affine function $\hat{t}$ we don't need &-gates. The block $B_\oplus$ computes a sum modulo 2 of functions $\hat{g}_1\hat{h}_1, ..., \hat{g}_l\hat{h}_l, x_1 \ldots x_n$ that have been already computed at the block C. The block $B_\oplus$ has no &-gates. Thus, the circuit C_f computes the function f, and this circuit has $(n-1)$ &-gates.

We obtain that $\mu(f) \le n-1$.

2. *Lower bound.* It's known [3] that $\mu(f) \ge \deg(f) - 1$. Therefore, $\mu(f) \ge n-1$.

Hence, by the upper bound and the lower bound, we obtain that $\mu(f) = n-1$.

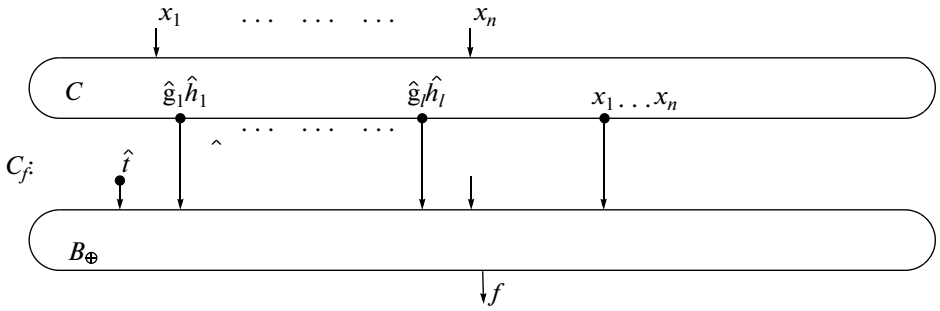

Fig. 2.

Corollary 3.2.1. If $n \geq 3$, $f(x_1, ..., x_n)$ is a Boolean function such that for some $g_1, ..., g_n \in A^n$ the Boolean function $f(g_1(x_1, ..., x_n), ..., g_n(x_1, ..., x_n))$ has the form $x_1 ... x_n \oplus q(x_1, ..., x_n)$, where q is a quadratic function, then $\mu(f) = n - 1$.

4. THE MULTIPLICATIVE COMPLEXITY OF SUMS OF MULTI-AFFINE BOOLEAN FUNCTIONS

A Boolean function f is called *multi-affine*, if f is represented in the form $\prod_{i=1}^{m} h_i$, where $h_1, ..., h_m$ are affine functions. Multi-affine functions are considered in [10] in connection with satisfiability problems. In [3] it was proved that $\mu(f) = \mathrm{def}(f) - 1$ for each multi-affine function f. We formulate some results from [3] (Lemma 4.1) that we need here.

Lemma 4.1 ([3]). *If $(x_1, ..., x_n)$ is a multi-affine Boolean function, and $f \neq 0$, then f can be represented in the form $\prod_{i=1}^{l} (g_i \oplus b_i)$, where $b_1, ..., b_l \in B$, $g_1, ..., g_l \in L^n$ are linearly independent, and $l = \deg(f)$.*

We see [3] that the multiplicative complexity of each multi-affine function of n variables is no more than $(n - 1)$. We consider functions which are represented in the form $x_1 ... x_n \oplus r(x_1, ..., x_n)$, where $r(x_1, ..., x_n)$ is a multi-affine function. We prove that the multiplicative complexity of such functions is, in some cases, equal to $(n - 1)$.

Theorem 4.2. *If a Boolean function $f(x_1, ..., x_n)$ is represented in the form $x_1 ... x_n \oplus r(x_1, ..., x_n)$, where $r(x_1, ..., x_n)$ is a multi-affine function, $r(1, ..., 1) = 1$, and $\deg(r) < n$, then $\mu(f) = n - 1$.*

Proof. 1. *Upper bound.* By Lemma 4.1, the function $r(x_1, ..., x_n)$ can be represented in the form $\prod_{i=1}^{l} g_i$, where $g_1, ..., g_l \in A^n$, $g_1, ..., g_l$ are linearly independent, and $l = \deg(r)$. But $\deg(r) < n$, therefore $l < n$. Consider the system of linear equations

$$\begin{aligned} g_1(x_1, \ldots, x_n) &= 1, \\ &\ldots, \\ g_l(x_1, \ldots, x_n) &= 1. \end{aligned} \tag{2}$$

