АЛГЕБРО-ЛОГИЧЕСКИЕ МЕТОДЫ В ИНФОРМАТИКЕ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

ALGEBRAIC AND LOGICAL METHODS IN COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE

Серия «Математика»
2019. Т. 30. С. 125—140

Онлайн-доступ к журналу:
http://mathizv.isu.ru

ИЗВЕСТИЯ
Иркутского государственного университета

УДК 519.714.4
MSC 68Q17
DOI https://doi.org/10.26516/1997-7670.2019.30.125

Complexity Lower Bound for Boolean Functions in the Class of Extended Operator Forms[*]

A. S. Baliuk
Irkutsk State University, Irkutsk, Russian Federation

Abstract. Starting with the fundamental work of D.E.Muller in 1954, the polynomial representations of Boolean functions are widely investigated in connection with the theory of coding and for the synthesis of circuits of digital devices. The operator approach to polynomial representations, proposed in the works of S. F. Vinokurov, made it possible, on the one hand, to uniformly describe all known types of polynomial forms of Boolean functions, and, on the other hand, to generalize them to the case of expansions by the operator images of arbitrary odd function, not only conjunction.

In the study of polynomial and, in the general case, operator forms, one of the main questions is obtaining lower and upper bounds of the complexity of the representation of Boolean functions in various classes of forms. The upper bounds of complexity are actually algorithms for minimizing Boolean functions in a particular class of forms.

The lower bounds of complexity can be divided into two types: combinatorial and effective. Combinatorial lower bounds make it possible to prove the existence of Boolean functions, having high complexity, without finding the explicit form of these functions. Effective lower bounds are based on explicit constructing Boolean functions that have high complexity in a particular class of forms.

In this paper, using an algebraic extension of a finite field of order 2, we obtain a lower bound for the complexity of Boolean functions in the class of extended operator forms. This lower bound strengthens the previously known lower bounds for this class

[*] This work was supported by Russian Foundation for Basic Research, grant N 19–01–00200.

of operator forms and is becoming asymptotically optimal if the sequence of Mersenne primes is infinite.

Keywords: Boolean function, lower bound, extension of finite field, Mersenne prime.

1. Introduction

In the initial work [9] Muller introduced several polynomial forms of Boolean functions. Since that, these and many other polynomial forms were widely investigated.

The uniform approach to polynomial forms of Boolean functions were proposed in [12], using the notion of operators and their bundles. In section 2 of the current paper we suggest another way to represent operators and bundles, using vectors and matrices. Such a way could be naturally generalized to multivalued functions, including functions over finite fields [3].

One of the problems in the area of Boolean functions polynomial representation is obtaining lower bounds of complexity in particular classes of polynomial, and more general, of operator forms. This paper is devoted to obtaining lower bound for the class of extended operator forms. To achieve this result we developed a method for counting zeros in vectors over arbitrary finite field, which is described in section 3.

An extended list of references on the complexity for polynomial forms of Boolean functions and multivalued functions can be found in [11].

2. Matrix representations of bundles of operators

Definition 1. *A word $\mathfrak{a}_n \dots \mathfrak{a}_1$ over the alphabet $\{\mathfrak{d}, \mathfrak{e}, \mathfrak{p}\}$ will be called* n-ary operator*.*

Let us construct the map v from the set of operators to Boolean vectors recursively as follows: $v(\mathfrak{a}_n \dots \mathfrak{a}_1) = v(\mathfrak{a}_n) \otimes v(\mathfrak{a}_{n-1} \dots \mathfrak{a}_1)$ for $n \geqslant 2$ and $v(\mathfrak{d}) = (11)$, $v(\mathfrak{e}) = (01)$, $v(\mathfrak{p}) = (10)$ for $n = 1$. The symbol $\otimes$ denotes the tensor product of vectors. For the sake of convenience let us introduce the vector (1), which corresponds to the 0-ary operator $\varnothing$, i.e. to empty word. As tensor product $\otimes$ is an associative operation we can simply write $v(\mathfrak{a}_n \dots \mathfrak{a}_1) = v(\mathfrak{a}_n) \otimes \dots \otimes v(\mathfrak{a}_1)$.

Let $N = 2^n$ and $\sigma^1, \dots, \sigma^N$ be all pairwise different binary n-tuples ordered lexicographically such that $j = 1 + \sigma^j_n 2^{n-1} + \dots + \sigma^j_2 2^1 + \sigma^j_1 2^0$ where σ^j_i denotes ith component of the tuple σ^j.

For every tuple $S = (g_1, \dots, g_N)$ of n-ary Boolean functions let us define a matrix M_S in the following way:

$$M_S = \begin{pmatrix} M_{11} & \dots & M_{1N} \\ \vdots & \ddots & \vdots \\ M_{N2} & \dots & M_{NN} \end{pmatrix}, \tag{2.1}$$

where $M_{jk} = g_j(\sigma_n^k, \dots, \sigma_1^k)$. For every n-ary Boolean function g let us define the tuple $S_g = (g_1, \dots, g_N)$, assuming that for all $1 \leqslant j \leqslant N$

$$g_j(x_n, \dots, x_1) = g(x_n \oplus \sigma_n^{N-j+1}, \dots, x_1 \oplus \sigma_1^{N-j+1}). \tag{2.2}$$

Proposition 1. *$g(x_n, \dots, x_1) = x_n \cdot \dots \cdot x_1$ iff M_{S_g} is an identity matrix.*

Proof. Let $g(x_n, \dots, x_1) = x_n \cdot \dots \cdot x_1$. By definition, $S_g = (g_1, \dots, g_N)$, where $g_j(x_n, \dots, x_1) = (x_n \oplus \sigma_n^{N-j+1}) \cdot \dots \cdot (x_1 \oplus \sigma_1^{N-j+1})$. If M_{S_g} has the form (2.1), then $M_{jk} = (\sigma_n^k \oplus \sigma_n^{N-j+1}) \cdot \dots \cdot (\sigma_1^k \oplus \sigma_1^{N-j+1})$. The binary tuples $\sigma^1, \dots, \sigma^N$ are ordered lexicographically. Thus, $\sigma^1 = (0, \dots, 0)$ and $\sigma^N = (1, \dots, 1)$. Further, σ^k is the k-th tuple from the beginning, and σ^{N-j+1} is the j-th tuple from the end. For σ^k, there is exactly one tuple which differs from σ^k in each component. It is σ^{N-k+1}. Consequently, $M_{jk} = (\sigma_n^k \oplus \sigma_n^{N-j+1}) \cdot \dots \cdot (\sigma_1^k \oplus \sigma_1^{N-j+1}) = 1$ if and only if $j = k$. Otherwise, $M_{jk} = 0$. This means that the matrix M_{S_g} is the identity matrix.

Conversely, let M be the identity $N \times N$ matrix of the form (2.1), and let n-ary Boolean functions $g_1, \dots, g_N$ are given by $g_j(\sigma_n^k, \dots, \sigma_1^k) = M_{jk}$, where $1 \leqslant j, k \leqslant N$. Then $g_j(\sigma_n^k, \dots, \sigma_1^k) = 1$ if and only if $M_{jk} = 1$, i.e. $k = j$. Further, $g_j(x_n, \dots, x_1) = 1$ only if $x_n = \sigma_n^j, \dots, x_1 = \sigma_1^j$. This means that $g_j(x_n, \dots, x_1) = (x_n \oplus \bar{\sigma}_n^j) \cdot \dots \cdot (x_1 \oplus \bar{\sigma}_1^j)$. Since $(\bar{\sigma}_n^j, \dots, \bar{\sigma}_1^j)$ is different from σ^j in each element, we have $(\bar{\sigma}_n^j, \dots, \bar{\sigma}_1^j) = \sigma^{N-j+1}$, and therefore $g_j(x_n, \dots, x_1) = (x_n \oplus \sigma_n^{N-j+1}) \cdot \dots \cdot (x_1 \oplus \sigma_1^{N-j+1})$. This means that $(g_1, \dots, g_N) = S_g$, where $g(x_n, \dots, x_1) = x_n \cdot \dots \cdot x_1$, and $M = M_{S_g}$. □

Following [5], let us define the action of an operator $\mathfrak{a}_n \dots \mathfrak{a}_1$ on an n-ary Boolean function g as follows: $\mathfrak{a}_n \dots \mathfrak{a}_1 g = f_n$, where for all $1 \leqslant m \leqslant n$

$$f_m(x_n, \dots, x_1) = \begin{cases} f_{m-1}(x_n, \dots, \bar{x}_m, \dots x_1) \oplus f_{m-1}(x_n, \dots, x_1), \text{ if } \mathfrak{a}_m = \mathfrak{d}; \\ f_{m-1}(x_n, \dots, x_1), \text{ if } \mathfrak{a}_m = \mathfrak{e}; \\ f_{m-1}(x_n, \dots, x_{m+1}, \bar{x}_m, x_{m-1}, \dots x_1), \text{ if } \mathfrak{a}_m = \mathfrak{p}; \end{cases} \tag{2.3}$$

and $f_0(x_n, \dots, x_1) = g(x_n, \dots, x_1)$.

