On affine rank of spectrum support for plateaued function

Yuriy Tarannikov

Mech. & Math. Department
Moscow State University
119992 Moscow, Russia
email: yutaran@mech.math.msu.su

Abstract

The plateaued functions have a big interest for the studying of bent functions and by the reason that many cryptographically important functions are plateaued. In this paper we study the possible values of the affine rank of spectrum support for plateaued functions. We consider for any positive integer h plateaued functions with a spectrum support of cardinality 4^h (the cardinality must have such form), give the bounds on the affine rank for such functions and construct functions where the affine rank takes all integer values from $2h$ till $2^{h+1}-2$. We solve completely the problem for $h=2$, namely, we prove that the affine rank of any plateaued function with a spectrum support of cardinality 16 is 4, 5 or 6.

1 Introduction and main definitions

We consider ${F_2}^n$, the vector space of n-tuples of elements from F_2. An n-variable Boolean function is a map from ${F_2}^n$ into F_2. In this paper we will denote a vector from ${F_2}^n$ by a letter, whereas the component of this vector by the same letter equipped with low indices pointed to the number of this component in a vector. Vectors x' and x'' are called *adjacent in the ith component* if they differ only in the ith component. We denote by x^i the vector that differs from x only in the ith component, $i=1,\dots,n$. The component x_i is called *fictitious* for a function f if for any vectors x' and x'' adjacent in the ith component we have $f(x')=f(x'')$. *The Hamming*

distance $d(x', x'')$ between two vectors x' and x'' is the number of components where vectors x' and x'' differ. For given function f from $\mathbf{F}_2^n$ the minimum of distances $d(f, l)$ where l ranges over the set of all affine functions on $\mathbf{F}_2^n$ is called *the nonlinearity* of f and denoted by $\mathrm{nl}(f)$. *The subfunction* of a Boolean function f is the function f' obtained by a substitution of some constants 0 or 1 instead of some components in f.

It is well known that a function f on ${F_2}^n$ can be uniquely represented by a polynomial (ANF) on F_2 whose degree in each variable in each term is at most 1. Namely, $f(x_1, \ldots, x_n) = \bigoplus_{(a_1,\ldots,a_n)\in F_2^n} g(a_1, \ldots, a_n) x_1^{a_1} \ldots x_n^{a_n}$, where g is also a function on ${F_2}^n$. This polynomial representation of f is called the *algebraic normal form* (briefly, ANF) of the function and each $x_1^{a_1} \ldots x_n^{a_n}$ is called a *term* in ANF of f. Sometimes the map $f(x) \to g(x)$ is called *the Möbius transform.*

The *algebraic degree* of f, denoted by $\deg(f)$, is defined as the number of variables in the longest term in ANF of 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 $f(x) = 1$. The function f 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.

Let $x = (x_1, \ldots, x_n)$ and $u = (u_1, \ldots, u_n)$ be vectors of length n over $\mathbf{F}_2$. *The inner product* of x and u is the function defined as

$$< x, u >= \sum_{i=1}^{n} x_i u_i$$

where the operations are produced over $\mathbf{F}_2$. By sum $x + u$ of two vectors x and u we understand their componentwise addition over $\mathbf{F}_2$.

The Walsh transform of a Boolean function f is called the integer valued function on $\mathbf{F}_2^n$ defined by the next way:

$$W_f(u) = \sum_{x\in F_2^n} (-1)^{f(x)+<u,x>}.$$

For any $u \in F_2^n$ the value $W_f(u)$ is called *the Walsh coefficient.* We will call the Walsh coefficients also *the spectral coefficients,* and the set of all 2^n Walsh coefficients — *the spectrum* of a Boolean function. Walsh coefficients satisfy the *Inversion formula* $(-1)^{f(x)} = 2^{-n} \sum_{u\in F_2^n} W_f(u)(-1)^{<u,x>}$ and Parseval's identity $\sum_{u\in F_2^n} W_f^2(u) = 2^{2n}$. The nonlinearity of a Boolean function f is expressed via its Walsh coefficients by the next way: $nl(f) = 2^{n-1} - \frac{1}{2} \max_{u\in\mathbf{F}_2^n} |W_f(u)|$.

The set S_f of all vectors u such that $W_f(u) \neq 0$ is called *the spectrum support* of a function f.

The Boolean function is called *a bent function* if the values of its Walsh coefficients at all vectors are exactly $\pm 2^{n/2}$. Bent functions exist for all even n and do not exist for all odd n. A bent function is a function with maximum possible nonlinearity $2^{n-1} - 2^{(n/2)-1}$ among all functions of n variables for even n. The Boolean function is called *plateaued* if its Walsh coefficients take exactly three possible values: 0 and $\pm 2^c$ for some integer c. The plateaued functions have a big interest for the studying of bent functions (for example, by the reason that the decomposition of a bent function $f = (x_i + 1)f_1 + x_i f_2$ gives two plateaued functions f_1 and f_2) and by the reason that many cryptographically important functions are plateaued (for example, m-resilient functions of n variables with maximum possible nonlinearity $2^{n-1} - 2^{m+1}$). For plateaued functions denote $\phi(x) = 2^{-c} W_f(x)$. Then for any $x \in \mathbf{F}_2^n$ the value $\phi(x)$ can take only three possible values: 0, -1 and 1. The set S_f of all vectors u such that $W_f(u) \neq 0$ is called *the spectrum support* of a plateaued function. We denote the set of all vectors x such that $\phi(x) = -1$ by T^-, and the set of all vectors x such that $\phi(x) = 1$ by T^+. From Parseval's identity it follows immediately that the cardinality of a spectrum support is 4^{n-c}. It is convenient to consider a bent function as the particular case of a plateaued function for $c = n/2$ and $|S_f| = 2^n$ that we will use below with some stipulations. (Although often formally bent functions are not referred to plateaued functions.) Plateaued functions were investigated in different works, see, for example, [6, 7, 10].

For any $u \in {F_2}^n$ *the autocorrelation coefficient* of the function f at the vector u is defined as $\Delta_f(u) = \sum_{x \in {F_2}^n} (-1)^{f(x)+f(x+u)}$. The function $D_u f = f(x) + f(x+u)$ is called *the derivative* of the function f in direction u. The vector $u \in {F_2}^n$ such that $D_u f \equiv \text{const}$ is called *the linear structure* of the function f. It is easy to check that the linear structures of a function f form a linear space in $\mathbf{F}_2^n$. The existence of a nontrivial linear structure for functions is a cryptographic weakness in some cases (but not in all).

Let E be an arbitrary subset of $\mathbf{F}_2^n$. *The rank* of a set E is the dimension of the subspace generated by E in $\mathbf{F}_2^n$. *The affine rank* of a set E is the dimension of a smallest coset in $\mathbf{F}_2^n$ that contains E. The rank and the affine rank of the spectrum support of a Boolean function will be denoted by k and $\mathbf{k}$, respectively. For the brevity in this paper the affine rank and the rank of a Boolean function shortly will be called by its *affine rank* and *rank,* respectively. It is easy to understand that $\mathbf{k} \in \{k, k-1\}$. It is well known (see, for example, [2]) that the dimension of the set of linear structures of a function f is equal to $n - \mathbf{k}$. If there exists the vector $u \in {F_2}^n$ such that

$D_u f \equiv 1$ then $k = \mathbf{k} + 1$. If such vector does not exist then $k = \mathbf{k}$.

For additional facts about properties of Boolean functions we refer to [8] and [9].

2 On affine transformations in $\mathbf{F}_2^n$

The affine transformation in $\mathbf{F}_2^n$ is the map $x \to x' = \mathbf{A}x = xA^T + a$ where A is a square nondegenerated matrix of order n over $\mathbf{F}_2$, and a is a vector of length n. The affine transformation is an automorphism $\mathbf{F}_2^n$ that transfers all cosets to cosets of the same dimension. If $a = 0$ then the affine transformation is called also *linear*.

