An asymptotic lower bound on the number of bent functions

V. N. Potapov[1], A. A. Taranenko[1], and Yu. V. Tarannikov[2]

[1] Sobolev Institute of Mathematics vpotapov@math.nsc.ru, taa@math.nsc.ru
[2] Lomonosov Moscow State University yutarann@gmail.com

Abstract. A Boolean function f on n variables is said to be a bent function if the absolute value of all its Walsh coefficients is $2^{n/2}$. Our main result is a new asymptotic lower bound on the number of Boolean bent functions. It is based on a modification of the Maiorana–McFarland family of bent functions and recent progress in the estimation of the number of transversals in latin squares and hypercubes. A by-product of our proof is the asymptotics of the logarithm of the numbers of partitions of the Boolean hypercube into 2-dimensional affine subspaces.

Keywords: bent functions · asymptotic bounds · plateaued functions · affine subspaces · transversals in latin hypercubes · perfect matchings

1 Definitions, preliminaries and main results

Boolean functions and, in particularly, bent functions are widely used in cryptography [6, 14, 20], and problems of their existence and enumeration are important. Asymptotic bounds on the numbers of certain cryptographic functions were obtained, for example, in [5, 15, 21].

The literature on bent functions is usually devoted to their existence and constructions whereas it does not pay much attention to bounds on cardinalities of classes of bent functions. The most known bounds are the cardinality of the Majorana–McFarland family as well as a cumbersome Agievich's formula [3].

In the following table we present without proof our analysis of the logarithms of cardinalities for some relatively rich classes of bent functions on n variables. It is well known that bent functions exist if and only if n is even.

Class and reference	Asymptotics of $\log_2$ of cardinality	Proof
MM family [13]	$\log_2 \lvert\mathcal{M}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1+o(1))$	E
completed MM family [14]	$\log_2 \lvert\mathcal{M}^{\#}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1+o(1))$	E
$\mathcal{C}$ class [8]	$\log_2 \lvert\mathcal{C}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1+o(1))$	E
$\mathcal{D}$ class [8]	$\log_2 \lvert\mathcal{D}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1+o(1))$	E
special subclass of $\mathcal{PS}$ [14]	$\log_2 \lvert\mathcal{PS}_{ap}(n)\rvert = 2^{n/2}(1+o(1))$	E
$\mathcal{P}$artial $\mathcal{S}$pread family [14]	$\log_2 \lvert\mathcal{PS}(n)\rvert \le \frac{n^2}{8} \cdot 2^{n/2}(1+o(1))$	H
Agievich bound [3]	$\log_2 A(n) = \frac{n}{2} \cdot 2^{n/2}(1+o(1))$	H
Construction from [1, 4]	$\log_2 \lvert K_{(n/2)-k}(n)\rvert \le \frac{(2k+1)n}{2^{k+1}} \cdot 2^{n/2}(1+o(1))$	H
Construction from [1, 4]	$\log_2 \lvert K_{(n/2)-1}(n)\rvert = \frac{3n}{4} \cdot 2^{n/2}(1+o(1))$	M

Here letter “E” means that the asymptotics can be easily derived from the description of a class and “H” stands for the necessity of additional analysis. The asymptotics in the last row of the table (labeled by “M”) is the main result of the present paper.

Our lower bound is given by a class (K) of bent functions proposed in [4] that is a variance of a construction from [1]. A similar construction of bent functions was also proposed in [11]. Moreover, in [7] and [3] it was considered an analog of the construction (K) that uses linear subspaces instead of affine ones. We show that the construction (K) and the mentioned versions produce new bent functions that were not discovered before.

Let $F_2 = \{0, 1\}$. The set F_2^n is called the *n-dimensional Boolean hypercube* (or the *Boolean n-cube*). The hypercube F_2^n equipped with scalar multiplication and coordinate-wise modulo 2 addition $\oplus$ is an n-dimensional vector space. Its zero element is $\overline{0} = (0, \dots, 0)$. A set $C \subseteq F_2^n$ is called a *k-dimensional affine subspace* if $C = a \oplus S$ for some $a \in F_2^n$ and a k-dimensional linear subspace S of F_2^n.

