Advances in Mathematics of Communications
Volume 5, No. 4, 2011, 609–621
doi:10.3934/amc.2011.5.609

ON THE NUMBER OF BENT FUNCTIONS FROM ITERATIVE CONSTRUCTIONS: LOWER BOUNDS AND HYPOTHESES

Natalia Tokareva

Sobolev Institute of Mathematics
Siberian Branch of the Russian Academy of Sciences
pr. Koptyuga 4, 630090, Novosibirsk, Russian Federation
and
Novosibirsk State University
st. Pirogova 2, 630090, Novosibirsk, Russian Federation

(Communicated by Joan-Josep Climent)

Abstract. In the paper we study lower bounds on the number of bent functions that can be obtained by iterative constructions, namely by the construction proposed by A. Canteaut and P. Charpin in 2003. The number of bent iterative functions is expressed in terms of sizes of finite sets and it is shown that evaluation of this number is closely connected to the problem of decomposing Boolean function into sum of two bent functions. A new lower bound for the number of bent iterative functions that is supposed to be asymptotically tight is given. Applying Monte–Carlo methods the number of bent iterative functions in 8 variables is counted. Based on the performed calculations several hypotheses on the asymptotic value of the number of all bent functions are formulated.

1. Introduction

Boolean functions with even number of variables that have extremal nonlinear properties are called *bent functions*. They were introduced by O. Rothaus [11, 12] in sixties of XX century. Till now bent functions are intensively studied since they have a lot of applications in coding theory and cryptography, see for example surveys [15, 14].

Precisely, Boolean function in n variables (n is even) is called *bent* if it is at the maximal possible Hamming distance $2^{n-1} - 2^{(n/2)-1}$ from the class of all affine Boolean functions. In other terms all Walsh–Hadamard coefficients of a bent function are the same in absolute values. There are many open problems in bent functions. The number of bent functions in n variables is still unknown if $n > 8$. Moreover, there is a large gap between lower $2^{2^{(n/2)+\log_2(n-2)-1}}$ and upper $2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}$ bounds for this number. There are several improvements of these bounds, see [1], [5] and [16], but not too significant. To find the asymptotic value for the number of all bent functions is a long-standing hard problem closely connected to the problem of enumeration of Hadamard matrices (unsolved since 1893).

2000 *Mathematics Subject Classification:* Primary: 06E30; Secondary: 94A60.

Key words and phrases: Bent function, iterative construction, asymptotic value, bent sum decomposition, Monte–Carlo methods.

The author is supported by the Russian Foundation for Basic Research (grants 09-01-00528, 10-01-00424, 11-01-00997) and Federal Target Grant for 2009-2013 (contract No. 02.740.11.0429).

In this paper we study lower bounds on the number of bent functions that can be obtained by iterative constructions, namely by the construction proposed by A. Canteaut and P. Charpin [2]. Bent functions obtained via this construction we call *bent iterative functions*. The number of such functions is expressed in terms of sizes of special finite sets. Then it is shown that evaluation of the number of bent iterative functions is closely connected to the problem of decomposing Boolean function into sum of two bent functions. A new lower bound for the number of bent iterative functions that is supposed to be asymptotically tight is given. The numbers of bent iterative functions in 4, 6 and 8 variables are determined. For the last case probabilistic approaches such as Monte–Carlo methods are applied. Based on the performed calculations we formulate several hypotheses on the asymptotic value of the number of all bent iterative functions and on the number of all bent functions.

The structure of the paper is the following. In section 2 we give some preliminaries: necessary definitions (subsection 2.1), a brief overview of the known iterative constructions for bent functions (subsection 2.2), a simplified variant of A. Canteaut's and P. Charpin's iterative construction (subsection 2.3). In section 3 the number of bent iterative functions is expressed in terms of sizes of finite sets. In section 4 bent sum decomposition problem and its connection to the evaluation of the number of bent iterative functions is considered. In section 5 applying probabilistic methods we study bent iterative functions in small number of variables. In section 6 several hypotheses on the number of bent functions are introduced.

2. Preliminaries

2.1. Necessary definitions. Let $+$ mean sum modulo 2. Denote by $\langle x, y\rangle$ the standard inner product of two binary vectors x and y of length n,

$$\langle x, y\rangle = x_1 y_1 + \ldots + x_n y_n.$$

It is well known that a Boolean function f in n variables can be uniquely represented by its *algebraic normal form* (briefly *ANF*)

$$f(x) = \left(\sum_{k=1}^{n} \sum_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k}\, x_{i_1} \cdot \ldots \cdot x_{i_k} \right) + a_0,$$

where for each k indices $i_1, \ldots, i_k$ are pairwise distinct and all together run trough all k-element subsets of the set $\{1, \ldots, n\}$. The coefficients $a_{i_1,\ldots,i_k}$, a_0 belong to $\mathbb{Z}_2$. *Algebraic degree* (briefly *degree*) of a Boolean function f is the number of variables in the longest item of its ANF. Denote it by $deg(f)$. An *affine function* is a function of degree 1. It has the form $f(x) = \langle x, y\rangle + a$ for some vector y and constant a.

Recall that *Walsh–Hadamard transform* of a Boolean function f in n variables is the integer-valued function

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x,y\rangle + f(x)}.$$

A Boolean function f in n variables (n is even) is called *bent* if $W_f(y) = \pm 2^{n/2}$ for all y. In other words bent function is on the maximal possible Hamming distance from the class of all affine Boolean functions in n variables. The set of all bent functions in n variables denote by $\mathcal{B}_n$.