The affine transformation of a function f defined on $\mathbf{F}_2^n$ is the transformation $f(x) \to f'(x) = f(\mathbf{A}x)$. If for functions f and f' there exists an affine transformation of a function that transfers f to f' then f and f' are called *affine equivalent.* If for functions f and f' there exists the linear transformation of a function that transfers f to f' then f and f' are called *linear equivalent.*

Lemma 1 *Let* $f(x) \to f'(x) = f(\mathbf{A}x)$ *be the affine transformation of a function* f *defined on* $\mathbf{F}_2^n$. *Then* $W_{f'(x)}(u) = (-1)^{<a,uA^{-1}>} \cdot W_f(uA^{-1})$.

Proof. By the formula for Walsh coefficients we have

$$W_{f'(x)}(u) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f'(x)+<x,u>} = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(\mathbf{A}x)+<x,u>} =$$
$$\sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+<\mathbf{A}^{-1}x,u>} = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+<x,uA^{-1}>+<a,uA^{-1}>} =$$
$$(-1)^{<a,uA^{-1}>} \cdot \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+<x,uA^{-1}>} = (-1)^{<a,uA^{-1}>} \cdot W_f(uA^{-1}).$$

□

Suppose that a Boolean function f is defined on $\mathbf{F}_2^n$. *The affine transformation of a spectrum* of a function f is the transformation $W_f(x) \to W'(x) = W_f(\mathbf{A}x)$. It is possible to show that coefficients $W'(x)$ are Walsh coefficients for some function f' that is not, generally speaking, affine equivalent to the function f.

Lemma 2 *Let* $W_f(x) \to W'(x) = W_f(\mathbf{A}x)$ *be the affine transformation of a spectrum of a function* f *defined on* $\mathbf{F}_2^n$. *Then coefficients* $W'(x)$ *are Walsh coefficients for some function* f', *moreover* $f'(x) = f(xA^{-1}) + < a, xA^{-1} >$.

Proof. Check that for all $x \in \mathbf{F}_2^n$ the sums in the inversion formula for the hypothetic function $f'(x)$ are ± 1. Denote

$$F(x) = 2^{-n} \sum_{u \in \mathbf{F}_2^n} W'(u)(-1)^{<u,x>}.$$

We have

$$F(x) = 2^{-n} \sum_{u \in \mathbf{F}_2^n} W'(u)(-1)^{<u,x>} = 2^{-n} \sum_{u \in \mathbf{F}_2^n} W_f(\mathbf{A}u)(-1)^{<u,x>} =$$
$$2^{-n} \sum_{v \in \mathbf{F}_2^n} W_f(v)(-1)^{<\mathbf{A}^{-1}v,x>} = 2^{-n} \sum_{v \in \mathbf{F}_2^n} W_f(v)(-1)^{<v,xA^{-1}>+<a,xA^{-1}>} =$$
$$(-1)^{<a,xA^{-1}>} \cdot 2^{-n} \sum_{v \in \mathbf{F}_2^n} W_f(v)(-1)^{<v,xA^{-1}>} = (-1)^{f(xA^{-1})+<a,xA^{-1}>}.$$

Thus, for all $x \in \mathbf{F}_2^n$ we have $F(x) = \pm 1$. Therefore the function $f'(x)$ exists, moreover, $f'(x) = f(xA^{-1}) + < a, xA^{-1} >$. □

The spectrum of functions f and f' that obtained one from another by an affine transformation of a spectrum are called *affine equivalent.* The spectrum of functions f and f' that obtained one from another by a linear transformation of a spectrum are called *linear equivalent.* Analogously, the affine equivalence of functions does not imply the affine equivalence of their spectra. For example, by the reason that under the affine transformation of a function f the value $wt(f)$ remains unchanged. Nevertheless, $wt(f) = 2^{n-1} - \frac{1}{2}W_f(0)$, therefore, transferring by the affine transformation of a spectrum into 0 a vector with another value of a Walsh coefficient we will obtain the function that is not affine equivalent to f. At the same time Lemmas 1 and 2 imply that the linear transformation of a spectrum is the linear transformation of a function, and vice versa.

Obviously, the affine transformation of a spectrum of a plateaued function f transfers it to a spectrum of also plateaued function f' with the same cardinality of a spectrum support, and the affine transformation of a plateaued function f transfers it to a plateaued function f' with the same cardinality of a spectrum support.

Lemma 3 *Let f be a Boolean function defined on $\mathbf{F}_2^n$, moreover, the spectrum support of this function lies in $\mathbf{F}_2^l \otimes (\underbrace{0 \ldots 0}_{n-l})$. Then the function f depends on variables $x_{l+1}, \ldots, x_n$ fictitiously. Let f' be a function on $\mathbf{F}_2^n$ obtained from f by deleting of fictitious variables $x_{l+1}, \ldots, x_n$. Then for any u from $\mathbf{F}_2^l$ we have $W_{f'}(u) = 2^{-(n-l)} W_f(u \underbrace{0 \ldots 0}_{n-l})$.*

Proof. Let x and x^i be an arbitrary pair of vectors adjacent in the ith component, $i \in \{l+1, \ldots, n\}$. By the inversion formula we have

$$(-1)^{f(x)} - (-1)^{f(x^i)} = 2^{-n} \sum_{u \in \mathbf{F}_2^n} W_f(u) \left[(-1)^{<x,u>} - (-1)^{<x^i,u>} \right] =$$

$$2^{-n} \sum_{u \in \mathbf{F}_2^l \otimes (\underbrace{0 \ldots 0}_{n-l})} W_f(u) \left[(-1)^{<x,u>} - (-1)^{<x^i,u>} \right] = 0.$$

Therefore $f(x) = f(x^i)$, and, thus, the variables x_{l+1}, ..., x_n are really fictitious. Consider now the function f' on $\mathbf{F}_2^n$ obtained from f be deleting of fictitious variables x_{l+1}, ..., x_n. For any its Walsh coefficient $u \in \mathbf{F}_2^l$ we have

$$W_{f'}(u) = \sum_{x \in \mathbf{F}_2^l} (-1)^{f'(x)+<x,u>} =$$

$$2^{-(n-l)} \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+<x,u\underbrace{0 \ldots 0}_{n-l}>} = 2^{-(n-l)} W_f(u \underbrace{0 \ldots 0}_{n-l}).$$

□

Lemma 4 *Let f be a Boolean function defined on $\mathbf{F}_2^n$. Let f' be a function on $\mathbf{F}_2^{n+1}$ defined as $f'(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n) + x_{n+1}$. Then if u is a vector from $\mathbf{F}_2^{n+1}$ that belongs to a spectrum support of the function f' then $u_{n+1} = 1$ and $W_{f'}(u_1, \ldots, u_n, 1) = 2W_f(u_1, \ldots, u_n)$.*

Proof. Suppose that $u \in \mathbf{F}_2^{n+1}$. Group in the sum

$$W_{f'}(u) = \sum_{x \in \mathbf{F}_2^{n+1}} (-1)^{f(x)+<x,u>}$$

into pairs vectors x and x^{n+1} that differ only in $(n+1)$th component. Let $x_{n+1} = 0$ for the definiteness. For these vectors $f'(x) = f'(x^{n+1}) + 1$ holds. If $u_{n+1} = 0$ then $< x, u >=< x^{n+1}, u >$. It follows $(-1)^{f'(x)+<x,u>} + (-1)^{f'(x^{n+1})+<x^{n+1},u>} = 0$. Therefore, $W_{f'}(u) = 0$. If $u_{n+1} = 1$ then $< x, u >=< x^{n+1}, u > +1$. It follows $(-1)^{f'(x)+<x,u>} + (-1)^{f'(x^{n+1})+<x^{n+1},u>} = 2 \cdot (-1)^{f'(x)+<x,u>} = 2 \cdot (-1)^{f(x_1,\ldots,x_n)+<(x_1,\ldots,x_n),(u_1,\ldots,u_n)>}$. Therefore, $W_{f'}(u) = 2W_f(u_1, \ldots, u_n)$. □