For $x, y \in F_2^n$, $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$, we define their *inner product* as

$$\langle x, y\rangle = x_1y_1 \oplus \cdots \oplus x_ny_n.$$

A function $f : F_2^n \to F_2$ is said to be a *Boolean function* on n variables.

The *Walsh transform* of a Boolean function f is a function $W_f : F_2^n \to \mathbb{Z}$ such that

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

The values $W_f(u)$ are called *Walsh coefficients*, and the set of all Walsh coefficients is called the *Walsh spectrum* of f. The *support* of the Walsh spectrum is the set $\{u : W_f(u) \neq 0\}$.

A Boolean function f on n variables is said to be a *bent function* if the Walsh spectrum of f consists of $\pm 2^{n/2}$, and f is a *plateaued function* if all its Walsh coefficients are equal to $\pm 2^k$ or 0, for some integer k. We use b_n to denote the number of bent functions on n variables.

Bent functions f and g are *affinely equivalent*, if there is a nondegenerate binary matrix L of size $n \times n$ and $a \in F_2^n$ such that

$$g(x) = f(Lx \oplus a).$$

For each bent function f there are no more than 2^{n^2+n} affinely equivalent bent functions.

It is well known (see [6, 10, 14]) that the algebraic degree (the degree of the Zhegalkin polynomial) of a bent function f on n variables is at most $n/2$. Therefore, the number b_n of bent functions is not greater than $2^{\sum\limits_{i=0}^{n/2} \binom{n}{i}}$, and, consequently, $\log_2 b_n \leq 2^{n-1} + \frac{1}{2}\binom{n}{n/2}$. In [9] and [2] there are slightly better upper bounds on the number of bent functions, but asymptotically both of them are $\log_2 b_n \leq 2^{n-1}(1 + o(1))$. In [16] the following improvement of the upper bound is stated.

Theorem 1 ([16]). *The number b_n of bent functions on n variables is not greater than $6^{3\cdot 2^{n-6}} 2^{\cdot 2^{n-2}(1+o(1))}$ as $n \to \infty$. In particular,*

$$\log_2 b_n \leq 3 \cdot 2^{n-3}(1 + o(1)).$$

Note that Tokareva's conjecture [21] on the decomposition of Boolean functions into a sum of bent functions suggests that $\log_2 b_n \geq 2^{n-2} + \frac{1}{2}\binom{n}{n/2}$.

Till the class of Maiorana–McFarland functions [13] was considered as the richest family of bent functions (up to some extensions). This class consists of functions of the form

$$f(x, y) = f(x_1, \ldots, x_m, y_1, \ldots, y_m) = \psi(y) \bigoplus_{i=1}^{m} x_i \pi_i(y)$$

and functions that affinely equivalent to them. Here $n = 2m$, $\psi(y)$ is an arbitrary Boolean function on m variables, and π is an arbitrary permutation of F_2^m, $\pi(y) = (\pi_1(y), \ldots, \pi_m(y))$.

The choice of permutation π and Boolean function ψ contributes $2^{n/2}! \cdot 2^{2^{n/2}}$ bent functions to the Maiorana–McFarland family. Taking into account affinely equivalent functions, we see that the completed Maiorana–McFarland family contains no more than $2^{n/2}! \cdot 2^{2^{n/2}} \cdot 2^{n^2+n}$ bent functions.

Using the Stirling's approximation,

$$\log_2 N! = N \log_2 N - N \log_2 e + o(N), \tag{1}$$

we conclude that the logarithm of the number b_n of bent functions on n variables satisfies

$$\log_2 b_n \geq \frac{n}{2} \cdot 2^{n/2} + (1 - \log_2 e) \cdot 2^{n/2} + o(2^{n/2}).$$

Our main result is the following asymptotic bound on the number of bent functions.

Theorem 2. *Let b_n be the number of bent functions on n variables, where n is even. Then*

$$\log_2 b_n \geq \frac{3n}{4} \cdot 2^{n/2} - 2\log_2 e \cdot 2^{n/2} + o(2^{n/2}).$$

For additional information on bent functions and their number the reader is reffered to papers and monographs [10, 14, 20, 21].

