S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 13, стр. 1346–1368 (2016) УДК 519.115.4
DOI 10.17377/semi.2016.13.105 MSC 06E30

Special issue: Graphs and Groups, Spectra and Symmetries — G2S2 2016

ON PLATEAUED BOOLEAN FUNCTIONS WITH THE SAME SPECTRUM SUPPORT

A.V. KHALYAVIN, M.S. LOBANOV, YU.V. TARANNIKOV

Abstract. In the first half of the paper we give a brief review of plateaued functions, regular functions and related topics including connections with problems on subgraphs of the Hamming graph. In the second half of the paper we discover wide infinite families of spectrum supports for which it is possible to count the number of plateaued Boolean functions with such spectrum supports and give corresponding formulas; only one infinite sequence of such spectrum supports was known before.

Keywords: Plateaued functions, Boolean functions, Walsh Spectrum, Fourier spectrum, Spectra, Spectrum support, Spectral analysis, Regular functions, Correlation immune functions, m-resilient functions, Address function, Recursive constructions, Hamming graph, Regular graphs, Equitable partitions, Symmetries.

1. Introduction and preliminaries

1.1. **Basic definitions.** We consider $\mathbf{F}_2^n$, the linear n-dimensional vector space over $\mathbf{F}_2$ that also can be considered as the vector set V^n or the n-dimensional Boolean cube (hypercube) or the Hamming graph

$$B^n = B^n(V^n, E^n)$$

Khalyavin, A.V., Lobanov, M.S., Tarannikov, Yu.V., On plateaued Boolean functions with the same spectrum support.

The work of the third author is supported by RFBR, grant 16–01–00226.
Received November, 7, 2016, published December, 26, 2016.

where V^n is the set of vertices, E^n is the set of edges of the Hamming graph B^n.

The n-variable *Boolean function* is a mapping from $\mathbf{F}_2^n$ into $\mathbf{F}_2$.

The support $\mathrm{supp}(f)$ of a Boolean function f is the set of all such vectors x, $x \in \mathbf{F}_2^n$, that $f(x) \neq 0$, i.e. $f(x) = 1$.

The subgraph of B^n induced by $\mathrm{supp}(f)$ is denoted by $B^n[\mathrm{supp}(f)]$.

The weight $\mathrm{wt}(f)$ of a function f on $\mathbf{F}_2^n$ is the number of vectors x from $\mathbf{F}_2^n$ such that $f(x) = 1$; $\mathrm{wt}(f) = |\mathrm{supp}(f)|$.

The function $\bar{f} = f \oplus 1$ is the negation of f; $\mathrm{supp}(\bar{f}) = V^n \setminus \mathrm{supp}(f)$.

We give some basic facts on Boolean functions without proofs; readers can find more details in [3, 18].

The Walsh Transform of a Boolean function f is the integer-valued function on $\mathbf{F}_2^n$ defined as

$$W_f(u) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+\langle u,x\rangle} \tag{1}$$

where $\langle u, x\rangle = u_1x_1 + \cdots + u_nx_n$ is a scalar product of the vectors u and x. For each $u \in \mathbf{F}_2^n$ the value $W_f(u)$ is called the *Walsh coefficient* or the *spectral coefficient.* The set $\{W_f(u), u \in \mathbf{F}_2^n\}$ of all 2^n Walsh coefficient is called *the spectrum* of the function f.

The Fourier Transform of a pseudo-Boolean function $\widehat{f}$, $\widehat{f} : \mathbf{F}_2^n \to \mathbf{R}$ is the real-valued function on $\mathbf{F}_2^n$ defined as

$$F_{\widehat{f}}(u) = \sum_{x \in \mathbf{F}_2^n} \widehat{f}(x) \cdot (-1)^{\langle u,x\rangle}. \tag{2}$$

For every $u \in \mathbf{F}_2^n$ the value $F_{\widehat{f}}(u)$ is called *the Fourier coefficient.*

The Walsh Transform can be considered as a particular case of the Fourier Transform when a function $\widehat{f}(x)$ takes only two values ± 1; thus, it is possible to define the function $f(x)$ as $(-1)^{f(x)} = \widehat{f}(x)$.

The Walsh and Fourier coefficients of the same Boolean function f on $\mathbf{F}_2^n$ are connected by the expression

$$W_f(u) = 2^n\delta_u^0 - 2F_f(u).$$

Sometimes in literature Walsh coefficients are called Fourier coefficients too especially if f is defined at $\{-1, 1\}^n$.

Every Boolean function on $\mathbf{F}_2^n$ satisfies *Parseval's Identity*

$$\sum_{u \in \mathbf{F}_2^n} W^2(u) = 2^{2n}. \tag{3}$$

For any pseudo-Boolean function $\widehat{f}$, $\widehat{f} : \mathbf{F}_2^n \to \mathbf{R}$, and any vector $x \in \mathbf{F}_2^n$ *the Inversion Formula* holds:

$$\widehat{f}(x) = 2^{-n} \sum_{u \in \mathbf{F}_2^n} F_{\widehat{f}}(u)(-1)^{\langle u,x\rangle}. \tag{4}$$

In fact, the Inversion Formula gives the expansion of $\widehat{f}(x)$ over the orthogonal basis $\{(-1)^{\langle u,x\rangle}\}|_{u \in \mathbf{F}_2^n}$ in 2^n-dimensional vector space $\mathbf{R}^{2^n}$, where $2^{-n}F_{\widehat{f}}(u)$ are expansion coefficients.

The Inversion Formula for Walsh coefficients

$$(-1)^{f(x)} = 2^{-n} \sum_{u \in F_2^n} W_f(u)(-1)^{\langle u,x \rangle}$$

is a criterion for $\{W(u)\}|_{u \in \mathbf{F}_2^n}$ to correspond to some Boolean function: the set of coefficients $\{W(u)\}|_{u \in \mathbf{F}_2^n}$ corresponds to some Boolean function if and only if for every $x \in \mathbf{F}_2^n$ the value of the expression $2^{-n} \sum\limits_{u \in F_2^n} W(u)(-1)^{\langle u,x \rangle}$ is equal to either -1 or $+1$.

Another criterion for $\{W(u)\}|_{u \in \mathbf{F}_2^n}$ to correspond to some Boolean function is given by the Titsworth's Theorem.

Theorem 1. (Titsworth's Theorem) *The set of coefficients $\{W(u)\}|_{u \in \mathbf{F}_2^n}$ corresponds to some Boolean function if and only if*

a) $\sum\limits_{u \in \mathbf{F}_2^n} W^2(u) = 2^{2n}$ *(Parseval's identity);*

b) $\sum\limits_{u \in \mathbf{F}_2^n} W(u)W(u+s) = 0$ *for any* $s \in \mathbf{F}_2^n$, $s \neq 0$.

The spectrum support S_f of a Boolean function f is the set of all vectors u such that $W_f(u) \neq 0$. The spectrum support of a plateaued function has the cardinality 4^{n-c}, it follows easily from Parseval's Identity.

Let E be an arbitrary subset of $\mathbf{F}_2^n$. *The rank* of the set E is the dimension of the subspace generated by E in $\mathbf{F}_2^n$. *The affine rank* of the set E is the dimension of a smallest coset in $\mathbf{F}_2^n$ that contains E. For the brevity we call the affine rank and the rank of the spectrum support of a Boolean function shortly its *affine rank* and *rank,* correspondingly.

The Hamming distance $d(x', x'')$ between two vectors x' and x'' is the number of components where vectors x' and x'' differ. For a given function f on $\mathbf{F}_2^n$ the minimum of distances $d(f, l)$ where l runs through the set of all affine functions on $\mathbf{F}_2^n$ is called *the nonlinearity* of f and denoted by $\mathrm{nl}(f)$.

The nonlinearity of a function f on $\mathbf{F}_2^n$ is expressed via its Walsh coefficients by formula

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbf{F}_2^n} |W_f(u)|.$$

Nonlinearity is invariant under any affine transformation of $\mathbf{F}_2^n$.

A Boolean function is called *bent* if the values of its Walsh coefficients at all vectors are exactly $\pm 2^{n/2}$. So bent functions have 2-valued Walsh spectrum. Bent functions exist for all even n and do not exist for all odd n. A bent function is the function with maximum possible nonlinearity $2^{n-1} - 2^{(n/2)-1}$ among all functions of n variables for even n. Bent functions have a great significance in cryptography. We recommend [5, 31] as recent reviews on bent functions.

A Boolean function f is called *plateaued* if there exists integer c such that for any vector $u \in \mathbf{F}_2^n$ it holds $W_f(u) \in \{0, \pm 2^c\}$. So plateaued functions have 3-valued Walsh spectrum. Plateaued functions are of great importance in the study of bent functions (one of the reasons is that decomposition of a bent function in some variable gives two plateaued functions) and by the reason that many cryptographically important functions are plateaued (for example, m-resilient functions of n variables with maximum possible nonlinearity $2^{n-1} - 2^{m+1}$ [24, 28]).

A Boolean function f on $\mathbf{F}_2^n$ is called *balanced* if $\mathrm{wt}(f) = \mathrm{wt}(f \oplus 1) = 2^{n-1}$ (i.e. the function takes the values 0 and 1 at the same number of vectors).

In terms of Walsh coefficients it is easy to see that f is balanced if and only if $W_f(0,\dots,0)=0$ since $\mathrm{wt}(f)$ is expressed via $W_f(0,\dots,0)$ as

$$\mathrm{wt}(f)=2^{n-1}-\frac{1}{2}W_f(0,\dots,0).$$

A Boolean function f is called *correlation-immune* of order m if $\mathrm{wt}(f')=\mathrm{wt}(f)/2^m$ for any its subfunction f' of $n-m$ variables. A balanced correlation-immune function of order m is called *m-resilient*. In other words, a Boolean function f is called m-resilient if $\mathrm{wt}(f')=2^{n-m-1}$ for any its subfunction f' of $n-m$ variables.

In terms of Walsh spectrum a function f on $\mathbf{F}_2^n$ is correlation-immune of order m if and only if $W_f(u)=0$ for all vectors $u\in\mathbf{F}_2^n$ such that $1\le|u|\le m$ [11]. In general, the order of correlation immunity is not invariant under affine transformations but it is invariant under isometric transformations.

1.2. **Regular functions.** Let f be a Boolean function on $\mathbf{F}_2^n$. If the induced graph $B^n[\mathrm{supp}(f)]$ is $(n-c_1)$-regular and the graph $B^n[\mathrm{supp}(\bar{f})]$ is $(n-c_2)$-regular then f corresponds to 2-*color perfect* (c_1,c_2)-*coloring* (or *equitable partition*). We call such function (c_1,c_2)-*regular*. It is easy to check that

$$\mathrm{wt}(f)\cdot c_1=(2^n-\mathrm{wt}(f))\cdot c_2$$

(both sides of this equality express the number of edges in B^n that connect vertices from $\mathrm{supp}(f)$ with vertices from $\mathrm{supp}(\bar{f})$). If additionally $W_f(0,\dots,0)=0$ (i.e. f is balanced) then $c_1=c_2=c$. In this case we call (c_1,c_2)-regular function simply *c-regular*. Any (c_1,c_2)-regular function is correlation-immune of order $\frac{c_1+c_2}{2}-1$ (it follows from [7] in combination with results of [8]). Moreover, if f is a (c_1,c_2)-regular function, then from $W_f(u)\neq 0$ it follows that $|u|\in\{0,\frac{c_1+c_2}{2}\}$.

