Noname manuscript No.
(will be inserted by the editor)

Algebraic normal form of a bent function: properties and restrictions

Natalia Tokareva
tokareva@math.nsc.ru

the date of receipt and acceptance should be inserted later

Abstract Maximally nonlinear Boolean functions in n variables, where n is even, are called bent functions. There are several ways to represent Boolean functions. One of the most useful is via algebraic normal form (ANF). What can we say about ANF of a bent function? We try to collect all known and new facts related to ANF of a bent function. A new problem in bent functions is stated and studied: is it true that a linear, quadratic, cubic, etc. part of ANF of a bent function can be arbitrary? The case of linear part is well studied before. In this paper we prove that a quadratic part of a bent function can be arbitrary too.

Keywords: Boolean function, bent function, linear function, quadratic function, homogeneous function.

1 Introduction

Recall that Boolean functions in even number of variables that are on the maximal possible Hamming distance from the set of all affine Boolean functions are called bent functions. Bent functions play an important role in constructions of symmetric ciphers since they help to defend ciphers against linear cryptanalysis. It is well known that every Boolean function can be in the unique way represented in its Algebraic Normal Form (ANF). This representation is used very often for property description and realization of a Boolean function. It is known that bent functions are far from classification. And no conditions on ANF of a Boolean function are known in order to say that it is bent.

In this paper we collect all known and new facts related to ANF of a bent function answering the question — which it can be? We deal with algebraic degrees of bent functions from different classes, classifications of ANFs for small number of variables, consider homogeneous, symmetric and rotation symmetric ANFs of bent functions. A new problem in bent functions is stated and studied: is it true that an arbitrary homogeneous Boolean function of degree k in n variables (n is even) is a k-degree part in ANF of some bent function in n variables? For small

Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk, Russia

k it can be formulated like this. Is it true that linear (quadratic, cubic, etc.) part of ANF of a bent function can be arbitrary? For sure, this question is interesting nor only for bent functions.

It is well known that a linear part in ANF of a bent function can be arbitrary. Moreover, any linear function can be added to a bent function without changing its property to be bent. In this paper we prove that a quadratic part of a bent function can also be arbitrary. Namely, we prove that an arbitrary quadratic homogeneous Boolean function in n variables is a quadratic part of some bent function in n variables, where n is even, $n \geqslant 6$. Several ideas for the general case of the problem are discussed.

2 Definitions

We use the following standard notation.

$\mathbb{F}_2^n$ — the vector space over $\mathbb{F}_2$;

$f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ — Boolean functions;

$dist(f, g)$ — *Hamming distance* between f and g, i. e. the number of coordinates in which their vectors of values differ;

$x = (x_1, \ldots, x_n)$ — a binary vector;

$\oplus$ — addition modulo 2 (XOR);

$\langle x, y\rangle = x_1 y_1 \oplus \ldots \oplus x_n y_n$ — the standard inner product modulo 2;

$W_f(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x,y\rangle \oplus f(x)}$ — the *Walsh — Hadamard transform* of a Boolean function f;

$\langle a, x\rangle \oplus b$ — an *affine function* in variables $x_1, \ldots, x_n$;

bent function — a Boolean function in n variables (n is even) that is on the maximal possible distance from the set of all affine functions. This distance is equal to $2^{n-1} - 2^{(n/2)-1}$.

$\mathcal{A}_n$ — the set of all affine functions in n variables;

$\mathcal{B}_n$ — the set of all bent functions in n variables.

Any Boolean function can be uniquely represented in its *algebraic normal form* (ANF):

$$f(x_1, \ldots, x_n) = \left(\bigoplus_{k=1}^{n} \bigoplus_{i_1, \ldots, i_k} a_{i_1, \ldots, i_k} \, x_{i_1} \cdot \ldots \cdot x_{i_k} \right) \oplus a_0,$$

where for each k indices $i_1, \ldots, i_k$ are pairwise distinct and sets $\{i_1, \ldots, i_k\}$ are exactly all different nonempty subsets of the set $\{1, \ldots, n\}$; coefficients $a_{i_1, \ldots, i_k}$, a_0 take values from $\mathbb{F}_2$. In Russian mathematical literature it is usually called a *Zhegalkin polynomial* in honor of Ivan Zhegalkin (1869–1947), a mathematician who introduced this representation in 1927.

For a Boolean function f the number of variables in the longest item of its ANF is called the *algebraic degree* of a function (or briefly *degree*) and is denoted by $deg(f)$. A Boolean function is *affine*, *quadratic*, *cubic* and so on if its degree is not more than 1, or equal to 2, 3, etc.

3 Degree of a bent function

In what follows let n be an even number. According to O.Rothaus (1966, 1976) [21] and V. A. Eliseev, O. P. Stepchenkov (1962) [31] it holds

Theorem 1 *Degree $deg(f)$ of a bent function f in $n \geqslant 4$ variables is not more than $n/2$. If $n = 2$ a bent function is quadratic.*

One can find a proof of this fact in the book [5] of T. W. Cusick and P. Stanica.

Obviously, a Boolean function of degree less or equal to one can not be bent. It is easy to see that there exist bent functions of all other possible degrees from 2 to $n/2$ if $n \geqslant 4$ (just use the Maiorana — McFarland construction for this, see [15]). E. g. the quadratic Boolean function $f(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{n-1}x_n$ is bent for any even n.

There are many generalizations of bent functions. One very natural of them is a generalization over finite fields, namely over prime fields. In 1985, P. V. Kumar, R. A. Scholtz, and L. R. Welch proposed [11] this generalization, aiming to construct q-valued bent sequences applicable in CDMA systems.

