Discrete Math. Appl., Vol. 20, No. 5–6, pp. 655–664 (2010) DOI 10.1515/DMA.2010.040

The group of automorphisms of the set of bent functions

N. N. TOKAREVA

Abstract — The bent functions are the Boolean functions of an even number of variables which are at the maximum possible distance from the set of all affine functions. In this paper, it is shown that each isometric mapping of the set of Boolean functions of n variables to itself preserving the class of bent functions is a combination of an affine transformation of coordinates and a shift by an affine function. It is proved that the affine functions are precisely all Boolean functions which are at the maximum possible distance from the class of bent functions.

The research was supported by the Program of President of Russian Federation for support of young Russian scientists, grant 1250.2009.1; by the Russian Foundation for Basic Research, grants 08–01–00671, 09–01–00528, 10–01–00424; and by the Federal Program for support of scientific and pedagogical staff of innovational Russia for 2009–2013, state contract 02.740.11.0429.

1. INTRODUCTION

The bent functions are the Boolean functions of an even number of variables which are at the maximum possible distance from all affine functions. They were introduced by O. Rothaus [6]. At present, the bent functions are actively investigated and have found many applications in the coding theory, cryptography, digital communication, and other fields (see the reviews [3, 4]). Nevertheless, the theory of bent functions contains many unsolved problems, among which is the question on the automorphism group of the set of bent functions. In this paper, we give an answer to this question.

Let A be a nondegenerate binary $n \times n$ matrix, let b and c be binary vectors of length n and d be a constant. It is known that any mapping of the form $g(x) \to g(Ax + b) + \langle c, x\rangle + d$ defined on the set of Boolean functions of n variables preserves the class of bent functions. A natural question arises whether there exist other isometric mappings of Boolean functions into itself which preserve the class of bent function. In this paper, we demonstrate that there are no other mappings possessing such a property.

Originally published in *Diskretnaya Matematika* (2010) **22**, No. 4 (in Russian).
Received April 19, 2010.

Let us briefly describe the structure of this paper. The main part is devoted to the proof that for any nonaffine function f there exists a bent function g such that the function $f + g$ is not a bent function (see Theorem 1). In other words, the set of bent function is closed under addition of affine Boolean functions. This fact implies that the affine functions are precisely all Boolean functions which are at the maximum distance from the class of bent functions. In other words, there exists a duality, in some sense, between the definitions of bent functions and affine functions. Further we show that the set of bent functions and the set of affine functions have the same groups of automorphisms. This common group is a semidirect product of the full affine group $\mathrm{GA}(n)$ and $\mathbf{Z}_2^{n+1}$ (Theorem 2).

2. DEFINITIONS AND FACTS

Let $\langle x, y\rangle$ denote the usual scalar product of binary vectors $x, y \in \mathbf{Z}_2^n$ modulo 2. The Hamming distance $d(x, y)$ between vectors x and y is the number of coordinates where the vectors differ.

The distance $\mathrm{dist}(f, g)$ between Boolean functions f and g is the distance between their vectors of values. We denote by $\mathrm{supp}(f)$ the support of the function f, that is, the set of vectors where the function f takes the value one. It is known that each Boolean function f can be represented in the algebraic normal form whose degree we denote by $\deg(f)$. The Boolean functions of degree 1 are called affine and are of the form $\langle c, x\rangle + d$ for an appropriate vector c and a constant d. The set of all affine function of n variables is denoted by $\mathcal{A}_n$.

The Walsh–Hadamard transformation of a Boolean function f of n variables is an integer-valued function

$$W_f(y) = \sum_x (-1)^{\langle x,y\rangle + f(x)}.$$

A bent function is a Boolean function of n variables, where n is even, such that the absolute value of each Walsh–Hadamard coefficient $W_f(y)$ of the function is equal to $2^{n/2}$. The derivative of a Boolean function f in the direction y is the function $f(x) + f(x + y)$. We observe that a Boolean function f is an affine function if and only if its derivative in any direction is a constant.