Lemmas 1, 2, 3 imply that the study of plateaued functions on $\mathbf{F}_2^n$ with a spectrum support of cardinality 4^h can be reduced in some sense to the study of plateaued functions with a spectrum support of the same cardinality 4^h defined on $\mathbf{F}_2^{\mathbf{k}}$. Moreover, if $\mathbf{k} > 2h$ then any plateaued function f' on $\mathbf{F}_2^n$

with a spectrum support of cardinality 4^h can be obtained from some function f on $\mathbf{F}_2^{\mathbf{k}}$ with a spectrum support of the same cardinality 4^h by adding of $n-\mathbf{k}$ fictitious variables and implementing of some linear transformation of a function. The same result can be achieved also in the case if $\mathbf{k}=2h$ and $W_{f'}(0)\neq 0$ (in this case the function f will be bent function). If $\mathbf{k}=2h$ and $W_{f'}(0)=0$ then the mentioned linear transform of a function does not exist but it is possible to use the affine transformation of a spectrum or to take a function f of $\mathbf{k}+1$ variables.

Note that the mentioned reduction can be insufficient if it is necessary to investigate additional properties of functions not preserved under affine transformations (for example, correlation immunity).

Point also to the next property that allows to avoid the separate consideration of the problem on possible values taken by a rank k.

Lemma 5 *If there exists a plateaued function with a spectrum support of cardinality* 4^h *and an affine rank taken the value* $\mathbf{k}$ *then there exist plateaued functions with a spectrum support of the same cardinality* 4^h *and ranks taken both values* $k=\mathbf{k}$ *and* $k=\mathbf{k}+1$.

Proof. By Lemma 2 an affine transformation of a spectrum support of a plateaued function gives again the plateaued function with a spectrum support of the same cardinality and with the same affine rank. If by some affine transformation to transfer to 0 one of vectors lain in the smallest coset contained S_f then for the obtained function, obviously, $k=\mathbf{k}$ will be hold. If to transfer to 0 a vector that does not lie in the smallest coset contained S_f then for the obtained function $k=\mathbf{k}+1$ holds. If for the initial function there do not exist vectors that do not belong to the smallest coset contained S_f (i. e. if $\mathbf{k}$ is equal to the number of variables) then it is possible simply to add a fictitious variable, and such vectors will appear whereas the function will remain plateaued with the same cardinality of a spectrum support. □

All mentioned above follows that the affine rank is an important characteristics of plateaued functions. It is obvious, that the affine rank of any plateaued function with a spectrum support of cardinality 4^h is at least $2h$ since the smaller cosets do not contain 4^h vectors. Any plateaued function with a spectrum support of cardinality 1 is an affine function and, obviously, its affine rank is equal to 0. It is well known that the affine rank of any plateaued function with a spectrum support of cardinality 4 is equal to 2. This fact was proved in [5] but it is evident that it was known much more early. The plateaued functions with the spectrum support of cardinality 16 (without the name of plateaued) were considered, in fact, in [4]. In the work [2] for the subclass of plateaued functions with a spectrum support of cardinality 16 (more exactly, for cubic resilient functions of order $n-4$) it was

obtained the bound $\mathbf{k} \leq k \leq 9$. In our paper we prove that the affine rank of any plateaued function with a spectrum support of cardinality 16 is equal to 4, 5 or 6. Besides, we consider for any positive integer h the plateaued functions with a spectrum support of cardinality 4^h, give the bounds on the affine rank for such functions and construct functions the affine rank of which takes all positive integer values from $2h$ till $2^{h+1} - 2$.

3 Auxiliary results

The next statement is well known (see, for example, the relation (2.16) in [8]). Earlier its proof was given in [3].

Lemma 6 *Let f be a Boolean function on $\mathbf{F}_2^n$. Suppose that U is a linear subspace of dimension l in $\mathbf{F}_2^n$, and $U^\perp$ is a space orthogonal to U in $\mathbf{F}_2^n$. Let v be an arbitrary vector from $\mathbf{F}_2^n$. Then*

$$\sum_{u \in U+v} W_f(u) = 2^l \sum_{x \in U^\perp} (-1)^{f(x)+<x,v>}.$$

Lemma 7 *[1] Let f be a plateaued function with a spectrum support of cardinality 4^h defined on $\mathbf{F}_2^n$. Suppose $\sum\limits_{a \in \mathbf{F}_2^n} \phi(a) = 2^h$. Then $\sum\limits_{a \in \mathbf{F}_2^n} \phi(a) \in \{-2^h, 2^h\}$.*

Proof. Take in Lemma 6 in the capacity of a subspace U whole $\mathbf{F}_2^n$. In the notations of Lemma 6 we have $W_f(u) = \phi(u) \cdot 2^{n-h}$, $l = n$. Then $U^\perp = \{0\}$. Therefore,

$$\sum_{u \in \mathbf{F}_2^n} W_f(u) = 2^n (-1)^{f(0)}.$$

For the function f it follows

$$\sum_{u \in \mathbf{F}_2^n} \phi(u) = 2^h (-1)^{f(0)} \in \{-2^h, 2^h\}.$$

□

Lemma 8 *Let f be a plateaued function with a spectrum support of cardinality 4^h defined on $\mathbf{F}_2^n$. Suppose $\sum\limits_{a \in \mathbf{F}_2^n} \phi(a) = 2^h$. Let H be an $(n-1)$-dimensional coset in $\mathbf{F}_2^n$. Then $\sum\limits_{a \in H} \phi(a) \in \{0, 2^h\}$.*

Proof. In the notations of Lemma 6 we have $W_f(u) = \phi(u) \cdot 2^{n-h}$, $l = n - 1$. Therefore, Lemma 6 follows that $\sum\limits_{a \in H} \phi(a) \in \{-2^h, 0, 2^h\}$. If the sum is equal to -2^h then $\sum\limits_{a \in \mathbf{F}_2^n \setminus H} \phi(a) = 2^{h+1}$ that is impossible according to what has been said above. □

The next statement is also well known (see, for example, Theorem 2.89 in [8]).

