S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

http://semr.math.nsc.ru

Том 19, №1, стр. 342–347 (2022) УДК 512.5
DOI 10.33048/semi.2022.19.029 MSC 13A99

A QUADRATIC PART OF A BENT FUNCTION CAN BE ANY

N.N. TOKAREVA

Abstract. Boolean functions in n variables that are on the maximal possible Hamming distance from all affine Boolean functions in n variables are called bent functions (n is even). They are intensively studied since sixties of XX century in relation to applications in cryptography and discrete mathematics. Often, bent functions are represented in their algebraic normal form (ANF). It is well known that the linear part of ANF of a bent function can be arbitrary. In this note 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 [7]. Bent functions play an important role in constructions of symmetric ciphers since they help to defend ciphers against linear cryptanalysis[4] and have many applications in discrete mathematics and communications, see [8]. 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 too far from classification. No conditions on ANF of a Boolean function are known in order to say that the function is bent.

In this paper 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

Tokareva, N.N., A quadratic part of a bent function can be any.

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2022-281 with the Ministry of Science and Higher Education of the Russian Federation.

Received March, 13, 2022, published June, 29, 2022.

even) is a k-degree part in ANF of some bent function in n variables? For small 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, $n \geqslant 6$. For cubic parts the question remains open.

2. Preliminaries

We use the following standard notation:

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

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

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

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

$a_1x_1 \oplus \ldots \oplus a_nx_n \oplus b$ — an *affine function* in variables $x_1, \ldots, x_n$, where $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2$, sign $\oplus$ stands for addition modulo 2 (XOR);

bent function — a Boolean function in n variables (n is even) that is on the maximal possible Hamming distance from the set of all affine functions. It is known [7] that 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.

Recall that 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 $\mathbb{F}_2$. 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.

In what follows let n be an even number.

According to O.Rothaus (1966, 1976) [7] and V. A. Eliseev, O. P. Stepchenkov (1962) [8], 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. For any possible degree from 2 to $n/2$ it is not difficult to construct a bent function of such degree.

Several restrictions on ANF of bent functions can be naturally considered. A bent function is called *homogeneous* if all monomials of its ANF are of the same degree. C. Qu, J. Seberri and J. Pieprzyk proved [14] that there are 30 homogeneous bent functions of degree 3 in 6 variables. Partial results on classification of cubic homogeneous bent functions in 8 variables were obtained by C.Charnes et al. in [1].

C. Charnes, M. Rotteler and T. Beth [2] have proved the following fact that we will use further.

Proposition 1. *There exist cubic homogeneous bent functions in each even number of variables n for $n \geqslant 6$.*

For the homogeneous bent functions of higher degrees it is known only a little.

3. On the quadratic part of ANF of a bent function

It is well known that the class of bent functions is closed under addition of affine functions and under affine transformations of variables, see [3]. In other words it holds

Proposition 2. *For any bent function g in n variables (n is even, $n \geqslant 2$) the function $g'(x) = g(Ax \oplus b) \oplus c_1x_1 \oplus \ldots \oplus c_nx_n \oplus d$ is also bent, where A is a nonsingular matrix, b, c are arbitrary binary vectors of length n, d is a constant from $\mathbb{F}_2$.*

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

Note that we can add an arbitrary affine function to a bent function without changing its property to be bent. Recall that it is not possible to find a non affine Boolean function that does the same, since for any non affine Boolean function f there exists a bent function g such that $f \oplus g$ is not bent, see [12], [9]. For instance, it is not possible even to add a quadratic function to all bent functions in order to save their property to be bent. But we want to prove that it is possible to find a bent function with an arbitrary quadratic part of ANF!

In this section we show 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 [6] one can find

Proposition 3. *There exist exactly 156 nonisomorphic graphs with 6 vertices.*

In [6] all these graphs can be found. Let us prove first the following result.

Proposition 4. *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 Proposition 2 does not change a property of a function to be bent.

According to Proposition 3 there are exactly 156 nonisomorphic graphs with 6 variables. We prove the statement by listing in the table 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. Note that we list quadratic parts in the lexicographical order. For every quadratic part we have found a cubic part of the minimal possible length. Sometimes it is of length 0 and we put sign "$-$" in the table: it means that a quadratic part is already a bent function. Symbol $|$ in both columns should be replaced by $\oplus$, and items like 12 and 123 by x_1x_2 and $x_1x_2x_3$ respectively. We use such short notation in the table for a compactness. Thus, we prove the statement. □

The following iterative construction was proposed by O. Rothaus (1966, 1976) and J. Dillon (1974), see [8].

Proposition 5. *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.