Theorem 2. (Fon-Der-Flaass Theorem)[9] *Let $f(x_1,\dots,x_n)$ be nonconstant unbalanced correlation-immune of order m. Then*

$$m\le\frac{2n}{3}-1.$$

Moreover, if $m=\frac{2n}{3}-1$ then $\big(\mathrm{supp}(f),\mathrm{supp}(\bar{f})\big)$ is an equitable partition.

Proof. We give an alternative proof of Fon-Der-Flaass Theorem using the technique of Walsh coefficients. This proof was proposed by Khalyavin near 2010, published in [27] and re-published in [1]. The function f is unbalanced, it follows $W_f(0,\dots,0)\neq 0$. The function f is nonconstant, it follows that there exists $s_0\in\mathbf{F}_2^n$, $s_0\neq(0,\dots,0)$, such that $W_f(s_0)\neq 0$. The function f is correlation-immune of order m, therefore for any $u\in\mathbf{F}_2^n$ such that $1\le|u|\le m$ the equality $W_f(u)=0$ holds. It follows that $|s_0|\ge m+1$.

By Titsworth's Theorem for this s_0 we have

$$\sum_{u\in\mathbf{F}_2^n}W(u)W(u+s_0)=0. \tag{5}$$

In the sum (5) we see two nonzero equal summands for $u=0,s_0$. Suppose that $m>\frac{2n}{3}-1$. Then $|u|,|s_0|>\frac{2n}{3}$ follow $|u+s_0|<\frac{2n}{3}$. So the sum (5) has exactly two equal nonzero summands and value of this sum is 0, which is a contradiction.

If $m = \frac{2n}{3} - 1$ then the only possibility for other nonzero summands in the sum (5) is $|u|, |s_0|, |u + s_0| = \frac{2n}{3}$. So from the inequality $W_f(u) \neq 0$ it follows that $|u| \in \{0, m + 1\}$. It means that $\big(\mathrm{supp}(f), \mathrm{supp}(\bar{f})\big)$ is an equitable partition. $\square$

The generalization of Fon-Der-Flaass Theorem for orthogonal arrays was formulated and proved in [12].

For $m = \frac{2n}{3} - 1$ several families of such functions are known. For example, for each n divisible by 3 consider the characteristic function f of the linear code C given by the parity check matrix

$$\left(\begin{array}{cccccccccccc} 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 \end{array} \right).$$

The function f is $\big(n, \frac{n}{3}\big)$-regular, correlation-immune of order $\frac{2n}{3} - 1$, $\mathrm{wt}(f) = 2^n/4$. This function f can be expressed by the direct formula

$$f(x_1, \dots, x_n) = \left(1 \oplus \bigoplus_{i=1}^{\frac{2n}{3}} x_i \right) \left(1 \oplus \bigoplus_{i=\frac{n}{3}+1}^{n} x_i \right).$$

The spectrum support S_f of the function f is given by the matrix

$$\left(\begin{array}{cccccccccccc} 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 & 1 & 1 & \dots & 1 \end{array} \right).$$

(all vectors from S_f are written in rows of this matrix).

If some Boolean function on $\mathbf{F}_2^n$ is an equitable partition, then the transform $x_i \to y_{i,1} \oplus \dots \oplus y_{i,l}$ for all $i = 1, \dots, n$ keeps the property of a function to be an equitable partition but does not change cardinality and rank of the spectrum support.

For example, under the transformation $x_i \to y_{i,1} \oplus y_{i,2} \oplus y_{i,3}$, $i = 1, 2, 3$, the spectrum support given by the matrix

$$\left(\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{array} \right)$$

goes into the spectrum support given by the matrix

$$\left(\begin{array}{ccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{array} \right).$$

Thus, any example of an unbalanced function on $\mathbf{F}_2^n$ that is correlation-immune of order $m = \frac{2n}{3} - 1$ generates an infinite family of such functions for different n. The functions within each family have the same cardinality and rank of the

spectrum supports. Only a few families are known. Two of them start with the initial spectrum supports given by the matrices below:

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Two more families were given in [15, 10].

It should be noted that the existence of an infinite sequence of unbalanced correlation-immune of order $m = \frac{2n}{3} - 1$ functions with growing cardinality and rank of the spectrum supports is an open problem.

The following properties are obvious but helpful.

If $f(x_1, \ldots, x_n)$ is c-regular function, then the function $f(x_1, \ldots, x_n) \oplus x_1 \oplus \cdots \oplus x_n$ is $(n - c)$-regular.

If $f(x_1, \ldots, x_n)$ is c-regular, then $f(x_1, \ldots, x_n) \oplus x_{n+1}$ is $(c + 1)$-regular. (the variable x_{n+1} in this case is called *the linear variable*).

If $f(x_1, \ldots, x_n)$ is c-regular, then $g(x_1, \ldots, x_{n+1}) = f(x_1, \ldots, x_n)$ is c-regular (the variable x_{n+1} in this case is called *the fictitious (or nonessential) variable).*

The bounds on the maximum number of essential variables in c-regular functions were given in [25].

Proposition 1. [25] *Let $c = \text{const}$, $c \geq 2$. Then the maximal n such that there exists a c-regular function of n essential variables satisfies*

$$3 \cdot 2^{c-1} - 2 \leq \max n \leq c \cdot 2^{c-1}.$$

Proposition 1 can be reformulated by the following way.

Proposition 2. [25] *For given n the minimal possible c such that there exist c-regular function of n essential variables satisfies*

$$\min c = \log_2 n + O(\log_2 \log_2 n).$$

This result has a close connection with Simon–Wegener theorem. We give the reformulations of the theorems to compare them.

Theorem 3. (Simon–Wegener Theorem)[22, 32] *Suppose that the Boolean function f depends of n variables, all variables of f are essential. Suppose that in $B^n[\text{supp}(f)]$ for any $x \in \text{supp}(f)$ it holds $\deg(x) \geq n - c$. Suppose that in $B^n[\text{supp}(\bar{f})]$ for any $x \in \text{supp}(\bar{f})$ it holds $\deg(x) \geq n - c$. Then $\min c = (1/2) \log_2 n + O(\log_2 \log_2 n)$.*

Theorem 4. [25] *Suppose that the Boolean function f depends of n variables, all variables of f are essential. Suppose that in $B^n[\text{supp}(f)]$ for any $x \in \text{supp}(f)$ it holds $\deg(x) = n - c$. Suppose that in $B^n[\text{supp}(\bar{f})]$ for any $x \in \text{supp}(\bar{f})$ it holds $\deg(x) = n - c$. Then $\min c = \log_2 n + O(\log_2 \log_2 n)$.*

More advanced results follow from the theory of covering sequences [6].

1.3. **Plateaued functions with the given Walsh spectrum support.** Consider $S_f \subseteq \mathbf{F}_2^n$, the Walsh spectrum support of some hypothetical function f. We will use the notation S_f even if the function f is not defined yet and even if the function with such spectrum support does not exist. It is supposed that f is plateaued. It follows by Parseval's Identity that $|S_f| = 4^h$ for some integer h, $W_f \in \{0, \pm 2^{n-h}\}$. The problem is to reconstruct f, i.e., to define signs of Walsh coefficients from S_f.

This problem is motivated by the problem of reconstruction of a function from its autocorrelation coefficients.

Let f be a Boolean function on $\mathbf{F}_2^n$. *The autocorrelation function* for the Boolean function f is the integer-valued function $\Delta_f : \mathbf{F}_2^n \to [-2^n, 2^n]$ defined as

$$\Delta_f(u) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+f(x+u)}. \tag{6}$$

For each $u \in \mathbf{F}_2^n$ the value $\Delta_f(u)$ is called the autocorrelation coefficient of f at the vector u.

Autocorrelation coefficients are expressed via Walsh coefficients by the formula

$$\Delta_f(u) = 2^{-n} \sum_{x \in \mathbf{F}_2^n} W_f^2(x)(-1)^{\langle u,x \rangle}.$$

Conversely, the squares of Walsh coefficients are expressed via autocorrelation coefficients by the formula

$$W_f^2(v) = \sum_{u \in \mathbf{F}_2^n} \Delta_f(u)(-1)^{\langle u,v \rangle}.$$

Thus, if we know all autocorrelation coefficients of f, then we know only all squares of Walsh coefficients, i.e. we do not know signs of Walsh coefficients.

Some structural necessary conditions on matrix of S_f to correspond to at least one Boolean function and prohibited configurations are given in [29, 30, 33].

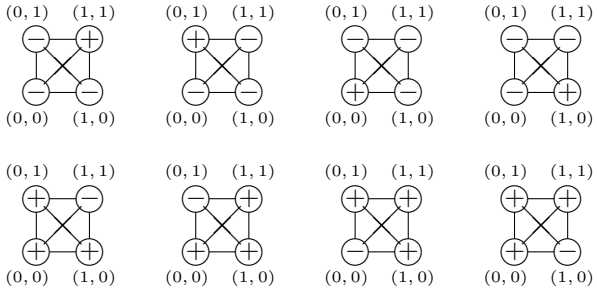
A powerful tool to investigate a choice of $\pm$ signs of Walsh coefficients is Titsworth's Theorem. The main condition in Titsworth's Theorem is

$$\sum_{u \in \mathbf{F}_2^n} W(u)W(u+s) = 0 \text{ for any } s \in \mathbf{F}_2^n, \ \ s \neq (0, \dots, 0).$$

Since f is plateaued it follows that all nonzero Walsh coefficients are equal by its absolute values.

We consider the complete graph K_{S_f} whose vertices correspond to vectors from S_f and divide the set of edges of K_{S_f} into subclasses of parallel edges. For each direction s, the number of edges $(u, u+s)$, $u \in S_f$, with the same signs at their ends (i.e. signs of Walsh coefficients $W_f(u)$ and $W_f(u+s)$) must be equal to the number of edges with different signs at their ends.

Consider the case $|S_f| = 4$. Four vectors from S_f must satisfy $x^1+x^2+x^3+x^4 = 0$. It is possible to translate S_f by an affine transformation to $\{(0,0,\dots), (0,1,\dots), (1,0,\dots), (1,1,\dots)\}$. It follows that the affine rank of S_f is 2. All variants to place signs $\pm$ near Walsh coefficients are given at the pictures below.



So we have exactly 8 plateaued functions with any given spectrum support S_f, $|S_f| = 4$.

The complete description of all Boolean functions (not necessary plateaued) with $|S_f| \leq 8$ was given in [19].

If f is plateaued and $|S_f| = 16$ then

$$4 \leq \text{Affine rank of } S_f \leq 6.$$

It was proved theoretically in [26].