For a bent function f it is possible to define the *dual function* $\widetilde{f}$. It is a Boolean function in n variables given by $2^{n/2}(-1)^{\widetilde{f}(y)} = W_f(y)$. It is well known that $\widetilde{f}$ is a bent function too and $\widetilde{\widetilde{f}} = f$.

2.2. Iterative constructions and lower bounds. Iterative constructions for bent functions have been investigated by many authors. Let us recall only some of them.

The first iterative construction was given by O. Rothaus [11, 12]. It tells that a Boolean function $f(x', x'') = g(x') + h(x'')$ is bent if and only if functions g and h are bent. From here one can get a bound $|\mathcal{B}_n| \geq \max_{m+k=n} |\mathcal{B}_m||\mathcal{B}_k|$, where $|M|$ means the size of a set M.

The next construction was obtained by O. Rothaus [11] and J. Dillon [7]. Let f', f'' and f''' be bent functions in n variables such that their sum is bent again. Then $g(a_1, a_2, x) = f'(x)f''(x) + f'(x)f'''(x) + f''(x)f'''(x) + a_1 f'(x) + a_1 f''(x) + a_2 f'(x) + a_2 f'''(x) + a_1 a_2$ is a bent function in $n+2$ variables. But to obtain the lower bound on $|\mathcal{B}_n|$ from this construction seems to be rather difficult. In general, it is not clear when for distinct collections $\{f'_1, f''_1, f'''_1\}$ and $\{f'_2, f''_2, f'''_2\}$ one can obtain distinct bent functions g.

Another construction was introduced by C. Carlet [4]. Suppose that f', f'' and f''' are bent functions in n variables such that their sum (denote it by s) is bent. Moreover, let $\widetilde{s} = \widetilde{f'} + \widetilde{f''} + \widetilde{f'''}$. Then function $g(x) = f'(x)f''(x) + f'(x)f'''(x) + f''(x)f'''(x)$ is bent in n variables. In this case one can try to find an equality containing $|\mathcal{B}_n|$ and a certain function of $|\mathcal{B}_n|^3$. But we guess that checking conditions (when s is bent and when it holds $\widetilde{s} = \widetilde{f'} + \widetilde{f''} + \widetilde{f'''}$) is difficult enough.

J.-J. Climent, F. García and V. Requena [6] suggested the construction of bent functions in $n+2$ variables from bent functions in n variables using minterms. Here we are not going to consider details of this construction. Let us give only the lower bound on the number of bent functions obtained via this construction. As usual this bound can be taken as the lower bound for the number of all bent functions: $|\mathcal{B}_{n+2}| \geq 6|\mathcal{B}_n|^2 - 8|\mathcal{B}_n|$.

An extensive study of the restrictions of bent functions to affine subspaces was proposed by A. Canteaut and P. Charpin [2]. In particular, they have established that restrictions of a bent function f to a subspace V of codimension 2 and to its cosets are bent if and only if the derivative of $\widetilde{f}$ with respect to $V^\perp$ is constant equal to 1. This last result can be interpreted as an iterative construction for bent functions. It is studied in the next section with respect to the lower bound on the number of all bent functions.

2.3. Bent Iterative functions. Let us present the iterative construction of A. Canteaut and P. Charpin [2] in the following simplified form and equip it with a new proof.

Let Boolean function g in $n+2$ variables be defined as

$$g(00, x) = f_0(x),\ g(01, x) = f_1(x),\ g(10, x) = f_2(x),\ g(11, x) = f_3(x), \tag{1}$$

here f_0, f_1, f_2 and f_3 are Boolean functions in n variables. Note that for distinct ordered collections $\{f_0, f_1, f_2, f_3\}$ we always obtain distinct functions g. From [2] it follows

Theorem 1. *Let functions f_0, f_1, f_2 be bent functions in n variables. Then function g defined by (1) is a bent function in $n+2$ variables if and only if f_3 is a bent function in n variables and $\widetilde{f_0} + \widetilde{f_1} + \widetilde{f_2} + \widetilde{f_3} = 1$.*

Proof. ($\Longleftarrow$) Let f_0, f_1, f_2 and f_3 be bent functions and $\widetilde{f_0} + \widetilde{f_1} + \widetilde{f_2} + \widetilde{f_3} = 1$ hold. Show that g is bent. We have

$$W_g(a_1, a_2, x) = W_{f_0}(x) + (-1)^{a_2} W_{f_1}(x) + (-1)^{a_1} W_{f_2}(x) + (-1)^{a_1+a_2} W_{f_3}(x).$$

Using dual functions we obtain

$$W_g(a_1, a_2, x) = 2^{n/2} \Big((-1)^{\widetilde{f_0}(x)} + (-1)^{a_2+\widetilde{f_1}(x)} + (-1)^{a_1+\widetilde{f_2}(x)} + (-1)^{a_1+a_2+1+\widetilde{f_0}(x)+\widetilde{f_1}(x)+\widetilde{f_2}(x)} \Big).$$

The possible values for the expression between parentheses are ± 4, ± 2 and 0. In fact this expression is always equal to ± 2. Indeed, in the case $\widetilde{f_0}(x) = \widetilde{f_1}(x) = \widetilde{f_2}(x) = 0$ we obtain the expression

$$R(a_1, a_2) = 1 + (-1)^{a_2} + (-1)^{a_1} + (-1)^{a_1+a_2+1}$$

that for any a_1, a_2 equals ± 2. It is easy to prove that in all other (seven) cases for $\widetilde{f_0}(x)$, $\widetilde{f_1}(x)$, $\widetilde{f_2}(x)$ the expression between parentheses differs from $R(a_1, a_2)$ only by changing the signs for even number of items. And hence it can be equal to ± 2 or $\pm 2 \pm 4$ only. Since it is not more than 4, only one possible value ± 2 remains. Thus, for any a_1, a_2, x it is true $W_g(a_1, a_2, x) = \pm 2^{(n+2)/2}$, and therefore g is a bent function.