Take integer $q \geqslant 2$, the imaginary unit $i = \sqrt{-1}$, and a primitive complex root of unity $\omega = e^{2\pi i/q}$ of degree q. Consider a q-valued function $f : \mathbb{F}_q^n \to \mathbb{F}_q$. The *Walsh — Hadamard transform* of a function f is the complex function

$$W_f(y) = \sum_{x \in \mathbb{F}_q^n} \omega^{\langle x,y \rangle + f(x)} \quad \text{for every} \quad y \in \mathbb{F}_q^n, \tag{1}$$

where the inner product and addition + are taken modulo q. Denote the absolute value of a complex number c by $|c|$. Given positive integer q, a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is called a *q-valued bent function* if $|W_f(y)| = q^{n/2}$ for every $y \in \mathbb{F}_q^n$. If $q = p$, where p is a prime number, such a function is usually called *p-ary bent function*.

In 2004 X. D. Hou [10] determined the bound for p-ary bent functions.

Theorem 2 *If f is a p-ary bent function (p is prime) in n variables,*

$$deg(f) \leqslant \frac{(p-1)n}{2} + 1.$$

If f is weakly regular, then

$$deg(f) \leqslant \frac{(p-1)n}{2}.$$

Recall that for a bent function f the *dual function* $\widetilde{f}$ in n variables is defined by the equality $W_f(y) = 2^{n/2}(-1)^{\widetilde{f}(y)}$. This definition is correct since $W_f(y) = \pm 2^{n/2}$ for any vector y. Recall that $\widetilde{f}$ is bent too. It holds $\widetilde{\widetilde{f}} = f$.

Note that if $deg(f) = n/2$ then $deg(\widetilde{f}) = n/2$. In general, the following fact is well known, see for instance chapter [1] of C. Carlet.

Theorem 3 *Let f be an arbitrary bent function in n variables. Then*

$$n/2 - deg(f) \geqslant \frac{n/2 - deg(\widetilde{f})}{deg(\widetilde{f}) - 1}.$$

4 All variables take part in ANF of a bent function

A Boolean function f in n variables *has a degenerate (fictitious) variable* x_i if for any vector $b \in \mathbb{F}_2^n$ it holds $f(b) = f(b \oplus e_i)$, where e_i is a vector of weight 1 with i-th coordinate being nonzero. In other words, a variable is *fictitious* if and only if it does not occur in ANF of f. A Boolean function is *nondegenerate* if it has no fictitious variables. The following fact is well known.

Theorem 4 *A bent function in n variables is nondegenerate, i. e. all variables are presented in its ANF.*

It is easy to prove it using the definition of a bent function as a function being on the maximum possible distance from all affine functions.

In 2013 A. Gorodilova (Frolova) proved a more strong result related to Kasami bent functions [7]. A Boolean function in n variables we call *k-nondegenerate* if for each product of any k pairwise different variables there exists a monomial in ANF of f that contains all variables from this product. For instance, the product $x_1x_5x_9$ we find in ANF like this: $\ldots \oplus \mathbf{x_1}x_2x_4\mathbf{x_5x_9} \oplus \ldots$ The maximal such number k for a Boolean function f we call its *order of nondegeneracy*. Theorem 4 can be reformulated like this: for any bent function the order of nondegeneracy is at least 1. A.Gorodilova proved [7]

Theorem 5 *The order of nondegeneracy of an arbitrary Kasami Boolean function of degree d equals $d-3$ or $d-2$.*

5 Can ANF of a bent function be homogeneous?

Yes, it can be. The subclass of homogeneous bent functions was introduced by C. Qu, J. Seberri and J. Pieprzyk in 2000, [20].

A bent function is called *homogeneous* if all monomials of its ANF are of the same degree. Let us briefly discuss the known facts about homogeneous bent functions. C. Qu, J. Seberri and J. Pieprzyk proved [20] that there are 30 homogeneous bent functions of degree 3 in 6 variables. Some partial results on classification of cubic homogeneous bent functions in 8 variables were obtained by C.Charnes, U.Dempwolff and J.Pieprzyk, [3].

C. Charnes, M. Rotteler and T. Beth [4] have proved the following fact.

Theorem 6 *There exist cubic homogeneous bent functions in each even number of variables n for $n \geqslant 6$.*

What about the homogeneous bent functions of higher degree? It was obtained that for $n > 3$, there are no homogeneous bent functions in n variables of the maximal possible degree $n/2$, see the paper of T. Xia, J. Seberry, J. Pieprzyk, and C. Charnes [32].

In 2007 Q. Meng, H. Zhang, M. C. Yang, and J. Cui generalized some previous results and proved [16]

Theorem 7 *For any nonnegative integer k, there exists a positive integer N such that for $n \geqslant 2N$ there exist no n-variable homogeneous bent functions having degree $(n/2) - k$ or more, where N is the least integer satisfying*

$$2^{N-1} > \binom{N+1}{0} + \binom{N+1}{1} + \ldots + \binom{N+1}{k+1}.$$

But what is the tight upper bound on the degree of a homogeneous bent function? For now there is no answer to this question. There is only

Conjecture (Q. Meng, et al. 2007). *For every $k > 1$, there is $N \geqslant 2$ such that homogeneous bent functions of degree k of n variables exist for every even $n > N$.*

In 2010 Q. Meng, L. Chen and F.-W. Fu presented partial results towards the conjectured nonexistence of homogeneous rotation symmetric bent functions having degree more than 2.

Let us describe several ideas on visualization of ANFs of homogeneous bent functions. In 2002 C. Charnes, M. Rotteler and T. Beth [4] proposed a simple method to get all 30 homogeneous bent functions of degree 3 in 6 variables. They proposed to consider so called Nagy graphs. *Nagy graph* (or *intersection graph*) $\Gamma_{(n,k)}$ can be defined like this: its vertices are all unordered k-element subsets of $\{1, 2, \ldots, n\}$; an edge connects vertices iff the corresponding subsets have exactly one common element.

The authors of [4] proposed the following steps in search of homogeneous bent functions in 6 variables: 1) find a maximal clique in $\Gamma_{(6,3)}$; 2) take the complement to it in the graph; 3) for every vertex $\{i, j, k\}$ of the complement put an item $x_i x_j x_k$ to the ANF; 4) get a homogeneous Boolean function of degree 3; the checking shows that it is bent.