Related results for $(n-4)$th order correlation-immune functions (plateaued functions with $|S_f| = 16$ are the most important particular case of such functions) were obtained in [2, 4].

Concerning the number of ways to place $\pm$ sings of Walsh coefficients, many researchers reported informally during last decade that they checked by a computer search that the number of plateaued functions f with $|S_f| = 16$ depends on the affine rank of S_f and is equal to

$$\begin{cases} 7 \cdot 2^7 & \text{if} \quad \text{the affine rank of } S_f \text{ is } 4, \\ 3 \cdot 2^7 & \text{if} \quad \text{the affine rank of } S_f \text{ is } 5, \\ 2^7 & \text{if} \quad \text{the affine rank of } S_f \text{ is } 6. \end{cases}$$

So this fact can be considered as a folklore.

If $|S_f| = 4^h$, $h > 2$, then to find the exact number of plateaued functions with this given S_f is generally a hard problem. To illustrate the hardness of this problem we give some examples.

The number of bent functions of n variables. Bent functions exist if and only if n is even. Bent functions can be considered as a particular but the most simple case of plateaued when $S_f = \mathbf{F}_2^n$. The number of n-variable bent functions is unknown for $n > 8$, n is even. For $n = 8$ the number of bent functions was found by Langevin and Leander in 2011 [16]. It is equal to

$$99270589265934370305785861242880 \approx 2^{106}.$$

The problem of existence of the $[9, 4, 240]$-CI functions, i.e. correlation-immune Boolean functions of the 4th order on $\mathbf{F}_2^9$ with nonlinearity 240. It is easy to demonstrate that such function (in the case of its existence) must be plateaued with the spectrum support $S_f = \{x \in \mathbf{F}_2^9 \mid |x| \in \{0, 5, 6, 7, 8\}\}$, $|S_f| = \binom{9}{0} + \binom{9}{5} + \binom{9}{6} + \binom{9}{7} + \binom{9}{8} = 256 = 4^4$. Beginning with 2000 some false proofs of the nonexistence of such function were produced and some of them were even published and reported at conferences. In 2010, Khalyavin [13] constructed a function with such parameters by means of advanced algorithms and a computer search.

The problem of existence of the $[17, 8, 2^{16}-2^8]$-CI functions [14]. It is easy to demonstrate that such function (in the case of its existence) must be plateaued with the spectrum support $S_f = \{x \in \mathbf{F}_2^{17} \mid |x| \in \{0, 9, 10, 11, 12, 13, 14,\ 15,\ 16\}\}$. It is still an open problem.

It seems that for the first time the exact number of plateaued functions for the concrete infinite sequence of spectrum supports of growing cardinality was found by Logachev-jr [17] for the recursive construction of Boolean functions introduced and investigated by Tarannikov [23, 24, 26].

The sequence of functions is defined recursively in the following way. Let f_0 be the Boolean function of $n_0 = 4$ variables,

$$f_0(x_1, x_2, x_3, x_4) = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_1 \oplus x_3.$$

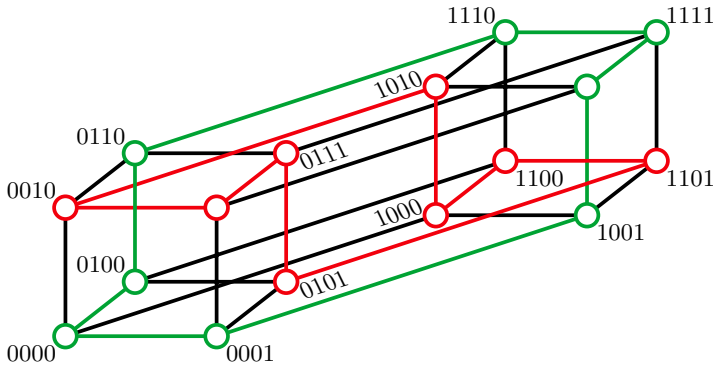
Then f_{k+1} is the Boolean function of $n_{k+1} = 2n_k + 2$ variables,

$$f_{k+1}(x, y, z) = (z_1 \oplus z_2 \oplus 1)(f_k(x) \oplus \langle 1^{n_k}, y\rangle) \oplus (z_1 \oplus z_2)(f_k(y) \oplus \langle 1^{n_k}, x\rangle) \oplus z_1$$

where $(x, y, z) \in \mathbf{F}_2^{n_{k+1}}$, $x, y \in \mathbf{F}_2^{n_k}$, $z \in \mathbf{F}_2^2$.

It follows that $n_k = 6 \cdot 2^k - 2$, f is plateaued.

The function f_0 is a 2-regular function (see the picture).



At this picture, the edges of the 2-regular graph $B^4[\mathrm{supp}(f)]$ are drawn by red, the edges of the 2-regular graph $B^4[\mathrm{supp}(\bar{f})]$ are drawn by green.

In the terminology of corresponding Walsh spectra, the matrix for S_{f_k} is denoted by A_k; the set of plateaued Boolean functions with the spectrum support S_{f_k} is denoted by M_k. Then [17] $A_0 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$,

$$A_k = \left(\begin{array}{cc|cc} & & 0 & 1 \\ A_{k-1} & 1\ldots1 & \vdots & \vdots \\ & & 0 & 1 \\ \hline & & 1 & 0 \\ A_{k-1} & 1\ldots1 & \vdots & \vdots \\ & & 1 & 0 \\ \hline & & 0 & 1 \\ 1\ldots1 & A_{k-1} & \vdots & \vdots \\ & & 0 & 1 \\ \hline & & 1 & 0 \\ 1\ldots1 & A_{k-1} & \vdots & \vdots \\ & & 1 & 0 \end{array}\right), \qquad \begin{array}{c} |M_{k+1}|{=}2|M_k|^2, \\ |M_k|{=}2^{4\cdot 2^k-1}, \\ f_k \text{ is the } (n-k-2)\text{-regular function.} \end{array}$$

It seems that the calculation of M_k in [17] was the first result on the exact number of plateaued functions for the concrete infinite sequence of spectrum supports of growing cardinality. We obtain new results in this direction in the following sections of our paper.

We will now make some remarks on symmetries of the functions f_{n_k}. Let T_n be the translation group, $g_t \in T_n$, $g_t : f(x) \to f(x+t)$, $|T_n| = 2^n$. Let $J_{T_n}(f) = \{t \in \mathbf{F}_2^n : f(x) + f(x+t) = 0\}$ be the inertia group of the function f relative to the group T_n.

Lemma 1. [17] *Any action of T_n does not change S_f.*

From Lemma 1 it follows ([17]) that $\{f_k\}_{T_{n_k}} \subseteq M_k$, $|J_{T_{n_k}}(f_k)| = 2^{2^{k+1}-1}$ and the number of equivalence classes of f_k respecting T_{n_k} is $|\{f_k\}_{T_{n_k}}| = \frac{|T_{n_k}|}{|J_{T_{n_k}}(f_k)|} = 2^{4\cdot 2^k - 1} = |M_k|$. Thus, $\{f_k\}_{T_{n_k}} = M_k$.

The new interesting direction of the spectral analysis of Boolean functions is the obtainment of bounds on the rank of a Boolean function f via its $|S_f| = s$ (s is called the sparsity of f in the terminology of [20, 21])

Recently Sanyal proved the following theorem.

Theorem 5. [20, 21] *For any Boolean function f the rank of S_f is $O(\sqrt{s}\log_2 s)$.*

It is not known whether the magnitude $O(\sqrt{s}\log_2 s)$ can be achieved. Sanyal pointed out [20, 21] that for the Address function Add_m (see Section 2 for the definition) the rank of S_{Add_m} is asymptotically $\sqrt{s}$. We discuss the spectral properties of Add_m in detail in Section 2.

At the same time for the recursive sequence of functions f_k (see above) the rank of S_{f_k} is asymptotically $2\sqrt{s}$ [26], this is currently the best known example.

As of today, the function f_k is the best known example of a Boolean function with some of the other extremal properties. It is an open problem to prove or to disprove that the function f_k given above is extremal in the following respects:

- $f_k \bigoplus_{i=1}^{n} x_i$ has the maximum possible number of essential variables among $(k+2)$-regular functions for fixed k;
- f_k has the maximum possible number n of variables for fixed k such that $B^n[\mathrm{supp}(f)]$ is a connected $(k+2)$-regular graph and $B^n[\mathrm{supp}(\bar{f})]$ is a connected $(k+2)$-regular graph;
- f_k has the maximum possible number of nonlinear variables for $(n-k-3)$-resilient functions;
- f_k has the maximum possible affine rank among all (plateaued) functions with $|S_f| = 4^{k+1}$.

2. Address function and its generalization

In this section we study the Address function and propose some its generalizations. We discover wide infinite families of spectrum supports for which we count the number of plateaued Boolean functions with such spectrum supports.

2.1. **Address function.**

In this subsection we study the Address function, prove that the Address function is plateaued, find its spectrum support and count the exact number of plateaued functions with such spectrum support.

We correspond the binary vector $(x_1, \ldots, x_m)$ to the integer number whose binary expansion is exactly this vector: $\xi(x_1, \ldots, x_m) = \sum\limits_{i=1}^{m} x_i \cdot 2^{m-i}$.

The Address function is a Boolean function on $\mathbf{F}_2^{m+2^m}$ defined in the following way:

$$\mathrm{Add}_m(x_1, \ldots, x_m, y_0, \ldots, y_{2^m-1}) = y_{\xi(x_1,\ldots,x_m)}.$$

The group of first m variables in the Address function will be referred to as *left,* the group of last 2^m variables will be referred to as *right.*

Proposition 3. *The Address function Add_m is plateaued, its spectrum support is $S_{Add_m} = \{(vu) \mid |u| = 1\}$.*

Proof. Let $v \in \mathbf{F}_2^m$, $u \in \mathbf{F}_2^{2^m}$. We have

$$W_{Add_m}(vu) = \sum_{xy \in \mathbf{F}_2^{m+2^m}} (-1)^{Add_m(xy)+\langle xy, vu\rangle} = W_{Add_m(xy)+\langle x,v\rangle+\langle y,u\rangle}(0, \ldots, 0) =$$

$$2^{m+2^m} - 2\mathrm{wt}(Add_m(xy) + \langle x, v\rangle + \langle y, u\rangle).$$

Expand the function $Add_m(xy) + \langle x, v\rangle + \langle y, u\rangle$ with respect to the left group of variables into 2^m subfunctions:

$$Add_m(xy) + \langle x, v\rangle + \langle y, u\rangle = \sum_{w \in \mathbf{F}_2^m} \left(\left(\prod_{i=1}^{m} (x_i \oplus w_i \oplus 1) \right) (y_{\xi(w)} + \langle y, u\rangle + \langle w, v\rangle) \right).$$

We see that every subfunction $y_{\xi(w)} + \langle y, u\rangle + \langle w, v\rangle$ has algebraic degree at most 1. If a subfunction has algebraic degree exactly 1, then it is balanced. Suppose $|u| \neq 1$, then all 2^m subfunctions are balanced, it follows that $\mathrm{wt}(Add_m(xy)+\langle x, v\rangle+\langle y, u\rangle) = 2^{m+2^m-1}$ and $W_{Add_m}(vu) = 0$, i.e. in this case we have $(vu) \notin S_{Add_m}$.