Lemma 9 *Let f be a Boolean function on $\mathbf{F}_2^n$. Suppose that U is a linear subspace of dimension l in $\mathbf{F}_2^n$, and $U^\perp$ is a space orthogonal to U in $\mathbf{F}_2^n$. Then*

$$\sum_{u \in U} W_f^2(u) = 2^l \sum_{v \in U^\perp} \Delta_f(v).$$

Lemma 10 *Let f be a Boolean function on $\mathbf{F}_2^n$, $n \geq 1$. Then $wt(f)$ is odd if and only if $\deg(f) = n$.*

Proof is obvious (see, for example, Corollary 1 in [9]). □

Lemma 11 *Let f be a Boolean function on $\mathbf{F}_2^n$, $f \not\equiv \mathrm{const}$. Then $2^{n-\deg(f)} \leq wt(f) \leq 2^n - 2^{n-\deg(f)}$.*

Proof is obvious (see, for example, Lemma 5.6 in [8] or Lemma 3 in [9]). □

Lemma 12 *[6] Let f be a plateaued Boolean function on $\mathbf{F}_2^n$ with a spectrum support of cardinality 4^h. Then $\deg(f) \leq h + 1$.*

Proof. Walsh coefficients of the function f take values from the set $\{0, \pm 2^{n-h}\}$. Consider the longest term $x_{i_1} x_{i_2} \ldots x_{i_s}$ in the polynomial of the function f (if there exist some longest terms then take one of them arbitrary). It is possible to assume that $s \geq 2$, in the opposite case the statement of Lemma is automatically true. Use Lemma 6. Take in the capacity of U the linear subspace $U = \{x \in \mathbf{F}_2^n \mid x_{i_1} = 0, \ldots, x_{i_s} = 0\}$ of dimension $l = n - s$, take 0 as the vector v. Then by Lemma 10 the orthogonal space $U^\perp$ contains odd number of vectors x such that $f(x) = 1$. Therefore the sum $\sum\limits_{x \in U^\perp} (-1)^{f(x)}$ is not divided by 4 for $s \geq 2$. Hence, in the equality

$$\sum_{u \in U} W_f(u) = 2^{n-s} \sum_{x \in U^\perp} (-1)^{f(x)}$$

the left part is divided by 2^{n-h} whereas the right part is not divided by 2^{n-s+2}. It follows $n - h < n - s + 2$. Taking into account that all coefficients are integer we obtain $s \leq h + 1$, as was to be proved. □

Lemma 13 *Let f be a plateaued Boolean function on $\mathbf{F}_2^n$ with a spectrum support of cardinality 4^h. Suppose that H is an $(n-1)$-dimensional coset in $\mathbf{F}_2^n$. Then either $\sum\limits_{u\in H}|\phi(u)|=0$, or $\sum\limits_{u\in H}|\phi(u)|=4^h$, or $2^h\le\sum\limits_{u\in H}|\phi(u)|\le 4^h-2^h$.*

Proof. Let at first that H is a linear subspace in $\mathbf{F}_2^n$. Then $H^\perp=\{0,v\}$ for some nonzero $v\in\mathbf{F}_2^n$. Obviously, $\Delta_f(0)=2^n$. By Lemma 9 we have

$$4^{n-h}\sum_{u\in H}|\phi(u)|=2^{n-1}(2^n+\Delta_f(v))=4^n-2^n wt(D_v f).$$

By Lemma 12 the inequality $\deg(f)\le h+1$ holds. The function $D_v f$ is the derivative of the function f, therefore, $\deg(D_v f)\le h$. If $D_v f\equiv 0$ then $\sum\limits_{u\in H}|\phi(u)|=4^h$. If $D_v f\equiv 1$ then $\sum\limits_{u\in H}|\phi(u)|=0$. If $D_v f\not\equiv$ const then by Lemma 11 we have $2^{n-h}\le wt(D_v f)\le 2^n-2^{n-h}$. It follows $2^h\le\sum\limits_{u\in H}|\phi(u)|\le 4^h-2^h$, as was to be proved. For the coset $\mathbf{F}_2^n\setminus H$ the same three cases take place by the proved above and Parseval's identity. □

Lemma 14 *Let f_1, f_2 be Boolean functions on $\mathbf{F}_2^n$, and let f be a Boolean function on $\mathbf{F}_2^{n+1}$, moreover, $f(xx_{n+1})=(x_{n+1}+1)f_1(x)+x_{n+1}f_2(x)$. Then $W_f(u0)=W_{f_1}(u)+W_{f_2}(u)$ and $W_f(u1)=W_{f_1}(u)-W_{f_2}(u)$.*

This Lemma is very well known. In fact, the Fast Walsh Transform is based on its application. □

4 On affine rank of Boolean functions with spectrum support of cardinality 16

In all statements of this section we suppose that f is a plateaued Boolean function on $\mathbf{F}_2^n$ and $|S_f|=16$. In this case $c=n-2$. By Lemma 7 one of two cases takes place: $|T^+|=10$, $|T^-|=6$, or $|T^+|=6$, $|T^-|=10$. Taking into account that for all u the relation $W_f(u)=-W_{f+1}(u)$ holds, it is possible without loss of generality to assume $|T^+|=10$, $|T^-|=6$, that we will do in the remained part of this section. Thus, we have $|S_f|=16$, $|T^+|=10$, $|T^-|=6$.

Our aim is to prove the next theorem.

Theorem 1. Let f be a plateaued function, $|S_f|=16$. Then for the affine rank $\mathbf{k}$ of the spectrum support S_f the inequality $\mathbf{k}\le 6$ holds.

The proof of Theorem 1 will be obtained by the proofs of several lemmas.

Suppose that the affine rank of the spectrum support S_f is $\mathbf{k}$, and the affine rank of T^- is $\mathbf{k}^-$. Obviously, $3 \leq \mathbf{k}^- \leq 5$. It is easy to see that by means of some affine transformation in $\mathbf{F}_2^n$ it is possible to embed the smallest coset containing the spectrum support S_f into $\mathbf{F}_2^{\mathbf{k}} \otimes (\underbrace{0 \ldots 0}_{n-\mathbf{k}})$ such that some $\mathbf{k}^- + 1$ vectors from T^- will be transferred to the vectors $(0,0,0,\ldots,0)$, $(1,0,0,\ldots,0)$, $(0,1,0,\ldots,0)$, $\ldots$, $(\underbrace{0,0,\ldots,0,1}_{\mathbf{k}^-},0,\ldots,0)$. Note that after such transformation all vectors from T^- will be transferred to the vectors that have all zeroes in all components i, $i > \mathbf{k}^-$. Note that the affine transformation of the spectrum described above, generally speaking, is not an affine transformation of a function f, but we do not need this. It is sufficient for us that the Boolean function obtained as a result of this map will be plateaued with the same set of absolute values of Walsh coefficients, and the same values $\mathbf{k}$ and $\mathbf{k}^-$. By Lemma 3 all variables from $(\mathbf{k}+1)$th till nth in the obtained function will be fictitious. Deleting them and dividing all Walsh coefficients by $2^{n-\mathbf{k}}$, by Lemmas 2 and 3 we obtain a plateaued function defined on $\mathbf{F}_2^{\mathbf{k}}$ with a spectrum support of the same cardinality 16. Thus, without loss of generality in the remained part of this section we will consider just such a spectrum support.

Lemma 15 *Let H be a $(\mathbf{k}-1)$-dimensional coset in $\mathbf{F}_2^{\mathbf{k}}$. Then $\sum\limits_{a \in H} \phi(a) \in \{0,4\}$.*

Proof. The statement of Lemma is a particular case of Lemma 8. □

Lemma 16 *[2] Let H be a $(\mathbf{k}-1)$-dimensional coset in $F_2^{\mathbf{k}}$. Then H contains 4, 6, 8, 10 or 12 vectors from S_f.*

Proof. By Lemma 15 the coset H contains even number of vectors from S_f. The cases 2 and 14 are impossible by Lemma 13. If H contains 16 vectors from S_f then S_f is contained in H; if H contains 0 vectors from S_f then S_f is contained in $\mathbf{F}_2^{\mathbf{k}} \setminus H$. The both last cases are impossible since $\mathbf{F}_2^{\mathbf{k}}$ is the smallest coset that contains the spectrum support S_f. □

Our aim is to prove that $\mathbf{k} \leq 6$. Assume the converse. Suppose that $\mathbf{k} \geq 7$. We will prove that this is impossible.