Several researchers were thinking about generalization of this method on the case of arbitrary graph $\Gamma_{(n,k)}$. P. Stanica (2017) proposed to study the complements of maximal cliques of the graphs $\Gamma_{(10,4)}$, $\Gamma_{(12,4)}$ (do they produce homogeneous quartic functions?) and $\Gamma_{(12,5)}$, $\Gamma_{(14,5)}$ (what about quintic functions?).

In 2018 A. Shaporenko [23] has studied this question. First, what are the maximal cliques in $\Gamma_{(k,n)}$? A. Shaporenko proved that the clique of size $k+1$ not necessarily exists in every $\Gamma_{(n,k)}$. And if it exists it is not necessary maximal. For instance in $\Gamma_{(8,3)}$ the maximal clique is of size 7. It was proven that if $n = k(k+1)/2$ then the clique of size $k+1$ is maximal in graph $\Gamma_{(n,k)}$. It was shown that homogeneous Boolean functions obtained from $\Gamma_{(10,4)}$ and $\Gamma_{(28,7)}$ by the mentioned method are not bent [23]. So, till now there are no other examples of homogeneous bent functions obtained in such way.

6 Can ANF of a bent function be symmetric?

A Boolean function f in n variables is called *symmetric* if for any permutation π on its coordinates it holds $f(x) = f(\pi(x))$. It is the strongest symmetric property for a Boolean function. One can easily obtain that there are exactly 2^{n+1} symmetric Boolean functions since the value $f(x)$ depends only on the Hamming weight of x.

In 1994 P. Savicky [22] classified all symmetric bent functions.

Theorem 8 *There are only four symmetric bent functions in n variables:* $f(x)$, $f(x)\oplus 1$, $f(x)\oplus\sum\limits_{i=1}^{n}x_i$ *and* $f(x)\oplus\sum\limits_{i=1}^{n}x_i\oplus 1$, *where* $f(x)=\bigoplus\limits_{i=1}^{n}\bigoplus\limits_{j=i+1}^{n}x_ix_j$.

In 2006 Y. Zhao and H. Li [33] discussed a kind of bent functions that have symmetric properties with respect to some variables.

7 When ANF of a bent function is rotation symmetric?

Rotation symmetry generalizes the symmetric property of a function; it is not so strong. In 1999 J. P. Pieprzyk and C. X. Qu [18] introduced this new concept of the rotation symmetry of a Boolean function and have applied it in studying of hash functions. Note that there were other related papers of E. Filiol and C. Fountain [8], of J. P. Pieprzyk [17].

Let ρ be a cyclic permutation on coordinates $x_1\dots x_n$ defined as

$$\rho(x_1,\dots,x_{n-1},x_n)=(x_n,x_1,\dots,x_{n-1}) \text{ for all } x.$$

A Boolean function f in n variables is *rotation symmetric* if $f(x)=f(\rho(x))$ for all $x\in\mathbb{F}_2^n$. There are several useful techniques for working with rotation symmetric Boolean functions, like the *short ANF* or *SANF*. To get ANF from SANF just take all cyclic shifts of it. For instance, the SANF of a rotation symmetric Boolean function $x_1x_2\oplus x_2x_3\oplus x_3x_4\oplus x_1x_4$ in 4 variables is x_1x_2, or briefly can be written as 12.

Let us discuss results on rotation symmetric bent functions.

Classification of rotation symmetric bent functions for small n was done by P. Stanica and S. Maitra in 2003, 2008, see [24], [25].

- If $n=4$ there are 8 rotation symmetric bent functions in 4 variables. Their SANFs (up to a linear part) are 13, $12+13$.
- If $n=6$ there are 48 rotation symmetric bent functions. All of them can be presented by the following 12 functions (free of linear terms): 14, $12\oplus13\oplus14$, $134\oplus13\oplus14$, $124\oplus13\oplus14$, $124\oplus12\oplus14$, $134\oplus12\oplus14$, $123\oplus135\oplus14$, $123\oplus135\oplus12\oplus13\oplus14$, $123\oplus134\oplus135\oplus13\oplus14$, $123\oplus134\oplus135\oplus12\oplus14$, $123\oplus124\oplus135\oplus12\oplus14$, $123\oplus124\oplus135\oplus13\oplus14$. We list them here in SANF. Then to get 48 rotation symmetric functions in 6 variables one can add a rotation symmetric affine part of 4 types: zero, one, $x_1\oplus\dots\oplus x_n$ or $x_1\oplus\dots\oplus x_n\oplus1$.
- If $n=8$. P. Stanica and S. Maitra found among the 2^{21} rotation symmetric Boolean functions in 8 variables that exactly 15 104 of them are bent functions.

There are exactly 8 homogeneous rotation symmetric bent functions in 8 variables: 15, $15\oplus12$, $15\oplus13$, $15\oplus14$, $15\oplus12\oplus13$, $15\oplus12\oplus14$, $15\oplus13\oplus14$, $15\oplus12\oplus13\oplus14$. Let us note that it is easy to see some *group structure* in this construction. Indeed, let us take some basis of an Abelian group G isomorphic to $\mathbb{Z}_2^3$; denote basic vectors by formal symbols "12", "13", "14". Then SANFs of all homogeneous bent functions in 8 variables are exactly elements of the set "15"$\oplus G$.

- If $n=10$. P. Stanica and S. Maitra studied this case in [25]. But to classify all rotation symmetric bent functions in 10 variables is still difficult. It was obtained that there are 12 homogeneous rotation symmetric bent functions in 10 variables of degree 2. All of them are here: 16, $16\oplus12$, $16\oplus13$, $16\oplus14$, $16\oplus15$, $16\oplus12\oplus15$, $16\oplus13\oplus14$, $16\oplus12\oplus13\oplus14$, $16\oplus12\oplus13\oplus15$, $16\oplus12\oplus14\oplus15$, $16\oplus13\oplus14\oplus15$,

$16 \oplus 12 \oplus 13 \oplus 14 \oplus 15$. They have not found homogeneous rotation symmetric bent functions of the greater degree. Then, they proposed a conjecture: *There are no homogeneous rotation symmetric bent functions of degree* 3 *or more.* There is a some progress in proving of this conjecture in works of P. Stanica.