Since $r(1, ..., 1) = 1$, we conclude that $x_1 = 1, ..., x_n = 1$ is a solution of the system (2). Add equations

$$\begin{aligned} g_{l+1}(x_1, \ldots, x_n) &= 1, \\ &\ldots, \\ g_n(x_1, \ldots, x_n) &= 1, \end{aligned}$$

where $g_{l+1}, \ldots, g_n \in A^n$, to the system (2) such that the system

$$\begin{gathered} g_1(x_1, \ldots, x_n) = 1, \\ \ldots, \\ g_l(x_1, \ldots, x_n) = 1, \\ g_{l+1}(x_1, \ldots, x_n) = 1, \\ \ldots, \\ g_n(x_1, \ldots, x_n) = 1 \end{gathered} \tag{3}$$

has a single solution, and this solution is $x_1 = 1, \ldots, x_n = 1$. We always do it, because the function $g_1, \ldots, g_l$ are linearly independent, and $x_1 = 1, \ldots, x_n = 1$ is a solution of the system (2). Then the expression $\prod_{i=1}^{l} g_i$ represents the Boolean function $x_1 \cdot \ldots \cdot x_n$. Therefore,

$$f(x_1, \ldots, x_n) = x_1 \ldots x_n \oplus \prod_{i=1}^{l} g_i = \prod_{i=1}^{n} g_i \oplus \prod_{i=1}^{l} g_i = \left(\prod_{i=1}^{l} g_i\right) \cdot \left(1 \oplus \prod_{j=l+1}^{n} g_j\right).$$

By this expression, it's clear how to construct a circuit that computes the function f, and that has $(n-1)$ &-gates.

2. *Lower bound.* Since $\deg(f) = n$, from [3] we obtain that $\mu(f) \geq n - 1$.

Hence, we obtain that $\mu(f) = n - 1$.

For example, by Theorem 4.2, we can conclude that the multiplicative complexity of the Boolean function $x_1 \ldots x_n \oplus (x_1 \oplus x_2 \oplus x_3)(x_2 \oplus x_3 \oplus 1)$ is equal to $(n-1)$, if $n \geq 4$.

Corollary 4.2.1. If a Boolean function $f(x_1, \ldots, x_n)$ is represented in the form $f_1(x_1, \ldots, x_n) \oplus f_2(x_1, \ldots, x_n)$, where the functions f_1, f_2 are multi-affine, $\deg(f) = n$, and there exists a tuple $\alpha \in B^n$ such that $f_1(\alpha) = f_2(\alpha) = 1$, then $\mu(f) = n - 1$.

Proof. Assume that $\alpha = (a_1, \ldots, a_n) \in B^n$. Without lost of generality, assume that $\deg(f_1) = n$, and $\deg(f_2) < n$. By Lemma 4.1 the multi-affine function $f_1(x_1, \ldots, x_n)$ can be represented in the form $\prod_{i=1}^{l} g_i$, where $g_1, \ldots, g_l \in A^n$, $g_1, \ldots, g_l$ are linearly independent, and $l = \deg(f_1)$. But $\deg(f_1) = n$, therefore $l = n$. Hence, the system of linear equations

$$\begin{gathered} g_1(x_1, \ldots, x_n) = 1, \\ \ldots, \\ g_n(x_1, \ldots, x_n) = 1 \end{gathered}$$

has a single solution, and this solution is $x_1 = a_1, \ldots, x_n = a_n$. Hence, the function $f_1(x_1, \ldots, x_n)$ has the form $\prod_{i=1}^{n} (x_i \oplus a_i \oplus 1)$. Denote $a_i \oplus 1$ by b_i, $i = 1, \ldots, n$.