We form the matrix M of size 16×7. In the rows of M we write first 7 components of the vectors from S_f (in the case $\mathbf{k} > 7$ we omit all components after 7th). In first 10 rows of M we write vectors from T^+, and in last 6 rows of M we write vectors from T^-. The left $\mathbf{k}^-$ columns of M we call *the left side of M*, the remained $7 - \mathbf{k}^-$ columns we call *the right side of M*.

$$\left(\begin{array}{c|c} & \\ \hline & \\ \mathbf{I} & \mathbf{0} \\ & \\ 0 \quad \ldots \quad 0 & \end{array}\right).$$

Denote by γ_i the columns from the left side of M, and by x_i the variables correspondent to these columns. Denote by δ_j the columns from the right side of M and by y_j the variables correspondent to these columns. We denote by γ_i^+ and δ_j^+ the subcolumns contained upper 10 elements of columns γ_i and δ_j, respectively.

Lemma 17 *For any set $\delta_{j_1}, \ldots, \delta_{j_s}$, $1 \le s \le 7 - \mathbf{k}^-$, of different columns from the right side of M we have $wt(\delta_{j_1}^+ + \ldots + \delta_{j_s}^+) = 4$.*

Proof. Denote $H = \{(x, y) \in F_2^{\mathbf{k}} \,|\, y_{j_1} + \ldots + y_{j_s} = 0\}$. The hyperplane H contains all 6 vectors of T^-, therefore by Lemma 15 the hyperplane H must contain 6 or 10 vectors from T^+, but if H contains 10 vectors from T^+ then H contains S_f. This is impossible since $\mathbf{k}$ is the dimension of the smallest flat contained S_f. Therefore H contains 12 vectors from S_f, and $\mathbf{F}_2^n \setminus H$ contains exactly 4 vectors from S_f. □

Lemma 18 *There exist at most 3 columns satisfying the condition of Lemma 17. Without loss of generality it is possible to choose these columns as $\delta_1^+ = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1,\ 1)^T$, $\delta_2^+ = (0,0,0,0,1,1,0,0,1,1)^T$, $\delta_3^+ = (0,0,0,1,0,1,0,1,0,1)^T$.*

Proof. It is easy to check that the vectors δ_1^+, δ_2^+, δ_3^+ given above can be chosen without the loss of generality. Suppose that it is possible to add some vector δ_4^+ to this set. For $c_1, c_2, c_3 \in \{0, 1\}$ denote $\delta^+(c_1, c_2, c_3) = c_1\delta_1^+ + c_2\delta_2^+ + c_3\delta_3^+$. Consider the sum

$$S = \sum_{c_1, c_2, c_3 \in \{0,1\}} d(\delta_4^+, \delta^+(c_1, c_2, c_3)).$$

Note that for any row from 4th till 10th exactly 4 of 8 vectors $\delta^+(c_1, c_2, c_3)$ have one in this row. Therefore $S = 28 + 8w_0 = 32$ where w_0 is the number of ones in rows 1–3 in δ_4^+. It follows that $w_0 = 0.5$ but w_0 is an integer number. This contradiction proves Lemma 18. □

Lemma 19 *The right side of the matrix M contains at most* 3 *columns.*

Proof. It follows from Lemmas 17 and 18. □

Lemma 19 follows that the case $\mathbf{k}^- = 3$ is impossible. The remained cases are $\mathbf{k}^- = 4$ and $\mathbf{k}^- = 5$.

Lemma 20 *Let γ_i be a column from the left side of the matrix M. Suppose that γ_i contains* 1 *one and* 5 *zeroes in low* 6 *rows. Then $wt(\gamma_i^+) = 5$.*

Proof. Denote $H = \{(x, y) \in F_2^{\mathbf{k}} \mid x_i = 0\}$. By the hypothesis of Lemma the hyperplane H contains exactly 5 vectors of T^-, therefore by Lemma 15 the hyperplane H must contain 5 or 9 vectors from T^+, but if H contains 9 vectors from T^+ then H contains exactly 14 vectors from S_f. This is impossible by Lemma 16. It follows that $wt(\gamma_i^+) = 5$. □

Lemma 21 *Let γ_i be a column from the left side of the matrix M. Suppose that γ_i contains* 2 *ones and* 4 *zeroes in low* 6 *row. Then $wt(\gamma_i^+) \in \{2, 6\}$.*

Proof. Denote $H = \{(x, y) \in F_2^{\mathbf{k}} \mid x_i = 0\}$. The hyperplane H contains exactly 4 vectors from T^-, therefore by Lemma 15 the hyperplane H must contain 4 or 8 vectors from T^+. It follows that $wt(\gamma_i^+) = 2$ or 6. □

Consider now separately the cases $\mathbf{k}^- = 4$ and $\mathbf{k}^- = 5$.

Case $\mathbf{k}^- = 5$.

In this case the right side of the matrix M contains two columns. By Lemma 18 without loss of generality we can assume that these columns are $\delta_1 = (0, 0, 0, 0, 0, 0, 1, 1, 1, 1)^T$, $\delta_2 = (0, 0, 0, 0, 1, 1, 0, 0, 1, 1)^T$. Without loss of generality we can assume that the matrix M has the form

$$\left(\begin{array}{ccccc|cc} * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & 0 & 0 \\ * & * & * & * & * & 0 & 1 \\ * & * & * & * & * & 0 & 1 \\ * & * & * & * & * & 1 & 0 \\ * & * & * & * & * & 1 & 0 \\ * & * & * & * & * & 1 & 1 \\ * & * & * & * & * & 1 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

By Lemma 20 we have that all columns γ_i^+, $i = 1, 2, 3, 4, 5$, contain exactly 5 ones.

Lemma 22 *Let* $\mathbf{k}^- = 5$. *Then for* $1 \le i_1 < i_2 \le 5$, *we have* $d(\gamma_{i_1}^+, \gamma_{i_2}^+) \in \{2, 6\}$.

Proof. Denote $H = \{(x, y) \in F_2^{\mathbf{k}} \mid x_{i_1} + x_{i_2} = 0\}$. The hyperplane H contains exactly 4 vectors from T^-, therefore by Lemma 15 the hyperplane H must contain 4 or 8 vectors from T^+. It follows that $d(\gamma_{i_1}^+, \gamma_{i_2}^+) = wt(\gamma_{i_1}^+ + \gamma_{i_2}^+) \in \{2, 6\}$. □

Lemma 23 *Let* $\mathbf{k}^- = 5$. *Then for any* $i \in \{1, 2, 3, 4, 5\}$, $c_1, c_2 \in \{0, 1\}$, *we have* $d(\gamma_i^+, c_1\delta_1^+ + c_2\delta_2^+) = 5$.

Proof. Denote $H = \{(x, y) \in F_2^{\mathbf{k}} \mid x_i + c_1 y_1 + c_2 y_2 = 0\}$. The hyperplane H contains exactly 5 vectors from T^-, therefore by Lemma 15 the hyperplane H must contain 5 or 9 vectors from T^+. But if H contains 9 vectors from T^+, then H contains exactly 14 vectors from S_f. This is impossible by Lemma 16. It follows that $d(\gamma_i^+, c_1\delta_1^+ + c_2\delta_2^+) = wt(\gamma_i^+ + c_1\delta_1^+ + c_2\delta_2^+) = 5$. □

Lemma 24 *Let* $\mathbf{k}^- = 5$. *Then for any* i, $i \in \{1, 2, 3, 4, 5\}$, *the column* γ_i^+ *contains exactly* 2 *ones in rows* 1–4, *exactly* 1 *one in rows* 5, 6, *exactly* 1 *one in rows* 7, 8, *exactly* 1 *one in rows* 9, 10.