Now let $|u| = 1$; let i be the unique component such that $u_i = 1$. Then the variable y_i will remain a linear variable in all subfunctions except the one defined by such vector w that $\xi(w) = i$. This unique subfunction will be equal to some constant c. Therefore, in this case we have

$$\mathrm{wt}(Add_m(xy) + \langle x, v\rangle + \langle y, u\rangle) = (2^m - 1) \cdot 2^{2^m-1} + \begin{cases} 2^{2^m}, & \text{if } c = 1, \\ 0, & \text{if } c = 0, \end{cases}$$

i.e.

$$\mathrm{wt}(Add_m(xy) + \langle x, v\rangle + \langle y, u\rangle) = 2^{m+2^m-1} \mp 2^{2^m-1}.$$

It follows that $W_{Add_m}(vu) = \pm 2^{2^m}$, i.e. in this case we have $(vu) \in S_{Add_m}$. Note that at all vectors from S_{Add_m} Walsh coefficients are equal to $\pm 2^{2^m}$, therefore the Address function Add_m is plateaued. □

At every vector (vu) from $S_{Add_m} = \{(vu) \mid |u| = 1\}$ we define the Walsh coefficient $W(vu)$ of some hypothetic Boolean function, which possibly does not exist. At vector (vu) that do not belong to S_{Add_m} we automatically assume $W(vu) = 0$.

For every i, $i = 0, 1, \ldots, 2^m - 1$, we define the function $\widehat{f_i}$ on $\mathbf{F}_2^m$ as

$$\widehat{f_i}(v) = W(ve^i).$$

For every function $\widehat{f_i}$, $i = 0, 1, \ldots, 2^m - 1$, at every vector $x \in \mathbf{F}_2^m$ we define its Fourier coefficient:

$$F_{\widehat{f_i}}(x) = \sum_{v \in \mathbf{F}_2^m} \widehat{f_i}(v)(-1)^{\langle x,v\rangle}.$$

Remark 1. By the Inversion Formula for Fourier coefficients we have

$$W(ve^i) = \widehat{f}_i(v) = 2^{-m} \sum_{x \in \mathbf{F}_2^m} F_{\widehat{f}_i}(x)(-1)^{\langle x,v\rangle}, \tag{7}$$

therefore the assignment of all Walsh coefficients $W(vu)$ for a function whose spectrum support belongs to S_{Add_m} is equivalent to the assignment of Fourier coefficients $F_{\widehat{f}_i}(x)$ for all $i = 0, 1, \ldots, 2^m - 1$ и $x \in \mathbf{F}_2^m$.

Proposition 4. *The set of Fourier coefficients* $\{F_{\widehat{f}_i}(x) \,|\, i = 0, 1, \ldots, 2^m - 1,\ x \in \mathbf{F}_2^m\}$ *defines some Boolean function on* $\mathbf{F}_2^{m+2^m}$ *with the spectrum support in* S_{Add_m} *if and only if for any* $x \in \mathbf{F}_2^m$ *exactly one of the Fourier coefficients* $F_{\widehat{f}_i}(x)$, $i = 0, 1, \ldots, 2^m - 1$, *is equal to* $\pm 2^{m+2^m}$ *whereas the others are equal to* 0.

Proof. Let $\{F_{\widehat{f}_i}(x) \,|\, i = 0, 1, \ldots, 2^m - 1,\ x \in \mathbf{F}_2^m\}$ be the set of Fourier coefficients. For this set of coefficients to define some Boolean function f, by the Inversion Formula, taking into account the fact that the spectrum support lies within S_{Add_m}, it should satisfy

$$(-1)^{f(xy)} = \frac{1}{2^{m+2^m}} \sum_{\substack{v \in \mathbf{F}_2^m \\ u \in \mathbf{F}_2^{2^m}}} W_f(vu) \cdot (-1)^{\langle (xy),(vu)\rangle} =$$

$$\frac{1}{2^{m+2^m}} \sum_{i=0}^{2^m-1} (-1)^{y_i} \sum_{v \in \mathbf{F}_2^m} \widehat{f}_i(v) \cdot (-1)^{\langle x,v\rangle}$$

for every $x \in \mathbf{F}_2^m$, $y \in \mathbf{F}_2^{2^m}$. It follows that

$$(-1)^{f(xy)} = \frac{1}{2^{m+2^m}} \sum_{i=0}^{2^m-1} (-1)^{y_i} F_{\widehat{f}_i}(x). \tag{8}$$

From (8) it follows that for fixed $x \in \mathbf{F}_2^m$ for every $y \in \mathbf{F}_2^{2^m}$ the value $A(x,y) = \sum\limits_{i=0}^{2^m-1} (-1)^{y_i} F_{\widehat{f}_i}(x)$ must be equal to $\pm 2^{m+2^m}$. This is possible only if one of values $F_{\widehat{f}_i}(x)$ is equal to $\pm 2^{m+2^m}$ whereas others are equal to 0. Indeed, if all $F_{\widehat{f}_i}(x) = 0$ then $A(x,y) = 0$ but not $\pm 2^{m+2^m}$. Let at least two Fourier coefficients not to be equal to 0: $F_{\widehat{f}_j}(x) \neq 0$ and $F_{\widehat{f}_j'}(x) \neq 0$, $j \neq j'$. Denote $B = \sum\limits_{\substack{0 \le i \le 2^m-1 \\ i \neq j, j'}} F_{\widehat{f}_i}(x)$. Then, choosing different vectors $y \in \mathbf{F}_2^{2^m}$, it is possible to obtain for $A(x,y)$ at least three different values: $B + |F_{\widehat{f}_j}(x)| + |F_{\widehat{f}_j'}(x)|$, $B + |F_{\widehat{f}_j}(x)| - |F_{\widehat{f}_j'}(x)|$ and $B - |F_{\widehat{f}_j}(x)| - |F_{\widehat{f}_j'}(x)|$ whereas it should be at most two different values: $\pm 2^{m+2^m}$. This contradiction eliminates all but one cases: when exactly one of the Fourier coefficients satisfies $F_{\widehat{f}_i}(x) \neq 0$. Then, obviously, the statement of the theorem is satisfied: $F_{\widehat{f}_i}(x) = \pm 2^{m+2^m}$.

The converse is trivial: if for any $x \in \mathbf{F}_2^m$ exactly one of the Fourier coefficients $F_{\widehat{f}_i}(x)$, $i = 0, 1, \ldots, 2^m - 1$, is equal to $\pm 2^{m+2^m}$ whereas others are equal to 0 then the expression in the right side of (8) is equal to ± 1, therefore the Boolean function is defined. □

Corollary 1. *There exist exactly* $2^{(m+1)2^m}$ *Boolean functions on* $\mathbf{F}_2^{m+2^m}$ *whose spectrum support belongs to* S_{Add_m}.

Proof. By Proposition 4 for every $x \in \mathbf{F}_2^m$ exactly one of Fourier coefficients $F_{\widehat{f}_i}(x)$ must be equal to $\pm 2^{m+2^m}$ whereas others should be equal to 0. For every $x \in \mathbf{F}_2^m$ it is possible to choose the position i for nonzero Fourier coefficient by 2^m ways and to choose its sign by two ways. Therefore the total number of ways to assign all Fourier coefficients is $(2^{m+1})^{2^m} = 2^{(m+1)2^m}$. □

Theorem 6. *There exist exactly* $2^{2^m} \cdot (2^m)!$ *Boolean functions on* $\mathbf{F}_2^{m+2^m}$ *whose spectrum support coincides with* S_{Add_m}. *All these functions are plateaued.*

Proof. If for some $i \in \{0, 1, \ldots, 2^m - 1\}$ Fourier coefficients $F_{\widehat{f}_i}(x)$ for all $x \in \mathbf{F}_2^m$ are equal to 0, then by the Inversion Formula (7) all $W(ve^i) = 0$ and the spectrum support does not coincide with S_{Add_m}. Thus, for every i, $i = 0, 1, \ldots, 2^m - 1$, there must exist such $x \in \mathbf{F}_2^m$ that $F_{\widehat{f}_i}(x) \neq 0$. At the same time by Proposition 4 there exist exactly 2^m nonzero Fourier coefficients (one for each $x \in \mathbf{F}_2^m$), therefore for every i such Fourier coefficient is unique. Choosing position x of the nonzero Fourier coefficient for each i can be done in $(2^m)!$ ways, each of them can be assigned a sign in two ways. Thus, the total number of ways is equal to $2^{2^m} \cdot (2^m)!$ Moreover, for each i, $i = 0, 1, \ldots, 2^m - 1$, and each $v \in \mathbf{F}_2^m$ by the Inversion Formula (7) we have $W(ve^i) = 2^{-m} \cdot (\pm 2^{m+2^m}) = \pm 2^{2^m}$. Thus, for any such assignment the spectrum support of the obtained function coincides with S_{Add_m} and the function is plateaued. □

2.2. **Generalizations of Address function.** In this subsection we generalize the Address function and count the exact number of plateaued Boolean functions for wide infinite families of spectrum supports. In Theorem 7 we give the expression for the exact number of plateaued Boolean functions with the spectrum support of such specific forms via the number of partitions of the vector space into translations of some set of linear subspaces. Thus, future solutions of the problem on the number of partitions for some new sets of subspaces will give new numbers of plateaued Boolean functions for given specific spectrum supports.

Let m_1, m_2 be integers, L_i be some subspaces of the space $\mathbf{F}_2^{m_1}$, $a^i \in \mathbf{F}_2^{m_1}$, $i = 1, \ldots, m_2$.

Until the end of Section 2 we assign the spectrum support S of a hypothetic function as: $S \subseteq \mathbf{F}_2^{m_1+m_2}$, $S = \{(vu) \,|\, v \in L_i + a^i,\, u = e^i, i \in \{1, \ldots, m_2\}\}$.

The aim of the investigation is to formulate conditions when it is possible to find an exact number of (plateaued) functions with the spectrum support S. In the remained part of this section we assume that the linear subspaces L_i and their translations $L_i + a^i$ are fixed as well as the spectrum support S.

In the same way as described in the previous subsection, let us consider the set of Walsh coefficients values $W(vu)$ with support inside of S. At vectors outside of S we assume $W(vu) = 0$. We need to check whether this set corresponds to some Boolean function.

In the same way as it was made in the previous subsection, for each i, $i = 1, \ldots, m_2$, we define the function $\widehat{f}_i$ on $\mathbf{F}_2^{m_1}$ as:

$$\widehat{f}_i(v) = W(ve^i).$$

For every function $\widehat{f}_i$, $i = 1, \ldots, m_2$, at every vector $x \in \mathbf{F}_2^{m_1}$ we define its Fourier coefficient:

$$F_{\widehat{f}_i}(x) = \sum_{v \in \mathbf{F}_2^{m_1}} \widehat{f}_i(v)(-1)^{\langle x, v \rangle}.$$

By the Inversion Formula for Fourier coefficients we have

$$W(ve^i) = \widehat{f_i}(v) = 2^{-m_1} \sum_{x \in \mathbf{F}_2^{m_1}} F_{\widehat{f_i}}(x)(-1)^{\langle x,v \rangle}, \tag{9}$$

therefore, Walsh coefficients $W(vu)$ with support inside of S can be fully determined by Fourier coefficients $F_{\widehat{f_i}}(x)$ for all $i = 1, \ldots, m_2$ and $x \in \mathbf{F}_2^{m_1}$.