For every n-ary Boolean function f let us introduce the binary vector V_f, assuming $V_f = (V_1, \dots, V_N)$ where $V_k = f(\sigma_n^k, \dots, \sigma_1^k)$ for all $1 \leqslant k \leqslant N$.

Proposition 2. *For every n-ary Boolean function g and every n-ary operator $\mathfrak{a}_n \dots \mathfrak{a}_1$ if $f = \mathfrak{a}_n \dots \mathfrak{a}_1 g$, then $V_f = v(\mathfrak{a}_n \dots \mathfrak{a}_1) M_{S_g}$.*

Proof. Let $\mathfrak{a}_n \dots \mathfrak{a}_1$ be an n-ary operator. Recall through $J_\mathfrak{d}$ the set of indices m for which $\mathfrak{a}_m = \mathfrak{d}$, and through $J_\mathfrak{p}$ the set of indices m for which $\mathfrak{a}_m = \mathfrak{p}$. Denote by $P(J_\mathfrak{d})$ the set of all subsets of $J_\mathfrak{d}$, including the empty set. First of all, note that since $j = 1 + \sigma^j_n 2^{n-1} + \dots + \sigma^j_1 2^0$ then

$$\sigma^{j+2^{m-1}} = (\sigma^j_n, \dots, \sigma^j_{m+1}, \bar{\sigma}^j_m, \sigma^j_{m-1}, \dots, \sigma^j_1) \tag{2.4}$$

holds for all $1 \leqslant j \leqslant 2^{m-1} \leqslant N$. Define sets of integers

$$I_m = \Big\{ 1 + \sum_{\substack{s \in J_\mathfrak{p} \\ s \leqslant m}} 2^{s-1} + \sum_{\substack{s \in S \\ s \leqslant m}} 2^{s-1} \;\Big|\; S \in P(J_\mathfrak{d}) \Big\}.$$

Obviously, $j \leqslant 2^m$ for all $j \in I_m$. Also define the vectors $V^m = v(\mathfrak{a}_m \dots \mathfrak{a}_1)$.

By induction, we will show that if f_m is defined in the same way as in (2.3), then $V^m_j = 1$ if and only if $2^m - j + 1 \in I_m$, as well as

$$f_m(\sigma^k_n, \dots, \sigma^k_1) = \sum_{j \in I_m} g(\sigma^k_n \oplus \sigma^j_n, \dots, \sigma^k_1 \oplus \sigma^j_1).$$

By the basis, we have $I_0 = \{1\}$, $V^0 = (1)$, $\sigma^1 = (0, \dots, 0)$. Thus, $V^0_j = 1$ if and only if $2^0 - j + 1 \in I_0$, and

$$\sum_{j \in I_0} g(\sigma^k_n \oplus \sigma^j_n, \dots, \sigma^k_1 \oplus \sigma^j_1) = g(\sigma^k_n, \dots, \sigma^k_1) = f_0(\sigma^k_n, \dots, \sigma^k_1).$$

By the step of induction, we take $\mathfrak{a}_m$.

1) If $\mathfrak{a}_m = \mathfrak{d}$, then $I_m = I_{m-1} \cup I^*_{m-1}$, where $I^*_{m-1} = \{ j + 2^{m-1} \mid j \in I_{m-1} \}$. By the induction hypothesis, $f_{m-1}(\sigma^k_n, \dots, \sigma^k_1) = \sum\limits_{j \in I_{m-1}} g(\sigma^k_n \oplus \sigma^j_n, \dots, \sigma^k_1 \oplus \sigma^j_1)$.

Thus, $\sum\limits_{j \in I^*_{m-1}} g(\sigma^k_n \oplus \sigma^j_n, \dots, \sigma^k_1 \oplus \sigma^j_1) = \sum\limits_{j \in I_{m-1}} g(\sigma^k_n \oplus \sigma^{j+2^{m-1}}_n, \dots, \sigma^k_1 \oplus \sigma^{j+2^{m-1}}_1)$

$$= \sum_{j \in I_{m-1}} g(\sigma^k_n \oplus \sigma^j_n, \dots, \sigma^k_m \oplus \bar{\sigma}^j_m, \dots, \sigma^k_1 \oplus \sigma^j_1) = f_{m-1}(\sigma^k_n, \dots, \bar{\sigma}^k_m, \dots, \sigma^k_1)$$

$$\begin{aligned} f_m(\sigma^k_n, \dots, \sigma^k_1) &= f_{m-1}(\sigma^k_n, \dots, \sigma^k_1) + f_{m-1}(\sigma^k_n, \dots, \bar{\sigma}^k_m, \dots, \sigma^k_1) \\ &= \sum_{j \in I_{m-1}} g(\sigma^k_n \oplus \sigma^j_n, \dots, \sigma^k_1 \oplus \sigma^j_1) + \sum_{j \in I^*_{m-1}} g(\sigma^k_n \oplus \sigma^j_n, \dots, \sigma^k_1 \oplus \sigma^j_1) \\ &= \sum_{j \in I_m} g(\sigma^k_n \oplus \sigma^j_n, \dots, \sigma^k_1 \oplus \sigma^j_1). \end{aligned}$$

Also, we have $V^m = (11) \otimes V^{m-1} = (V^{m-1}_1, \dots, V^{m-1}_{2^{m-1}}, V^{m-1}_1, \dots, V^{m-1}_{2^{m-1}})$. Hence, if $j \leqslant 2^{m-1}$, then $V^m_j = 1$ if and only if $2^{m-1} - j + 1 \in I_{m-1}$, and if $2^{m-1} < j \leqslant 2^m$, then $V^m_j = 1$ if and only if $2^{m-1} - (j - 2^{m-1}) + 1 \in I_{m-1}$.