($\Longrightarrow$) Let g be a bent function. Then its Walsh–Hadamard coefficient

$$W_g(a_1, a_2, x) = 2^{n/2} \Big((-1)^{\widetilde{f_0}(x)} + (-1)^{a_2+\widetilde{f_1}(x)} + (-1)^{a_1+\widetilde{f_2}(x)} + (-1)^{a_1+a_2} \frac{W_{f_3}(x)}{2^{n/2}} \Big)$$

is equal to $\pm 2^{(n+2)/2}$ for all a_1, a_2, x. It is obvious that the expression between parentheses should be equal to ± 2. The necessary condition for it is that the fourth item between parentheses has to be a natural number. But according to the Parseval's equality for W_{f_3} it is true if and only if $W_{f_3}(x) = \pm 2^{n/2}$ for all x, i. e. f_3 is a bent function. Thus, the fourth item has the form $(-1)^{x_1+x_2+\widetilde{f_3}(x)}$.

It is easy to see now that the value $\widetilde{f_3}(x)$ has to be defined by the values $\widetilde{f_0}(x)$, $\widetilde{f_1}(x)$ and $\widetilde{f_2}(x)$ in the unique way. It is true since the sum in parentheses is equal to ± 2. It remains to note that we have already found this appropriate way for $\widetilde{f_3}(x)$ to be defined. Namely, $\widetilde{f_3} = \widetilde{f_0} + \widetilde{f_1} + \widetilde{f_2} + 1$. □

Let us give some concrete examples. Here Boolean functions are presented by their vector of values.

- bent iterative function g = (0001 0001 0001 1110) is obtained by taking $f_0 = f_1 = f_2 = (0001)$. Note that $\widetilde{f_0} = f_0$. Function f_3 can be found from the equality $\widetilde{f_3} = \widetilde{f_0} + \widetilde{f_1} + \widetilde{f_2} + 1 = (1110)$. Note also that here $\widetilde{f_3} = f_3$.
- bent iterative function g = (0001 0010 0001 1101) is constructed by taking $f_0 = (0001)$, $f_1 = (0010)$, $f_2 = (0001)$. Note that again $\widetilde{f_0} = f_0 = f_2$, but $\widetilde{f_1} = (0100)$. The function f_3 is derived from $\widetilde{f_3} = \widetilde{f_0} + \widetilde{f_1} + \widetilde{f_2} + 1 = (1011)$. Then $f_3 = (1101)$.

• bent iterative function $g = (0010\ 0001\ 0001\ 1101)$ is constructed by taking $f_0 = (0010)$, $f_1 = (0001)$, $f_2 = (0001)$. Here $\widetilde{f_0} = (0100)$, $\widetilde{f_1} = f_1 = f_2$. The function f_3 is obtained from $\widetilde{f_3} = \widetilde{f_0} + \widetilde{f_1} + \widetilde{f_2} + 1 = (1011)$. Then $f_3 = (1101)$.

Note that three distinct bent functions in n variables can produce up to 6 distinct bent functions in $n+2$ variables, since it is possible to order them in 3! ways.

Bent functions that can be obtained by Theorem 1 we call *bent iterative functions*. Let $\mathcal{BI}_{n+2}$ (it means "Bent Iterative") denote the class of all such functions in $n+2$ variables.

Note that according to [2] there exist bent functions from Maiorana–McFarland class [10] and from the class $\mathcal{PS}$ (Partial Spreads) [7] that can not be represented as bent iterative functions. Also as it follows from investigation [3] of nonnormal functions there exist bent functions in $\mathcal{BI}_n$ that are nonequivalent to Maiorana–McFarland bent functions.

3. The number of bent iterative functions

Here it is shown how it is possible to calculate the number of bent iterative functions. This task is reformulated in terms of finite sets and then several open problems are given.

Theorem 2. *For any even $n \geq 4$*

$$|\mathcal{BI}_n| = \sum_{f' \in \mathcal{B}_{n-2}} \sum_{f'' \in \mathcal{B}_{n-2}} |\,(\mathcal{B}_{n-2} + f') \cap (\mathcal{B}_{n-2} + f'')\,|.$$

Proof. Let us study in how many ways one can construct a bent iterative function g in n variables. It is possible to do it as follows. First, take arbitrary ordered pair of two bent functions f_0, f_1 in $n-2$ variables. These functions may coincide or may not. The number of all distinct such pairs is $|\mathcal{B}_{n-2}|^2$. Then take a suitable bent function f_2 in $n-2$ variables. Bent function f_2 we call *suitable* for f_0, f_1 if function $\widetilde{f_0} + \widetilde{f_1} + \widetilde{f_2}$ is bent. It is clear that according to Theorem 1 for any suitable bent function f_2 one can construct a bent iterative function g by determining f_3 from the equality $\widetilde{f_3} = \widetilde{f_0} + \widetilde{f_1} + \widetilde{f_2} + 1$. So, if $k(f_0, f_1)$ is the number of suitable bent functions f_2 for given bent functions f_0, f_1, then

$$|\mathcal{BI}_n| = \sum_{f_0 \in \mathcal{B}_{n-2}} \sum_{f_1 \in \mathcal{B}_{n-2}} k(f_0, f_1). \tag{2}$$

Indeed, any bent iterative function g can be obtained in the way presented. Note that g is uniquely determined by the ordered triple f_0, f_1, f_2.