Proof. If γ_i^+ contains 0 ones in rows 9, 10 then $d(\gamma_i^+, \delta_1^+) = d(\gamma_i^+, \delta_2^+) = 5$ follows that γ_i^+ contains only ones in rows 5, 6, 7, 8. But in this case $d(\gamma_i^+, \delta_1^+ + \delta_2^+) = 1$ that contradicts to Lemma 23. If γ_i^+ contains 2 ones in rows 9, 10 then $d(\gamma_i^+, \delta_1^+) = d(\gamma_i^+, \delta_2^+) = 5$ follows that γ_i^+ contains only zeroes in rows 5, 6, 7, 8. But in this case $d(\gamma_i^+, \delta_1^+ + \delta_2^+) = 9$ that contradicts to Lemma 23. Therefore γ_i^+ contains exactly 1 one in rows 9, 10. It follows that γ_i^+ contains exactly 1 one in rows 7, 8, exactly 1 one in rows 5, 6 and exactly 2 ones in rows 1–4. □

Lemma 25 *The case* $\mathbf{k}^- = 5$ *is impossible.*

Proof. There exist 3 pairs of opposite vectors of the length 4 with exactly 2 ones. Therefore there exist two columns γ_{i_1} and γ_{i_2}, $i_1 \ne i_2$, in the left side of M that are either the same or the opposite inside of first 4 rows. Let γ_{i_3} be some other column in the left side of M, $i_1 \ne i_3$, $i_2 \ne i_3$. Then from Lemma 24 it is easy to see that every group of rows (1–4), (5, 6), (7, 8), (9, 10) gives to the sum $S = d(\gamma_{i_1}^+, \gamma_{i_2}^+) + d(\gamma_{i_1}^+, \gamma_{i_3}^+) + d(\gamma_{i_2}^+, \gamma_{i_3}^+)$ the contribution divided by 4. Therefore the sum S is divided by 4. On the other hand, by Lemma 22 all terms in S are congruent 2 modulo 4. Therefore S is congruent 2 modulo 4 too. This contradiction proves the Lemma. □

Thus, we have proved that the case $\mathbf{k}^- = 5$ is impossible.

Case $\mathbf{k}^- = 4$.

In this case the right side of the matrix M contains exactly three columns. By Lemma 18 without loss of generality we can assume that these columns are $\delta_1 = (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1,\ 1)^T$, $\delta_2 = (0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 1,\ 1)^T$, $\delta_3 = (0,0,0,1,0,1,0,1,0,1)^T$. Without loss of generality we can assume that the matrix M has the form

$$\left(\begin{array}{cccc|ccc} * & * & * & * & 0 & 0 & 0 \\ * & * & * & * & 0 & 0 & 0 \\ * & * & * & * & 0 & 0 & 0 \\ * & * & * & * & 0 & 0 & 1 \\ * & * & * & * & 0 & 1 & 0 \\ * & * & * & * & 0 & 1 & 1 \\ * & * & * & * & 1 & 0 & 0 \\ * & * & * & * & 1 & 0 & 1 \\ * & * & * & * & 1 & 1 & 0 \\ * & * & * & * & 1 & 1 & 1 \\ \hline * & * & * & * & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Let $c_1, c_2, c_3 \in \{0,1\}$. Denote $\delta^+(c_1,c_2,c_3) = c_1\delta_1^+ + c_2\delta_2^+ + c_3\delta_3^+$.

Lemma 26 *Let $\mathbf{k}^- = 4$. Then any column γ_i in the left side of the matrix M can not have zero in 11th row.*

Proof. Suppose that some column γ_i have zero in 11th row. Then by Lemma 20 we have $wt(\gamma_i^+) = 5$. By the same way like to the proof of Lemma 23 it is possible to show that for any $c_1, c_2, c_3 \in \{0,1\}$ we have $d(\gamma_i^+, \delta^+(c_1,c_2,c_3)) = 5$. Consider the sum

$$S = \sum_{c_1,c_2,c_3 \in \{0,1\}} d(\gamma_i^+, \delta^+(c_1,c_2,c_3)).$$

Note that for any row from 4th till 10th exactly 4 of 8 vectors $\delta^+(c_1,c_2,c_3)$ have one in this row. Therefore $S = 28 + 8w_0 = 40$ where w_0 is the number of ones in γ_i in rows from 1st till 3rd. It follows that $w_0 = 1.5$ but w_0 is an integer number. This contradiction proves Lemma 26. □

Lemma 26 follows that without loss of generality the 11th row of M is (1111000) and the matrix M has the form

$$\left(\begin{array}{cccc|ccc}
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 1 \\
* & * & * & * & 0 & 1 & 0 \\
* & * & * & * & 0 & 1 & 1 \\
* & * & * & * & 1 & 0 & 0 \\
* & * & * & * & 1 & 0 & 1 \\
* & * & * & * & 1 & 1 & 0 \\
* & * & * & * & 1 & 1 & 1 \\
\hline
1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right).$$

Lemma 27 *Let* $\mathbf{k}^- = 4$. *Then for any* $1 \le i_1 < i_2 \le 4$ *we have* $d(\gamma_{i_1}^+, \gamma_{i_2}^+) \in \{2, 6\}$.

Proof. Denote $H = \{(x, y) \in F_2^{\mathbf{k}} \,|\, x_{i_1} + x_{i_2} = 0\}$. The hyperplane H contains exactly 4 vectors from T^-, therefore by Lemma 15 the hyperplane H must contain 4 or 8 vectors from T^+. It follows that $d(\gamma_{i_1}^+, \gamma_{i_2}^+) \in \{2, 6\}$. □

Lemma 28 *Let* $\mathbf{k}^- = 4$. *Then any column* γ_i *in the left side of the matrix* M *has exactly* 2 *ones in rows from* 1*st till* 3*rd and coincides with a vector* $\delta^+(c_1, c_2, c_3)$ *in rows from* 4*th till* 10*th for some* $c_1, c_2, c_3 \in \{0, 1\}$.

Proof. By Lemma 21 we have $wt(\gamma_i^+) \in \{2, 6\}$. By the same way it is possible to show that for any $c_1, c_2, c_3 \in \{0, 1\}$ we have $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) \in \{2, 6\}$.

Suppose that $wt(\gamma_i^+) = 2$. If γ_i^+ does not contain both its ones in rows from 1st till 3rd then it is easy to find some $c_1, c_2, c_3 \in \{0, 1\}$ such that the vector $\delta^+(c_1, c_2, c_3)$ contains exactly 1 one in two rows where γ_i^+ has ones. Then we have $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) = 4$ that is impossible. Therefore γ_i^+ contains both ones in rows from 1st till 3rd and coincides with the vector $\delta^+(0, 0, 0)$ in rows from 4th till 10th, i. e. γ_i^+ has the desired form.

Now suppose that $wt(\gamma_i^+) = 6$. Consider the sum

$$S = \sum_{c_1, c_2, c_3 \in \{0,1\}} d(\gamma_i^+, \delta^+(c_1, c_2, c_3)).$$

Note that for any row from the group (4–10) exactly 4 of 8 vectors $\delta^+(c_1, c_2, c_3)$ have one in this row. Therefore $S = 28 + 8w_0$ where w_0 is the number of ones in rows from 1st till 3rd in γ_i. If for any $c_1, c_2, c_3 \in \{0, 1\}$ we have $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) = 6$ then $S = 48$ and $w_0 = 2.5$, but w_0 is an integer number. Therefore there exists the set of values $c_1, c_2, c_3 \in \{0, 1\}$ such that $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) = 2$. Denote $\delta^+(c_1, c_2, c_3)$ by δ_0^+. Then $wt(\gamma_i^+ + \delta_0^+) = 2$ and for any $c_1, c_2, c_3 \in \{0, 1\}$ we have $d(\gamma_i^+ + \delta_0^+, \delta^+(c_1, c_2, c_3)) \in \{2, 6\}$. As it was pointed out in the beginning of this proof the vector $\gamma_i^+ + \delta_0^+$ must have exactly 2 ones in rows from 1st till 3rd, and only zeroes in rows from 4th till 10th. Hence, the vector γ_i^+ has exactly 2 ones in rows from 1st till 3rd and coincides with the vector δ_0^+ in rows from 4th till 10th. □