In the first case, we have $2^m - (j + 2^{m-1}) + 1 \in I_{m-1}$, in the second case we have $2^m - j + 1 \in I_{m-1}$ and, therefore, $V_j^m = 1$ if and only if $2^m - j + 1 \in I_m$.
2) If $\mathfrak{a}_m = \mathfrak{e}$, then $I_m = I_{m-1}$,

$$f_m(\sigma_n^k, \dots, \sigma_1^k) = f_{m-1}(\sigma_n^k, \dots, \sigma_1^k) =$$
$$= \sum_{j \in I_{m-1}} g(\sigma_n^k \oplus \sigma_n^j, \dots, \sigma_1^k \oplus \sigma_1^j) = \sum_{j \in I_m} g(\sigma_n^k \oplus \sigma_n^j, \dots, \sigma_1^k \oplus \sigma_1^j).$$

Since $V^m = (01) \otimes V^{m-1} = (0, \dots, 0, V_1^{m-1}, \dots, V_{2^{m-1}}^{m-1})$, we have $V_j^m = 1$ if and only if $2^{m-1} - (j - 2^{m-1}) + 1 \in I_{m-1}$. The latter means that $2^m - j + 1 \in I_m$.
3) If $\mathfrak{a}_m = \mathfrak{p}$, then $I_m = \{j + 2^{m-1} \mid j \in I_{m-1}\}$ and

$$\sum_{j \in I_m} g(\sigma_n^k \oplus \sigma_n^j, \dots, \sigma_1^k \oplus \sigma_1^j) = \sum_{j \in I_{m-1}} g(\sigma_n^k \oplus \sigma_n^j, \dots, \bar{\sigma}_m^k \oplus \sigma_m^j, \dots, \sigma_1^k \oplus \sigma_1^j)$$
$$= f_{m-1}(\sigma_n^k, \dots, \bar{\sigma}_m^k, \dots, \sigma_1^k) = f_m(\sigma_n^k, \dots, \sigma_1^k).$$

In this case, $V^m = (10) \otimes V^{m-1} = (V_1^{m-1}, \dots, V_{2^{m-1}}^{m-1}, 0, \dots, 0)$ and, therefore, $V_j^m = 1$ if and only if $2^{m-1} - j + 1 \in I_{m-1}$ or $2^m - j + 1 \in I_m$, which is the same.

At this point, we have $f(\sigma_n^k, \dots, \sigma_1^k) = \sum_{j \in I_n} g(\sigma_n^k \oplus \sigma_n^j, \dots, \sigma_1^k \oplus \sigma_1^j)$ for $f = \mathfrak{a}_n \dots \mathfrak{a}_1 g$. Now consider k-th element of the product $v(\mathfrak{a}_n \dots \mathfrak{a}_1) M_{S_g}$. According to (2.2) it is equal to

$$\sum_{j=1}^{N} V_j^n g(\sigma_n^k \oplus \sigma_n^{N-j+1}, \dots, \sigma_1^k \oplus \sigma_1^{N-j+1}) = \sum_{j \in I_n} g(\sigma_n^k \oplus \sigma_n^j, \dots, \sigma_1^k \oplus \sigma_1^j).$$

This means that $V_f = v(\mathfrak{a}_n \dots \mathfrak{a}_1) M_{S_g}$ and completes the proof. □

Definition 2. *A* bundle *of n-ary operators is a set $\mathfrak{A}$, which contains of N pairwise different n-ary operators.*

Definition 3. *A bundle is called* generated by a pair *or just* pair-generated *if it can be represented as $\mathfrak{A} = \{\mathfrak{a}_n^1 \dots \mathfrak{a}_1^1, \mathfrak{a}_n^2 \dots \mathfrak{a}_1^2, \dots, \mathfrak{a}_n^N \dots \mathfrak{a}_1^N\}$ where $\mathfrak{a}_j^k = \mathfrak{a}_j^1$ if $\sigma_j^k = 0$ and $\mathfrak{a}_j^k = \mathfrak{a}_j^N$ if $\sigma_j^k = 1$. In this case, the operators $\mathfrak{a}_n^1 \dots \mathfrak{a}_1^1$ and $\mathfrak{a}_n^N \dots \mathfrak{a}_1^N$ are called* generators *or* generating operators *for the bundle $\mathfrak{A}$.*

An $N \times N$ Boolean matrix M *represents* a bundle of n-ary operators $\mathfrak{A} = \{\mathfrak{a}_n^k \dots \mathfrak{a}_1^k \mid 1 \leqslant k \leqslant N\}$ if the elements of k-th row of the matrix M are pairwise equal to the corresponding elements of the vector $v(\mathfrak{a}_n^k \dots \mathfrak{a}_1^k)$. As operators in a bundle can be ordered in various ways, a matrix, representing the bundle, is not uniquely determined. But all such matrices can be reduced to each other by permutation of their rows.

For the sake of convenience, let us introduce the following notation. Let $V = (V_1, \dots, V_m)$ be a Boolean vector. Then, the number of zero elements of the vector V is denoted by $Z(V)$, i.e. $Z(V) = \#\{i \mid V_i = 0,\ 1 \leqslant i \leqslant m\}$.

Definition 4. *Let $\mathfrak{A} = \{\mathfrak{a}_n^k \dots a_1^k \mid 1 \leqslant k \leqslant N\}$ be a bundle of n-ary operators. If every n-ary Boolean function f can be represented as*

$$f(x_1, \dots, x_n) = C_1 \mathfrak{a}_n^1 \dots \mathfrak{a}_1^1 (x_n \cdot \dots \cdot x_1) \oplus \dots \oplus C_N \mathfrak{a}_n^N \dots \mathfrak{a}_1^N (x_n \cdot \dots \cdot x_1) \quad (2.5)$$

where $C = (C_1, \dots, C_N)$ is a Boolean vector, then the bundle $\mathfrak{A}$ is called base *and the value $L_{\mathfrak{A}}(f) = N - Z(C)$ is called* the complexity *of the representation of Boolean function f by images of operators from the bundle $\mathfrak{A}$.*

Proposition 3. *If $\mathfrak{A}$ is a base bundle of n-ary operators, and $M_{\mathfrak{A}}$ is a matrix, representing the bundle $\mathfrak{A}$, then $M_{\mathfrak{A}}$ is non-degenerate. Moreover, for arbitrary n-ary Boolean functions f it holds that $L_{\mathfrak{A}}(f) = N - Z(V_f M_{\mathfrak{A}}^{-1})$.*

Proof. Let $\mathfrak{A} = \{\mathfrak{a}_n^k \dots a_1^k \mid 1 \leqslant k \leqslant N\}$ be a base bundle of n-ary operators. For each j, $1 \leqslant j \leqslant N$, take a Boolean vector $C^j = (C_1^j, \dots, C_N^j)$ and a Boolean function $f_j(x_n, \dots, x_1) = (x_n \oplus \sigma_n^{N-j+1}) \cdot \dots \cdot (x_1 \oplus \sigma_1^{N-j+1})$ such that $f_j(x_n, \dots, x_1) = C_1^j \mathfrak{a}_n^1 \dots \mathfrak{a}_1^1 (x_n \cdot \dots \cdot x_1) \oplus \dots \oplus C_N^j \mathfrak{a}_n^N \dots \mathfrak{a}_1^N (x_n \cdot \dots \cdot x_1)$. By Definition 4, such a vector C^j exists for every $1 \leqslant j \leqslant N$.

Let the function $g(x_n, \dots, x_1) = x_n \cdot \dots \cdot x_1$. By Proposition 1, the matrix M_{S_g} is the identity $N \times N$ matrix. Thus, from Proposition 2 it follows that $V_{f_j} = C_1^j v(\mathfrak{a}_n^1 \dots \mathfrak{a}_1^1) \oplus \dots \oplus C_N^j v(\mathfrak{a}_n^N \dots \mathfrak{a}_1^N)$ or $V_{f_j} = C^j M_{\mathfrak{A}}$ in vector form. Consider a matrix whose rows are vectors $V_{f_1}, \dots, V_{f_N}$. This is exactly the matrix M_{S_g} since f_j satisfies (2.2). Let M be a matrix whose rows are vectors $C^1, \dots, C^N$. Then we have the matrix equality $M_{S_g} = M M_{\mathfrak{A}}$. Since M_{S_g} is the identity matrix, both matrices M and $M_{\mathfrak{A}}$ are necessarily non-degenerate.