For a homogeneous degree d rotation symmetric Boolean function f with its SANF given by $\bigoplus_{i=1}^{s} \beta_i$, where $\beta_i = x_{k_1^{(i)}} x_{k_2^{(i)}} \cdots x_{k_d^{(i)}}$ (assume that $k_1^{(i)} = 1$ for all i), define a sequence $d_j^{(i)}$, $j = 1, 2, \ldots, k_{i-1}^{(i)}$, by $d_j^{(i)} = k_{j+1}^{(i)} - k_j^{(i)}$. Let $d_f = \max_{i,j}\{d_j^{(i)}\}$, that is, the largest distance between two consecutive indices in all monomials of f. The next theorem was proved by P. Stanica in [26].

Theorem 9 *The following hold for a homogeneous rotation symmetric Boolean function f of degree $\geqslant 3$ in $n \geqslant 6$ variables:*
(i) if the SANF of f is $x_1 \cdots x_d$, then f is not a bent function;
(ii) if the SANF of f is $x_1 x_2 \cdots x_{d-1} x_d \oplus x_1 x_2 \cdots x_{d-1} x_{d+1}$, then f is not bent, assuming: $(n-2)/4 > \lfloor n/d \rfloor$, if $n \neq 1 \pmod d$; $n/4 > \lfloor n/d \rfloor$, if $n = 1 \pmod d$;
(iii) in general, if $d_f < (n/2 - 1)/\lfloor n/d \rfloor$, then f is not bent.

In 2009 D. K. Dalai, S. Maitra and S. Sarkar [6] have analyzed combinatorial properties related to the Walsh — Hadamard spectra of rotation symmetric Boolean functions in even number of variables. These results were then applied in studying of rotation symmetric bent functions. Constructions of quadratic and cubic rotation symmetric bent functions can be found in the paper of G. Gao, X. Zhang, W. Liu and C. Carlet [9]. For example, they construct the first infinite class of *cubic* rotation symmetric bent functions. In 2014 new constructions of rotation symmetric bent functions via idempotents were proposed by C. Carlet, G. Gao and W. Liu, see [2]. Namely, they found the first infinite class of such functions of degree more than 3.

8 A linear part of ANF of a bent function can be any

It is well known that the class of bent functions is closed under addition of affine functions and under affine transformations of variables. In other words it holds

Theorem 10 *For any bent function g in n variables (n is even, $n \geqslant 2$) the function*

$$g'(x) = g(Ax \oplus b) \oplus c_1 x_1 \oplus \ldots \oplus c_n x_n \oplus d$$

is also bent, where A is a nonsingular matrix, b, c are arbitrary binary vectors, d is a constant from $\mathbb{F}_2$.

Functions g and g' are called *EA-equivalent.*

Recall [27], [29] that we can not "add" to a bent function something else to preserve the property to be bent, since for any non affine Boolean function f there exists a bent function g such that $f \oplus g$ is not bent.

9 A quadratic part of ANF of a bent function can be any

Here we present a new result obtained together with my student E. Ponomareva. We prove that an arbitrary quadratic homogeneous Boolean function in n variables is a quadratic part of some bent function in n variables, where n is even, $n \geqslant 6$.

To prove this fact, we need the following statements.

In [13] one can find

Proposition 1 *There exist exactly* 156 *nonisomorphic graphs with* 6 *vertices.*

In [12] all these graphs can be found. Let us prove first the following result.

Proposition 2 *An arbitrary quadratic homogeneous Boolean function in* 6 *variables is a quadratic part of some bent function in* 6 *variables.*

Proof Let us put into the correspondence to an arbitrary quadratic homogeneous Boolean function f in 6 variables a graph G_f on 6 vertices by the following rule: vertices correspond to variables; there is an edge between two vertices if and only if the product of corresponding variables belongs to ANF of f.

Consider only those quadratic homogeneous Boolean functions that correspond to nonisomorphic graphs. It is clear that if a quadratic homogeneous function f is a quadratic part of some bent function then any quadratic homogeneous function f' with graph $G_{f'}$ isomorphic to G_f is also a quadratic part of some bent function. It holds since any permutation on vertices produce an affine transformation of variables and hence by Theorem 10 does not change a property of a function to be bent.

According to Proposition 1 there are exactly 156 nonisomorphic graphs with 6 variables. We prove the statement by listing in Appendix 1 all 156 corresponding (to graphs) homogeneous quadratic Boolean functions and cubic parts that can be added to them in order to get a bent function in every case. So, the function equal to the sum of the quadratic function from the second column and cubic function from the third column of the table is always bent. Thus, we prove the statement. □

The following iterative construction was proposed by O. Rothaus (1966, 1976) and J. Dillon (1974), see [31].

Theorem 11 *Let f', f'', f''' be bent functions in n variables such that $f' \oplus f'' \oplus f'''$ is a bent function too. Then*

$$g(x, x_{n+1}, x_{n+2}) = f'(x)f''(x) \oplus f'(x)f'''(x) \oplus f''(x)f'''(x) \oplus$$

$$x_{n+1}f'(x) \oplus x_{n+1}f''(x) \oplus x_{n+2}f'(x) \oplus x_{n+2}f'''(x) \oplus x_{n+1}x_{n+2}$$

is a bent function in $n+2$ variables.

Now let us prove the main result of this section.

Theorem 12 *An arbitrary quadratic homogeneous Boolean function in n variables is a quadratic part of some bent function in n variables, where n is even, $n \geqslant 6$.*

Proof Let us prove it by induction.

For $n = 6$ the result follows from Proposition 2.

Suppose that it is proven for some n. Consider the case of $n+2$ variables. Let x be a vector of variables $(x_1, \ldots, x_n)$. Assume that $q(x, x_{n+1}, x_{n+2})$ is an arbitrary homogeneous quadratic Boolean function in $n + 2$ variables. If q is identically zero, then by Theorem 6 there exists a cubic homogeneous bent function in every number of variables.