An affine function can be equivalently defined as in [1].

Proposition 1. *A Boolean function g is a bent function if and only if its derivative in any nonzero direction y is balanced, that is, the relation*

$$\sum_x (-1)^{g(x)+g(x+y)} = 0$$

is true.

The set of all bent functions of n variables is denoted by $\mathcal{B}_n$. The following property of bent functions is well known.

Proposition 2. *Let A be a nondegenerate binary $n \times n$ matrix, b and c be binary vectors, d be a constant. Any mapping of the form $g(x) \to g(Ax + b) + \langle c, x\rangle + d$ defined on the set of Boolean functions of n variables preserves the class of bent functions.*

Further we will use the known construction of bent functions given by McFarland [5].

Proposition 3. *The function*

$$f(x', x'') = \langle x', \pi(x'')\rangle + h(x'')$$

is a bent function of n variables, where π is an arbitrary permutation on $\mathbf{Z}_2^{n/2}$ and the Boolean function h of $n/2$ variables is arbitrary.

Note that the partition of the variables into two equal parts x' and x'' can be arbitrary.

Consider the vectors with fixed values of some $n - k$ coordinates and the remaining coordinates arbitrarily chosen. The set of all such vectors is called the facet of dimension k of the space $\mathbf{Z}_2^n$. For example, the set

$$\Gamma = \{(x', x''): x'' = a\}$$

is a facet of dimension $n/2$; here $x', x'' \in \mathbf{Z}_2^{n/2}$.

3. ON SHIFTS OF THE CLASS OF BENT FUNCTIONS

We will prove the following fact from which the main results of the paper will be obtained.

Theorem 1. *For any nonaffine function f there exists a bent function g such that the function $f + g$ is not a bent function.*

Proof. Assume that for some fixed function f such that $\deg(f) \geq 2$ the equality $f + \mathcal{B}_n = \mathcal{B}_n$ is true. Let us show that this leads to a contradiction.

The idea of the proof is as follows. First we show that some sum has to be equal to zero for any bent function, see sum (1) below. Then we find a bent function g' in the McFarland class which is a counterexample and for which this equality is false. The bent function g' will be obtained from a specially chosen bent function g by inversion of its values on some facet Γ of dimension $n/2$. The key condition for the possibility of choice of such a facet is that for some nonzero y the set $D = \operatorname{supp}(f(x)+f(x+y))$ is a proper subset of the space $\mathbf{Z}_2^n$. This is possible if and only if f is nonaffine.

It is convenient to divide the proof into several stages.

3.1. *The equality for any bent function*

Since $\deg(f) \geq 2$, there exists a nonzero vector y such that the derivative of the function f in the direction y is not a constant. It is possible to assume that $y = 1$. Indeed, if y is other nonzero vector, then from the function f we turn to the function $f'(x) = f(Ax)$, where $A \cdot 1 = y$. It is clear that the derivative of the function f' in the direction 1 is not a constant, and, as for the function f, the equality $f' + \mathcal{B}_n = \mathcal{B}_n$ is true (that is, it is possible to prove the theorem for f'). Then in what follows we assume that $y = 1$.

Let g be an arbitrary bent function. Then $f + g$ is also a bent function, and according to Proposition 1 the equalities

$$\sum_x (-1)^{g(x)+g(x+y)} = 0,$$

$$\sum_x (-1)^{g(x)+f(x)+g(x+y)+f(x+y)} = 0$$

are true. Subtracting the second equality from the first one, we obtain the equality

$$\sum_x (-1)^{g(x)+g(x+y)}(1 - (-1)^{f(x)+f(x+y)}) = 0.$$

Denote by D the set $\mathrm{supp}(f(x)+f(x+y))$. Then for any bent function g the equality

$$\sum_{x \in D} (-1)^{g(x)+g(x+y)} = 0 \tag{1}$$

has to be true.