Theorem 1. *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 4. Suppose that it is proven for some n. Consider the case of $n + 2$ variables. Let x be a vector of variables $(x_1, \dots, x_n)$. 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 Proposition 1 there exists a cubic homogeneous bent function in every number of variables: it will be a bent function with an empty quadratic part.

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 Proposition 2 functions f'', f''' are bent too. Note that $f' \oplus f'' \oplus f'''$ is also bent by the same reason.

Then, by Proposition 5 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 $q(x, x_{n+1}, x_{n+2})$. □

4. Future remarks

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

In particular, 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: $123 \oplus 14 \oplus 25 \oplus 36$, $123 \oplus 245 \oplus 12 \oplus 14 \oplus 26 \oplus 35 \oplus 45$ and $123 \oplus 245 \oplus 346 \oplus 14 \oplus 26 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 46$, 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. Here in notation we again use 123 for $x_1x_2x_3$ and so on.
- 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 [5]) 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.

In 2011 we have formulated the following hypothesis, see [11].

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.* It is closely connected to the problem of asymptotic of the number of all bent functions.

For now the following is known in relation to this hypothesis.

- Hypothesis is confirmed for $n = 2, 4, 6$ (see [11] and [13]).
- Hypothesis was proved for quadratic Boolean functions, Maiorana—McFarland bent functions, partial spread functions, see [13].
- A weakened variant of the hypothesis was proved: every Boolean function in n variables of a constant degree d, where $d \leqslant n/2$, n is even, can be represented as the sum of constant number of bent functions in n variables, see [10].

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 $\sqrt{2^{\binom{n}{k}}}$ 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 $2^{\binom{n}{k}}$.

5. Conclusion

It is very interesting to study if it is 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 functions. The author is very grateful to E. Ponomareva for valuable contribution in proving of Theorem 1, to V. Idrisova for kind help and remarks, and to the reviewer of this paper for the careful reading of the work and comments.

References

[1] C. Charnes, U. Dempwolff, J. Pieprzyk, *The eight variable homogeneous degree three bent functions*, J. Discrete Algorithms, **6**:1 (2008), 66–72. Zbl 1147.94010

[2] C. Charnes, M. Rötteler, T. Beth, *Homogeneous bent functions, invariants, and designs*, Des. Codes Cryptography, **26**:1-3 (2002), 139–154. Zbl 1026.06015

[3] T. Cusick, P. Stănică, *Cryptographic Boolean functions and applications*, Elsevier, Amsterdam, 2009. Zbl 1173.94002

[4] M. Matsui, *Linear cryptanalysis method for DES cipher*, In: Helleseth T. (ed.), *Advances in cryptology - EUROCRYPT '93*, Lect. Notes Comput. Sci., **765**, 1994, 386–397. Zbl 0951.94519

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

[6] *List of all 156 nonisomorphic graphs on 6 vertices*, **https://users.cecs.anu.edu.au/ bdm/data/graphs.html**.

[7] O. Rothaus, *On "bent" functions*, J. Comb. Theory, Ser. A, **20**:3 (1976), 300–305. Zbl 0336.12012

[8] N. Tokareva, *Bent functions. Results and applications to cryptography*, Elsevier, Amsterdam, 2015. Zbl 1372.94002

[9] N.N. Tokareva, *Duality between bent functions and affine functions*, Discrete Math., **312**:3 (2012), 666–670. Zbl 1234.94068

[10] N.N. Tokareva, *On decomposition of a Boolean function into sum of bent functions*, Sib. Èlectron. Math. Izv, **11** (2014), 745–751. Zbl 1325.94143

[11] N.N. Tokareva, *On the number of bent functions from iterative constructions: lower bounds and hypotheses*, Adv. Math. Commun., **5**:4 (2011), 609–621. Zbl 1238.94032

[12] N.N. Tokareva, *The group of automorphisms of the set of bent functions*, Discrete Math. Appl., **20**:5-6 (2010), 655–664. Zbl 1211.94057

[13] L. Qu, S. Fu, Q. Dai, C. Li, *When a Boolean function can be expressed as the sum of two bent functions*, Cryptology ePrint Archive, **2014**, Report 2014/048, available on **http://eprint.iacr.org/2014/048**.

[14] C. Qu, J. Seberry, J. Pieprzyk, *Homogeneous bent functions*, Discrete Appl. Math., **102**:1-2 (2000), 133–139. Zbl 1016.94029

Natalia Nikolaevna Tokareva
Sobolev Institute of Mathematics,
4, Koptyuga, ave.,
Novosibirsk, 630090, Russia
Novosibirsk State University,
2, Pyrogova str.,
Novosibirsk, 630090, Russia
Email address: tokareva@math.nsc.ru