Let f be an arbitrary n-ary Boolean function and (2.5) hold. Then $L_{\mathfrak{A}}(f) = N - Z(C)$. As shown above, (2.5) can be represented in vector form as $V_f = C M_{\mathfrak{A}}$. Since $M_{\mathfrak{A}}$ is non-degenerate, the inverse matrix $M_{\mathfrak{A}}^{-1}$ exists. So $C = V_f M_{\mathfrak{A}}^{-1}$ and $L_{\mathfrak{A}}(f) = N - Z(V_f M_{\mathfrak{A}}^{-1})$. □

Definition 5. The complexity *of an n-ary Boolean function f* in the set *K of base bundles of n-ary operators is the value $L_K(f)$, which is defined as $L_K(f) = \min\{L_{\mathfrak{A}}(f) \mid \mathfrak{A} \in K\}$.*

Proposition 4. *For arbitrary n-ary Boolean function f and every set K of base bundles of n-ary operators the value $L_K(f)$ can be calculated by the expression $L_K(f) = N - \max\{Z(V_f M_{\mathfrak{A}}^{-1}) \mid \mathfrak{A} \in K\}$.*

Proof. Let the matrices $M_{\mathfrak{A}}$ and $M'_{\mathfrak{A}}$ represent the same base bundle $\mathfrak{A}$ of n-ary operators, and let f be arbitrary n-ary Boolean function. According to Proposition 3, the expression (2.5) in vector form can be represented as

$V_f = CM_{\mathfrak{A}}$ or $V_f = C'M'_{\mathfrak{A}}$, depending on the choice of the representing matrix. Since the matrices $M_{\mathfrak{A}}$ and $M'_{\mathfrak{A}}$ differ from each other only by the permutation of the rows, the vectors C and C' also differ in the same permutation of their elements. Thus, $Z(C) = Z(C')$ and, consequently, $L_{\mathfrak{A}}(f)$ does not depend on the choice of the representing matrix. The rest of the proof follows directly from Definition 5 and Proposition 3. □

Definition 6. *For a given bundle* $\mathfrak{A} = \{\mathfrak{a}_n^k \dots \mathfrak{a}_1^k \mid 1 \leqslant k \leqslant N\}$*, generated by pair, its* extension $E_{\mathfrak{A}}$ *is a set of bundles* $E_{\mathfrak{A}} = \{\mathfrak{A}\} \cup \{\mathfrak{B}^j \mid 1 \leqslant j \leqslant N\}$*, where* $\mathfrak{B}^j = \{\mathfrak{a}_n^k \dots \mathfrak{a}_1^k \mid 1 \leqslant k \leqslant N,\ k \neq j\} \cup \{\mathfrak{b}_n \dots \mathfrak{b}_1\}$ *and* $\mathfrak{b}_n \dots \mathfrak{b}_1$ *is an operator such that* $v(\mathfrak{b}_n \dots \mathfrak{b}_1) = \sum\limits_{k=1}^{N} v(\mathfrak{a}_n^k \dots \mathfrak{a}_1^k)$*.*

By Proposition 3.10 of [6], the operator $\mathfrak{b}_n \dots \mathfrak{b}_1$ from Definition 6 always exists and is uniquely determined by a pair-generated bundle $\mathfrak{A}$. By Theorem 3.17, in [6] all bundles in $E_{\mathfrak{A}}$, including $\mathfrak{A}$ itself, are the base bundles. It is also true for $n = 0$, since $\mathfrak{A} = \{\varnothing\}$ and $E_{\mathfrak{A}} = \{\mathfrak{A}\}$ for this case.

Definition 7. *The set of all pair-generated bundles of n-ary operators will be called* the class of pair-generated bundles *of n-ary operators and will be denoted as* $\mathrm{H}^{(n)}$*. The set* $\mathrm{ExH}^{(n)} = \bigcup\limits_{\mathfrak{A} \in \mathrm{H}^{(n)}} E_{\mathfrak{A}}$ *will be called* the extended class of pair-generated bundles *of n-ary operators.*

Proposition 5. *For arbitrary n-ary Boolean function f*

$$L_{\mathrm{ExH}^{(n)}}(f) = \min_{\mathfrak{A} \in \mathrm{H}^{(n)}} \{N - Z(V_f M_{\mathfrak{A}}^{-1}), 1 + Z(V_f M_{\mathfrak{A}}^{-1})\}.$$

Proof. It is known (see Expression (3) in [5]) that for every n-ary Boolean function f it holds that $L_{E_{\mathfrak{A}}}(f) = \min\{L_{\mathfrak{A}}(f), N + 1 - L_{\mathfrak{A}}(f)\}$. By Proposition 3, $L_{E_{\mathfrak{A}}}(f) = \min\{N - Z(V_f M_{\mathfrak{A}}^{-1}), 1 + Z(V_f M_{\mathfrak{A}}^{-1})\}$. This leads to the desired expression. □

Let S be a set of 2×2 Boolean matrices. The set $S^{\otimes n}$ is defined as $S^{\otimes n} = \{M_n \otimes \dots \otimes M_1 \mid M_i \in S\}$, where $\otimes$ is Kronecker product of matrices. The set $S^{\otimes 0}$ consists of exactly one 1×1 matrix which only element is equal to 1. The set of all non-degenerate 2×2 Boolean matrices will be denoted as $\textsc{Kro}_2$.

Proposition 6. *Let* $\mathfrak{A} \in \mathrm{H}^{(n)}$ *be a pair-generated bundle of n-ary operators. Then there exists a matrix* $M \in \textsc{Kro}_2^{\otimes n}$ *such that M represents* $\mathfrak{A}$*. And vice versa, for every matrix* $M \in \textsc{Kro}_2^{\otimes n}$ *there exists* $\mathfrak{A} \in \mathrm{H}^{(n)}$ *such that M represents* $\mathfrak{A}$*.*

Proof. Let $\mathfrak{A}$ be a pair-generated bundle and $\mathfrak{b}_n \dots \mathfrak{b}_1$ and $\mathfrak{c}_n \dots \mathfrak{c}_1$ be its generators. By induction on m, let us show that if $\mathfrak{A}_m$ is the bundle generated by the pair $\mathfrak{b}_m \dots \mathfrak{b}_1$ and $\mathfrak{c}_m \dots \mathfrak{c}_1$, then there exists a matrix $M_{\mathfrak{A}_m} \in \textsc{Kro}_2^{\otimes m}$ representing $\mathfrak{A}_m$.

The basis of induction is obvious, since $\mathfrak{A}_0 = \{\varnothing\}$, $v(\varnothing) = (1)$, $M_{\mathfrak{A}_0} = (1)$, and $\textsc{Kro}_2^{\otimes 0} = \{(1)\}$.

Let $m > 0$ and $\mathfrak{A}_m = \{\mathfrak{a}_m^k \dots \mathfrak{a}_1^k \mid 1 \leqslant k \leqslant 2^m\}$ be generated by the pair $\mathfrak{b}_m \dots \mathfrak{b}_1$ and $\mathfrak{c}_m \dots \mathfrak{c}_1$, such that $\mathfrak{a}_j^k = \mathfrak{b}_j$ if $\sigma_j^k = 0$ and $\mathfrak{a}_j^k = \mathfrak{c}_j$ if $\sigma_j^k = 1$. $\{v(\mathfrak{a}_m^k \dots \mathfrak{a}_1^k) \mid 1 \leqslant k \leqslant 2^{m-1}\} = \{v(\mathfrak{b}_m) \otimes v(\mathfrak{a}_{m-1}^k \dots \mathfrak{a}_1^k) \mid 1 \leqslant k \leqslant 2^{m-1}\}$, since $\sigma_m^k = 0$ whenever $1 \leqslant k \leqslant 2^{m-1}$. This means that the $2^{m-1} \times 2^m$ matrix M_0, whose rows are the vectors $v(\mathfrak{a}_m^1 \dots \mathfrak{a}_1^1), \dots, v(\mathfrak{a}_m^{2^{m-1}} \dots \mathfrak{a}_1^{2^{m-1}})$, can be expressed as $M_0 = v(\mathfrak{b}_m) \otimes M_{\mathfrak{A}_{m-1}}$ if the vector $v(\mathfrak{b}_m)$ is considered as 1×2 matrix. Similarly, the $2^{m-1} \times 2^m$ matrix M_1 whose rows are exactly the vectors $v(\mathfrak{a}_m^{2^{m-1}+1} \dots \mathfrak{a}_1^{2^{m-1}+1}), \dots, v(\mathfrak{a}_m^{2^m} \dots \mathfrak{a}_1^{2^m})$, can be expressed as $M_1 = v(\mathfrak{c}_m) \otimes M_{\mathfrak{A}_{m-1}}$. Thus, the $2^m \times 2^m$ matrix, consisting of the rows of the matrices M_0 and M_1, represents the bundle $\mathfrak{A}_m$ and can be denoted by $M_{\mathfrak{A}_m}$. Moreover, $M_{\mathfrak{A}_m} = M^* \otimes M_{\mathfrak{A}_{m-1}}$, where M^* is the 2×2 matrix, whose rows are $v(\mathfrak{b}_m)$ and $v(\mathfrak{c}_m)$. Since $\mathfrak{b}_m$ and $\mathfrak{c}_m$ must be different (otherwise the set $\mathfrak{A}_m$ contains less than 2^m elements), the vectors $v(\mathfrak{b}_m)$ and $v(\mathfrak{c}_m)$ are also different and non-zero. This means that M^* is non-degenerate and, thus, belongs to $\textsc{Kro}_2$. Hence, by the induction hypothesis, $M_{\mathfrak{A}_m} \in \textsc{Kro}_2^{\otimes m}$.