Now let us study numbers $k(f_0, f_1)$. Let $\mathcal{B}(f_0, f_1)$ be the set of all suitable bent functions in $n-2$ variables for f_0, f_1. So, $|\mathcal{B}(f_0, f_1)| = k(f_0, f_1)$. Show that the set $\mathcal{B}(f_0, f_1)$ is in 1–to–1 correspondence with $(\mathcal{B}_{n-2} + \widetilde{f_0}) \cap (\mathcal{B}_{n-2} + \widetilde{f_1})$.

Define a map

$$\phi : \mathcal{B}(f_0, f_1) \to (\mathcal{B}_{n-2} + \widetilde{f_0}) \cap (\mathcal{B}_{n-2} + \widetilde{f_1})$$

by the rule

$$\phi(f_2) = \widetilde{f_0} + \widetilde{f_2}, \text{ for all } f_2 \in \mathcal{B}(f_0, f_1).$$

First check that ϕ is defined correctly. Since f_2 is suitable, there exists a bent function h in $n-2$ variables such that $h = \widetilde{f_0} + \widetilde{f_1} + \widetilde{f_2}$. Then function $s = \widetilde{f_0} + \widetilde{f_2}$ belongs to the set $\mathcal{B}_{n-2} + \widetilde{f_0}$ and also belongs to the set $\mathcal{B}_{n-2} + \widetilde{f_1}$ as far as $s = \widetilde{f_1} + h$. Thus, ϕ is defined correctly.

Prove that ϕ is a bijective mapping. It is easy to see that if $f_2 \neq f_2'$ then $\phi(f_2) \neq \phi(f_2')$. Let s be a function from $(\mathcal{B}_{n-2}+\widetilde{f}_0)\cap(\mathcal{B}_{n-2}+\widetilde{f}_1)$. Then bent function f_2 defined by $\widetilde{f}_2 = s + \widetilde{f}_0$ is suitable for f_0, f_1 (since function $\widetilde{f}_0 + \widetilde{f}_1 + \widetilde{f}_2 = \widetilde{f}_1 + s$ is bent) and it holds $\phi(f_2) = s$. Thus, ϕ is bijective.

So, it is proven that

$$k(f_0, f_1) = |\ (\mathcal{B}_{n-2} + \widetilde{f}_0) \cap (\mathcal{B}_{n-2} + \widetilde{f}_1)\ |.$$

Now replace $k(f_0, f_1)$ by this expression in formula (2) and change variables f_0, f_1 to variables $f' = \widetilde{f}_0$, $f'' = \widetilde{f}_1$. In such a way we get the statement of theorem. □

Consider an example. Let us construct all bent iterative functions for $n = 4$. The total number of them is $|\mathcal{BI}_4| = \sum\limits_{f'\in\mathcal{B}_2}\sum\limits_{f''\in\mathcal{B}_2} |\ (\mathcal{B}_2 + f') \cap (\mathcal{B}_2 + f'')\ |$. Recall that $\mathcal{B}_2$ consists of all functions with odd number of nonzero values, $|\mathcal{B}_2| = 8$. Let us present their vectors of values: (0001), (0010), (0100), (1000), (1110), (1101), (1011), (0111). Note that any set $\mathcal{B}_2 + f'$ is the set of all Boolean functions with even number of ones. So, $|\ (\mathcal{B}_2 + f') \cap (\mathcal{B}_2 + f'')\ | = 8$ for any bent functions f', f''. It means that any bent function in 2 variables is suitable for all fixed bent functions f_0, f_1. Then by Theorem 2 we get $|\mathcal{BI}_4| = 8 \cdot 8 \cdot 8 = 512$. Recall that $\mathcal{B}_4$ consists of 896 functions.

It is known that if function f' is bent then function $f' + \ell$ is bent too for every affine Boolean function ℓ. That is why any set $(\mathcal{B}_{n-2} + f') \cap (\mathcal{B}_{n-2} + f'')$ contains at least all affine functions in $n - 2$ variables:

$$\ell = (f' + \ell) + f' = (f'' + \ell) + f''.$$

The number of these affine functions is 2^{n-1} and hence we get

Proposition 1. *For any bent functions f', f'' in $n - 2$ variables*

$$2^{n-1} \leq |\ (\mathcal{B}_{n-2} + f') \cap (\mathcal{B}_{n-2} + f'')\ | \leq |\mathcal{B}_{n-2}|. \tag{3}$$

In [13] it is proven

Proposition 2. *For bent functions f', f'' in $n - 2$ variables the equality*

$$|\ (\mathcal{B}_{n-2} + f') \cap (\mathcal{B}_{n-2} + f'')\ | = |\mathcal{B}_{n-2}|$$

holds if and only if $f' + f''$ is an affine function.

From Theorem 2 and Propositions 1, 2 it follows

Corollary 1. $2^{n-1}|\mathcal{B}_{n-2}|^2 < |\mathcal{BI}_n| < |\mathcal{B}_{n-2}|^3$ *for any even $n \geq 4$.*

Indeed, it is enough to note that there exist bent functions f', f'' for which upper bound in (3) holds. And there exist f', f'' for which it does not hold.