2 Construction of bent functions

For a Boolean variable $a \in F_2$, we use a notation $a^1 = a$ and $a^0 = a \oplus 1$. In particular, $a^b = 1 \Leftrightarrow a = b$. Moreover, for $x, y \in F_2^n$, $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$, we define $x^y = x_1^{y_1} \cdots x_n^{y_n}$.

Let us describe a family of Boolean functions that gives the lower bound in Theorem 2.

Construction (K): Let $n = n_1 + n_2$, $n_2 \geq n_1$, n and $n_2 - n_1$ be even. Assume that $\{C_a\}_{a \in F_2^{n_1}}$, $C_a \subseteq F_2^{n_2}$ is an ordered partition of $F_2^{n_2}$ into 2^{n_1} affine subspaces of dimensions $n_2 - n_1$. Define a Boolean function f on n variables as

$$f(x, y) = \bigoplus_{a \in F_2^{n_1}} f_a(y) x^a,$$

where $x \in F_2^{n_1}, y \in F_2^{n_2}$, and f_a are plateaued functions such that the support of the Walsh spectrum of f_a is exactly C_a.

To prove that such a function f is well defined, it is sufficient to construct a plateaued function g such that the support of its Walsh spectrum is equal to any given affine subspace C of even dimension. This fact was previously established in [19], but we prove it here for the sake of completeness.

For this purpose, we need the following properties of Walsh coefficients. They can be found, e.g., in books [14, 20] or can be derived directly from the definitions.

Proposition 1. *Let f be a Boolean function on n variables.*

1. *Suppose that f has a form $f(x, y) = g(x)$, where $x \in F_2^k$, $y \in F_2^{n-k}$, and g is a Boolean function on k variables. Then for all $u \in F_2^k$ the Walsh coefficients $W_f(u, \overline{0}) = 2^{n-k} W_g(u)$ and $W_f(u, v) = 0$ if $v \in F_2^{n-k} \setminus \{\overline{0}\}$.*
2. *Let $f(x) = g(Lx)$ for some nondegenerate binary matrix L of sizes $n \times n$ and a Boolean function g on n variables. Then $W_f(u) = W_g((L^{-1})^T u)$.*
3. *Assume that $f(x) = g(x) \oplus \langle a, x \rangle$ for some $a \in F_2^n$ and a Boolean function g on n variables. Then $W_f(u) = W_g(u \oplus a)$.*

Proposition 2 ([19]). *Let $C \subseteq F_2^n$ be an affine subspace of even dimension k. There exists a one-to-one correspondence between plateaued functions f on n variables, whose support of the Walsh spectrum is equal to C, and bent functions g on k variables. Moreover, the absolute value of all nonzero Walsh coefficients W_f of the function f is $2^{n-k/2}$.*

Proof. Let g be a bent function on k variables. By the definition, $|W_g(u)| = 2^{k/2}$ for all $u \in F_2^k$. Using Proposition 1(1), we construct a Boolean function h on n variables all of whose nonzero Walsh coefficients are equal to $\pm 2^{n-k/2}$ and located in a k-dimensional subcube of the Boolean n-cube. With the help of Proposition 1(2) and (3), we put the support of the Walsh spectrum of h to the affine subspace C and obtain the desired plateaued function f. Note that the absolute value of all nonzero Walsh coefficients of f is $2^{n-k/2}$.

Reversing this reasoning, we have the equivalence.

It also can be proved that the construction (K) produces only bent functions.

Theorem 3 ([4]). *Every function f given by the construction (K) is bent.*

In what follows, we denote by $\widetilde{N}_m^k$ the number of ordered partitions of the space F_2^m into k-dimensional affine subspaces and by N_m^k the number of all such unordered partitions. (A partition of F_2^m into affine subspaces is unordered when the order of subspaces in the partition does not matter). Proposition 2 and Theorem 3 easily imply the following formula for the number of bent functions in the construction (K).