Since $\mathfrak{A} = \mathfrak{A}_n$, we have a matrix $M \in \textsc{Kro}_2^{\otimes n}$, which represents $\mathfrak{A}$.

Conversely, let $M = M_n \otimes \dots \otimes M_1$, where $M_j \in \textsc{Kro}_2$ and

$$M_j = \begin{pmatrix} M_j[0,0] & M_j[0,1] \\ M_j[1,0] & M_j[1,1] \end{pmatrix}.$$

By the definition of Kronecker product, the k-th row in M can be written as the vector $(M_n[\sigma_n^k, 0]\ M_n[\sigma_n^k, 1]) \otimes \dots \otimes (M_1[\sigma_1^k, 0]\ M_1[\sigma_1^k, 0])$. Since the rows of each matrix M_j are non-zero and are not equal to each other, there are unary operators $\mathfrak{b}_j$ and $\mathfrak{c}_j$ such that the first row in M_j is represented by the vector $v(\mathfrak{b}_j)$ and the second one by the vector $v(\mathfrak{c}_j)$. Moreover, $\mathfrak{b}_j \neq \mathfrak{c}_j$. Thus, the k-th row of the matrix M can be represented as $v(\mathfrak{a}_n^k) \otimes \dots \otimes v(\mathfrak{a}_1^k)$ where $\mathfrak{a}_j^k = \mathfrak{b}_j$ if $\sigma_j^k = 0$ and $\mathfrak{a}_j^k = \mathfrak{c}_j$ if $\sigma_j^k = 1$. By Definition 3 the bundle $\mathfrak{A} = \{\mathfrak{a}_n^k \dots \mathfrak{a}_1^k \mid 1 \leqslant k \leqslant N\}$ is generated by the pair of the operators $\mathfrak{b}_n \dots \mathfrak{b}_1$, $\mathfrak{c}_n \dots \mathfrak{c}_1$, and the matrix M represents $\mathfrak{A}$. □

Corollary 1. *For every n-ary Boolean function*

$$L_{\mathrm{ExH}^{(n)}}(f) = \min_{M \in \textsc{Kro}_2^{\otimes n}} \{N - Z(V_f M), 1 + Z(V_f M)\}.$$

Proof. By Proposition 5 $L_{\mathrm{ExH}^{(n)}}(f) = \min\limits_{\mathfrak{A} \in \mathrm{H}^{(n)}} \{N - Z(V_f M_{\mathfrak{A}}^{-1}), 1 + Z(V_f M_{\mathfrak{A}}^{-1})\}$. By Proposition 6 $L_{\mathrm{ExH}^{(n)}}(f) = \min\limits_{M \in \textsc{Kro}_2^{\otimes n}} \{N - Z(V_f M^{-1}), 1 + Z(V_f M^{-1})\}$. Since the set $\textsc{Kro}_2$ consists of all non-degenerate 2×2 matrices, a matrix

M belongs to $\textsc{Kro}_2^{\otimes n}$ together with the matrix M^{-1}. It follows that $L_{\mathrm{ExH}^{(n)}}(f) = \min\limits_{M \in \textsc{Kro}_2^{\otimes n}} \{N - Z(V_f M), 1 + Z(V_f M)\}$. □

3. Counting zeros in vectors over finite fields

In this section several notions of theory of finite field will be used. Non familiar reader can obtain missing information in [7].

Let $\mathbb{F}_{q^s}$ be a finite field of order q^s, and let ζ be its primitive element. Let ℓ be a linear map from finite field $\mathbb{F}_{q^s}$ onto its subfield $\mathbb{F}_q$ such that $\ell(a\beta + \delta) = a\ell(\beta) + \ell(\delta)$ for every $a \in \mathbb{F}_q$ and $\beta, \delta \in \mathbb{F}_{q^s}$.

Proposition 7. $\#\{t \mid \ell(\zeta^t) = 0,\ 0 \leqslant t \leqslant q^s - 2\} = q^{s-1} - 1$.

Proof. For each $a \in \mathbb{F}_q$, denote by S_a the set $\{\beta \in \mathbb{F}_{q^s} \mid \ell(\beta) = a\}$. Since ℓ is onto, every S_a is non-empty. Let us fix some $\delta \in S_1$. For each a, consider the set $S'_a = \{a\delta + \beta \mid \beta \in S_0\}$. Since $\ell(a\delta + \beta) = a$ for all $\beta \in S_0$, $S'_a \subseteq S_a$ for every $a \in \mathbb{F}_q$. As $a\delta + \beta_1 \neq a\delta + \beta_2$ whenever $\beta_1 \neq \beta_2$, we get $S'_a = S_a$ and $\#S_a = \#S_0$. The sets S_a are pairwise distinct and together contain all elements from $\mathbb{F}_{q^s}$. Thus, $\#S_a = \#\mathbb{F}_{q^s}/\#\mathbb{F}_q = q^{s-1}$. Therefore, $\#\{t \mid \ell(\zeta^t) = 0,\ 0 \leqslant t \leqslant q^s - 2\} = \#(S_0 \setminus \{0\}) = q^{s-1} - 1$. □

For each vector $V = (V_1, \ldots, V_n)$ which components belongs to the field $\mathbb{F}_{q^s}$ put $\ell(V) = (\ell(V_1), \ldots, \ell(V_n))$.

For integers t and j let us define series of maps from $\mathbb{F}_{q^s}$ to complex numbers as follows: $\chi_j(\zeta^t) = e^{-2\pi i j t/r}$, where $r = \frac{q^s-1}{q-1}$. It is easy to see that the map χ_j is a multiplicative character of finite field $\mathbb{F}_{q^s}$.

Let p be a prime integer such that $q = p^k$ for some integer k. An absolute trace for finite field $\mathbb{F}_q$ is defined by $\mathrm{Tr}_q(a) = a^{p^0} + \cdots + a^{p^{k-1}}$ for all $a \in \mathbb{F}_q$. It is known that for every $a \in \mathbb{F}_q$ the value $\mathrm{Tr}_q(a)$ belongs to $\mathbb{Z}_p$. Let us define a map ψ_ℓ from $\mathbb{F}_{q^s}$ to complex numbers, which maps each element $\beta \in \mathbb{F}_{q^s}$ to $\psi_\ell(\beta) = e^{2\pi i \mathrm{Tr}_q(\ell(\beta))/p}$. It easy to see that the map ψ_ℓ is an additive character of finite field $\mathbb{F}_{q^s}$.

Definition 8. A Gauss sum *for multiplicative character* χ_j *and additive character* ψ_ℓ *of finite field* $\mathbb{F}_{q^s}$ *is defined by* $G(\chi_j, \psi_\ell) = \sum\limits_{t=0}^{q^s-2} \chi_j(\zeta^t)\psi_\ell(\zeta^t)$.