Absolutely similarly to the proof of the Proposition 4 it is possible to prove the following proposition.

Proposition 5. *The set of Fourier coefficients* $\{F_{\widehat{f_i}}(x) \,|\, i = 1, \ldots, m_2,\, x \in \mathbf{F}_2^{m_1}\}$ *defines some Boolean function on* $\mathbf{F}_2^{m_1+m_2}$ *with the spectrum support inside of* $S^* = \{(vu) \,|\, v \in \mathbf{F}_2^{m_1}, u = e^i, i \in \{1, \ldots, m_2\}\}$*, if and only if for any* $x \in \mathbf{F}_2^{m_1}$ *exactly one of Fourier coefficients* $F_{\widehat{f_i}}(x)$*,* $i = 1, \ldots, m_2$*, is equal to* $\pm 2^{m_1+m_2}$*, whereas others are equal to* 0*.*

Note that $S \subset S^*$ (except the case when all $L_i = \mathbf{F}_2^{m_1}$) and, in general, the spectrum support lying in S^* might not lie in S.

Lemma 2. *Let* $i \in \{1, \ldots, m_2\}$*,* $b \in L_i^{\perp}$*. Then for every* $v \in \mathbf{F}_2^{m_1}$ *the equality*

$$F_{\widehat{f_i}}(v + b) = (-1)^{\langle a^i, b \rangle} \cdot F_{\widehat{f_i}}(v)$$

holds.

Proof. Taking into account that $\widehat{f_i}(x) = 0$ outside of $L_i + a^i$, making the change of a variable $x + a^i = y$, using $(-1)^{\langle b,y \rangle} = 1$ and then changing the variable back, we have

$$F_{\widehat{f_i}}(v + b) = \sum_{x \in \mathbf{F}_2^{m_1}} \widehat{f_i}(x)(-1)^{\langle v+b,x \rangle} = \sum_{x \in L + a^i} \widehat{f_i}(x)(-1)^{\langle v+b,x \rangle} =$$

$$\sum_{y \in L_i} \widehat{f_i}(y + a^i)(-1)^{\langle v+b,y+a^i \rangle} = (-1)^{\langle a^i,b \rangle} \sum_{y \in L_i} \widehat{f_i}(y + a^i)(-1)^{\langle v,y+a^i \rangle} =$$

$$(-1)^{\langle a^i,b \rangle} \sum_{x \in L_i + a^i} \widehat{f_i}(x)(-1)^{\langle v,x \rangle} = (-1)^{\langle a^i,b \rangle} \cdot F_{\widehat{f_i}}(v).$$

□

Corollary 2. *If the spectrum support of a Boolean function* f *on* $\mathbf{F}_2^{m_1+m_2}$ *lies in* S *and for some* i*,* $i \in \{1, \ldots, m_2\}$*, we have* $\widehat{f_i}(x) \not\equiv 0$ *then the number of nonzero Fourier coefficients* $F_{\widehat{f_i}}(v)$ *of the function* $\widehat{f_i}$ *is not less than* $2^{\dim L_i^{\perp}} = 2^{m_1 - \dim L_i}$*.*

Proof. From Lemma 2 it follows that all vectors of $\mathbf{F}_2^{m_1}$ are divided into groups of $2^{\dim L_i^{\perp}} = 2^{m_1 - \dim L_i}$ vectors where the Fourier coefficients $F_{\widehat{f_i}}(v)$ of the function $\widehat{f_i}$ are equal in absolute values. □

Corollary 3. *If* $\sum\limits_{i=1}^{m_2} 2^{m_1 - \dim L_i} > 2^{m_1}$ *then there do not exist Boolean functions on* $\mathbf{F}_2^{m_1+m_2}$ *with the spectrum support* S*.*

Proof. By Corollary 2, the total number, over all i, of nonzero Walsh coefficients $F_{\widehat{f_i}}(v)$ of the function $\widehat{f_i}$ is greater than 2^{m_1}, whereas by Proposition 5 this number is exactly equal to 2^{m_1}. □

Corollary 4. *If* $\sum_{i=1}^{m_2} 2^{m_1-\dim L_i} = 2^{m_1}$ *and there exists a Boolean function on* $\mathbf{F}_2^{m_1+m_2}$ *with the spectrum support* S *then for each* i, $i=1,\dots,m_2$, *the number of nonzero Walsh coefficients* $F_{\widehat{f}_i}(v)$ *of the function* $\widehat{f}_i$ *is exactly equal to* $2^{\dim L_i^\perp} = 2^{m_1-\dim L_i}$.

Proof. It follows immediately from Corollary 2 and Proposition 5. □

Lemma 3. *Suppose that the spectrum support of a Boolean function* f *on* $\mathbf{F}_2^{m_1+m_2}$ *lies in* S *and for some* i, $i\in\{1,\dots,m_2\}$, *the number of nonzero Fourier coefficients* $F_{\widehat{f}_i}(v)$ *of the function* $\widehat{f}_i$ *is exactly equal to* $2^{\dim L_i^\perp} = 2^{m_1-\dim L_i}$. *Then for every* $v\in\mathbf{F}_2^{m_1}$ *it holds*

$$W_f(ve^i) = \begin{cases} \pm 2^{m_1+m_2-\dim L_i}, & \text{if} \quad v\in L_i+a^i,\\ 0, & \text{if} \quad v\notin L_i+a^i. \end{cases}$$

Proof. Let v^0 be some vector from $\mathbf{F}_2^m$ such that $F_{\widehat{f}_i}(v^0)\neq 0$. By Proposition 5 we have $F_{\widehat{f}_i}(v^0) = \pm 2^{m_1+m_2}$. By the formula (9) using Lemma 2 we have

$$W_f(ve^i) = \widehat{f}_i(v) = 2^{-m_1}\sum_{x\in\mathbf{F}_2^{m_1}} F_{\widehat{f}_i}(x)(-1)^{\langle x,v\rangle} = 2^{-m_1}\sum_{x\in L_i^\perp+v^0} F_{\widehat{f}_i}(x)(-1)^{\langle x,v\rangle} =$$

$$2^{-m_1}\sum_{b\in L_i^\perp} F_{\widehat{f}_i}(v^0+b)(-1)^{\langle v^0+b,v\rangle} = 2^{-m_1}(-1)^{\langle v^0,v\rangle}\sum_{b\in L_i^\perp}(-1)^{\langle a^i,b\rangle}F_{\widehat{f}_i}(v^0)(-1)^{\langle b,v\rangle} =$$

$$2^{-m_1}(-1)^{\langle v^0,v\rangle}F_{\widehat{f}_i}(v^0)\sum_{b\in L_i^\perp}(-1)^{\langle a^i+v,b\rangle} = \pm 2^{m_2}\sum_{b\in L_i^\perp}(-1)^{\langle a^i+v,b\rangle}.$$

If $a^i+v\notin L_i$ then $\sum_{b\in L_i^\perp}(-1)^{\langle a^i+v,b\rangle} = 0$. In the opposite case if $a^i+v\in L_i$ then $\sum_{b\in L_i^\perp}(-1)^{\langle a^i+v,b\rangle} = 2^{\dim L_i^\perp} = 2^{m_1-\dim L_i}$. From this the statement of the lemma follows. □

Corollary 5. *Suppose that the spectrum support of a Boolean function* f *on* $\mathbf{F}_2^{m_1+m_2}$ *lies in* S. *If* $\sum_{i=1}^{m_2} 2^{m_1-\dim L_i} = 2^{m_1}$ *and for every* i, $i=1,\dots,m_2$, *the number of nonzero Fourier coefficients* $F_{\widehat{f}_i}(v)$ *of functions* $\widehat{f}_i$ *is equal to exactly* $2^{\dim L_i^\perp} = 2^{m_1-\dim L_i}$, *then the spectrum support of the function* f *coincides with* S. *Moreover,* f *is plateaued if and only if all values* $\dim L_i$ *are equal to each other,* $i=1,\dots,m_2$.

Proof. It follows directly from Lemma 3. □

Lemma 4. *Let* $\{F_{\widehat{f}_i}(x)\}$, $i=1,\dots,m_2$, $x\in\mathbf{F}_2^{m_1}$ *be the set of Fourier coefficients such that for any* $i\in\{1,\dots,m_2\}$, *any* $b\in L_i^\perp$, *any* $v\in\mathbf{F}_2^{m_1}$ *the equality* $F_{\widehat{f}_i}(v+b) = (-1)^{\langle a^i,b\rangle}\cdot F_{\widehat{f}_i}(v)$ *holds. Then for the spectrum support* $S_{\{F\}}$ *defined by* $\{F_{\widehat{f}_i}(x)\}$ *we have* $S_{\{F\}}\subseteq S$.

Proof. Let v^j, $j=1\dots,s$, be representatives of all different translations of $L_i^\perp$. Then for any $i\in\{1,\dots,m_2\}$ we have

$$W_f(ve^i) = \widehat{f}_i(v) = 2^{-m_1}\sum_{x\in\mathbf{F}_2^{m_1}} F_{\widehat{f}_i}(x)(-1)^{\langle x,v\rangle} = 2^{-m_1}\sum_{j=1}^{s}\sum_{x\in L_i^\perp+v^j} F_{\widehat{f}_i}(x)(-1)^{\langle x,v\rangle} =$$

$$2^{-m_1}\sum_{j=1}^{s}\sum_{b\in L_i^\perp} F_{\widehat{f}_i}(v^j+b)(-1)^{\langle v^j+b,v\rangle} =$$

$$2^{-m_1}\sum_{j=1}^{s}(-1)^{\langle v^j,v\rangle}\sum_{b\in L_i^\perp}(-1)^{\langle a^i,b\rangle}F_{\widehat{f}_i}(v^j)(-1)^{\langle b,v\rangle} =$$

$$2^{-m_1}\sum_{j=1}^{s}(-1)^{\langle v^j,v\rangle}F_{\widehat{f}_i}(v^j)\sum_{b\in L_i^\perp}(-1)^{\langle a^i+v,b\rangle}.$$

If $a^i+v\notin L_i$ then $\sum\limits_{b\in L_i^\perp}(-1)^{\langle a^i+v,b\rangle}=0$. It means that if $v\notin L_i+a^i$ then $W(ve^i)=0$. Thus, $S_{\{F\}}\subseteq S$. □

Let $N(r_1,L_{i_1}^\perp;\dots;r_s,L_{i_s}^\perp)$ be the number of ways to divide the space $\mathbf{F}_2^{m_1}$ into linear subspaces among which there are exactly r_j subspaces of the form $L_{i_j}^\perp+b$, $j=1,\dots,s$.