Theorem 4. *Let $n = n_1 + n_2$, $n_2 \geq n_1$, and n and $n_2 - n_1$ be even. Then the number B_n of bent functions given by the construction (K) is*

$$B_n = (b_{n_2-n_1})^{2^{n_1}} \cdot \widetilde{N}_{n_2}^{n_2-n_1},$$

where $b_{n_2-n_1}$ is the number of bent functions over $n_2 - n_1$ variables, $\widetilde{N}_{n_2}^{n_2-n_1}$ is the number of ordered partitions of the space $F_2^{n_2}$ into 2^{n_1} affine subspaces of dimensions $n_2 - n_1$.

3 Proof of the lower bound

The key element of the proof of Theorem 2 is an estimation of the number of ordered partitions of F_2^m into 2-dimensional affine subspaces. Meanwhile, here we establish an asymptotics of the logarithm of the number of the unordered ones. For shortness, we denote the number of unordered partitions of F_2^m into 2-dimensional affine subspaces by N_m ($N_m = N_m^2$).

Theorem 5. *The number N_m of all unordered partitions of F_2^m into 2-dimensional affine subspaces satisfies*

$$\frac{m}{2} \cdot 2^m + c_1 \cdot 2^m + o(2^m) \leq \log_2 N_m \leq \frac{m}{2} \cdot 2^m + c_2 \cdot 2^m + o(2^m),$$

where $c_1 = -1 - \frac{3}{4}\log_2 e \approx -2.08$, $c_2 = \frac{7}{16} - \frac{11}{16}\log_2 3 \approx -0.65$.

It is easy to see that the numbers of ordered and unordered partitions of F_2^m into k-dimensional affine subspaces are connected in the following way.

Proposition 3. *If $\widetilde{N}_m^k$ is the number of ordered partitions of the space F_2^m into k-dimensional affine subspaces and N_m^k is the number of unordered ones, then*

$$\widetilde{N}_m^k = 2^{m-k}! \cdot N_m^k.$$

The proof of Theorem 5 needs more definitions and some auxiliary results on latin hypercubes, their transversals, and perfect matchings in hypergraphs.

A *d-dimensional latin hypercube of order n* is a d-dimensional matrix $Q = (q_\alpha)$ of order n whose entries indexed by $\alpha = (\alpha_1, \dots, \alpha_d)$, $\alpha_i \in \{1, \dots, n\}$, where Q is filled by n symbols so that each symbol appears in each line (1-dimensional submatrix) exactly once. A *transversal* in a latin hypercube is a collection of n entries hitting each hyperplane ($(d-1)$-dimensional submatrix) and each symbol exactly once.

Actually, we are interested in transversals in specific latin hypercubes. Let Q_m be the 3-dimensional latin hypercube of order 2^m correspoding to the Cayley table of the iterated group $\mathbb{Z}_2^m$. In more details, its entry $q_{\alpha_1,\alpha_2,\alpha_3} = \alpha_4$, $\alpha_i \in F_2^m$, if and only if $\alpha_1 \oplus \cdots \oplus \alpha_4 = \overline{0}$.

In what follows, instead of entries of Q_m we consider tuples $(\alpha_1, \dots, \alpha_4)$, $\alpha_i \in F_2^m$ satisfying $\alpha_1 \oplus \cdots \oplus \alpha_4 = \overline{0}$. Such a notation comprises the index and the value of an entry of the latin hypercube. Then a transversal in the latin hypercube Q_m is a collection of 2^m tuples

$$(\alpha_1^1, \dots, \alpha_4^1), \dots, (\alpha_1^{2^m}, \dots, \alpha_4^{2^m})$$

such that for each $j = 1, \dots, 4$ all α_j^i are different, $i = 1, \dots, 2^m$.

In [12, Theorem 7.2] it was found the asymptotics of the number of transversals in iterated abelian groups. In particular, we have the following estimation of the number of transversals in Q_m.

Theorem 6 ([12]). *The number T_m of transversals in the 3-dimensional latin hypercube Q_m of order 2^m that is the Cayley table of the iterated group $\mathbb{Z}_2^m$ is*

$$T_m = (1 + o(1)) \frac{2^m!^3}{2^{m(2^m-1)}}$$

as $m \to \infty$.