It is known (see theorem 5.11 in [7]) that if χ_j and ψ_ℓ are both non trivial, then $|G(\chi_j, \psi_\ell)| = q^{s/2}$. It is easy to see that χ_j is non trivial for all integers $j \not\equiv 0 \pmod r$, and ψ_ℓ is also non trivial for above defined ℓ.

Lemma 1. *Let a vector $V = (\zeta^{d_1}, \dots, \zeta^{d_N})$ for some integers $d_1, \dots, d_N$, $r = \frac{q^s-1}{q-1}$, $\omega = e^{2\pi i/r}$. Then $Z(\ell(V)) = \frac{q^{s-1}-1}{q^s-1}N + R(V)$, where $R(V)$ is given by $R(V) = \frac{1}{qr}\sum\limits_{j=1}^{r-1} G(\chi_j, \psi_\ell)\sum\limits_{k=1}^{N}\omega^{jd_k}$.*

Proof. The proof technique is taken from Chapter 12 of [4].

First of all, note that $\mathbb{F}_q = \{0\} \cup \{\zeta^{mr} \mid 0 \leqslant m \leqslant q-2\}$, since ζ^r is a generator of the multiplicative group of the subfield $\mathbb{F}_q$. As $\zeta^{mr} \in \mathbb{F}_q$ and ℓ is linear, we have $\ell(\zeta^{t+mr}) = \zeta^{mr}\ell(\zeta^t)$. Thus, if $\ell(\zeta^d) = 0$, then there is a unique integer t such that $0 \leqslant t \leqslant r-1$, $d \equiv t \pmod r$, and $\ell(\zeta^t) = 0$. Let us apply this observation to $Z(\ell(V))$ as follows.

$$Z(\ell(V)) = \sum_{\substack{k=1\\ \ell(\zeta^{d_k})=0}}^{N} 1 = \sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{r-1}\ \sum_{\substack{k=1\\ d_k\equiv t \pmod r}}^{N} 1 \tag{3.1}$$

The following well-known equation can be easily proved if we consider it as a geometric progression.

$$\sum_{j=0}^{r-1}\omega^{(d-t)j} = \begin{cases} r & \text{if } d \equiv t \pmod r\\ 0 & \text{if } d \not\equiv t \pmod r. \end{cases} \tag{3.2}$$

Applying this equation to (3.1), we get

$$Z(\ell(V)) = \frac{1}{r}\sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{r-1}\sum_{k=1}^{N}\sum_{j=0}^{r-1}\omega^{(d_k-t)j} = \frac{1}{r}\sum_{j=0}^{r-1}\Bigl(\sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{r-1}\omega^{-jt}\Bigr)\sum_{k=1}^{N}\omega^{jd_k} \tag{3.3}$$

Introduce the value E_j^* as follows and, using similar transformations as in (3.1) and observing that $\omega^{-jd} = \omega^{-jt}$ whenever $d \equiv t \pmod r$, we get

$$E_j^* = \sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{q^s-2}\omega^{-jt} = \sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{r-1}\ \sum_{\substack{d=0\\ d\equiv t \pmod r}}^{q^s-2}\omega^{-jd} \ = \sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{r-1}\omega^{-jt}\sum_{\substack{d=0\\ d\equiv t \pmod r}}^{q^s-2} 1 = (q-1)\sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{r-1}\omega^{-jt}$$

By Proposition 7 $E_0^* = q^{s-1} - 1$. Using the equality $\omega^r = 1$, we get

$$E_j^* = \sum_{t=0}^{q^s-2}\omega^{-jt} - \sum_{m=0}^{q-2}\sum_{\substack{t=0\\ \ell(\zeta^t)=\zeta^{mr}}}^{q^s-2}\omega^{-jt} = \sum_{t=0}^{q^s-2}\omega^{-jt} - \sum_{m=0}^{q-2}\sum_{\substack{t=0\\ \ell(\zeta^{t-mr})=1}}^{q^s-2}\omega^{-j(t-mr)}$$

If $0 < j < r$, the first sum is zero, as indicated in (3.2). So we have

$$E_j^* = -\sum_{m=0}^{q-2}\sum_{\substack{t=0\\ \ell(\zeta^t)=1}}^{q^s-2}\omega^{-jt} = (1-q)\sum_{\substack{t=0\\ \ell(\zeta^t)=1}}^{q^s-2}\omega^{-jt}$$

Let $\nu = e^{2\pi i/p}$. Since $\mathrm{Tr}_q(a)$ takes each value from $\mathbb{Z}_p$ k times when a runs through all values from $\mathbb{F}_q$, it follows that

$$\sum_{m=0}^{q-2} \nu^{\mathrm{Tr}_q(\zeta^{mr})} = -\nu^{\mathrm{Tr}_q(0)} + \sum_{a\in\mathbb{F}_q} \nu^{\mathrm{Tr}_q(a)} = -1. \tag{3.4}$$

Split the Gauss sum $G(\chi_j, \psi_\ell)$ by zero and non-zero images of ℓ:

$$G(\chi_j, \psi_\ell) = \sum_{t=0}^{q^s-2} \chi_j(\zeta^t)\psi_\ell(\zeta^t) = \sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{q^s-2} \chi_j(\zeta^t)\psi_\ell(\zeta^t) + \sum_{m=0}^{q-2}\sum_{\substack{t=0\\ \ell(\zeta^t)=\zeta^{mr}}}^{q^s-2} \chi_j(\zeta^t)\psi_\ell(\zeta^t)$$

Consider the first part of the previous equation.

$$\sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{q^s-2} \chi_j(\zeta^t)\psi_\ell(\zeta^t) = \sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{q^s-2} \omega^{-jt}\nu^{\mathrm{Tr}_q(0)} = \sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{q^s-2} \omega^{-jt} = E_j^*$$

Now consider the second part, applying (3.4) just before the end.

$$\sum_{m=0}^{q-2}\sum_{\substack{t=0\\ \ell(\zeta^t)=\zeta^{mr}}}^{q^s-2} \chi_j(\zeta^t)\psi_\ell(\zeta^t) = \sum_{m=0}^{q-2}\sum_{\substack{t=0\\ \ell(\zeta^t)=\zeta^{mr}}}^{q^s-2} \omega^{-jt}\nu^{\mathrm{Tr}_q(\zeta^{mr})} = \sum_{m=0}^{q-2} \nu^{\mathrm{Tr}_q(\zeta^{mr})} \sum_{\substack{t=0\\ \ell(\zeta^{t-mr})=1}}^{q^s-2} \omega^{-j(t-mr)}$$

$$= \sum_{m=0}^{q-2} \nu^{\mathrm{Tr}_q(\zeta^{mr})} \sum_{\substack{t=0\\ \ell(\zeta^t)=1}}^{q^s-2} \omega^{-jt} = \sum_{\substack{t=0\\ \ell(\zeta^t)=1}}^{q^s-2} \omega^{-jt} \sum_{m=0}^{q-2} \nu^{\mathrm{Tr}_q(\zeta^{mr})} = -\sum_{\substack{t=0\\ \ell(\zeta^t)=1}}^{q^s-2} \omega^{-jt} = \frac{1}{q-1}E_j^*$$

Putting it all together, we have $G(\chi_j, \psi_\ell) = \frac{q}{q-1}E_j^*$ and

$$\sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{r-1} \omega^{-jt} = \frac{1}{q-1}E_j^* = \frac{1}{q}G(\chi_j, \psi_\ell).$$

Recall that this is true only for $0 < j < r$. From (3.3) it follows that

$$Z(\ell(V)) = \frac{1}{r}\Big(\sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{r-1} 1\Big)\sum_{k=1}^{N} 1 + \frac{1}{r}\sum_{j=1}^{r-1}\Big(\sum_{\substack{t=0\\ \ell(\zeta^t)=0}}^{r-1}\omega^{-jt}\Big)\sum_{k=1}^{N}\omega^{jd_k} =$$

$$= \frac{N}{r}\frac{E_0^*}{q-1} + \frac{1}{r}\sum_{j=1}^{r-1}\frac{E_j^*}{q-1}\sum_{k=1}^{N}\omega^{jd_k} = \frac{q^{s-1}-1}{q^s-1}N + \frac{1}{qr}\sum_{j=1}^{r-1} G(\chi_j, \psi_\ell)\sum_{k=1}^{N}\omega^{jd_k}$$