3.2. *Choice of the facet*

Since the function $f(x) + f(x + y)$ is not a constant, the set D is not empty and does not coincide with the whole Boolean cube. Then there exists an $(n/2)$-dimensional facet Γ such that it has a nonempty intersection with the set D and with its complement $\mathbf{Z}_2^n \setminus D$, that is, the relation

$$0 < m < |\Gamma| = 2^{n/2}, \tag{2}$$

where $m = |\Gamma \cap D|$, is true. Indeed, such a facet can be always constructed, for example, with the use of any vector $u \notin D$ and one of the vectors v or $v + y$, where $v \in D$, since either the distance $d(u, v)$ or the distance $d(u, v + y)$ does not exceed $n/2$.

We observe that the facet $\Gamma + y$ also has an intersection of cardinality m with the set D, since, as it is not difficult to see, $D + y = D$. We also observe that the facets Γ and $\Gamma + y$ do not overlap (by virtue of the choice of $y = 1$). The partition of the set D

$$D = (\Gamma \cap D) \cup ((\Gamma + y) \cap D) \cup (D \setminus (\Gamma \cup (\Gamma + y))) \tag{3}$$

takes place. It will be needed later.

Without loss of generality we assume that the facet Γ is of the form

$$\Gamma = \{(x', x''): x'' = a\}$$

for some vector $a \in \mathbf{Z}_2^{n/2}$ (in the case where the fixed coordinates of a base are placed in other way, the proof is similar). Let the set $\Gamma \cap D$ be represented in the form

$$\Gamma \cap D = \{(b^{(1)}, a), (b^{(2)}, a), \ldots, (b^{(m)}, a)\}$$

with appropriate vectors $b^{(1)}, b^{(2)}, \ldots, b^{(m)}$ of length $n/2$.

3.3. *A special subset of bent functions*

Consider the subset G of bent functions of the form

$$g(x', x'') = \langle x', \pi(x'')\rangle$$

of the McFarland class such that permutations π are linear transformations of the space, that is, each π is defined as $\pi(x'') = Ax''$ with an appropriate nondegenerate matrix A. Let us show that the class G contains a bent function g such that the sum

$$S = \sum_{x \in \Gamma \cap D} (-1)^{g(x)+g(x+y)}$$

is not equal to zero. Consider this sum for an arbitrary function of G. Since

$$\pi(x'' + y'') = A(x'' + y'') = Ax'' + Ay'',$$

where $y = (y', y'')$, we obtain

$$\begin{aligned} g(x) + g(x + y) &= \langle x', Ax''\rangle + \langle x' + y', Ax'' + Ay''\rangle \\ &= \langle x', Ay''\rangle + \langle y', Ax'' + Ay''\rangle. \end{aligned}$$

Then, substituting this into the sum S, we obtain

$$S = (-1)^{\gamma} \sum_{i=1}^{m} (-1)^{\langle b^{(i)}, Ay''\rangle},$$

where $\gamma = \langle y', Aa + Ay''\rangle$ is a constant depending on the choice of the matrix A. Since y'' is a nonzero vector (due to the choice of $y'' = 1$) and the matrix A can be an arbitrary nondegenerate matrix, we see that the vector $z = Ay''$ also can be an arbitrary nonzero vector of length $n/2$. Thus, our problem is to show that there exists a nonzero vector z such that the sum

$$\sum_{i=1}^{m} (-1)^{\langle b^{(i)}, z\rangle} \tag{4}$$

is not equal to zero.