There is a connection between the number of unordered partitions of F_2^m into 2-dimensional affine spaces and the number of transversals in Q_m.

Proposition 4. *The number N_m of unordered partitions of F_2^m into 2-dimensional affine subspaces is not less than the number of transversals in the latin hypercube Q_{m-2}:*

$$N_m \geq T_{m-2}.$$

Proof. For shortness, we use a notation $M = 2^{m-2}$. Let a collection R of M tuples

$$(\alpha_1^1, \dots, \alpha_4^1), \dots, (\alpha_1^M, \dots, \alpha_4^M)$$

be a transversal in the latin hypercube Q_{m-2}. Recall that $\alpha^i_j \in F_2^{m-2}$, $\alpha^i_1 \oplus \dots \oplus \alpha^i_4 = \overline{0}$ for all i, and for a fixed j all α^i_j are different.

To each such collection R we put in correspondence a collection R' of M tuples

$$(\beta^1_1, \dots, \beta^1_4), \dots, (\beta^M_1, \dots, \beta^M_4),$$

where $\beta^i_j \in F_2^m$ and

$$\beta^i_j = \begin{cases} (\alpha^i_j, 0, 0) \text{ if } j = 1; \\ (\alpha^i_j, 0, 1) \text{ if } j = 2; \\ (\alpha^i_j, 1, 0) \text{ if } j = 3; \\ (\alpha^i_j, 1, 1) \text{ if } j = 4. \end{cases}$$

Let us show that R' is an unordered partition of F_2^m into 2-dimensional affine subspaces.

First of all, we still have $\beta^i_1 \oplus \dots \oplus \beta^i_4 = \overline{0}$ for all i. It means that each tuple $(\beta^i_1, \dots, \beta^i_4)$ is a 2-dimensional affine subspace in F_2^m.

Since R is a transversal in the latin hypercube Q_{m-2}, for given $\alpha \in F_2^{m-2}$ and $j \in \{1, \dots, 4\}$ there is a unique $i \in \{1, \dots, M\}$ such that α coincides with some α^j_i from the collection R. So by the construction, for each $\beta \in F_2^m$ there is a unique β^i_j from the collection R' such that $\beta = \beta^j_i$. Since each tuple in R' has all different components, we conclude that R' is a partition of F_2^m.

Thus, R' is an unordered partition of F_2^m into 2-dimensional affine subspaces, and different transversals R in Q_{m-2} give different partitions R'.

To prove the upper bound in Theorem 5, one can use bounds on the number of perfect matchings in an appropriate hypergraph.

Let $H(X, W)$ be a hypergraph with the vertex set X and a hyperedge set W. A hypergraph H is said to be *d-uniform* if each hyperedge consists of exactly d vertices and *k-regular* if each vertex appears in exactly k hyperedges.

A *perfect matching* in a hypergraph H is a collection of hyperedges that cover each vertex of a hypergraph exactly once. Let $PM(H)$ denote the number of perfect matchings in H.

Consider a hypergraph $\mathcal{H}_m$, whose vertex set $V(\mathcal{H}_m)$ is the set F_2^m and the hyperedge set $W(\mathcal{H}_m)$ is the set of all affine subspaces in F_2^m:

$$(x_1, \dots, x_4) \in W(\mathcal{H}_m) \Leftrightarrow x_1 \oplus \dots \oplus x_4 = \overline{0}.$$

It is easy to see that $\mathcal{H}_m$ is a 4-uniform k-regular hypergraph on 2^m vertices, where $k = \frac{1}{6}(2^m - 1)(2^m - 2)$. Moreover, the number N_m of unordered partitions of F_2^m is exactly the number of perfect matchings in $\mathcal{H}_m$.

From [18, Corollary 2] we have the following upper bound on the number of perfect matchings in uniform regular hypergraphs.