This completes the proof. □

Lemma 2. *Let* $V = (\zeta^{d_{n1}}, \ldots, \zeta^{d_{nq}}) \otimes \cdots \otimes (\zeta^{d_{11}}, \ldots, \zeta^{d_{1q}})$ *for some integers* $d_{11}, \ldots, d_{1q}, \ldots, d_{n1}, \ldots, d_{nq}$, $r = \frac{q^s-1}{q-1}$, $\omega = e^{2\pi i/r}$. *Then*

$$Z(\ell(V)) = \frac{q^{s-1}-1}{q^s-1} q^n + R(V),$$

where $R(V) = \frac{1}{qr} \sum\limits_{j=1}^{r-1} G(\chi_j, \psi_\ell) \prod\limits_{t=1}^{n} \left(\omega^{jd_{t1}} + \cdots + \omega^{jd_{tq}}\right)$. *Moreover, if* r *is prime and for every* t, $1 \leqslant t \leqslant n$, *among the numbers* $d_{t1}, \ldots, d_{tq}$ *there are incomparable modulo* r, *then* $R(V) = O\left((q - 2 + 2\cos\frac{\pi}{r})^n\right) = o(q^n)$.

Proof. The number of elements in the vector V is equal to q^n. Let V_k denote the k-th element in V. Each integer k in the range $1 \leqslant k \leqslant q^n$ can be uniquely represented as $k = 1 + (k_n - 1)q^{n-1} + (k_{n-1} - 1)q^{n-2} + \cdots + (k_1 - 1)q^0$, where $1 \leqslant k_j \leqslant q$, $1 \leqslant j \leqslant n$. By the definition of tensor product $\otimes$, $V_k = \zeta^{d_{nk_n}} \cdot \ldots \cdot \zeta^{d_{1k_1}}$, i.e. $V_k = \zeta^{d_{nk_n} + \cdots + d_{1k_1}}$. On the other hand,

$$\prod_{t=1}^{n} \left(\omega^{jd_{t1}} + \cdots + \omega^{jd_{tq}}\right) = \sum_{k=1}^{q^n} \omega^{D_k}$$

where $D_k = \omega^{jd_{nk_n}} \cdot \ldots \cdot \omega^{jd_{1k_1}} = \omega^{j(d_{nk_n} + \cdots + d_{1k_1})}$, referring to the previous representation of k. After this observation, the first part of Lemma 2 is essentially Lemma 1, slightly reformulated.

Now consider the case when r is a prime integer, and evaluate the value of $|R(V)|$. By Theorem 5.11 in [7], $|G(\chi_j, \psi_\ell)| = \sqrt{q^s}$, since ψ_ℓ and χ_j are nontrivial characters if $0 < j < r - 1$.

Consider the value of $|\omega^{jd_{t1}} + \cdots + \omega^{jd_{tq}}|$. Without loss of generality, let d_{t1} and d_{t2} be incomparable modulo r. Thus, denoting $d^* = d_{t2} - d_{t1}$,

$$|\omega^{jd_{t1}} + \cdots + \omega^{jd_{tq}}| = |\omega^{jd_{t1}}| \cdot |1 + \omega^{jd^*} + \cdots + \omega^{j(d_{tq} - d_{t1})}| \leqslant |1 + \omega^{jd^*}| + q - 2$$

As $\omega^{jd*} = e^{2\pi i j d^*/r}$, we have

$$|1 + \omega^{jd*}| = \sqrt{\left(1 + \cos\frac{2\pi jd^*}{r}\right)^2 + \sin^2\frac{2\pi jd^*}{r}} = \sqrt{2 + 2\cos\frac{2\pi jd^*}{r}} = 2\left|\cos\frac{\pi jd^*}{r}\right|$$

Since j and d^* are relatively prime with r, we have $\left|\cos\frac{\pi jd^*}{r}\right| < 1$ and, moreover, $\left|\cos\frac{\pi jd^*}{r}\right| \leqslant \cos\frac{\pi}{r}$, which completes the proof. □

4. Lower bound in the class of extended operator forms

Theorem 1. *Let $p = 2^s - 1$ be a Mersenne prime, ℓ be a linear map from finite field $\mathbb{F}_{2^s}$ onto $\mathbb{F}_2$, ζ be a primitive element of $\mathbb{F}_{2^s}$, and n-ary Boolean function f is represented by a vector $V_f = \ell\left((1,\zeta)^{\otimes n}\right)$. Then*

$$L_{\mathrm{ExH}^{(n)}}(f) \geqslant \left(\frac{1}{2} - \frac{1}{2p}\right) 2^n - o(2^n). \tag{4.1}$$

Proof. Let $M \in \textsc{Kro}_2^{\otimes n}$. Then $M = M_n \otimes \cdots \otimes M_1$ where $M_j \in \textsc{Kro}_2$.

$$\begin{aligned} V_f M = \ell\left((1,\zeta)^{\otimes n}\right) M &= \ell\left((1,\zeta)^{\otimes n}(M_n \otimes \cdots \otimes M_1)\right) \\ &= \ell\left(((1,\zeta)M_n) \otimes \cdots \otimes ((1,\zeta)M_1)\right) \end{aligned}$$

Since $\textsc{Kro}_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$, $(1,\zeta)M_j \in \left\{(1,\zeta), (1+\zeta,\zeta), (1,1+\zeta), (\zeta,1), (\zeta,1+\zeta), (1+\zeta,1)\right\}$. As ζ is a generator of the multiplicative group of the finite field $\mathbb{F}_{2^s}$ there exists an integer t such that $1+\zeta = \zeta^t$ and $1 < t < p$. Recall also that $1 = \zeta^0$. Since 0, 1, and t are incomparable modulo p, we can apply Lemma 2, which gives us the following: $Z(V_f M) = \frac{2^{s-1}-1}{2^s-1}2^n + o(2^n) = \left(\frac{1}{2} - \frac{1}{2p}\right)2^n + o(2^n)$ for every $M \in \textsc{Kro}_2^{\otimes n}$.

By Corollary 1, $L_{\mathrm{ExH}^{(n)}}(f) = \min\limits_{M \in \textsc{Kro}_2^{\otimes n}} \{2^n - Z(V_f M), 1 + Z(V_f M)\}$. Thus, $L_{\mathrm{ExH}^{(n)}}(f) = \min\limits_{M \in \textsc{Kro}_2^{\otimes n}} \left\{ \left(\frac{1}{2} + \frac{1}{2p}\right)2^n - o(2^n), \left(\frac{1}{2} - \frac{1}{2p}\right)2^n + 1 + o(2^n) \right\}$ which leads us to expression (4.1). □

Note that the largest currently known Mersenne prime is $2^{82589933} - 1$ [1]. From Theorem 1 it follows that there exists an n-ary Boolean function f, such that $L_{\mathrm{ExH}^{(n)}}(f) \geqslant \left(\frac{1}{2} - \frac{1}{2^{82589934}-2}\right) - o(2^n)$. This is asymptotically stronger than the lower bound of the form $L_{\mathrm{ExH}^{(n)}}(f) > \left(\frac{1}{2} - \frac{1}{12}\right)2^n$, previously obtained in [5].

Corollary 2. *If the sequence of Mersenne primes is infinite then for every $\varepsilon > 0$ there exist an n-ary Boolean function f, such that*

$$L_{\mathrm{ExH}^{(n)}}(f) \geqslant \left(\frac{1}{2} - \varepsilon\right) 2^n - o(2^n).$$

Proof. Given $\varepsilon > 0$ take a Mersenne prime p such that $p > \frac{1}{2\varepsilon}$. Since the sequence of Mersenne primes is infinite, such p exists. Thus, $\frac{1}{2p} < \varepsilon$, and using Theorem 1, we obtain the desired result. □

5. Conclusion

In this paper we have proposed a general approach to obtain lower bounds of complexity in a certain class of polynomial forms of Boolean functions. Lemma 6 and lemma 8 in [2] can be considered as a special case of lemma 1 and lemma 2 of this work. As showed in [2] (see theorems 1 and 2) lower bounds in [8; 10] can be also obtained as a consequences of lemma 1 of this work.