Let us consider a nonzero q. Since it is nonzero, there exists at least one item in its ANF. W.l.o.g. suppose that ANF of q contains item $x_{n+1}x_{n+2}$. Otherwise by renumbering of variables we turn to this case. So, $q(x, x_{n+1}, x_{n+2})$ is of the form:

$$q(x, x_{n+1}, x_{n+2}) = h(x) \oplus a(x)x_{n+1} \oplus b(x)x_{n+2} \oplus x_{n+1}x_{n+2},$$

where h is a homogeneous quadratic Boolean function in n variables, a, b are some linear functions in n variables.

Consider the quadratic homogeneous Boolean function $h(x) \oplus a(x)b(x)$ in n variables. By induction, there exists a cubic homogeneous Boolean function $c(x)$ such that $f'(x) = c(x) \oplus h(x) \oplus a(x)b(x)$ is a bent function in n variables. Let $f''(x) = f'(x) \oplus a(x)$ and $f'''(x) = f'(x) \oplus b(x)$. According to Theorem 10 functions f'', f''' are bent too. Note that $f' \oplus f'' \oplus f'''$ is also bent by the same reason.

Then, by Theorem 11 a Boolean function

$$g(x, x_{n+1}, x_{n+2}) = f'(x)f''(x) \oplus f'(x)f'''(x) \oplus f''(x)f'''(x)$$

$$\oplus x_{n+1}f'(x) \oplus x_{n+1}f''(x) \oplus x_{n+2}f'(x) \oplus x_{n+2}f'''(x) \oplus x_{n+1}x_{n+2}$$

is a bent function in $n + 2$ variables. We see that

$$g(x, x_{n+1}, x_{n+2}) = f'(x)(f'(x) \oplus a(x)) \oplus f'(x)(f'(x) \oplus b(x)) \oplus (f'(x) \oplus a(x))(f'(x) \oplus b(x))$$

$$\oplus x_{n+1}f'(x) \oplus x_{n+1}(f'(x) \oplus a(x)) \oplus x_{n+2}f'(x) \oplus x_{n+2}(f'(x) \oplus b(x)) \oplus x_{n+1}x_{n+2} =$$

$$f'(x) \oplus a(x)b(x) \oplus a(x)x_{n+1} \oplus b(x)x_{n+2} \oplus x_{n+1}x_{n+2}.$$

Hence, we get a bent function

$$g(x, x_{n+1}, x_{n+2}) = c(x) \oplus h(x) \oplus a(x)x_{n+1} \oplus b(x)x_{n+2} \oplus x_{n+1}x_{n+2} = c(x) \oplus q(x, x_{n+1}, x_{n+2})$$

in $n + 2$ variables with prescribed quadratic part $q(x, x_{n+1}, x_{n+2})$. □

Remark. Note that a cubic part for the fixed quadratic function $q(x, x_{n+1}, x_{n+2})$ was found easy enough. Moreover it was "'reused" from the previous step of induction. May be it can be explained by "a high degree of freedom" in construction of bent function's ANF? We think so.

10 Can a k-degree part of ANF of a bent function be any?

Is it true that the cubic part of a bent function can be arbitrary?

- In case $n = 6$ the answer is **no**, since there exists only three classes of nonequivalent cubic bent functions: 123+14+25+36, 123+245+12+14+26+35+45 and $123 + 245 + 346 + 14 + 26 + 34 + 35 + 36 + 45 + 46$, but there are five classes of nonequivalent homogeneous cubic Boolean functions in 6 variables. So, we need to have items of the next degree in order to have a possibility to "put" all variants of the cubic part in a bent function.
- Case $n = 8$ is still open. The problem is that the existing classification of quartic bent functions in 8 variables (obtained by P. Langevin and G. Leander in 2011, see [14]) does not include the list of representatives of EA-classes.

We think it is a very interesting open problem to study in the general case.

11 Bent decomposition problem in terms of ANF

In 2011 we have formulated the following hypothesis, see [28].

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, $n \geqslant 2$).*

The problem to prove or disprove this hypothesis is known now as the *Bent sum decomposition problem*, see [31]. It is closely connected to the problem of asymptotic of the number of all bent functions.

This question appeared in 2011 while iterative bent functions were studied. For now the following is known in relation to this hypothesis.

- Hypothesis is confirmed for $n = 2, 4, 6$ (see [28] and [19]).
- Hypothesis was proved for quadratic Boolean functions, Maiorana—McFarland bent functions, partial spread functions, see [19].
- A weakened variant of the hypothesis was proved: any Boolean function of degree not more than $n/2$ can be represented as the sum of *constant* number of bent functions in n variables, see [30].

Hypothesis 1 can be reformulated like this: *an arbitrary ANF of degree not more than $n/2$ can be divided into two parts — every part gives the ANF of a bent function.*

Here we just give an idea that follows from Hypothesis 1 (assuming it holds): *k-degree part of the ANF of a bent function "tends" to be arbitrary.* It is necessary that at least $\sqrt{2^{\binom{n}{n/2}}}$ different variants of k-degree part of ANF should be realized in a bent function. Recall that the total number of all such variants is $2^{\binom{n}{n/2}}$.

12 Conclusion

It is very interesting to study what are relations between ANF and polynomial representation of a bent function? And is it possible to define a bent function through

the conditions on ANF? Of course these questions are interesting in respect to an arbitrary class of cryptographic Boolean functions, not only to bent.

The author is very grateful to E.Ponomareva for valuable contribution in proving of Theorem 12.

This work has been supported by the Russian Foundation for Basic Research (projects no. 17-41-543364, 18-07-01394), by the program of fundamental scientific researches of the SB RAS no.I.5.1. (project no. 0314-2016-0017) by Russian Ministry of Education and Science (Project No. 1.12875.2018/12.1 and the 5-100 Excellence Program).