3.4. *Searching for the vector z*

Assume the contrary: let for any nonzero vector z sum (4) be equal to zero. Consider the binary matrix M of size $(n/2) \times m$, the columns of the matrix are the vectors $b^{(1)}, \ldots, b^{(m)}$. Then sum (4) is the difference between the number of zeros and the number of ones in the linear combination of the rows of the matrix M defined by the vector z (the row i is contained in the combination if $z_i = 1$). By the assumption, the matrix M must satisfy the following condition: any nonzero linear combination of the rows of the matrix M contains the equal numbers of zeros and ones. It is not difficult to see that, up to permutation of the columns, this matrix must be of the form

$$\begin{pmatrix} \underbrace{0\ldots0}_{m/8} & \underbrace{0\ldots0}_{m/8} & \underbrace{0\ldots0}_{m/8} & \underbrace{0\ldots0}_{m/8} & \underbrace{1\ldots1}_{m/8} & \underbrace{1\ldots1}_{m/8} & \underbrace{1\ldots1}_{m/8} & \underbrace{1\ldots1}_{m/8} \\ 0\ldots0 & 0\ldots0 & 1\ldots1 & 1\ldots1 & 0\ldots0 & 0\ldots0 & 1\ldots1 & 1\ldots1 \\ 0\ldots0 & 1\ldots1 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 1\ldots1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{pmatrix}$$

Hence it is seen that the number of columns of the matrix has to be at least $2^{n/2}$, where $n/2$ is the number of rows. Thus, for the existence of such a matrix M it is necessary that the inequality $m \geq 2^{n/2}$ is true. But this contradicts the condition of the choice of the base Γ, namely, inequality (2). Thus, there always exists a vector z such that sum (4) is not equal to zero. We fix this vector z.

3.5. *Construction of the function which is the counterexample*

Let A be a nondegenerate matrix such that $Ay'' = z$, let the permutation π be defined by the equality $\pi(x'') = Ax''$. It follows from the choice of the vector z that for the function $g(x', x'') = \langle x', \pi(x'')\rangle$ the equality

$$S = \sum_{x \in \Gamma \cap D} (-1)^{g(x)+g(x+y)} \neq 0 \tag{5}$$

is true.

Define a new bent function g' differing from g only on the facet Γ. Further we will see that the functions $f + g$ and $f + g'$ cannot be simultaneously bent functions, and this will lead to the contradiction with the main assumption. Let

$$g'(x', x'') = g(x', x'') + h(x''),$$

where

$$h(x'') = \begin{cases} 1 & \text{if } x'' = a, \\ 0 & \text{otherwise.} \end{cases}$$

In other words, g' is obtained from the function g by inverting its values on the facet Γ. Since g belongs to the McFarland class, the functions g' is also a bent function and

also belongs to the McFarland class. Note that by virtue of partition (3)

$$\begin{aligned}\sum_{x\in D}(-1)^{g'(x)+g'(x+y)} &= \left(\sum_{x\in\Gamma\cap D}(-1)^{g(x)+1+g(x+y)+0}\right)\\ &\quad+\left(\sum_{x\in(\Gamma+y)\cap D}(-1)^{g(x)+0+g(x+y)+1}\right)\\ &\quad+\left(\sum_{x\in(D\setminus(\Gamma\cup(\Gamma+y))}(-1)^{g(x)+g(x+y)}\right)\\ &=\left(\sum_{x\in(D\setminus(\Gamma\cup\Gamma+y))}(-1)^{g(x)+g(x+y)}\right)-2S.\end{aligned}$$

Thus,

$$\sum_{x\in D}(-1)^{g'(x)+g'(x+y)}=\sum_{x\in D}(-1)^{g(x)+g(x+y)}-4S.$$

It follows from this equality, equality (1), and inequality (5) that

$$\sum_{x\in D}(-1)^{g'(x)+g'(x+y)}\neq 0.$$

But equality (1) must hold true for any bent function including g'. The obtained contradiction proves the theorem.