Theorem 7. *Let* $\sum\limits_{i=1}^{m_2}2^{m_1-\dim L_i}=2^{m_1}$. *Let* $L_{i_1},\dots,L_{i_s}$ *be all different linear subspaces among* $L_1,\dots,L_{m_2}$. *Let* r_j *be the number of times that* L_{i_j} *appears among linear subspaces* $L_1,\dots,L_{m_2}$. *Then the number of Boolean functions on* $\mathbf{F}_2^{m_1+m_2}$ *with the spectrum support* S *is exactly equal to*

$$N(r_1,L_{i_1}^\perp;\dots;r_s,L_{i_s}^\perp)\cdot 2^{m_2}\cdot\prod_{j=1}^{s}(r_j)!$$

Proof. From the condition $\sum\limits_{i=1}^{m_2}2^{m_1-\dim L_i}=2^{m_1}$ and Lemma 2 it follows that for each i, $i\in\{1,\dots,m_2\}$, the number of nonzero Fourier coefficients $F_{\widehat{f}_i}(v)$ of the function $\widehat{f}_i$ is exactly equal to $2^{\dim L_i^\perp}=2^{m_1-\dim L_i}$. Moreover, for any fixed i all nonzero Fourier coefficients of $\widehat{f}_i$ must be at all vectors of some translation of $L_i^\perp$ and can be assigned there in exactly two ways. For any j, $j=1,\dots,s$, the components for r_j different translations of L_{i_j} can be permuted in exactly $r_j!$ ways. Lemma 4 and Corollary 5 guarantee that after any such assignment the spectrum support will coincide with S. □

Remark 2. From Lemma 3 it follows easily that if in Theorem 7 all values $\dim L_i$, $i=1,\dots,m_2$, are equal to each other, then all Boolean functions with the spectrum support S are plateaued. If $\dim L_{i'}\neq\dim L_{i''}$ for at least one pair (i',i'') of indexes then all Boolean functions with the spectrum support S are not plateaued.

Example 1. Let $m_2=2^{m_1-1}$, $L_1=\dots=L_t=\{x\in\mathbf{F}_2^{m_1}\,|\,x_1=0\}$, $L_{t+1}=\dots=L_{m_2}=\{x\in\mathbf{F}_2^{m_1}\,|\,x_2=0\}$. In this case we have $s=2$, L_1 and L_{t+1} are all different linear subspaces; $L_1^\perp=\{\vec{0},e^1\}$, $L_{t+1}^\perp=\{\vec{0},e^2\}$; $r_1=t$, $r_2=m_2-t$. For obvious reasons all vectors from $\mathbf{F}_2^{m_1}$ are divided into 2^{m_1-2} groups of four vectors: $\{a,a+e^1,a+e^2,a+e^1+e^2\}$. So, the vector a must be covered either by the translation $L_1^\perp+a$ or by the translation $L_{t+1}^\perp+a$. In the first case the translation $L_1^\perp+(a+e^2)$ must be taken into the partition of $\mathbf{F}_2^{m_1}$ together with $L_1^\perp+a$. In the second case the translation $L_{t+1}^\perp+(a+e^1)$ must be taken into the partition of $\mathbf{F}_2^{m_1}$ together with $L_{t+1}^\perp+a$. Thus, any group of four vectors can be covered by exactly two ways. It is necessary to choose $t/2$ groups of 2^{m_1-2} that will be covered

by two translations of $L_1^\perp$, all remained groups must be covered by two translations of $L_{t+1}^\perp$. Therefore, we have

$$N(t, L_1^\perp; m_2 - t, L_{t+1}^\perp) = \begin{cases} \binom{2^{m_1-2}}{t/2} & \text{if} \quad t \text{ even}, \\ 0 & \text{if} \quad t \text{ odd} \end{cases}$$

and the number of Boolean functions with the spectrum support S is exactly equal to 0 for odd t and

$$N(t, L_1^\perp; m_2 - t, L_{t+1}^\perp) \cdot 2^{m_2} \cdot \prod_{j=1}^{s} (r_j)! = \binom{2^{m_1-2}}{t/2} \cdot 2^{2^{m_1-1}} \cdot t! \cdot (2^{m_1-1} - t)! \tag{10}$$

for even t, all these functions are plateaued.

2.3. **On the number of functions whose spectrum support is a subset of S.** Let $H(L_{i_1}^\perp, \dots, L_{i_s}^\perp)$ be the set of partitions of the subspace $\mathbf{F}_2^{m_1}$ into translations of linear subspaces $L_{i_1}^\perp, \dots, L_{i_s}^\perp$.

Theorem 8. *Let $L_{i_1}, \dots, L_{i_s}$ be all different linear subspaces among $L_1, \dots, L_{m_2}$. Let r_j be the number of times that the subspace L_{i_j} appears among linear subspaces $L_1, \dots, L_{m_2}$. Let $(l_1(h), \dots, l_s(h))$ be the vector of numbers of occurrences of translations of subspaces $L_{i_1}^\perp, \dots, L_{i_s}^\perp$ in the partition $h \in H(L_{i_1}^\perp, \dots, L_{i_s}^\perp)$. Then the number of Boolean functions with the spectrum support inside of S is exactly equal to*

$$\sum_{h \in H(L_{i_1}^\perp, \dots, L_{i_s}^\perp)} 2^{\sum_{j=1}^{s} l_j(h)} \prod_{j=1}^{s} r_j^{l_j(h)}.$$

Proof. Any Boolean function with the spectrum support inside of S^* is defined by the set of Fourier coefficients $\{F_{\widehat{f}_i}(x)\}$, $i = 1, \dots, m_2$, $x \in \mathbf{F}_2^{m_1}$. By Proposition 5 for any $x \in \mathbf{F}_2^{m_1}$ exactly one of Fourier coefficients $F_{\widehat{f}_i}(x)$, $i = 1, \dots, m_2$, is equal to $\pm 2^{m_1+m_2}$, whereas others are equal to 0. By Lemma 2 for any $v \in \mathbf{F}_2^{m_1}$, $b \in L_i^\perp$ the equality $F_{\widehat{f}_i}(v + b) = (-1)^{\langle a^i, b \rangle} \cdot F_{\widehat{f}_i}(v)$ holds. It means that for given i all Fourier coefficients of $\widehat{f}_i$ at some translation $L_i^\perp + b$ of $L_i^\perp$ are defined uniquely by the value $F_{\widehat{f}_i}(b)$ where b is some representative of this translation of $L_i^\perp$. On the other hand, if for any $i \in \{1, \dots, m_2\}$, any $b \in L_i^\perp$, any $v \in \mathbf{F}_2^{m_1}$ the equality $F_{\widehat{f}_i}(v + b) = (-1)^{\langle a^i, b \rangle} \cdot F_{\widehat{f}_i}(v)$ holds, then by Lemma 4 the spectrum support of the Boolean function will be inside of S.

So the vector space $\mathbf{F}_2^{m_1}$ must be divided into translations of $L_{i_1}^\perp$, …, $L_{i_s}^\perp$. For any such partition $h \in H(L_{i_1}^\perp, \dots, L_{i_s}^\perp)$ we can choose in two ways the sign $\pm$ of nonzero Fourier coefficient at the representative of each of $\sum_{j=1}^{s} l_j(h)$ translations and we can choose in r_j ways the component i where Fourier coefficients at this translation of $L_{i_j}^\perp$ will be nonzero. □

2.4. **Modifications of S.** The spectrum support S can be modified with the preservation of the number of (plateaued) functions with such spectrum support. Let $D \subseteq \mathbf{F}_2^{m_2'}$, $|D| = m_2$ and for any vectors $a, b, c \in D$ their sum $a + b + c$ does not belong to D. Let $\tau : \{1, \dots, m_2\} \to D$ be a bijection. Let $\mu : S^* \to \mathbf{F}_2^{m_1+m_2'}$ be a mapping such that $\mu(ve^i) = v\tau(i)$ for any $v \in \mathbf{F}_2^{m_1}$, $i = 1, \dots, m_2$.

Define some real-valued function $W(u)$ on S. Extend this function to $\mathbf{F}_2^{m_1+m_2}$ putting $W(u) = 0$ if $u \in \mathbf{F}_2^{m_1+m_2} \setminus S$. Define the real valued function $W'(u')$ on $\mathbf{F}_2^{m_1+m_2'}$ as $W'(\mu(u)) = 2^{m_2'-m_2}W(u)$, $W'(u') = 0$ if $u' \neq \mu(u)$ for any $u \in S$.

Proposition 6. *The set of values $\{W(u)\}$ is the set of Walsh coefficients of some Boolean function on $\mathbf{F}_2^{m_1+m_2}$ if and only if $\{W'(u')\}$ is the set of Walsh coefficients of some Boolean function on $\mathbf{F}_2^{m_1+m_2'}$.*

Proof. It is easy to see that conditions from Titsworth's Theorem for the set $\{W(u)\}$ are in one-to-one correspondence with the conditions for the set $\{W'(u')\}$. □

Remark 3. The words «real-valued» instead of «integer-valued» in the definition of Walsh coefficients should not embarrass us. In fact, the proof of Titsworth's Theorem is correct even for real-valued coefficients but the set with at least one non-integer coefficient cannot correspond to any Boolean function.

3. Recursive construction of spectrum supports

In this section we generalize the recursive construction of spectrum supports from [17]. It gives more possibilities to count new exact numbers of plateaued Boolean functions with given specific spectrum supports.

Formally, in [17] the exact number of plateaued functions was found only for one concrete infinite sequence of spectrum supports. At the same time Lemma 2 in [17] can be applied to different initial spectrum supports in the recursive construction (but neither another spectrum supports nor the proof of their existence were given). In this Section we generalize Lemma 2 in [17] and prove the exact number of functions with the combined spectrum support depending on the exact numbers of functions with initial spectrum supports.

Let $S^1 \subseteq \mathbf{F}_2^{n_1}$, $S^2 \subseteq \mathbf{F}_2^{n_2}$, $(0,\dots,0) \notin S^1$, $(0,\dots,0) \notin S^2$, $|S^1| = |S^2| = 4^{h-1}$. Let A be the matrix of S^1, i.e. rows of A are exactly all vectors from S^1. Let B be the matrix of S^2. Let p_1 and p_2 be the exact numbers of plateaued functions with the spectrum supports S^1 and S^2, correspondingly. Consider the spectrum support in $\mathbf{F}_2^n$, $n = n_1 + n_2 + 2$, defined by the matrix

$$C = \left(\begin{array}{cccc}
 & 0\dots0 & 0 & 1 \\
A & \cdots & \vdots & \vdots \\
 & 0\dots0 & 0 & 1 \\
\hline
 & 0\dots0 & 1 & 0 \\
A & \cdots & \vdots & \vdots \\
 & 0\dots0 & 1 & 0 \\
\hline
0\dots0 & & 0 & 1 \\
\cdots & B & \vdots & \vdots \\
0\dots0 & & 0 & 1 \\
\hline
0\dots0 & & 1 & 0 \\
\cdots & B & \vdots & \vdots \\
0\dots0 & & 1 & 0
\end{array}\right).$$

Theorem 9. *The number of plateaued functions with the spectrum support of cardinality 4^h defined by the matrix C is exactly $2p_1p_2$.*

Proof. We follow the proof of Lemma in [17] (the main difference is that in [17] the matrices A and B were identical).