Corollary 2. $|\mathcal{BI}_n| > 2^{2^{(n/2)+2}-n-3}$ *for any even $n \geq 4$.*

Proof. From Corollary 1 it follows $|\mathcal{BI}_n| > 2^{n-1}|\mathcal{B}_{n-2}|^2$. Since $\mathcal{BI}_{n-2}$ is a subset of $\mathcal{B}_{n-2}$, we have $|\mathcal{B}_{n-2}| > |\mathcal{BI}_{n-2}|$ and hence

$$|\mathcal{BI}_n| > 2^{n-1}|\mathcal{BI}_{n-2}|^2.$$

Applying Corollary 1 and inequality $|\mathcal{B}_{n-4}| > |\mathcal{BI}_{n-4}|$, we obtain

$$|\mathcal{BI}_n| > 2^{n-1} \cdot 2^{(n-3)\cdot 2} \cdot |\mathcal{BI}_{n-4}|^{2^2}.$$

Continue in this way,

$$|\mathcal{BI}_n| > 2^{n-1} \cdot 2^{(n-3)\cdot 2} \cdot 2^{(n-5)\cdot 2^2} \cdot \ldots \cdot 2^{3\cdot 2^{(n/2)-2}} |\mathcal{B}_2|^{2^{(n/2)-1}}.$$

Then by substitution $|\mathcal{B}_2| = 2^3$ we obtain

$$|\mathcal{BI}_n| > 2^{3\cdot 2^{(n/2)-1}} \cdot 2^d,$$

where

$$d = (n-1) + (n-3)\cdot 2 + (n-5)\cdot 2^2 + \ldots + (n-(n-3))\cdot 2^{(n/2)-2}.$$

One can see that

$$d = n\left(\sum_{i=0}^{(n/2)-2} 2^i\right) - \sum_{i=0}^{(n/2)-2} (2i+1)2^i = (n-1)(2^{(n/2)-1}-1) - 2\sum_{i=0}^{(n/2)-2} i\cdot 2^i.$$

Using combinatorial formula

$$\sum_{i=0}^{k} i\cdot 2^i = (k-1)2^{k+1} + 2,$$

we get $d = 5\cdot 2^{(n/2)-1} - n - 3$. And hence, $|\mathcal{BI}_n| > 2^{2^{(n/2)+2}-n-3}$. □

It is interesting to find better bounds on $|\mathcal{BI}_n|$ and clarify is this number more close to $|\mathcal{B}_{n-2}|^2$ or rather to $|\mathcal{B}_{n-2}|^3$. Note that answer to this question has direct applications to the problem of lower bound for $|\mathcal{B}_n|$.

In the next section several techniques helpful to this question are presented.

4. Bent sum decomposition problem

Define the following set

$$X_n = \{\ f + h\ :\ f, h \in \mathcal{B}_n\ \}$$

and consider the system $\{C_f : f \in \mathcal{B}_n\}$ of its subsets defined as $C_f = \mathcal{B}_n + f$. So,

$$X_n = \bigcup_{f\in\mathcal{B}_n} C_f.$$

One can prove

Proposition 3. *$|\mathcal{B}_n| > \sqrt{2|X_n|}$ for any even $n \geq 2$.*

Let ψ be an element of X_n. The number of subsets C_f that cover ψ we call *multiplicity* of ψ and denote it by $m(\psi)$. Note that if ψ is covered by C_f then it is covered by any set $C_{f'}$, where f' is obtained from f by adding an affine function.

It is clear that

$$\sum_{\psi\in X_n} m(\psi) = |\mathcal{B}_n|^2. \tag{4}$$

Theorem 3. *For any even $n \geq 2$*

$$|\mathcal{BI}_{n+2}| = \sum_{\psi\in X_n} m(\psi)^2.$$

Proof. The statement follows from Theorem 2. Indeed, let us fix any function ψ from X_n. It is covered exactly by $m(\psi)$ sets, say $C_{f^1}, C_{f^2}, \ldots, C_{f^{m(\psi)}}$. Now let pair (f', f'') run trough all the ordered pairs of bent functions in n variables. Then function ψ is covered by set $(\mathcal{B}_n + f') \cap (\mathcal{B}_n + f'')$ if and only if both functions f', f'' belong to the set $\{f^1, f^2, \ldots, f^{m(\psi)}\}$. The number of such ordered pairs is $m(\psi)^2$.

Thus, by Theorem 2 we get the formula $|\mathcal{BI}_{n+2}| = \sum_{\psi \in X_n} m(\psi)^2$. □

So, in order to evaluate $|\mathcal{BI}_{n+2}|$ (and then $|\mathcal{B}_{n+2}|$) we have to study the set X_n and the distribution of multiplicities for its elements.

Theorem 4. *For any even $n \geq 2$*

$$|\mathcal{B}_{n+2}| \geq |\mathcal{BI}_{n+2}| \geq \frac{|\mathcal{B}_n|^4}{|X_n|}.$$

Proof. By (4) we have

$$\sum_{\psi \in X_n} m(\psi) = |\mathcal{B}_n|^2.$$

Note that the minimal value of the sum

$$\sum_{\psi \in X_n} m(\psi)^2$$

is reachable if and only if all the multiplicities are the same, i. e. if and only if $m(\psi) = |\mathcal{B}_n|^2/|X_n|$ for all $\psi \in X_n$. Then by Theorem 3 we have

$$|\mathcal{B}_{n+2}| \geq |\mathcal{BI}_{n+2}| = \sum_{\psi \in X_n} m(\psi)^2 \geq |X_n| \cdot \left(\frac{|\mathcal{B}_n|^2}{|X_n|}\right)^2 = \frac{|\mathcal{B}_n|^4}{|X_n|}.$$

□

Corollary 3. *The average value of square of multiplicity in X_n is not less than*

$$|\mathcal{B}_n|^4/|X_n|^2.$$

It is well known [12] that for a bent function in n variables, $n \geq 4$, it holds $deg(f) \leq n/2$. Then the set X_n can include only functions of degree less or equal to $n/2$. Therefore, it holds

Corollary 4. *For any even $n \geq 4$*

$$|\mathcal{B}_{n+2}| \geq |\mathcal{BI}_{n+2}| \geq \frac{|\mathcal{B}_n|^4}{2^{1+n+\binom{n}{2}+\ldots+\binom{n}{n/2}}} = \frac{|\mathcal{B}_n|^4}{2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}}.$$

In order to find the exact number of bent iterative functions one has to find the distribution of multiplicities in X_n. Thus, we come to a new problem statement.