4. DUALITY OF DEFINITIONS OF BENT FUNCTIONS AND AFFINE FUNCTIONS

For an even n, the class of bent functions $\mathcal{B}_n$ can be defined as the set of functions which are at the maximum possible distance $N_{\max}$ from the class of affine Boolean functions $\mathcal{A}_n$, that is,

$$\mathcal{B}_n=\{g\colon \operatorname{dist}(g,\mathcal{A}_n)=N_{\max}\}.$$

It is known that

$$N_{\max}=2^{n-1}-2^{(n/2)-1}.$$

Is it possible to invert this definition? In other words, is it true that $\mathcal{A}_n$ is the set of all Boolean functions which are at the maximum possible distance $N'_{\max}$ from the class $\mathcal{B}_n$? Let

$$\mathcal{A}'_n=\{f\colon \operatorname{dist}(f,\mathcal{B}_n)=N'_{\max}\}.$$

Let us show that such inversion of the definitions is possible indeed, that is, the equalities

$$N_{\max}=N'_{\max},\qquad \mathcal{A}_n=\mathcal{A}'_n$$

are true.

Proposition 4. *The equality*

$$N'_{\max} = 2^{n-1} - 2^{(n/2)-1}$$

is true.

Proof. By the definition,

$$N'_{\max} = \max_f \min_{g \in \mathcal{B}_n} \operatorname{dist}(f, g).$$

We observe that

$$\operatorname{dist}(f, g) = 2^{n-1} - \tfrac{1}{2} W_{f+g}(0).$$

Therefore,

$$N'_{\max} = 2^{n-1} - \tfrac{1}{2} \min_f \max_{g \in \mathcal{B}_n} |W_{f+g}(0)|.$$

Fix an arbitrary bent function g' of n variables. Since the class $\mathcal{B}_n$ is closed under addition of affine functions, each function of the form $g' + l_a$, where $l_a(x) = \langle a, x \rangle$, is a bent function. We observe that that

$$W_{f+g'+l_a}(0) = W_{f+g'}(a).$$

Then it is obvious that

$$\max_{g \in \mathcal{B}_n} |W_{f+g}(0)| \geq \max_{\substack{g \in \mathcal{B}_n \\ g = g' + l_a \text{ for some } a}} |W_{f+g}(0)| = \max_a |W_{f+g'}(a)|.$$

It follows from the Parseval inequality for the Boolean function $f + g'$ that

$$\max_a |W_{f+g'}(a)| \geq 2^{n/2}.$$

Hence,

$$N'_{\max} \leq 2^{n-1} - 2^{(n/2)-1}.$$

On the other hand, the distance $2^{n-1} - 2^{(n/2)-1}$ to the class of bent function is attained, for example, for an affine function f. The proposition is proved.

Proposition 5. *The equality $\mathcal{A}_n = \mathcal{A}'_n$ is true.*

Proof. It is clear that $\mathcal{A}_n \subseteq \mathcal{A}'_n$. Assume that there exists a function $f \in \mathcal{A}'_n \setminus \mathcal{A}_n$. Then by virtue of Theorem 1 there exists a bent function g such that $f + g$ is not a bent function, that is, there exists a vector a such that $|W_{f+g}(a)| > 2^{n/2}$. Consider the bent function $g'(x) = g(x) + \langle a, x \rangle$. For this function, the equality $W_{f+g'}(0) = W_{f+g}(a)$ is true, and by the equality

$$\operatorname{dist}(f, \mathcal{B}_n) = 2^{n-1} - \tfrac{1}{2} \max_{g \in \mathcal{B}_n} |W_{f+g}(0)|$$

the inequality

$$\operatorname{dist}(f, \mathcal{B}_n) < N'_{\max},$$

which contradicts the choice of f, is true. Thus, $\mathcal{A}_n = \mathcal{A}'_n$.

We note that the main fact which gives a possibility to discover the duality between the definitions of affine functions and bent functions is Theorem 1.

5. AUTOMORPHISMS OF BENT FUNCTIONS

A mapping φ of the set of all Boolean functions of n variables to itself is called isometric if it preserves the distances between Boolean functions, that is,

$$\operatorname{dist}(\varphi(f), \varphi(g)) = \operatorname{dist}(f, g).$$

It is known that any such mapping is uniquely representable in the form

$$g(x) \to g(s(x)) + f(x), \tag{6}$$

where $s: \mathbf{Z}_2^n \to \mathbf{Z}_2^n$ is an arbitrary permutation, f is an arbitrary function of n variables.