The number of rows in the matrix C is 4^h. So at any vector u, $u \in S_f$, by Parseval's Identity we have $W_f(u) = \pm 2^{n-h}$. Since we are interested only in signs $\pm$ of Walsh coefficients, we introduce auxiliary values φ, $\varphi(u) = 2^{-n+h} W_f(u)$; also we introduce the similar values $\varphi(u) = 2^{-n_1+h-1} W_f(u)$ and $\varphi(u) = 2^{-n_2+h-1} W_f(u)$ for the spectrum supports S^1 and S^2, correspondingly.

Thus, $\varphi(u) \in \{\pm 1\}$ if $u \in S_f$ and $\varphi(u) = 0$ if $u \notin S_f$. From Titsworth's Theorem it follows that

$$\sum_{u \in \mathbf{F}_2^n} \varphi(u)\varphi(u+s) = 0 \tag{11}$$

for all $s \in \mathbf{F}_2^n$, $s \neq (0, \ldots, 0)$. We call the vectors s in (11) *the directions.* It is sufficient to consider only such directions s that there exists at least one vector u provided $\varphi(u) \neq 0$, $\varphi(u+s) \neq 0$. For given s we call all pairs of vector $(u, u+s)$ such that $\varphi(u) \neq 0$, $\varphi(u+s) \neq 0$ *the bundle of parallel lines.* We call the first quarter of rows of the matrix C *the first band*; we call the second, third, fourth quarters of rows of C *the second, third, fourth bands,* correspondingly. For brevity, we write I instead of «the first band», analogously for the second, third and fourth bands.

Let $\alpha^0 \in I$, $\beta^0 \in III$. Then, for the direction $s = \alpha^0 + \beta^0$ it is easy to see from the structure of the matrix C that the bundle of parallel lines consists of only two pair of vectors $\{(\alpha^0, \beta^0), (\alpha^*, \beta^*)\}$ where $\alpha^* \in II$, $\beta^* \in IV$, $\alpha^0 + \alpha^* = \beta^0 + \beta^* = (0, \ldots, 0, 1, 1)$. Thus, the formula (11) takes the form

$$\varphi(\alpha^0)\varphi(\beta^0) + \varphi(\alpha^*)\varphi(\beta^*) = 0. \tag{12}$$

If $\varphi(\alpha^0)\varphi(\alpha^*) = 1$ then $\varphi(\beta^0)\varphi(\beta^*) = -1$. Fix $\varphi(\alpha^0)$ and $\varphi(\alpha^*)$. Then, going through all $\beta^0 \in III$ we obtain that $\varphi(\beta^0)\varphi(\beta^*) = -1$ for all $\beta^0 \in III$. Now fix $\varphi(\beta^0)$ and $\varphi(\beta^*)$. Then, going through all $\alpha^0 \in I$ we obtain that $\varphi(\alpha^0)\varphi(\alpha^*) = 1$ for all $\alpha^0 \in I$.

If $\varphi(\alpha^0)\varphi(\alpha^*) = -1$ then $\varphi(\beta^0)\varphi(\beta^*) = 1$. Fix $\varphi(\alpha^0)$ and $\varphi(\alpha^*)$. Then, going through all $\beta^0 \in III$ we obtain that $\varphi(\beta^0)\varphi(\beta^*) = 1$ for all $\beta^0 \in III$. Now fix $\varphi(\beta^0)$ and $\varphi(\beta^*)$. Then, going through all $\alpha^0 \in I$ we obtain that $\varphi(\alpha^0)\varphi(\alpha^*) = -1$ for all $\alpha^0 \in I$.

Let $\alpha^0 \in I$, $\beta^0 \in IV$. Then, for the direction $s = \alpha^0 + \beta^0$ it is easy to see from the structure of the matrix C that the bundle of parallel lines consists of only two pair of vectors $\{(\alpha^0, \beta^0), (\alpha^*, \beta^*)\}$ where $\alpha^* \in II$, $\beta^* \in III$, $\alpha^0 + \alpha^* = \beta^0 + \beta^* = (0, \ldots, 0, 1, 1)$. Thus, the formula (11) takes the form (12).

If $\varphi(\alpha^0)\varphi(\alpha^*) = 1$ then $\varphi(\beta^0)\varphi(\beta^*) = -1$. Fix $\varphi(\alpha^0)$ and $\varphi(\alpha^*)$. Then, going through all $\beta^0 \in IV$ we obtain that $\varphi(\beta^0)\varphi(\beta^*) = -1$ for all $\beta^0 \in IV$. Now fix $\varphi(\beta^0)$ and $\varphi(\beta^*)$. Then, going through all $\alpha^0 \in I$ we obtain that $\varphi(\alpha^0)\varphi(\alpha^*) = 1$ for all $\alpha^0 \in I$.

If $\varphi(\alpha^0)\varphi(\alpha^*) = -1$ then $\varphi(\beta^0)\varphi(\beta^*) = 1$. Fix $\varphi(\alpha^0)$ and $\varphi(\alpha^*)$. Then, going through all $\beta^0 \in IV$ we obtain that $\varphi(\beta^0)\varphi(\beta^*) = 1$ for all $\beta^0 \in III$. Now fix $\varphi(\beta^0)$ and $\varphi(\beta^*)$. Then, going through all $\alpha^0 \in I$ we obtain that $\varphi(\alpha^0)\varphi(\alpha^*) = -1$ for all $\alpha^0 \in I$.

Thus, we obtain two cases. In the first case the arrangements of signs $\pm$ at first and second bands are the same, whereas at third and fourth bands the arrangements are the opposite. In the second case the arrangements of signs $\pm$ at first and second

bands are the opposite, whereas at third and fourth bands the arrangements are the same.

We have already considered all directions s for which there exists a pair (α^0, β^0), $\alpha^0 + \beta^0 = s$, $\alpha^0 \in I, II$, $\beta^0 \in III, IV$. Let $\alpha^0 \in I$, $\beta^0 \in I$. Then, for the direction $s = \alpha^0 + \beta^0$ it is easy to see from the structure of the matrix C that the bundle of parallel lines consists of two sets of pairs of vectors $\{(\alpha, \beta)\}$, $\{(\alpha^*, \beta^*)\}$ where $\alpha^* \in II$, $\beta^* \in II$, $\alpha+\beta = \alpha^*+\beta^* = \alpha^0+\beta^0 = s$, $\alpha+\alpha^* = \beta+\beta^* = (0, \ldots, 0, 1, 1)$. Thus, the formula (11) takes the form

$$\sum_{\alpha \in I} \varphi(\alpha)\varphi(\alpha + s) + \sum_{\alpha^* \in II} \varphi(\alpha^*)\varphi(\alpha^* + s) = 0 \tag{13}$$

for all $s = \alpha^0 + \beta^0$.

In the preceding argument we have found that the arrangements of signs $\pm$ at the first and second bands must be either the same or the opposite. If the arrangements of signs $\pm$ at the first and second bands are the same, then both sums in the expression (13) coincide. If the arrangements of signs $\pm$ at the first and second bands are the opposite, then both sums in the expression (13) coincide too. Therefore,

$$\sum_{\alpha \in I} \varphi(\alpha)\varphi(\alpha + s) = 0 \tag{14}$$

for all $s = \alpha^0 + \beta^0$.

In the expression (14) only vectors from the first band participate. Obviously, the equality in (14) holds if and only if the arrangement of signs $\pm$ at the first band is identical to some arrangement of signs $\pm$ in the matrix A.

Let $\alpha^0 \in I$, $\beta^0 \in II$, $s = \alpha^0 + \beta^0 = (0, \ldots, 0, 1, 1)$. Then, for the direction $s = \alpha^0 + \beta^0$ it is easy to see from the structure of the matrix C that the bundle of parallel lines consists of two sets of pairs of vectors $\{(\alpha, \beta)\}$, $\{(\alpha^*, \beta^*)\}$ where $\alpha^* \in III$, $\beta^* \in IV$, $\alpha + \beta = \alpha^* + \beta^* = \alpha^0 + \beta^0 = s = (0, \ldots, 0, 1, 1)$. From the preceding argument it follows that either $\varphi(\alpha)\varphi(\alpha+s) = 1$, $\varphi(\alpha^*)\varphi(\alpha**+s) = -1$ or $\varphi(\alpha)\varphi(\alpha + s) = -1$, $\varphi(\alpha^*)\varphi(\alpha ** + s) = 1$ for all $\alpha \in I$, $\alpha^* \in III$. Therefore, the equalities (11) will be held.

Let $\alpha^0 \in I$, $\beta^0 \in II$, $s = \alpha^0 + \beta^0 \neq (0, \ldots, 0, 1, 1)$. Then, for the direction $s = \alpha^0 + \beta^0$ it is easy to see from the structure of the matrix C that the bundle of parallel lines consists of two sets of pairs of vectors $\{(\alpha, \beta)\}$, $\{(\alpha^*, \beta^*)\}$ where $\alpha, \beta^* \in I$, $\alpha^*, \beta \in II$, $\alpha+\alpha^* = \beta+\beta^* = (0, \ldots, 0, 1, 1)$. Then, the formula (11) takes the form (13). In the preceding argument we have found that the arrangements of signs $\pm$ at the first and second bands must be either the same or the opposite. In both cases both sums in the expression (13) coincide. Therefore,

$$\sum_{\alpha \in I} \varphi(\alpha)\varphi(\alpha + s) = 0 \tag{15}$$

for all $s = \alpha^0 + \beta^0$.

In the expression (15) only vectors from the first band participate. We have that the equality in (15) holds if and only if the arrangement of signs $\pm$ at the first band is identical to some arrangement of signs $\pm$ in the matrix A.

The cases $\alpha^0 \in II$, $\beta^0 \in II$; $\alpha^0 \in III$, $\beta^0 \in III$; $\alpha^0 \in III$, $\beta^0 \in IV$; $\alpha^0 \in IV$, $\beta^0 \in IV$ are either included into already considered cases or into their tight copies. Thus, we have analyzed all possible directions in the matrix C and obtained the rule

of the arrangement of signs $\pm$: either the arrangements of signs $\pm$ at the first and second bands are the same, whereas at the third and fourth bands the arrangements are the opposite or the arrangements of signs $\pm$ at the first and second bands are the opposite, whereas at the third and fourth bands the arrangements are the same. Moreover, the arrangements of signs $\pm$ at the first and second bands of the matrix C must coincide or be opposite to the arrangements of signs $\pm$ in the matrix A; the arrangements of signs $\pm$ at the third and fourth bands of the matrix C must coincide or be opposite to the arrangements of signs $\pm$ in the matrix B. So we can choose in p_1 ways the arrangement of signs $\pm$ in the matrix A; in p_2 ways the arrangement of signs $\pm$ in the matrix B; and in two ways at which of two pairs of bands in the matrix C the signs will coincide. Thus, the number of the arrangements of signs $\pm$ in the matrix C is exactly $2p_1p_2$. □

Remark 4. We replaced all-ones sub-rows in [17] by all-zero sub-rows in our matrix C to make arguments clearer. It is easy to satisfy conditions $(0,\dots,0) \notin S^1$ and $(0,\dots,0) \notin S^2$ by an affine transformation or by the adding all-ones columns to the matrices A and B (that adds a new linear variable in corresponding Boolean functions).