Open problem: bent sum decomposition. *What Boolean functions can be represented as the sum of two bent functions in n variables? How many such representations does a Boolean function admit?*

We suppose that the answers to these questions can be given in terms of probability theory. In the next section the case of small number of variables is studied.

5. Monte–Carlo methods for enumeration of bent iterative functions if n is small

Here we study bent sum decomposition problem for small dimensions. Sizes of X_n and $\mathcal{BI}_{n+2}$ are determined for $n = 2, 4, 6$. In the last case probabilistic methods are applied.

For $n = 2$ the set X_2 consists of all Boolean functions with even number of nonzero values, $|X_2| = 8$. Multiplicities of all functions from X_2 are maximal and equal to 8. Thus, by Theorem 3 we have $|\mathcal{BI}_4| = 8 \cdot 8^2 = 512$. Recall that $\mathcal{B}_4$ consists of 896 functions.

For $n = 4$ the set X_4 consists of all Boolean functions of degree not more than 2, $|X_4| = 2^{11} = 2048$. All affine functions in X_4 (number of them is 2^5) have maximal multiplicities equal to 896. All the others have multiplicities equal to 384. Thus, $|\mathcal{BI}_6| = 32 \cdot 896^2 + 2016 \cdot 384^2 = 77 \cdot 2^{22} = 322\,961\,408 \approx 2^{28,3}$. Note that via Maiorana–McFarland construction [10] (with a fixed division of variables into halves) it is possible to obtain only $2^8(2^3)! = 315 \cdot 2^{15} = 10\,321\,920 \approx 2^{23,3}$ bent functions. It remains to add that total number of bent functions in 6 variables is about $2^{32,3}$, see the survey [15] for detail.

Proposition 4. *$|\mathcal{BI}_4| = 512$, $|\mathcal{BI}_6| = 322\,961\,408 \approx 2^{28,3}$.*

If $n = 6$ the set X_6 again is the set of all Boolean functions of degree less or equal to 3, $|X_6| = 2^{42}$. It is checked via exhaustive search.

Now let us do the following probabilistic investigation. We apply Monte–Carlo methods for enumerating the sum $\sum_{\psi \in X_6} m(\psi)^2$ that is equal to $|\mathcal{BI}_8|$ by Theorem 3. We have taken at random $N = 346\,981 \approx 2^{18,4}$ Boolean functions in 6 variables of degree not more than 3 without linear parts in ANFs (by linear part we mean all ANF items of degree less or equal to 1). While checking multiplicities for these N functions it is obtained that there are only 30 distinct values of them. In Table 1 one can see the distribution of multiplicities for the taken functions. By n_i the number of Boolean functions with multiplicity m_i is denoted.

i	m_i	n_i	i	m_i	n_i	i	m_i	n_i
1	$26880 \cdot 2^7$	102	11	$54784 \cdot 2^7$	67960	21	$82176 \cdot 2^7$	179
2	$33024 \cdot 2^7$	28	12	$56064 \cdot 2^7$	240	22	$83200 \cdot 2^7$	265
3	$36096 \cdot 2^7$	327	13	$56832 \cdot 2^7$	8559	23	$86784 \cdot 2^7$	109
4	$46464 \cdot 2^7$	38946	14	$57088 \cdot 2^7$	2130	24	$91392 \cdot 2^7$	56
5	$46848 \cdot 2^7$	12641	15	$57600 \cdot 2^7$	4	25	$119616 \cdot 2^7$	238
6	$47616 \cdot 2^7$	67687	16	$62208 \cdot 2^7$	596	26	$121600 \cdot 2^7$	42
7	$48896 \cdot 2^7$	6327	17	$63360 \cdot 2^7$	6073	27	$172800 \cdot 2^7$	22
8	$50496 \cdot 2^7$	36417	18	$65088 \cdot 2^7$	11019	28	$237312 \cdot 2^7$	6
9	$51968 \cdot 2^7$	12655	19	$66048 \cdot 2^7$	4272	29	$272640 \cdot 2^7$	15
10	$53952 \cdot 2^7$	67906	20	$80640 \cdot 2^7$	2159	30	$1521408 \cdot 2^7$	1

Table 1. Distribution of multiplicities in a sample of $N = 346\,981$ Boolean functions in 6 variables.

Then count the *sample average value* Q for the square of multiplicity,

$$Q = \left(\sum_{i=1}^{30} n_i \cdot m_i^2 \right) / N = 45\,508\,981\,169\,513,30 \approx 2^{45,37}.$$

Since $|X_6| = 2^{42}$, we obtain the estimation

$$|\mathcal{BI}_8| \approx Q \cdot |X_6| = 200\,150\,615\,856\,476\,000\,000\,000\,000 \approx 2^{87,37}.$$

Now evaluate the mistake of our approximation of $|\mathcal{BI}_8|$. In Monte–Carlo methods one has to choose the *reliability* ν of approximation, $0 < \nu < 1$. The closer to 1 is ν, the higher is reliability. Then the approximate upper bound for the mistake of estimation can be obtained by the known formula

$$\delta = t_\nu S/\sqrt{N}$$

(see for example [8]), where S is the *corrected standard deviation* for our approximation and t_ν is the standard parameter determined by ν. We get the value S by the known formula

$$S = \sqrt{\left(\sum_{i=1}^{30} n_i (m_i^2 - Q)^2\right)/(N-1)}.$$

So, $S = 65\,975\,029\,301\,812,10$. Now let $\nu = 0,999$. The corresponding standard parameter is $t_\nu = 3,291$ (see [8] for detail). Then the approximate upper bound for the mistake is

$$\delta = 368\,599\,402\,514,14.$$

It means that with probability 0.999 the average value of square of multiplicity in the set X_6 is in the interval $(Q - \delta; Q + \delta)$. And hence it is proven

Proposition 5. *With probability* 0.999 *it holds* $2^{87,36} < |\mathcal{BI}_8| < 2^{87,38}$.

