# Automorphism group of the set of all bent functions

Natalia N. Tokareva [1]

Sobolev Institute of Mathematics,
Novosibirsk State University,
Novosibirsk, Russian Federation
e-mail: tokareva@math.nsc.ru

**Abstract.** Boolean function in even number of variables is called *bent* if it is at the maximal possible Hamming distance from the class of all affine Boolean functions. We have proven that every isometric mapping of the set of all Boolean functions into itself that transforms bent functions into bent functions is a combination of an affine transform of coordinates and an affine shift.

## 1 Introduction

Boolean function in $n$ variables $x = x_1, \ldots, x_n$ ($n$ is even) is called *bent* if it is at the maximal possible Hamming distance $2^{n-1} - 2^{(n/2)-1}$ from the class $\mathcal{A}_n$ of all affine Boolean functions [4]. Denote by $\mathcal{B}_n$ the set of all bent functions in $n$ variables.

Bent functions are intensively studied since sixties of XX. Now they have a lot of applications in coding theory, digital communications (in constructing codes for CDMA) and cryptography (e.g. in S-boxes resistant to linear cryptanalysis). See surveys [5, 6] of main results in this area. There are many open problems on bent functions. E. g. to count the exact number of them (or to get bounds for it), to find their constructions, etc. One of the problems is to find automorphism group of the set of all bent functions. It is done in this paper.

It is well known that $\mathcal{B}_n$ is closed under addition of affine functions and under affine transformations of variables. It means that for any bent function $g$ the function

$$g'(x) = g(Ax + b) + \langle c, x\rangle + d$$

is bent again, here $A$ is a binary nonsingular $n \times n$–matrix, $b$, $c$ are any binary vectors of length $n$, and $d$ is a constant. By $\langle c, x\rangle$ we denote the standard inner product, and by $+$ denote sum modulo 2. In our paper we prove that there are *no* other isometric transforms under which $\mathcal{B}_n$ is closed.

[1]This research is supported by the RF President grant for young Russian scientists (MK-1250.2009.1) and by the Russian Foundation for Basic Research (grants 08-01-00671, 09-01-00528, 10-01-00424).

Consider the paper structure. Firstly, we prove that for any non affine Boolean function $f$ there exists a bent function $g$ such that $f+g$ is not bent (Theorem 1). In other words, the set of bent functions is closed under addition of affine functions *only*. Then it follows that affine functions can be defined as all Boolean functions that are at the maximal possible distance from the set of all bent functions. There is, so to say, a *duality* between definitions for bent and affine functions. Further we prove that sets $\mathcal{B}_n$ and $\mathcal{A}_n$ have the same automorphism groups. This very group is a semidirect product of the general affine group $GA(n)$ and $\mathbb{Z}_2^{n+1}$ (Theorem 2).

## 2 Definitions

The *Hamming distance* (or briefly, *distance*) between two Boolean functions $f$ and $g$ is the number of distinct elements in their vectors of values, denote

$$dist(f,g) = |\{\ x : f(x) \neq g(x)\ \}|.$$

So, the set of all Boolean functions can be considered as a metric space. *Walsh–Hadamard transform* for a Boolean function $g$ in $n$ variables is

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

*Bent function* is a Boolean function $g$ in $n$ variables ($n$ is even) such that $W_g(y) = \pm 2^{n/2}$ for any $y$.

Equivalently, bent functions can be defined like this [1].

**Proposition 1.** *Boolean function $g$ is bent if and only if for any nonlinear $y$*

$$\sum_{x\in\mathbb{Z}_2^n} (-1)^{g(x)+g(x+y)} = 0.$$

It is well known the following property.

**Proposition 2.** *Any transform $g(x) \to g(Ax+b)+\langle c,x\rangle+d$ maps bent functions to bent functions.*

We need also the known MacFarland construction [3] for bent functions.

**Proposition 3.** *Let $\pi$ be any permutation on the set of all binary vectors of length $n/2$, let $h$ be any Boolean function in $n/2$ variables. Then*

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

*is a bent function in $n$ variables. Here $x', x''$ are of length $n/2$.*

Note that partitioning of $n$ variables into halves $x'$ and $x''$ can be any.

All these propositions we use in the proof of Theorem 1.

## 3 Shifts of bent functions

Here we prove the main (and most complicated) fact of the paper.

**Theorem 1.** *For any non affine Boolean function $f$ there exists a bent function $g$ such that $f+g$ is not bent.*

Let us give here an **idea of the proof** only. We do it in steps.

**Step 1.** Prove from the contrary. Suppose that for a fixed non affine $f$ and any bent function $g$ function $f+g$ is bent.

**Step 2.** Since $f$ is not affine there exists nonlinear $y$ such that $f(x)+f(x+y)$ is not a constant function. Hence, the set $D = \mathrm{supp}(f(x)+f(x+y))$ is not empty and does not coincide with $\mathbb{Z}_2^n$. W.l.o.g. suppose $y = 1$.