References

1. Carlet C. Boolean functions for cryptography and error-correcting codes // Boolean Models and Methods in Mathematics, Computer Science, and Engineering / Eds. P. Hammer, Y. Crama. Cambridge Univ. Press, 2010. Chapter 8. P. 257–397. URL: www.math.univ-paris13.fr/∼carlet/
2. Carlet C., Gao G., Liu W. A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions // J. Combin. Theory. Ser. A. 2014. V. 127, P. 161–175.
3. Charnes C., Dempwolff U. and Pieprzyk J. The eight variable homogeneous degree three bent functions // J. of Discrete Algorithms. 2008. V. 6, N 1. P. 66–72.
4. Charnes C., Rotteler M., Beth T. Homogeneous bent functions, invariants, and designs // Designs, Codes and Cryptography. 2002. V. 26, N 1–3. P. 139–154.
5. Cusick T. W., Stănică P. Cryptographic Boolean Functions and Applications. USA: Acad. Press. Elsevier, 2009. 245 p. (Second edition in 2017).
6. Dalai D. K., Maitra S., Sarkar S. Results on rotation symmetric bent functions // Discrete Mathematics. 2009. V. 309, N 8. P. 2398–2409. Proc. of the 2nd Inter. Workshop on Boolean Functions — Cryptography and Applications — BFCA. 2006. (Rouen, France. March 13–15, 2006).
7. Frolova A.A. The essential dependence of Kasami bent functions on the products of variables // Journal of Applied and Industrial Mathematics. 2013. V. 7, N 2, P. 166–176.
8. Filiol E., Fountain C. Highly Nonlinear Balanced Boolean Functions with a Good Correlation Immunity // Advances in Cryptography — EUROCRYPT'98 Workshop on the Theory and Application of Cryptographic Techniques. Proc. Berlin: Springer, 1998. P. 475–488.
9. Gao G., Zhang X., Liu W., Carlet C. Constructions of quadratic and cubic rotation symmetric bent functions // IEEE Trans. Inform. Theory. 2012. V. 58, N 7. P. 4908–4913.
10. Hou X.D. p-ary and q-ary versions of certain results about bent functions and resilient functions // Finite Fields and Applications. 2004. V. 10. N 4. P. 566–582.
11. Kumar P. V., Scholtz R. A., Welch L. R. Generalized bent functions and their properties // J. Combin. Theory. Ser. A. 1985. V. 40, N 1. P. 90–107.
12. The On-Line Encyclopedia of Integer Sequences // Edited by N.J.A.Sloane https://oeis.org/
13. List of all 156 nonisomorphic graphs on 6 vertices, https://users.cecs.anu.edu.au/ bdm/data/graphs.html
14. Langevin P., Leander G. Counting all bent functions in dimension eight 99270589265934370305785861242880 // Designs, Codes and Cryptography. 2011. V. 59, N 1–3. P. 193–205.
15. McFarland R. L. A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15, N 1. P. 1–10.
16. Meng Q., Zhang H., Yang M. C., Cui J. On the degree of homogeneous bent functions // Discrete Applied Mathematics, 2007. V. 155, N 5. P. 665–669.
17. Pieprzyk J. P. On bent permutations // Finite Fields, Coding Theory and Adv. in Communications and Computing. 1993. V. 141. P. 173–181.
18. Pieprzyk J. P., Qu C. X. Fast Hashing and Rotation-Symmetric Functions, J. Universal Computer Science. 1999. V. 5. P. 20–31.

19. Qu L., Fu S., Dai Q., Li C. When a Boolean Function can be Expressed as the Sum of two Bent Functions // Cryptology ePrint Archive, Report 2014/048, available at http://eprint.iacr.org/.
20. Qu C., Seberry J., Pieprzyk J. Homogeneous bent functions // Discrete Appl. Math. 2000. V. 102, N 1-2. P. 133–139.
21. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20, N 3. P. 300–305.
22. Savicky P. On the bent Boolean functions that are symmetric // Eur. J. Combinatorics. 1994. V. 15, N 4. P. 407–410.
23. Shaporenko A.S. Bent functions and intersections graphs // J. of Applied and Industrial Mathematics. 2019. To appear.
24. Stănică P., Maitra S. A constructive count of rotation symmetric functions // Inform. Process. Lett. 2003. V. 88. P. 299–304.
25. Stănică P., Maitra S. Rotation Symmetric Boolean Functions — Count and Cryptographic Properties // Discrete Appl. Math. 2008. V. 156. P. 1567–1580; preliminary version appeared in Electronic Notes in Discrete Math. 2003. V. 15. P. 141–147.
26. Stănică P. On the nonexistence of homogeneous rotation symmetric bent Boolean functions of degree greater than two, Proceedings of NATO Adv. Stud. Instit. — Boolean Functions (ASI07, Moscow, Russia), 2008.
27. Tokareva N. N. The group of automorphisms of the set of bent functions // Discrete Math. Appl. 2010. V. 20. N 5–6. P. 655–664.
28. Tokareva N. N. On the number of bent functions from iterative constructions: lower bounds and hypotheses // Advances in Math. of Communications. 2011. V. 5, N 4. P. 609–621.
29. Tokareva N. N. Duality between bent functions and affine functions // Discrete Mathematics. 2012. V. 312. N 3. P. 666–670.
30. Tokareva N. N. On decomposition of a Boolean function into sum of bent functions // Siberian Electronic Mathematical Reports. 2014. V. 11. P. 745–751.
31. Tokareva N. Bent functions: results and applications to cryptography. Elsevier. 2015. 220 p. ISBN-10: 012802318X. ISBN-13: 978-0128023181.
32. Xia T., Seberry J., Pieprzyk J., Charnes C. Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$ // Discrete Applied Mathematics. 2004. V. 142, N 1–3. P. 127–132.
33. Zhao Y., Li H. On bent functions with some symmetric properties // Discrete Applied Mathematics. 2006. V. 154, N 17. P. 2537–2543.