Theorem 7 ([18]). *Let H be a d-uniform k-regular hypergraph on n vertices, $d \geq 3$. Then the number $PM(H)$ of perfect matchings in H satisfies*

$$PM(H) \leq (\mu \cdot k)^{n/d},$$

where $\mu = \mu(d) = \frac{d^d d!^{1/d}}{d!^2}$ for $d \geq 4$ and $\mu = \frac{3}{2^{2/3}}$ for $d = 3$.

Now we are ready to find the asymptotics of the logarithm of the number of unordered partitions of F_2^m into 2-dimensional affine subspaces.

Proof (of Theorem 5).

We start with the proof of the lower bound. By Proposition 4, the number N_m of unordered partitions of F_2^m into 2-dimensional affine subspaces is not less than the number of transversals in the latin hypercube Q_{m-2}:

$$N_m \geq T_{m-2}.$$

By Theorem 6, we have that

$$T_{m-2} = (1+o(1))\frac{2^{(m-2)}!^3}{2^{(m-2)\cdot(2^{m-2}-1)}} \text{ as } m \to \infty.$$

Using the Stirling's approximation (1), we deduce

$$\log_2 N_m \geq \log_2 T_{m-2} = \frac{m}{2} \cdot 2^m - \left(1 + \frac{3}{4}\log_2 e\right) \cdot 2^m + o(2^m).$$

For the upper bound we use Theorem 7 and the fact that N_m is the number of perfect matchings in the hypergraph $\mathcal{H}_m$:

$$N_m \leq \left(\frac{\mu}{6} \cdot (2^m-1)(2^m-2)\right)^{2^{m-2}}.$$

$$\log_2 N_m \leq \frac{m}{2} \cdot 2^m + \frac{1}{4}\log_2 \frac{\mu}{6} \cdot 2^m + o(2^m).$$

Since $\mu = \frac{4^4 \cdot 4!^{1/4}}{4!^2}$, we have $\log_2 \frac{\mu}{6} = \frac{7}{4} - \frac{11}{4}\log_2 3$.

At last, let us prove the lower bound on the number of bent functions.

Proof (of Theorem 2).

Let n be even, $n_1 = n/2-1$, $n_2 = n/2+1$.

By Theorem 4 and Proposition 3, the number of bent functions given by the construction (K) for these n_1 and n_2 is

$$B_n = 2^{3\cdot 2^{n/2-1}} \cdot 2^{n/2-1}! \cdot N_{n/2+1},$$

since there are $8 = 2^3$ bent functions on 2 variables.

Using Theorem 5 and the Stirling's approximation (1), we get

$$\log_2 B_n \geq \frac{3n}{4} \cdot 2^{n/2} - 2\log_2 e \cdot 2^{n/2} + o(2^{n/2}).$$

Remark 1. The asymptotically maximal number of bent functions given by the construction (K) is achieved for $n_1 = n/2-1$, $n_2 = n/2+1$.

Proof. If $n_1 = n_2 = n/2$, then the construction (K) coincides with the Maiorana–McFarland family of bent functions, whose number is smaller than one from Theorem 2.

Let $n_1 = n/2 - k$, $n_2 = n/2 + k$, where $k \in \mathbb{N}$, $k \geq 1$. A fundamental contribution to the number of such bent functions is given by the number $\widetilde{N}_{n_2}^{2k}$ of ordered partitions of $F_2^{n_2}$ into $2k$-dimensional affine subspaces. For this purpose we again use a connection to perfect matchings in a special hypergraph and Theorem 7.

Let $\mathcal{H}_{n_2}^k$ be 2^{2k}-uniform hypergraph on 2^{n_2} vertices, where each hyperedge is a $2k$-dimensional affine subspace in 2^{n_2}. The degree of this hypergraph (number of $2k$-dimensional affine subspaces containing a given $x \in F_2^{n_2}$) is not greater than 2^{2kn_2}. By Theorem 7 and Proposition 3,

$$\widetilde{N}_{n_2}^{2k} \leq 2^{n/2-k}! \cdot (2^{2k(n/2+k)})^{2^{n/2-k}},$$

since the constant μ in Theorem 7 is not greater than 1. Using the Stirling's approximation (1), we see that

$$\log_2 \widetilde{N}_{n_2}^{2k} \leq (n/2-k) \cdot 2^{n/2-k} + 2k(n/2+k) \cdot 2^{n/2-k} + o(n2^{n/2}) = \frac{2k+1}{2^{k+1}} \cdot n2^{n/2} + o(n2^{n/2}).$$

This number is maximal when $k = 1$.