Lemma 29 *The case* $\mathbf{k}^- = 4$ *is impossible.*

Proof. By Lemma 28 all columns γ_i in the left side of M have exactly 2 ones in rows from 1st till 3rd. The left side of M contains 4 columns, therefore there exist columns γ_{i_1} and γ_{i_2}, $1 \le i_1 < i_2 \le 4$ that coincide in rows from 1st till 3rd. In rows from 4th till 10th the columns γ_{i_1} and γ_{i_2} coincide by Lemma 28 with some vectors $\delta^+(c_1', c_2', c_3')$ and $\delta^+(c_1'', c_2'', c_3'')$, respectively. By Lemma 17 we have $d(\delta^+(c_1', c_2', c_3'), \delta^+(c_1'', c_2'', c_3'')) \in \{0, 4\}$. It follows $d(\gamma_{i_1}^+, \gamma_{i_2}^+) \in \{0, 4\}$ that contradicts to Lemma 27. □

All cases are considered. Theorem 1 is proved.

Thus, we obtained that the affine rank of a plateaued function with a spectrum support of cardinality 16 can not take another values with the exception of 4, 5 and 6. The functions with such parameters are known and their examples were given, for example, in [2]. We will not give examples in this section separately. These examples will be constructed in the next section in the framework of a general construction.

5 Bounds on affine rank of plateaued functions with arbitrary cardinality of spectrum support

Lemma 30 *Suppose that there exists a plateaued function with a spectrum support of cardinality* 4^h *and the affine rank* $\mathbf{k}$*. Then for any positive integer* s *satisfied inequalities* $\mathbf{k} + 2 \le s \le 2\mathbf{k} + 2$ *there exists a plateaued function with a spectrum support of cardinality* 4^{h+1} *and the affine rank* s*.*

Proof. If there exists a plateaued function with a spectrum support of cardinality 4^h and the affine rank $\mathbf{k}$ then by Lemmas 2 and 3 starting with

this function by means of an affine transformation of a spectrum and following deleting of fictitious variables it is possible to obtain the plateaued function f on $\mathbf{F}_2^{\mathbf{k}}$ with a spectrum support of cardinality 4^h, moreover, this spectrum support of f will contain the zero vector as well as all vectors of weight 1. Consider the function $f_1(x_1, \ldots, x_s) = f(x_{s-\mathbf{k}}, \ldots, x_{s-1}) + x_s$ on $\mathbf{F}_2^s$ (the variables x_1, ..., $x_{s-\mathbf{k}-1}$ will be fictitious for the function f_1). By Lemmas 3 and 4 the function f_1 will be plateaued again with the same cardinality of a spectrum support, moreover, to all vectors from S_f in the spectrum support of S_{f_1} it will be assigned $s - \mathbf{k} - 1$ zeroes from the left side, and it will be assigned one from the right side. The linear subspace of dimension $\mathbf{k}$ in $\mathbf{F}_2^{\mathbf{k}}$ contained S_f passing to the function f_1 will transfer to the coset of dimension $\mathbf{k}$ in $\mathbf{F}_2^s$ contained S_{f_1} which is not a linear space. Therefore the rank of the function f_1 is equal to $\mathbf{k} + 1$. Note that the spectrum support S_{f_1} contains the next vectors: all vectors of weight 2 with ones in the components i and s, $i = s-\mathbf{k}, \ldots, s-1$, and also the vector of weight 1 with one in the component s. Form the function

$$f_2(x_1, \ldots, x_s) = f_1(x_s, \ldots, x_1)$$

on $\mathbf{F}_2^s$ renaming all variables of f_1 in reverse order. It is clear that the function f_2 has the properties, analogous to the properties of the function f_1. The spectrum support S_{f_2} contains among others the next vectors: all vectors of weight 2 with ones in the components 1 and i, $i = 2, \ldots, \mathbf{k}+1$, and also the vector of weight 1 with one in the component 1. Note that all vectors from S_{f_1} have zero in the first component whereas all vectors from S_{f_2} have one in the first component. Therefore the sets S_{f_1} and S_{f_2} in $\mathbf{F}_2^s$ do not intersect.

Form the function

$$f'(x_1, \ldots, x_{s+1}) = (x_{s+1} + 1)f_1(x_1, \ldots, x_s) + x_{s+1}f_2(x_1, \ldots, x_s)$$

on $\mathbf{F}_2^{s+1}$. By Lemma 14 for any $u \in \mathbf{F}_2^s$ we have $W_{f'}(u0) = W_{f_1}(u) + W_{f_2}(u)$, $W_f(u1) = W_{f_1}(u) - W_{f_2}(u)$. As it was pointed out above, the sets S_{f_1} and S_{f_2} in $\mathbf{F}_2^s$ do not intersect. Therefore any vector u from S_{f_1} or S_{f_2} in $\mathbf{F}_2^s$ will give exactly two vectors $u0$ and $u1$ contained in the spectrum support $S_{f'}$ of the function f' on $\mathbf{F}_2^{s+1}$, moreover, the values of nonzero Walsh coefficients of the function f' will be the same as the values of nonzero Walsh coefficients of the functions f_1 and f_2. Thus, the cardinality of $S_{f'}$ is equal to 4^{h+1}, and the function f' is also a plateaued function.

The said above follows that $S_{f'}$ contains all vectors of weight 2 with ones in the components 1 and i, $i = 2, \ldots, \mathbf{k}+1$, all vectors of weight 2 with ones in the components i and s, $i = s - \mathbf{k}, \ldots, s-2, s-1, s+1$, and also the vectors of weight 1 with one in the components 1, s. It is easy to see that the

rank of the system of vectors pointed out above is equal to $s+1$. Therefore the rank of the function f' on $\mathbf{F}_2^{s+1}$ is equal to $s+1$. At the same time for any vector from $S_{f'}$ the sum of values of 1st and sth components is equal to 1. Therefore S_f belongs to the hyperplane $H = \{x \in \mathbf{F}_2^{s+1} \mid x_1 + x_s = 1\}$, and the affine rank of the function f' is smaller than $s+1$ but it is not smaller than the rank of the function f' minus 1. It follows that the affine rank of the function f' is equal to s. Thus, the desired function is constructed. □

Theorem 2. For any positive integer $\mathbf{k}$ satisfied inequalities $2h \le \mathbf{k} \le 2^{h+1} - 2$ there exists a plateaued function with a spectrum support of cardinality 4^h and the affine rank $\mathbf{k}$.

Proof. The proof is by induction on h. For $h = 1$ the value $\mathbf{k}$ can be only 2. The example of such function is, for example, bent function x_1x_2 on $\mathbf{F}_2^2$. (If we do not want to consider bent function as a plateaued function then add to it a fictitious variable.) If the statement of Theorem holds for h then its validity for $h+1$ follows immediately from Lemma 30. □

Corollary. The affine rank of a plateaued function with a spectrum support of cardinality 16 can take only values 4, 5 and 6.

Proof. The upper bound $\mathbf{k} \le 6$ is proved in Theorem 1. The lower bound $\mathbf{k} \ge 4$ is obvious. The existence of functions with $\mathbf{k} = 4, 5, 6$ follows from Theorem 2. Note that examples of such functions were given in [2]. □

A trivial upper bound for the affine rank $\mathbf{k}$ of a plateaued function with a spectrum support of cardinality 4^h is $\mathbf{k} \le 4^h - 1$. Here we give an improved bound.