Appendix 1

N	homogeneous quadratic function	homogeneous cubic function
1	–	$123+125+126+134+136+145+146+156+234+235+245+246+256+345+346+356$
2	$16+23+26+34+35+36+56$	$123+124+125+126+145+156+235$
3	$16+23+24+25+26+34+36+45+56$	$123+134+135+136+145+156+234+235+245$
4	$13+23+45$	$124+126+134+135+145+146+156+246+256$
5	12	$125+126+134+136+145+146+156+234+235+245+246+256+345+346+356$
6	$12+34$	$125+126+136+145+146+156+235+245+246+256+356$
7	$12+34+56$	–
8	$12+23$	$123+125+126+134+136+145+146+156+234+235+245+246+256+345+346+356$
9	$12+23+45$	$125+135+136+146+156+234+256+346$
10	$12+23+45+56$	$124+125+134+136+145+146+156+246$
11	$12+23+34$	$125+126+135+145+146+156+235+245+246+256+356$
12	$12+23+34+56$	–
13	$12+23+34+45$	$124+126+135+136+145+146+156+236+246+256$
14	$12+23+34+45+56$	–
15	$12+23+34+35+45$	$124+126+145+146+156+246+256$
16	$12+23+34+35+45+56$	–
17	$12+23+26+35+45+56$	$125+126+134+135+136+146+234+235+345$
18	$12+23+26+34+56$	–
19	$12+23+26+34+45+56$	–
20	$12+23+26+34+35+45+56$	–
21	$12+23+26+34+35+36+45+56$	$135+136+156$
22	$12+23+25+34$	$123+126+135+145+146+156+234+246+356$
23	$12+23+25+34+45$	$123+126+134+135+136+146+156+234+235+236+246+256$
24	$12+23+25+34+35+56$	–
25	$12+23+25+34+35+45$	$123+126+134+136+146+234+236+246$
26	$12+23+25+34+35+36+45+56$	$123+124+134+135+136+145+146+234+235+236+245+246$
27	$12+23+25+26+34+45+46$	$123+124+134+135+136+156+234+235+245+345$
28	$12+23+24+34+45$	$123+126+135+136+156+236+256$
29	$12+23+24+34+45+46+56$	–
30	$12+23+24+34+35+36+45+46+56$	–
31	$12+23+24+26+34+56$	–
32	$12+23+24+26+34+46+56$	–

N	homogeneous quadratic function	homogeneous cubic function
33	$12+23+24+26+34+45+56$	–
34	$12+23+24+26+34+45+46+56$	–
35	$12+23+24+26+34+36+45+56$	$123+124+134+135+145+234+245$
36	$12+23+24+26+34+35+36+45+46+56$	–
37	$12+23+24+25+34+45$	$123+126+135+136+156+235+236+256$
38	$12+23+24+25+34+35+45$	$123+126+134+136+146+236+246$
39	$12+23+24+25+26+34+56$	–
40	$12+23+24+25+26+34+45+56$	–
41	$12+23+24+25+26+34+35+36+45$	–
42	$12+23+24+25+26+34+35+36+45+46+56$	–
43	$12+16+26+34+35+45$	$123+125+134+135+136+145+146$
44	$12+16+23+34+45+56$	$124+126+146$
45	$12+16+23+26+34+45+56$	$123+125+135$
46	$12+16+23+26+34+35$	$124+145+245$
47	$12+16+23+26+34+35+45$	–
48	$12+16+23+25+34+36+45+56$	$123+124+135+234+235+245$
49	$12+16+23+25+26+34+36+45+56$	$123+134+136+234+236$
50	$12+16+23+24+26+34+45+46+56$	$124+126+146$
51	$12+16+23+24+26+34+35+45+46+56$	$123+124+234+235+245$
52	$12+16+23+24+25+34+36+45+56$	$123+135+235$
53	$12+16+23+24+25+34+36+45+46+56$	$123+134+136+234+236+246$
54	$12+15+23+34+45$	$126+146+246$
55	$12+15+23+24+34+45$	$126+146+246$
56	$12+15+23+24+34+35+45$	$123+126+136+146+234+236+246$
57	$12+15+23+24+25+35+45$	$123+126+134+135+136+146+156+234+235+236+246+256$
58	$12+15+23+24+25+34+35+45$	$126+136+156+236+256$
59	$12+15+16+23+24+45+46$	$123+125+135+136+156+256$
60	$12+15+16+23+24+45+46+56$	$134+135+145$
61	$12+15+16+23+24+34+45+56$	$123+125+126+136+145$
62	$12+14+23+34$	$123+124+125+126+134+135+136+145+156+235+245+246+256+356$
63	$12+14+23+34+56$	$123+135+145+146+156+235+236$
64	$12+14+23+34+45+56$	$124+126+146$

N	homogeneous quadratic function	homogeneous cubic function
65	$12+14+23+26+35+45+56$	$123+135+235$
66	$12+14+23+25+34+45$	$123+126+135+136+156+235+236+256$
67	$12+14+16+34+45$	$123+124+135+235+236+256$
68	$12+14+16+23+34+45$	–
69	$12+14+16+23+34+45+56$	–
70	$12+14+14+16+23+34+45+46+56$	$124+125+145$
71	$12+14+16+23+26+34+35+45+56$	$123+125+135$
72	$12+14+16+23+25+34+36+45+56$	$123+124+134+135+145+234+235+245$
73	$12+14+16+23+24+45+56$	$134+136+146$
74	$12+14+16+23+24+34+56$	$123+124+125+126+134+136+145$
75	$12+14+15+16+23+34$	$123+124+126+135+145+235+245+246+256+356$
76	$12+14+15+16+23+26+34+45+56$	$123+125+135$
77	$12+14+15+16+23+26+34+35$	$124+134+234$
78	$12+14+15+16+23+24+34$	$123+145+235+256+356$
79	$12+13+23$	$125+126+134+136+145+146+156+234+235+245+246+256+345+346+356$
80	$12+13+23+45+56$	$124+134+145+146+234+246+345$
81	$12+13+23+34+56$	–
82	$12+13+23+34+45+56$	–
83	$12+13+23+34+35$	$124+126+134+136+145+146+156+245+246+256+346$
84	$12+13+23+34+35+45$	$136+146+346$
85	$12+13+23+34+35+36+45+46+56$	–
86	$12+13+23+24+26+34+35+56$	$123+125+135$
87	$12+13+16+23+34+35+45+46+56$	–
88	$12+13+16+23+25+34+45+56$	–
89	$12+13+16+23+25+34+35+45+56$	–
90	$12+13+16+23+24+34+45$	–
91	$12+13+16+23+24+34+45+56$	–
92	$12+13+15+23+34+35+45$	$126+134+136+146+236+246$
93	$12+13+15+23+26+34+35+36+45+46$	–
94	$12+13+15+16+45$	$123+136+234+235+236+256+346$
95	$12+13+15+16+34+45+46$	$123+124+134+135+145+234+235+236+256+345$
96	$12+13+15+16+34+35$	$123+245+246+256$