References

1. Agievich, S.: Bent rectangles. In: Proceedings of the NATO advanced study institute on Boolean functions in cryptology and information security, NATO Science for Peace and Security Series D: Information and Communication Security **18**, 3–22, Amsterdam (2008).
2. Agievich, S. V.: On the continuation to bent functions and upper bounds on their number. Prikl. Diskr. Mat. Suppl. **13**, 18–21 (2020)
3. Agievich, S. V.: On the representation of bent functions by bent rectangles. In: Probabilistic Methods in Discrete Mathematics, Proceedings of the Fifth International Petrozavodsk Conference, pp. 121–135, Utrecht, Boston (2002)
4. Baksova, I. P., Tarannikov, Yu. V.: On a construction of bent functions. Surveys on Applied and Industrial Math. **27**(1), 64–66 (2020)
5. Canfield, E. R., Gao, Z., Greenhill, C., McKay, B. D., Robinson, R. W.: Asymptotic enumeration of correlation-immune Boolean functions. Cryptogr. Commun. **2**(1), 111–126 (2010)
6. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press (2020)
7. Carlet, C.: On the confusion and diffusion properties of Maiorana–McFarland's and extended Maiorana–McFarland's functions. In: Special Issue "Complexity Issues in Coding and Cryptography", dedicated to Prof. H. Niederreiter on the occasion of his 60th birthday, pp. 182–204, J. of Complexity **20** (2004)
8. Carlet, C.: Two New Classes of Bent Functions. In: Helleseth T. (eds) Advances in Cryptology — EUROCRYPT'93. EUROCRYPT 1993. Lecture Notes in Computer Science **765**. Springer, Berlin, Heidelberg (1994)

9. Carlet, C., Klapper, A.: Upper bounds on the number of resilient functions and of bent functions. In: Proceedings of the 23rd Symposium on Information Theory in the Benelux, Louvain-La-Neuve, Belgium (2002)
10. Carlet, C., Mesnager, S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5–50 (2016)
11. Çeşmelioğlu, A., Meidl, W.: A construction of bent functions from plateaued functions. Des. Codes Cryptogr. **66**(1–3), 231–242 (2013)
12. Eberhard, S.: More on additive triples of bijections, https://arxiv.org/abs/1704.02407.
13. McFarland, R. L.: A family of difference sets in non-cyclic groups. J. Combinatorial Theory Ser. A **15**, 1–10 (1973)
14. Mesnager, S.: Bent functions. Fundamentals and results. Springer, Cham (2016)
15. Potapov, V. N.: A lower bound on the number of Boolean functions with median correlation immunity. In: Proceedings of XVI International Symposium "Problems of Redundancy in Information and Control Systems", pp. 45–46. IEEE, Moscow, Russia (2019)
16. Potapov, V. N.: An Upper Bound on the Number of Bent Functions. In Proceedings of XVII International Symposium "Problems of Redundancy in Information and Control Systems", pp. 95–96. IEEE, Moscow, Russia (2021)
17. Potapov, V. N., Taranenko, A. A., Tarannikov, Yu. V.: Asymptotic bounds on numbers of bent functions and partitions of the Boolean hypercube into linear and affine subspaces, https://arxiv.org/abs/2108.00232
18. Taranenko, A. A.: On the numbers of 1-factors and 1-factorizations of hypergraphs. Discrete Math. **340**(4), 753–762 (2017)
19. Tarannikov, Yu. V.: On the values of the affine rank of the support of a spectrum of a plateaued function. Diskret. Mat. **18**(3), 120–137 (2006)
20. Tokareva, N.: Bent functions. Elsevier/Academic Press, Amsterdam (2015)
21. Tokareva, N.: On the number of bent functions from iterative constructions: lower bounds and hypothesis. Adv. Math. Commun. **5**(4), 609–621 (2011)