Example 2. Consider the case $|S_f| = 64$. We have mentioned above (see Subsection 1.3) that the exact number of plateaued functions with the spectrum support of cardinality 16 is 2^7, $3 \cdot 2^7$ or $7 \cdot 2^7$. So Theorem 9 provides the spectrum supports of cardinality 64 such that the exact number of plateaued functions with these spectrum supports are 2^{15}, $3 \cdot 2^{15}$, $7 \cdot 2^{15}$, $3^2 \cdot 2^{15}$, $3 \cdot 7 \cdot 2^{15}$ or $7^2 \cdot 2^{15}$.

Now in Example 1 take $m_1 = 4$, $m_2 = 8$, $\dim L_i = m_1 - 1 = 3$ for each i, $i = 1,\dots,8$. Then $|S_f| = 64$. By the formula (10) we have that the exact number of plateaued functions with such spectrum support is

$$\begin{cases} 3^2 \cdot 5 \cdot 7 \cdot 2^{15} & \text{if} \quad t = 0, 8; \\ 3^2 \cdot 5 \cdot 2^{15} & \text{if} \quad t = 2, 6; \\ 3^3 \cdot 2^{15} & \text{if} \quad t = 4. \end{cases}$$

Note that the number of bent functions of 6 variables (i.e. plateaued functions with the spectrum support $\mathbf{F}_2^6$) is equal to $5425430528 = 7^2 \cdot 31 \cdot 109 \cdot 2^{15}$.

References

[1] S. Bhasin, C. Carlet, S. Guilley, *Theory of masking with codewords in hardware: low-weight dth-order correlation-immune Boolean functions*, ePrint IACR Archive Report 2013/303 (`http://eprint.iacr.org/2013/303`).

[2] A. Braeken, Y. Borissov, S. Nikova, B. Preneel, *Classification of cubic* $(n-4)$*-resilient Boolean functions*, IEEE Trans. Inf. Theory, **52**:4 (2006), 1670–1676. Zbl 1283.94157

[3] C. Carlet, *Boolean functions for cryptography and error correcting codes*, Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Y. Crama and P.L. Hammer (eds.), Cambridge University Press, Cambridge, 2010, 257–397. Zbl 1209.94035

[4] C. Carlet, P. Charpin, *Cubic Boolean functions with highest resiliency*, IEEE Trans. Inf. Theory, **51**:2 (2005), 562–571. Zbl 1184.94231

[5] C. Carlet, S. Mesnager, *Four decades of research on bent functions*, Des. Codes Cryptography, **78**:1 (2016), 5–50. Zbl 06538689

[6] C. Carlet, Yu. Tarannikov, *Covering sequences of Boolean functions and their cryptographic significance*, Des. Codes Cryptography, **25**:3 (2002), 263–279. Zbl 1035.94009

[7] B. Courteau, A. Monpetit, *Dual distances of completely regular codes*, Discrete Math., **89**:1 (1991), 7–15.

[8] Ph. Delsarte, *Four fundamental parameters of a code and their combinatorial significance*, Inform. and Control, **23**:5 (1973), 407–438. Zbl 0274.94010

[9] D.G. Fon-Der-Flaass, *A bound on correlation immunity*, Siberian Electronic Mathematical Reports, **4** (2007), 133–135 (`http://semr.math.nsc.ru/v4/p133-135.pdf`). Zbl 1132.05309

[10] D.G. Fon-Der-Flaass, *Perfect colorings of the* 12*-cube that attain the bound on correlation immunity*, Siberian Electronic Mathematical Reports, **4** (2007), 292–295 (Russian, English abstract). Zbl 1132.05314 English translation: `http://arxiv.org/abs/1403.8091`

[11] X. Guo-Zhen, J.L. Massey, *A spectral characterization of correlation-immune combining functions*, IEEE Trans. Inf. Theory, **34**:3 (1988), 569–571. Zbl 0653.94011

[12] A.V. Khalyavin, *Estimates of the capacity of orthogonal arrays of large strength*, Moscow Univ. Math. Bull., **65**:3 (2010), 130–131; translation from Vest. Mosk. Univ. Mat. Mekh., **65**:3 (2010), 49–51. Zbl 1304.05011

[13] A.V. Khalyavin, *The construction of* 4*th order correlation-immune Boolean functions of* 9 *variables with nonlinearity* 240, Proc. Xth Int. Seminar "Discrete Mathematics and Its Applications" (Moscow, 1–6 February, 2010), Izdatel'stvo mekhaniko-matematicheskogo fakul'teta MGU, Moscow, 2010, 534–537 (Russian).

[14] A.V. Khalyavin, *Upper bounds on nonlinearity of correlation immune Boolean functions*, Prikladnaja Diskretnaja Matematika, **11**:1 (2011), 34–69 (Russian). `http://mi.mathnet.ru/eng/pdm261`

[15] D. Kirienko, *On new infinite family of high order correlation immune unbalanced Boolean functions*, Proc. 2002 IEEE International Symposium on Information Theory ISIT 2002, Lausanne, Switzerland, June 30 – July 5, 2002, Piscataway, NJ, 2002, 465–465. DOI: 10.1109/ISIT.2002.1023737

[16] P. Langevin, G. Leander, *Counting all bent functions in dimension eight* 99270589265934370305785861242880, Des. Codes Cryptography, **59**:1–3 (2011), 193–205. Zbl 1215.94059

[17] A.O. Logachev, *On a recursive class of plateaued Boolean functions*, Discrete Math. Appl, **20**:5–6 (2011), 537–551; translation from Diskretn. Mat., **22**:4 (2010), 20–33. Zbl 1211.94056

[18] O.A. Logachev, A.A. Salnikov, V.V. Yashchenko, *Boolean Functions in Coding Theory and Cryptography*, Translations of Mathematical Monographs, **241**, American Mathematical Society, Providence, RI. 2012. Zbl 1253.94002

[19] D. Pei, W. Qin, *The correlation of a Boolean function with its variables*, Proc. Progress in Cryptology — INDOCRYPT 2000, First International Conference in Cryptology in India Calcutta, India, December 10–13, 2000, Lect. Notes Comput. Sci., **1977**, Springer, Berlin, 2000, 1–8. Zbl 1074.94519

[20] S. Sanyal, *Near-optimal upper bound on Fourier dimension of Boolean functions in terms of Fourier sparsity*, Electronic Colloquium on Computational Complexity (ECCC), **2014**, Revision 1 of Report No. 88 (2014), 1–9. `http://eccc.hpi-web.de/report/2014/088/`

[21] S. Sanyal, *Near-optimal upper bound on Fourier dimension of Boolean functions in terms of Fourier sparsity*, Automata, Languages, and Programming. 42nd Int. Colloquium, ICALP 2015, Kyoto, Japan, July 6–10, 2015. Proceedings. Part I. Springer, Berlin, 2015, 1035–1045. Zbl 06498711

[22] H.-U. Simon, *A tight* $\Omega(\log\log n)$*-bound on the time for parallel RAM's to compute nondegenerated Boolean functions*, Foundations of Computation Theory, Proc. Int. FCT-Conf., Borgholm, Sweden, August 21–27, 1983, Lect. Notes Comput. Sci., **158** (1983), 439–444. Zbl 0523.68036

[23] Yu.V. Tarannikov, *On a method for the constructing of cryptographically strong Boolean functions*, Preprint No. 6, Moscow Lomonosov State University, French–Russian Liapunov Institute of Applied Mathematics and Informatics, Moscow, 1999.

[24] Yu.V. Tarannikov, *On resilient Boolean functions with maximal possible nonlinearity*, Proc. Progress in Cryptology — INDOCRYPT 2000, First International Conference in Cryptology in India Calcutta, India, December 10–13, 2000, Lect. Notes Comput. Sci., **1977**, Springer, Berlin, 2000, 19–30. Zbl 0963.94012

[25] Yu.V. Tarannikov, *On correlation immune and resilient Boolean functions*, Matematicheskie voprosy kibernetiki, **11**, O.B. Lupanov (ed.), Fizmatlit, Moscow, 2002, 91–148 (Russian).

[26] Yu.V. Tarannikov, *On values of the affine rank of the support of spectrum of a plateaued function*, Discrete Math. Appl., **16**:4 (2006), 401–421; translation from Diskretn. Mat., **18**:3 (2006), 120–137. Zbl 1121.94030

[27] Yu.V. Tarannikov, *Combinatorial Properties of Discrete Structures and Applications in Cryptology*, Izdatel'stvo MCNMO, Moscow, 2011 (Russian).

[28] Yu.V. Tarannikov, *Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters*, Siberian Electronic Mathematical Reports, **11** (2014), 229–245 (`http://semr.math.nsc.ru/v11/p229-245.pdf`). Zbl 06510889

[29] Yu. Tarannikov, D. Kirienko, *Spectral analysis of high order correlation immune functions*, ePrint IACR Archive Report, 2000/050 (`http://eprint.iacr.org/2000/050`).

[30] Yu. Tarannikov, D. Kirienko, *Spectral analysis of high order correlation immune functions*, Proc. 2001 IEEE International Symposium on Information Theory ISIT 2001, Washington, USA, June 24–29, 2001, Piscataway, NJ, 2001, 69–69. DOI: 10.1109/ISIT.2001.935932

[31] N. Tokareva, *Bent Functions: Results and Applications to Cryptography*, Elsevier, Amsterdam, 2015. Zbl 06508183

[32] I. Wegener, *The Complexity of Boolean Functions*, B.G.Teubner, Stuttgart, J.Wiley & Sons, Chichester etc., 1987. Zbl 0623.94018

[33] A. Zverev, *On the structure of the spectrum support of Boolean functions*, Boolean Functions in Cryptology and Information Security, B. Preenel and O.A. Logachev (eds.), NATO Science for Peace and Security Series, Ser. D: Information and Communication Security, **18**, IOS Press, Amsterdam, 2008, 331–340. Zbl 1154.94445

Andrey Vyacheslavovich Khalyavin
Yandex,
16, Leo Tolstoy St.,
119021, Moscow, Russia
E-mail address: `halyavin@gmail.com`

Mikhail Sergeevich Lobanov
Mech. & Math. Department,
Lomonosov Moscow State University,
119992, Moscow, Russia
E-mail address: `misha_msu@mail.ru`

Yuriy Valer'evich Tarannikov
Mech. & Math. Department,
Lomonosov Moscow State University,
119992, Moscow, Russia
E-mail address: `yutarann@gmail.com`