Theorem 3. Let f be a plateaued function, $|S_f| = 4^h$. Then for the affine rank $\mathbf{k}$ of a spectrum support S_f the inequality $\mathbf{k} \le 2^{2h-1} - 2^{h-1} + h$ holds.

Proof. We will follow the way, analogous to the proof of Theorem 1. By Lemma 8 we have $|T^+|, |T^-| \in \{2^{2h-1} + 2^{h-1}, 2^{2h-1} - 2^{h-1}\}$. Without loss of generality we can assume that $|T^+| = 2^{2h-1} + 2^{h-1}$, $|T^-| = 2^{2h-1} - 2^{h-1}$. Suppose that the affine rank of a spectrum support S_f is equal to $\mathbf{k}$, and the affine rank of T^- is equal to $\mathbf{k}^-$. Obviously, $\mathbf{k}^- \le 2^{2h-1} - 2^{h-1} - 1$. It is easy to see that by means of some affine transformation in $\mathbf{F}_2^n$ it is possible to embed the smallest coset contained the spectrum support S_f into $\mathbf{F}_2^{\mathbf{k}} \otimes (\underbrace{0 \dots 0}_{n-\mathbf{k}})$ such that some $\mathbf{k}^- + 1$ vectors from T^- will transfer to the vectors $(0,0,0,\dots,0), (1,0,0,\dots,0), (0,1,0,\dots,0), \dots, (\underbrace{0,0,\dots,0,1}_{\mathbf{k}^-},0,\dots,0)$. The Boolean function obtained as a result of this transformation will be plateaued with the same set of absolute values of Walsh coefficients, and with the same values of $\mathbf{k}$ and $\mathbf{k}^-$. By Lemma 3 the variables from $(\mathbf{k}+1)$th till nth in the obtained functions will be fictitious. Deleting them and dividing all Walsh coefficients by $2^{n-\mathbf{k}}$ we obtain by Lemmas 2 and 3 a plateaued function

defined on $\mathbf{F}_2^{\mathbf{k}}$ with a spectrum support of the same cardinality 2^h. Thus, without loss of generality in the remained part of this section we will consider just such a spectrum support.

Form the matrix M of size $4^h \times \mathbf{k}$. In the rows of M we write all vectors from S_f. In the first $2^{2h-1}+2^{h-1}$ rows of M we write vectors from T^+, and in the last $2^{2h-1}-2^{h-1}$ rows of M we write vectors from T^-. The left $\mathbf{k}^-$ columns of M we call *the left side of* M, the remained $\mathbf{k}-\mathbf{k}^-$ columns we call *the right side of* M. The equality $|T^-| = 2^{2h-1} - 2^{h-1}$ follows $\mathbf{k}^- \le 2^{2h-1} - 2^{h-1} - 1$.

Denote by δ_j the columns from the right side of M, and by y_j — the variables corresponded to these columns. Denote by δ_j^+ the subcolumns contained upper $2^{2h-1} + 2^{h-1}$ elements of columns δ_j, respectively.

Lemma 31 *For any set $\delta_{j_1}, \ldots, \delta_{j_s}$, $1 \le s \le \mathbf{k} - \mathbf{k}^-$, of different columns from the right side of M the equality $wt(\delta_{j_1}^+ + \ldots + \delta_{j_s}^+) = 2^h$ holds.*

Proof. Denote $H = \{(x, y) \in F_2^{\mathbf{k}} \,|\, y_{j_1} + \ldots + y_{j_s} = 0\}$. The hyperplane H contains all $2^{2h-1} - 2^{h-1}$ vectors of T^-, therefore by Lemma 8 the hyperplane H must contain $2^{2h-1}-2^{h-1}$ or $2^{2h-1}+2^{h-1}$ vectors from T^+, but if H contains $2^{2h-1} + 2^{h-1}$ vectors from T^+ then H contains S_f. This is impossible, since $\mathbf{k}$ is the dimension of the smallest coset contained S_f. Therefore H contains $4^h - 2^h$ vectors from S_f, and $\mathbf{F}_2^n \setminus H$ contains exactly 2^h vectors from S_f. □

Lemma 32 *The right side of the matrix M contains at most $h+1$ columns.*

Proof. Suppose that the right side of the matrix M contains m columns $\delta_1, \ldots, \delta_m$. For $c_1, \ldots, c_m \in \{0, 1\}$ denote $\delta^+(c_1, \ldots, c_m) = c_1\delta_1^+ \ldots + c_m\delta_m^+$. Consider the sum

$$S = \sum_{c_1,\ldots,c_m \in \{0,1\}} wt(\delta^+(c_1, \ldots, c_m)).$$

Any term in S, besides the term that corresponds to zero vector, is equal to 2^h by Lemma 31. Denote by r the number of rows among upper $2^{2h-1}+2^{h-1}$ rows of the matrix M that contain at least 1 one in the right side of the matrix M. Note that if a row from the upper $2^{2h-1} + 2^{h-1}$ rows of M contains at least 1 such one then exactly 2^{m-1} from $2^m - 1$ nonzero vectors $\delta^+(c_1, \ldots, c_3)$ have one in this row. Therefore $S = 2^h(2^m - 1) = r \cdot 2^{m-1}$. It follows $r = 2^{h+1} - 2^{h-m+1}$. The value r is positive integer, therefore we have $m \le h + 1$, as was to be proved. □

The **proof** of Theorem 3 follows immediately from the structure of the matrix M and Lemma 32.

For $h = 2$ the bound of Theorem 3 can not be achieved. We brave to formulate the hypothesis.

Hypothesis. For any positive integer h the maximum possible affine rank of a plateaued function with a spectrum support of cardinality 4^h is equal to $2^{h+1} - 2$.

References

[1] A. Canteaut, P. Charpin, Decomposing bent functions, IEEE Trans. Inform. Theory, 49(8), pp. 2004-19, August 2003.

[2] C. Carlet, P. Charpin, Cubic Boolean functions with highest resiliency, Proceedings of 2004 IEEE International Symposium on Information Theory ISIT 2004, Chicago, USA, June 2004, p. 497, full version is submitted to IEEE Transactions on Information Theory.

[3] C. Carlet, P. Sarkar, Spectral domain analysis of correlation immune and resilient Boolean functions, Finite fields and Applications, V. 8, 2002, pp. 120–130.

[4] T. Kasami, N. Tokura, S. Azumi, On the weight enumeration of weights less than $2.5d$ of Reed–Muller codes, Information and Control, Vol. 30 (4), April 1976, pp. 380–395.

[5] D. Pei, W. Qin, The correlation of a Boolean function with its variables, Progress in cryptology — Indocrypt 2000, Lecture Notes in Computer Science, V. 1977, Springer-Verlag, 2000, pp. 1–8.

[6] Y. Zheng, X.-M. Zhang, Plateaued functions, Proceedings of ICICS 1999, Lecture Notes in Computer Science, V. 1726, Springer-Verlag, 1999, pp. 284–300.

[7] Ю. В. Кузнецов, О носителях платовидных функций, Материалы VIII Международного семинара "Дискретная математика и ее приложения" (2–6 февраля 2004 г.), М., Изд-во механико-математического факультета МГУ, 2004, с. 424-426.

[8] О. А. Логачев, А. А. Сальников, В. В. Ященко, Булевы функции в теории кодирования и криптографии, М.: Изд-во МЦНМО, 2004.

[9] Ю. В. Тарannиков, О корреляционно-иммунных и устойчивых булевых функциях, Математические вопросы кибернетики, Вып. 11, М., Физматлит, 2002, с. 91–148.

[10] Ю. В. Таранников, О платовидных устойчивых функциях, Материалы VIII Международного семинара "Дискретная математика и ее приложения" (2–6 февраля 2004 г.), М., Изд-во механико-математического факультета МГУ, 2004, с. 431-435.