Note that according to P. Langevin and G. Leander, see [9], the total number of bent functions in 8 variables is $2^9 \times 193\,887\,869\,660\,028\,067\,003\,488\,010\,240 \simeq 2^{106,29}$. Note also that number of Maiorana–McFarland's bent functions in 8 variables is just about $2^{60,25}$.

We see that Q is close to the lower bound $|B_n|^4/|X_n|^2$ from Corollary 3. For $n = 6$ this lower bound is $44\,793\,743\,175\,843,84 \approx 2^{45,348}$. So, from Theorem 4 it follows

Proposition 6. $|\mathcal{BI}_8| > 197\,004\,891\,331\,091\,000\,000\,000\,000 \approx 2^{87,35}$.

Since $|\mathcal{B}_8| \simeq 2^{106,29}$ [9], by Theorem 4 we have

Proposition 7. $|\mathcal{B}_{10}| > |\mathcal{BI}_{10}| > 830\,602\,255\,559\,379 \cdot 10^{64} > 2^{262,16}$.

Let us summarize in Table 2 what is known now about sizes of $\mathcal{BI}_n$, $\mathcal{B}_n$ and X_n if n is small. We put here also the corresponding values of lower and upper bounds for the number of all bent functions in n variables.

Numbers	$n=2$	$n=4$	$n=6$	$n=8$	$n=10$
Lower bound: $2^{2^{n/2}} \cdot (2^{n/2})!$ (# of McFarland's bent functions)	8	384	$\approx 2^{23,3}$	$\approx 2^{60,25}$	$\approx 2^{149,66}$
Size of $\mathcal{BI}_n$	8	512	$\approx 2^{28,3}$	$\approx 2^{87,37}$	$> 2^{262,16}$
Size of $\mathcal{B}_n$	8	896	$\approx 2^{32,3}$	$\approx 2^{106,29}$	unknown
Upper bound: $2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}$ (# of functions of degree $\le n/2$)	8	2048	2^{42}	2^{163}	2^{638}
Size of X_n	8	2048	2^{42}	unknown	unknown

Table 2. Sizes of $\mathcal{BI}_n$, $\mathcal{B}_n$, X_n for small n and corresponding values of lower and upper bounds for the number of all bent functions in n variables.

6. Problem of asymptotic value of the number of all bent functions. Hypotheses.

One of the main open problem in bent functions is to find the asymptotic value of the number of them. It is very difficult to do any step in this area. Indeed, for $n \geq 10$ the number of bent functions in n variables is unknown. And there is a large gap between lower $2^{2^{(n/2)+\log(n-2)-1}}$ and upper $2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}$ bounds for this number. There are several improvements of these bounds, see [1], [5] and [16], but not too significant with respect to $\log\log|\mathcal{B}_n|$. Here by log we mean $\log_2$. In this section several hypotheses based on the obtained results and performed calculations are formulated.

In the previous section we have seen that for $n = 2, 4, 6$ the set X_n contains all Boolean functions of degree not more than $n/2$. The case $n = 6$ was checked via exhaustive search. We have used processor Intel Core i7 3.0 Ghz 256 Gb. The program has worked 14 days with full loading of RAM. Note that case $n = 8$ is too hard for the exhaustive search now. In this case one has to find bent decompositions for about 2^{163} Boolean functions in 8 variables. Recall that the number of all bent functions in 8 variables has been found only a few years ago [9] and is about $2^{106,29}$. Case $n = 10$ can not be checked even theoretically since the number of bent functions in 10 variables is unknown.

Results on X_2, X_4, X_6 lead us to the following strong hypothesis.

Hypothesis 1. *Any Boolean function in n variables of degree not more than $n/2$ can be represented as the sum of two bent functions in n variables (n is even, $n \geq 2$).*

So, we suppose that X_n is as large as possible, i. e. $|X_n| = 2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}$. In other words we conjecture that for any Boolean function f in n variables there exists a bent function g in n variables such that $f + g$ is bent. Note that this hypothesis has a similarity to the previously obtained fact, see [13]: for any non affine Boolean function f in n variables there exists a bent function g in n variables such that $f+g$ is not bent.

If Hypothesis 1 is right then by Proposition 3 one can prove

Hypothesis 2. *For the number of bent functions in n variables it is true*

$$2^{2^{n-2}+\frac{1}{4}\binom{n}{n/2}} \leq |\mathcal{B}_n| \leq 2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}.$$

Thus, we suppose that the number of all bent functions is very close to the existing upper bound.

Hypothesis 3. *The number of all bent functions in n variables (n is even, $n \geq 2$) is asymptotically equal to $2^{2^{n-c}+d\binom{n}{n/2}}$, where c, d are constants and $1 \leq c \leq 2$.*

If Hypothesis 1 is right then using Theorem 4 one can prove

Hypothesis 4. *The class $\mathcal{BI}_n$ is the* basic class *in $\mathcal{B}_n$, i. e.*

$$\lim_{n\to\infty} \frac{\log\log|\mathcal{BI}_n|}{\log\log|\mathcal{B}_n|} = 1.$$

In Table 3 one can see these relations for small n.