**Step 3.** Then we show that for any bent function $g$ it holds

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

**Step 4.** We take a face $\Gamma$ in Boolean cube $\mathbb{Z}_2^n$ such that $\dim \Gamma = n/2$ and both sets $\Gamma \cap D$ and $\Gamma \cap (\mathbb{Z}_2^n \setminus D)$ are not empty. W.l.o.g. we consider

$$\Gamma = \{(x', x'') : x'' = a\} \text{ for some } a \in \mathbb{Z}_2^{n/2}.$$

**Step 5.** Consider the subclass $G$ of bent functions of the MacFarland type $g(x', x'') = \langle x', \pi(x'')\rangle$, where $\pi(x'') = Ax''$ and $A$ is a nonsingular matrix.

**Step 6.** We show that in $G$ there exists a function $g$ such that

$$S = \sum_{x \in \Gamma \cap D} (-1)^{g(x)+g(x+y)} \neq 0. \tag{2}$$

**Step 7.** Then we get bent function $g'(x', x'') = g(x', x'') + t(x'')$ of MacFarland type, where

$$t(x'') = \begin{cases} 1, & \text{if } x'' = a; \\ 0, & \text{in other cases.} \end{cases}$$

**Step 8.** From (2) we obtain that equality (1) can not be satisfied for bent functions $g$ and $g'$ simultaneously. This contradiction proves the theorem.

## 4 Duality between definitions

Let us study the definitions of bent functions and affine functions.

For an even $n$ the class of bent functions is

$$\mathcal{B}_n = \{f : dist(f, \mathcal{A}_n) = N_{\max}\},$$

where

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

Is it possible to *invert* this definition? In other words is it true that $\mathcal{A}_n$ is the set of all Boolean functions that are at the maximal distance (say $N'_{\max}$) from $\mathcal{B}_n$? Here several questions arise. What is $N'_{\max}$? What is the connection between $\mathcal{A}_n$ and $\mathcal{A}'_n$, where

$$\mathcal{A}'_n = \{f : dist(f, \mathcal{B}_n) = N'_{\max}\}?$$

We have proven that this inverting of definitions is right in fact. There hold

**Proposition 4.** *It is true* $N'_{\max} = 2^{n-1} - 2^{(n/2)-1}$.

**Proposition 5.** *It holds* $\mathcal{A}_n = \mathcal{A}'_n$.

Thus, there is, so to say, a *duality* between definitions for bent and affine functions. Note that Theorem 1 is a key fact for it.

## 5 Automorphisms of bent functions

Mapping $\varphi$ of the set of all Boolean functions in $n$ variables into itself is *isometric*, if it preserves Hamming distances between functions, i. e.

$$dist(\varphi(f), \varphi(g)) = dist(f, g).$$

It is known that any such a mapping can be given as

$$g(x) \to g(s(x)) + f(x), \tag{3}$$

where $s : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ ia a substitution, $f$ is a Boolean function in $n$ variables. *Automorphism group* of a subset of Boolean functions $\mathcal{M}$ is the group of all isometric mappings of $\mathbb{Z}_2^n$ into itself that transform $\mathcal{M}$ again to $\mathcal{M}$. Denote it by $Aut(\mathcal{M})$.

Let $GA(n)$ be the *general affine group*,

$$GA(n) = GL(n) \ltimes \mathbb{Z}_2^n,$$

i. e. the group of all transforms $x \to Ax + b$, where $A$ is nonsingular, $b$ is any.

Note that the group $Aut(\mathcal{A}_n)$ is a semidirect product of the general affine group $GA(n)$ and $\mathbb{Z}_2^{n+1}$. Indeed, for any automorphism (3) of $\mathcal{A}_n$ the shift by function $f$ can be defined only by an affine function (as far as the image of zero function should be affine as well). The set of all affine functions in $n$ variables form a group isomorphic to $\mathbb{Z}_2^{n+1}$. It remains to note that every substitution $s$, as one knows, should be from $GA(n)$, see for instance, [2].

We prove the following fact.

**Theorem 2.** *It is true* $Aut(\mathcal{B}_n) = Aut(\mathcal{A}_n) = GA(n) \ltimes \mathbb{Z}_2^{n+1}$.

Thus, if (3) transforms bent functions into themselves then it has form

$$g(x) \to g(Ax + b) + \langle c, x \rangle + d. \tag{4}$$

Recall that bent functions that can be obtained one from the other via (4) are called *affine equivalent*. Now we see that there are no other isometric mappings that preserve bent functions. Thus, definition of affine equivalence of bent functions seems now indeed very natural.

# References


[1] *Logachev O. A., Sal'nikov A. A., Yashenko V. V.* Boolean functions in coding theory and cryptology. Moscow center for the uninterrupted mathematical education, 2004.

[2] *MacWilliams F. J., Sloane N. J. A.* The Theory of Error–Correcting Codes. Amsterdam: North–Holland, 1977.

[3] *McFarland R. L.* A family of difference sets in non-cyclic groups // J. of Combin. Theory, Ser. A. 1973. V. 15. N 1. P. 1–10.

[4] *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.

[5] *Tokareva N. N.* Bent functions: results and applications. Survey. // Prikladnaya Discretnaya Matematika (Applied Discrete Mathematics), 2009. V. 2. N 1. P. 15-37.

[6] *Tokareva N. N.* Generalizations of bent functions. Survey // Diskretnyi Analiz i Issledovanie Operacii (Discrete Analysis and Operation Research), 2010. V. 17, N 1. P. 34–64.