The group of automorphisms of a subset of Boolean functions $\mathcal{M}$ is the group of isometric mappings of the set of all Boolean function into itself preserving the fixed set $\mathcal{M}$. We denote this group by $\operatorname{Aut}(\mathcal{M})$.

Recall that the full affine group $\mathrm{GA}(n)$ consists of all mappings of the form $g(x) \to g(Ax + b)$, where A is a nonsingular matrix, b is an arbitrary vector.

The following assertion is true.

Proposition 6. *The group* $\operatorname{Aut}(\mathcal{A}_n)$ *is equal to the semidirect product of the full affine group* $\mathrm{GA}(n)$ *and* $\mathbf{Z}_2^{n+1}$.

Indeed, for any automorphism (6) the shift by a function f can be defined only for an affine function (since the image of the null function is also an affine function). The set of all affine functions of n variables forms a group isomorphic to $\mathbf{Z}_2^{n+1}$. It remains to note that, as it is well known, each permutation s must belong to the group $\mathrm{GA}(n)$, see, for example, [2].

Theorem 2. *The equalities*

$$\operatorname{Aut}(\mathcal{B}_n) = \operatorname{Aut}(\mathcal{A}_n) = \mathrm{GA}(n) \ltimes \mathbf{Z}_2^{n+1}.$$

Proof. It is obvious that $\operatorname{Aut}(\mathcal{A}_n) \subseteq \operatorname{Aut}(\mathcal{B}_n)$. Indeed, for any mapping $\varphi \in \operatorname{Aut}(\mathcal{A}_n)$ and any bent function g

$$\operatorname{dist}(g, \mathcal{A}_n) = \operatorname{dist}(\varphi(g), \varphi(\mathcal{A}_n)) = \operatorname{dist}(\varphi(g), \mathcal{A}_n).$$

Therefore, any bent function is transformed by φ to some other bent function.

Similarly, $\mathrm{Aut}(\mathcal{B}_n) \subseteq \mathrm{Aut}(\mathcal{A}_n)$. For any automorphism $\psi \in \mathrm{Aut}(\mathcal{B}_n)$ and any affine function f

$$\mathrm{dist}(f, \mathcal{B}_n) = \mathrm{dist}(\psi(f), \psi(\mathcal{B}_n)) = \mathrm{dist}(\psi(f), \mathcal{B}_n).$$

In view of Propositions 4 and 5, hence it follows that $\psi(\mathcal{A}_n) = \mathcal{A}_n$.

We see that $\mathrm{Aut}(\mathcal{B}_n) = \mathrm{Aut}(\mathcal{A}_n)$. The form of this group follows from Proposition 6.

Thus, if mapping (6) transfers the class of bent functions into itself, then it is of the form

$$g(x) \to g(Ax + b) + \langle c, x \rangle + d.$$

Recall that the bent functions derived from one another by such a mapping are called affinely equivalent. It follows from the obtained results that a more general approach to equivalence of bent functions than that on the base of isometric mappings does not exist.

REFERENCES

1. O. A. Logachev, A. A. Salnikov, and V. V. Yashchenko, *Boolean Functions in Coding Theory and Cryptology*. MCCME, 2004 (in Russian).
2. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, **1–2**. North-Holland, Amsterdam, 1977.
3. N. N. Tokareva, Bent functions: results and applications. Survey. *Prikl. Diskretn. Mat.* (2009) **2**, 15–37 (in Russian).
4. N. N. Tokareva, Generalisations of bent functions. Survey. *Diskr. Anal. Issled. Oper.* (2010) **17**, 34–64 (in Russian).
5. R. L. McFarland, A family of difference sets in non-cyclic groups. *J. Comb. Theory, Ser.* A (1973) **15**, 1–10.
6. O. Rothaus, On bent functions. *J. Comb. Theory, Ser.* A (1976) **20**, 300–305.