Numbers	$n=2$	$n=4$	$n=6$	$n=8$
$a=\log\log\lvert\mathcal{BI}_n\rvert$	≈ 1.584962501	≈ 3.169925001	≈ 4.821035977	≈ 6.449066085
$b=\log\log\lvert\mathcal{B}_n\rvert$	≈ 1.584962501	≈ 3.293864089	≈ 5.015117973	≈ 6.731862061
a/b	1	0.962372738	0.961300612	0.957991419

Table 3. Relations between $\log\log|\mathcal{BI}_n|$ and $\log\log|\mathcal{B}_n|$ if n is small.

If n is small the dynamics of the corresponding relations is not still impressive. But it can be explained by an *effect of small values*.

We have seen in Propositions 5, 6 that lower bound for $|\mathcal{BI}_n|$ from Theorem 4 is very close to the tight value if n is small. We do the following assumption.

Hypothesis 5. *The bound of Theorem 4 is asymptotically tight, i. e.*

$$\lim_{n\to\infty}\frac{\log\log(|\mathcal{B}_{n-2}|^4/|X_{n-2}|)}{\log\log|\mathcal{BI}_n|}=1.$$

In order to confirm this hypothesis one can see the values $\log\log(|\mathcal{B}_{n-2}|^4/|X_{n-2}|)$ and $\log\log|\mathcal{BI}_n|$ for small n in Table 4. They are indeed very close to each other.

Numbers	$n=4$	$n=6$	$n=8$
$a=\log\log(\lvert\mathcal{B}_{n-2}\rvert^4/\lvert X_{n-2}\rvert)$	≈ 3.169925001	≈ 4.819127567	≈ 6.448708743
$b=\log\log\lvert\mathcal{BI}_n\rvert$	≈ 3.169925001	≈ 4.822730148	≈ 6.449066085
a/b	1	0.999604149	0.99994459

Table 4. Relations between $\log\log(|\mathcal{B}_{n-2}|^4/|X_{n-2}|)$ and $\log\log|\mathcal{BI}_n|$ if n is small.

7. Conclusion

In this paper a simplified variant of the A. Canteaut's and P. Charpin's construction was presented (Theorem 1). The number of bent iterative functions is expressed in terms of sizes of finite sets (Theorem 2) and it is shown how evaluation of it is connected to the bent sum decomposition problem (Theorem 3). A new lower bound for the number of bent iterative functions is given (Theorem 4). Obtained results lead us to a new vision of the enumeration problem for bent functions. Hypotheses 1, 4 and 5 give the following directions in the future studying of the problem. First, to study the size of X_n. If it is big enough it is possible to get a good lower bound for the number of bent functions. Second, to study distributions of multiplicities in X_n in order to find the number of bent iterative functions. This number by Hypothesis 5 is asymptotically equal to the number of all bent functions. It is interesting also to study several weakened variants of the given hypotheses.

References

[1] S. V. Agievich, *On the representation of bent functions by bent rectangles*, in "Proc. of the Int. Petrozavodsk Conf. on Probabilistic Methods in Discrete Mathematics," (2000), 121–135; preprint, arXiv:math/0502087v1

[2] A. Canteaut and P. Charpin, *Decomposing bent functions*, IEEE Trans. Inform. Theory, **49** (2003), 2004–2019.

[3] A. Canteaut, M. Daum, H. Dobbertin and G. Leander, *Finding nonnormal bent functions*, Discrete Appl. Math., **154** (2006), 202–218.

[4] C. Carlet, *On bent and highly nonlinear balanced/resilient functions and their algebraic immunities*, in "Applied Algebra, Algebraic Algorithms and Error Correcting Codes," Las Vegas, USA, (2006), 1–28.

[5] C. Carlet and A. Klapper, *Upper bounds on the numbers of resilient functions and of bent functions*, in "Proc. of 23rd Symposium on Information Theory," (2002), 307–314.
[6] J.-J. Climent, F. García and V. Requena, *On the construction of bent functions of $n + 2$ variables from bent functions of n variables*, Adv. Math. Commun., **2** (2008), 421–431.
[7] J. F. Dillon, "Elementary Hadamard Difference Sets," Ph.D Thesis, University of Maryland, 1974.
[8] V. E. Gmurman, "Probability Theory and Mathematical Statistics," Higher Educ., Moscow, 2006.
[9] P. Langevin, G. Leander *Counting all bent functions in dimension eight 99270589265934370305785861242880*, Des. Codes Crypt., **59** (2011), 193–205.
[10] R. L. McFarland, *A family of difference sets in non-cyclic groups*, J. Combin. Theory Ser. A, **15** (1973), 1–10.
[11] O. Rothaus, *On bent functions*, IDA CRD W. P. No. 169, 1966.
[12] O. Rothaus, *On bent functions*, J. Combin. Theory Ser. A, **20** (1976), 300–305.
[13] N. N. Tokareva, *Automorphism group of the set of all bent functions*, Discrete Math. Appl., **20** (2010), 655–664.
[14] N. N. Tokareva, *Generalizations of bent functions. A survey*, Discrete Anal. Oper. Res., **17** (2010), 34–64.
[15] N. Tokareva, "Nonlinear Boolean Functions: Bent Functions and Their Generalizations," LAP LAMBERT Academic Publishing, Saarbrucken, Germany, 2011.
[16] L. Wang and J. Zhang, *A best possible computable upper bound on bent functions*, J. West China, **33** (2004), 113–115.

Received July 2010; revised August 2011.

E-mail address: tokareva@math.nsc.ru