N	homogeneous quadratic function	homogeneous cubic function
97	$12+13+15+16+26+34+45$	$123+134+234$
98	$12+13+15+16+23+34+45+56$	$124+126+146$
99	$12+13+15+16+23+34+35+36+45+56$	–
100	$12+13+15+16+23+25+26+45+46+56$	$134+135+145+146+156$
101	$12+13+15+16+23+25+26+34+36+45+56$	$123+134+135+234+345$
102	$12+13+15+16+23+24+34+45$	–
103	$12+13+15+16+23+24+34+45+46$	$123+124+126+136+145+245+345$
104	$12+13+15+16+23+24+34+45+46+56$	$124+125+145$
105	$12+13+15+16+23+24+26+34+36$	$123+245+246+256$
106	$12+13+15+16+23+24+26+34+35+45+46+56$	$123+124+134+135+136+145+146+234+235+236+245+246$
107	$12+13+14$	$123+125+126+134+136+146+156+234+235+245+246+256+345+346+356$
108	$12+13+14+56$	$234+235+236+246+345$
109	$12+13+14+45+56$	$234+236+246$
110	$12+13+14+23$	$125+126+134+136+146+156+234+235+245+246+256+345+346+356$
111	$12+13+14+23+34$	$124+125+126+136+145+156+235+245+246+256+356$
112	$12+13+14+23+34+56$	$123+135+145+146+156+235+236$
113	$12+13+14+23+24+34$	$125+126+136+156+235+256+356$
114	$12+13+14+23+24+34+56$	–
115	$12+13+14+23+24+34+35+36+45+46+56$	–
116	$12+13+14+23+24+25+34+35+45$	$123+126+134+136+146+236+246$
117	$12+13+14+23+24+25+26+34+35+36+46+56$	–
118	$12+13+14+16+24+25+26+34+35+36+45$	$123+124+234$
119	$12+13+14+16+23+45+46+56$	$124+126+134+135+145+146+156$
120	$12+13+14+16+23+34+56$	$123+125+235$
121	$12+13+14+16+23+34+45+56$	–
122	$12+13+14+16+23+34+45+46+56$	–
123	$12+13+14+16+23+26+34+36+45+56$	–
124	$12+13+14+16+23+26+34+35+45+56$	–
125	$12+13+14+16+23+25+34+36+45+56$	$123+124+134+145+234+235+245$
126	$12+13+14+16+23+24+34+56$	–
127	$12+13+14+16+23+24+34+45$	–
128	$12+13+14+16+23+24+26+34+35+45+56$	–

N	homogeneous quadratic function	homogeneous cubic function
129	$12+13+14+15$	$123+125+126+134+136+145+146+156+234+235+245+246+256+345+346+356$
130	$12+13+14+15+23+34+35+36+45+46+56$	–
131	$12+13+14+15+23+25+34+45$	$123+126+135+136+156+235+236+256$
132	$12+13+14+15+23+24+25+34+35+45$	$146+156+236+256+346$
133	$12+13+14+15+23+24+25+26+34+35+36+45+46$	–
134	$12+13+14+15+23+24+25+26+34+35+36+45+46+56$	$125+126+134+136+145$
135	$12+13+14+15+16$	$123+125+134+145+234+235+245+246+256+345+346+356$
136	$12+13+14+15+16+56$	$124+134+234+235+236+246+345$
137	$12+13+14+15+16+26+34+45$	$123+134+234$
138	$12+13+14+15+16+24+34+45+46$	$124+125+126+136+145+234+235+236+256+345$
139	$12+13+14+15+16+23+34$	$124+125+146+235+245+246+256+356$
140	$12+13+14+15+16+23+34+45+56$	–
141	$12+13+14+15+16+23+34+45+46$	$135+145+345$
142	$12+13+14+15+16+23+34+35$	$124+134+135+145+245+246+256$
143	$12+13+14+15+16+23+34+35+36+45+56$	$124+134+145+234+245$
144	$12+13+14+15+16+23+26+35+56$	$123+124+136+234+236+246$
145	$12+13+14+15+16+23+26+34+35+56$	$123+125+235$
146	$12+13+14+15+16+23+26+34+35+45+56$	$123+125+135$
147	$12+13+14+15+16+23+25+34+36+45+56$	$123+124+134+135+145+234+235+245$
148	$12+13+14+15+16+23+25+34+35+36+45+56$	$123+124+134+145+234+235+245$
149	$12+13+14+15+16+23+25+26+35+36$	$125+135+136+156+245+246+256$
150	$12+13+14+15+16+23+25+26+34+56$	$124+125+145$
151	$12+13+14+15+16+23+25+26+34+36+45+56$	$123+135+136+156+235$
152	$12+13+14+15+16+23+25+26+34+35+36+45+46+56$	$124+125+126+134+146+234+245$
153	$12+13+14+15+16+23+24+34$	$125+145+235+256+356$
154	$12+13+14+15+16+23+24+34+45+46$	$123+124+126+136+145+245+345$
155	$12+13+14+15+16+23+24+26+34+35+45+46+56$	$123+135+136+234+235+236+245+246$
156	$12+13+14+15+16+23+24+25+26+34+35+36+45+46+56$	–