Math-Net.Ru

Общероссийский математический портал

N. A. Kolomees, Об одном свойстве квадратичных булевых функций, *Матем. вопр. криптогр.*, 2014, том 5, выпуск 2, 79–85

DOI: <https://doi.org/10.4213/mvk119>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.210.77.194

26 апреля 2023 г., 07:23:56

On a property of quadratic Boolean functions

N. A. Kolomeec ¹

Sobolev Institute of Mathematics SB RAS, Novosibirsk

Received 25.09.2013

Let a Boolean function f in $2k$ variables be affine on an affine subspace of dimension k if and only if f is affine on any its shift. Then it is proved that algebraic degree of f may be more than 2 only if there is no affine subspace of dimension k that f is affine on it.

Keywords: Boolean functions, bent functions, quadratic functions.

Об одном свойстве квадратичных булевых функций

Н. А. Коломеец

Институт математики им. С. Л. Соболева СО РАН, Новосибирск

Аннотация. Пусть булева функция f от $2k$ переменных такова, что если она является аффинной на аффинном подпространстве размерности k , то она является аффинной и на всех его сдвигах. Доказано, что тогда алгебраическая степень f может быть больше 2 только если f не является аффинной ни на каком аффинном подпространстве размерности k .

Ключевые слова: булевы функции, бент-функции, квадратичные функции.

¹The author is supported by the Russian Foundation for Basic Research (grant 12-01-31097) and by grant NSh-1939.2014.1 of President of Russia for Leading Scientific Schools.

1 Introduction

In this work we consider a property of Boolean functions connected to affine property on affine subspaces. Concerning bent functions, the property may be applied to construct new bent functions from the given one. Bent functions are Boolean functions with maximal nonlinearity. Such functions are important for cryptographic applications.

Let $\mathbb{Z}_2^n$ denote n -ary binary cube. A mapping $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ is called a Boolean function in n variables. Degree of algebraic normal form of a Boolean function is called an *algebraic degree* or briefly *degree*. A Boolean function is called *affine* if its algebraic degree is not more than 1 and *quadratic* if its algebraic degree is equal to 2. A set $U \subseteq \mathbb{Z}_2^n$ is called an *affine subspace* if $U = a \oplus L$, where $a \in \mathbb{Z}_2^n$ and L is a linear subspace of $\mathbb{Z}_2^n$; dimension of U is equal to the dimension of L . For vectors u and v we denote by $\langle u, v \rangle$ their inner product.

A Boolean function f in n variables is *affine on the set* $D \subseteq \mathbb{Z}_2^n$ if $f|_D(x) = \langle a, x \rangle \oplus c$ for some $a \in \mathbb{Z}_2^n$, $c \in \mathbb{Z}_2$. Denote by Ind_D the indicator function of the set D .

Boolean functions f and g in n variables are *affine equivalent* if there exist nonsingular $n \times n$ matrix A over $\mathbb{Z}_2$, vector $b \in \mathbb{Z}_2^n$ and affine function l in n variables such that $g(x) = f(Ax \oplus b) \oplus l(x)$. By *distance* between two Boolean functions we mean the *Hamming distance* between their vectors of values.

All quadratic Boolean functions have the following property.

Statement 1. *Let f be a quadratic Boolean function in $2k$ variables. Then f is affine on an affine subspace L of dimension k if and only if f is affine on $a \oplus L$ for any $a \in \mathbb{Z}_2^{2k}$.*

The proof of the statement follows from inequality $\deg(f(x) \oplus f(x \oplus s)) \leq 1$ for any $s \in \mathbb{Z}_2^{2k}$.

Of course, the statement is true for subspaces of dimension more than k , but in this case there exist quadratic functions which are not affine on all affine subspaces of such dimension k .

For bent functions such subspaces have an interesting application. A Boolean function f in even number of variables is called a *bent function* if it is on the maximal possible distance from the set of all affine functions. Bent functions were introduced by O. Rothaus [4]. These functions are the objects of great interest for specialists in cryptography and coding theory in view of many applications in these areas. Till now there are a lot of unsolved problems on bent functions (for example, see [5]).

It is known that if f is a bent function in $2k$ variables and f is affine on an affine subspace L of dimension k , then $f \oplus Ind_L$ is also a bent function (for example, see [2]). Moreover, two bent functions in $2k$ variables are on the minimal distance 2^k if and only if their difference is non-zero on an affine subspace and both functions are affine on this subspace (see [1]). So, such subspaces of dimension k may be used to construct a bent function from the given bent function in $2k$ variables.

A question appears: is there a Boolean function of degree more than 2 that satisfies the property mentioned in Statement 1? Here we prove that such a function may have

degree more than 2 if and only if there is no affine subspace of dimension k such that the function is affine on it.

2 An affine property on affine subspaces

Define the following property.

Property (*). A Boolean function f in $2k$ variables satisfies the property (*) if

1. If f is affine on an affine subspace L of dimension k , then f is affine on any shift of L .
2. There exists at least one affine subspace of dimension k such that f is affine on it.

Let us prove that only Boolean functions of degree no more than 2 satisfy this property.

Let $k, l \in \mathbb{N}, y \in \mathbb{Z}_2^l$. Denote

$$L_y^k = \{(x_1, \dots, x_k, y_1, \dots, y_l) \mid x_i \in \mathbb{Z}_2\}, \text{ where } y = (y_1, \dots, y_l).$$

At first we prove several lemmas.