References

1. A000043 - OEIS. *The On-Line Encyclopedia of Integer Sequences.* Available at: https://oeis.org/A000043
2. Baliuk A.S., Zinchenko A.S. Lower Bounds of Complexity for Polarized Polynomials over Finite Fields. *Siberian Mathematical Journal*, 2019, vol. 60, issue 1, pp. 1-9. https://doi.org/10.1134/S0037446619010014
3. Baliuk A.S., Yanushkovskiy G.V. Operatornye polinomial'nye formy funktsiy nad konechnymi polyami [Operator polynomial forms of functions over finite fields]. *Proceedings of IX International conference ,,Diskretnye modeli v teorii upravlyayushchikh sistem".* Moscow, MAKS Press Publ., 2015, pp. 28-30. (in Russian)
4. Berndt B.C., Evans R.J., Williams K.S. *Gauss and Jacobi sums.* John Wiley & Sons Inc., Toronto, 1998, 600 p.
5. Frantseva A.S. Complexity of Boolean functions' representations in classes of extended pair-generated operator forms. *Siberian Electronic Mathematical Reports*, 2019, vol. 16, pp. 523-541. (in Russian) https://doi.org/10.33048/semi.2019.16.034
6. *Izbrannye voprosy teorii bulevykh funktsiy* [Selected questions in the theory of Boolean functions]. Eds. Vinokurov S.F. and Peryazev N A. Moscow, Fizmatlit Publ., 2001, 192 p. (in Russian)
7. Lidl R., Niederreiter H. *Finite Fields (Encyclopedia of Mathematics and its Applications).* Cambridge University Press, England, 1984, 660 p. https://doi.org/10.1017/CBO9780511525926
8. Markelov N.K. A lower estimate of the complexity of three-valued logic functions in the class of polarized polynomials. *Moscow Univ. Comput. Math. Cybern.*, 2012, vol. 36, issue 3, pp. 150-154. https://doi.org/10.3103/S0278641912030041
9. Muller D.E. Application of Boolean algebra to switching circuit design and to error detection. *IRE Trans. Electron. Comput.*, 1954, vol. EC–3, issue 3, pp. 6-12. https://doi.org/10.1109/IREPGELC.1954.6499441
10. Peryazev N.A. Complexity of Boolean functions in the class of polarized polynomial forms. *Algebra and Logic*, 1995, vol. 34, no. 3, pp 177-179. https://doi.org/10.1007/BF02341875
11. Selezneva S.N. Upper Bound for the Length of Functions over a Finite Field in the Class of Pseudopolynomials. *Computational Mathematics and Mathematical Physics*, 2017, vol. 57, no. 5, pp. 898-903. https://doi.org/10.1134/S0965542517050116
12. Vinokurov S.F. *Smeshannye operatory v bulevykh funktsiyakh i ikh svoystva* [Mixed operators in Boolean functions and their properties]. Irkutsk, Irkutsk University, 2000, 36 p. (Series Discrete mathematics and informatics, Issue 12). (in Russian)

Aleksandr Baliuk, Candidate of Sciences (Physics and Mathematics), Irkutsk State University, 1, K. Marx st., Irkutsk, 664003, Russian Federation tel.: (3952)242210, e-mail: sacha@hotmail.ru.

Received 09.09.19

Нижняя оценка сложности булевых функций в классе расширенных операторных форм

А. С. Балюк

Иркутский государственный университет, Иркутск, Российская Федерация

Аннотация. Полиномиальные представления булевых функций активно исследуются в связи с применением в теории кодирования и для синтеза схем цифровых устройств, начиная с основопологающей работы Мюллера. Операторный подход к полиномиальным представлениям предложенный в работах Винокурова позволил, с одной стороны, единообразно описать все известные виды полиномиальных форм булевых функций, с другой стороны, обобщить их на случай разложений по образом нечетных функций, отличных от конъюнкции.

При исследовании полиномиальных и, в общем случае, операторных форм один из главных вопросов — это получение оценок сложности представления булевых функций в различных классах форм. Верхние оценки сложности фактически представляют собой алгоритмы минимизации булевых функций в том или ином классе форм.

Нижние оценки сложности можно разделить на два вида: комбинаторные и эффективные. Комбинаторные оценки позволяют доказать существование булевых функций, имеющих высокую сложность, без нахождения явного вида этих функций. Эффективные же нижние оценки основаны на конструировании в явном виде булевых функций, имеющих высокую сложность в том или ином классе форм.

В настоящей работе с использованием алгебраического расширения конечного поля порядка 2 получена нижняя оценка сложности булевых функций в классе расширенных операторных форм. Данная оценка усиливает ранее известные оценки для данного класса операторных форм и будет являться асимптотически оптимальной в случае, если последовательность простых чисел Мерсенна бесконечна.

Ключевые слова: булевы функции, нижние оценки сложности, расширение конечного поля, простые числа Мерсенна.

Список литературы

1. A000043 - OEIS // The On-Line Encyclopedia of Integer Sequences. URL: https://oeis.org/A000043 (дата обращения: 24.08.2019)
2. Балюк А. С., Зинченко А. С. Нижние оценки сложности поляризованных полиномов над конечными полями // Сибирский математический журнал. 2019. Т. 60, № 1, С. 3–13. https://doi.org/10.33048/smzh.2019.60.101
3. Балюк А. С., Янушковский Г. В. Операторные полиномиальные формы функций над конечными полями // Труды IX Международной конференции «Дискретные модели в теории управляющих систем». М. : МАКС Пресс, 2015. С. 28–30.

4. Berndt B. C., Evans R. J., Williams K. S. Gauss and Jacobi sums. Toronto : John Wiley & Sons Inc., 1998. 600 p.
5. Францева А. С. Сложность представлений булевых функций в классах расширенных двупорожденных операторных форм // Сибирские электронные математические известия. 2019. Т. 16. С. 523–541. https://doi.org/10.33048/semi.2019.16.034
6. Избранные вопросы теории булевых функций / под ред. С. Ф. Винокурова, Н. А. Перязева. М. : Физматлит, 2001. 192 с.
7. Лидл Р., Нидеррайтер Г. Конечные поля : пер. с англ. М.: Мир, 1988. Т. 1. 430 с.
8. Маркелов Н. К. Нижняя оценка сложности функций трехзначной логики в классе поляризованных полиномов // Вестник Московского университета. Сер. 15, Вычислительная математика и кибернетика. 2012. Вып. 3, С. 40–45.
9. Muller D. E. Application of Boolean algebra to switching circuit design and to error detection // IRE Trans. Electron. Comput. 1954. Vol. EC—3, Issue 3. P. 6–12. https://doi.org/10.1109/IREPGELC.1954.6499441
10. Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. 1995. Т. 34, № 3. С. 323–326.
11. Селезнева С. Н. Верхняя оценка длины функций над конечным полем в классе псевдополиномов // Журнал вычислительной математики и математической физики. 2017. Т. 57, № 5. С. 899–904.
https://doi.org/10.7868/S0044466917050118
12. Винокуров С. Ф. Смешанные операторы в булевых функциях и их свойства. Иркутск : Иркутский университет, 2000. 36 с. (Дискретная математика и информатика ; вып. 12).

Александр Сергеевич Балюк, кандидат физико-математических наук, доцент, Институт математики, экономики и информатики, Иркутский государственный университет, Российская Федерация, 664003, г. Иркутск, ул. К. Маркса, 1, тел.: (3952)242210, e-mail: sacha@hotmail.ru

Поступила в редакцию 09.09.19