Consider the Boolean function

$$\hat{f}(x_1, \ldots, x_n) = f(x_1 \oplus b_1, \ldots, x_n \oplus b_n).$$

The function $\hat{f}(x_1, \ldots, x_n)$ has the form $x_1 \ldots x_n \oplus \hat{f}_2(x_1, \ldots, x_n)$, where $\hat{f}_2(x_1, \ldots, x_n)$ is a multi-affine, and $\deg(\hat{f}_2) < n$. Moreover,

$$\hat{f}_2(1, \ldots, 1) = f_2(1 \oplus b_1, \ldots, 1 \oplus b_n) = f_2(\alpha) = 1.$$

Apply Theorem 4.2 to the function $\hat{f}$. We obtain that $\mu(\hat{f}) \leq n - 1$.

Since $f(x_1, \ldots, x_n) = \hat{f}(x_1 \oplus b_1, \ldots, x_n \oplus b_n)$, we obtain that $\mu(f) \leq n - 1$.

From [3] $\mu(f) \geq n - 1$, because $\deg(f) = n$.

Hence, we obtain that $\mu(f) = n - 1$.

5. CONCLUSIONS

In this paper, we proved that $\mu(f) = n - 1$, if $f(x_1, ..., x_n)$ is represented in the form $x_1 ... x_n \oplus q(x_1, ..., x_n)$, where q is a quadratic function, and if $f(x_1, ..., x_n)$ is represented in the form $x_1 ... x_n \oplus r(x_1, ..., x_n)$, where $r(x_1, ..., x_r)$ is a multi-affine function for which $\deg(r) < n$, and $r(1, ..., 1) = 1$.

ACKNOWLEDGMENTS

The paper is supported by the Russian Foundation for Basic Research, grants 13-01-00684-a, 13-01-00958-a.

REFERENCES

1. E. I. Nechiporuk, "On the complexity of schemes in some bases containing nontrivial elements with zero weights," *Problems in Cybernetics* (Fizmatlit, Moscow, 1962), Vol. 8, pp. 123–160 [in Russian].
2. J. Boyar, R. Peralta, and D. Pochuev, "On the multiplicative complexity of boolean functions over the basis $\{\wedge, \oplus, 1\}$," Theor. Comput. Sci. **235**, 43–57 (2000).
3. C. P. Schnorr, "The multiplicative complexity of Boolean functions," *Proceedings of the 6th International Conference AAECC-6*, Lecture Notes Comput. Sci. (Springer, Berlin, 1989), Vol. 357, pp. 45–58.
4. R. Mirwald and C. P. Schnorr, "The multiplicative complexity of quadratic Boolean forms," Theor. Comput. Sci. **102**, 307–328 (1992).
5. J. Boyar, R. Peralta, and D. Pochuev, "Concrete multiplicative complexity of symmetric functions," Technical Report YALEU/DCS/TR1219, Computer Science Department (Yale University, 2001).
6. J. Boyar and R. Peralta, "The exact multiplicative complexity of the Hamming weight function," Electron. Colloquium Comput. Complexity **12** (2005).
7. T. I. Krasnova, "On the conjunction complexity of circuits in the Zhegalkin basis for one sequence of Boolean functions," *Proceedings of the 11th International Seminar on Discrete Mathematics and Its Applications* (Moscow, Mosk. Gos. Univ., 2012), pp. 138–141.
8. A. Kojevnikov and A. S. Kulikov, "Circuit complexity and multiplicative complexity of Boolean functions," *Proceedings of the 6th Conference on Computability (CiE 2010)*, Lecture Notes Comput. Sci. (Springer, Berlin, 2010), Vol. 6158, pp. 239–245.
9. I. S. Sergeev, "A relation between additive and multiplicative complexity of Boolean functions," arXiv:1303.4177 (2013).
10. T. J. Schaefer, "The complexity of satisfiability problems," *Proceedings of the 10th ACM Symposium on Theory of Computing* (ACM, New York, 1978), pp. 216–226.
11. S. V. Yablonskii, *Introduction to Discrete Mathematics* (Mir, Moscow, 1989; Vysshaya Shkola, Moscow, 2001).
12. A. G. Kurosh, *A Course in Higher Algebra* (Nauka, Moscow, 1971; Mir, Moscow, 1975).