Lemma 1. *The following statements are true.*

1. Let $n, m \in \mathbb{N}$ and s_1, s_2 be different elements of $\mathbb{Z}_2^m$.
Then $L_{s_1}^n \cup L_{s_2}^n$ is an affine subspace of dimension $n + 1$.
2. Let $n, m \in \mathbb{N}$ and s_1, s_2, s_3, s_4 be different elements of $\mathbb{Z}_2^m$.
Then $L_{s_1}^n \cup L_{s_2}^n \cup L_{s_3}^n \cup L_{s_4}^n$ is an affine subspace of dimension $n + 2 \iff s_1 \oplus s_2 \oplus s_3 \oplus s_4 = 0$.

Proof. The first statement is obvious. Prove the second statement. According to the first statement, $L_{s_1}^n \cup L_{s_2}^n$ and $L_{s_3}^n \cup L_{s_4}^n$ are disjoint affine subspaces of dimension $n + 1$. So, their union is an affine subspace if and only if both subspaces are shifts of the same linear subspace. It means that $s_1 \oplus s_2 = s_3 \oplus s_4$. The lemma is proved. $\square$

Lemma 2. Let $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ and s_1, s_2 be different elements of $\mathbb{Z}_2^{n-k}$, where $0 < k < n$, and for some $a_i \in \mathbb{Z}_2^k, c_i \in \mathbb{Z}_2$

$$f(x, s_i) = \langle a_i, x \rangle \oplus c_i \quad \forall x \in \mathbb{Z}_2^k, \quad i \in \{1, 2\}.$$

Then f is affine on $L_{s_1}^k \cup L_{s_2}^k$ if and only if $a_1 = a_2$.

Proof. Rewrite the equalities from the hypotheses. For any $r_1, r_2 \in \mathbb{Z}_2^{n-k}$

$$f(x, s_i) = \langle (a_i, r_i), (x, s_i) \rangle \oplus \langle r_i, s_i \rangle \oplus c_i.$$

So, the function f is affine on $L_{s_1}^k \cup L_{s_2}^k$ if and only if there exist r_1, r_2 such that

$$\begin{aligned} (a_1, r_1) &= (a_2, r_2), \\ \langle r_1, s_1 \rangle \oplus c_1 &= \langle r_2, s_2 \rangle \oplus c_2. \end{aligned}$$

It is equivalent to the following:

$$\begin{aligned} a_1 &= a_2, \\ \langle r_1, s_1 \oplus s_2 \rangle &= c_1 \oplus c_2. \end{aligned}$$

Because $s_1 \oplus s_2 \neq 0$, there exists r_1 that $\langle r_1, s_1 \oplus s_2 \rangle = c_1 \oplus c_2$. The lemma is proved. $\square$

Lemma 3. Let $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ and s_1, s_2, s_3, s_4 be different elements of $\mathbb{Z}_2^{n-k}$, $0 < k < n-1$, such that $s_1 \oplus s_2 \oplus s_3 \oplus s_4 = 0$, and for some $a_i \in \mathbb{Z}_2^k, c_i \in \mathbb{Z}_2$ it holds

$$f(x, s_i) = \langle a_i, x \rangle \oplus c_i \quad \forall x \in \mathbb{Z}_2^k, \quad i \in \{1, 2, 3, 4\}.$$

Then f is affine on $U = L_{s_1}^k \cup L_{s_2}^k \cup L_{s_3}^k \cup L_{s_4}^k$ if and only if $a_1 = a_2 = a_3 = a_4$ and $c_1 \oplus c_2 \oplus c_3 \oplus c_4 = 0$.

Proof. As in the proof of lemma 2, rewrite the equalities from the hypotheses. For any $r_1, r_2, r_3, r_4 \in \mathbb{Z}_2^{n-k}$

$$f(x, s_i) = \langle (a_i, r_i), (x, s_i) \rangle \oplus \langle r_i, s_i \rangle \oplus c_i.$$

Function f is affine on U if and only if there exist r_1, r_2, r_3, r_4 such that for any i, j

$$\begin{aligned} (a_i, r_i) &= (a_j, r_j), \\ \langle r_i, s_i \rangle \oplus c_i &= \langle r_j, s_j \rangle \oplus c_j. \end{aligned}$$

So, $a_1 = a_2 = a_3 = a_4$ and $r_1 = r_2 = r_3 = r_4$. Denoting r_1 by r we obtain equations

$$\begin{aligned} \langle r, s_2 \rangle \oplus c_2 &= \langle r, s_1 \rangle \oplus c_1, \\ \langle r, s_3 \rangle \oplus c_3 &= \langle r, s_1 \rangle \oplus c_1, \\ \langle r, s_4 \rangle \oplus c_4 &= \langle r, s_1 \rangle \oplus c_1. \end{aligned}$$

Replace the last equation by the sum of all equations:

$$\begin{aligned} \langle r, s_2 \rangle \oplus c_2 &= \langle r, s_1 \rangle \oplus c_1, \\ \langle r, s_3 \rangle \oplus c_3 &= \langle r, s_1 \rangle \oplus c_1, \\ \langle r, s_1 \oplus s_2 \oplus s_3 \oplus s_4 \rangle &= c_1 \oplus c_2 \oplus c_3 \oplus c_4. \end{aligned}$$

This system is equivalent to

$$\begin{aligned}\langle r, s_1 \oplus s_2 \rangle &= c_1 \oplus c_2, \\ \langle r, s_1 \oplus s_3 \rangle &= c_1 \oplus c_3, \\ c_1 \oplus c_2 \oplus c_3 \oplus c_4 &= 0.\end{aligned}$$

Since s_i are different, there exists r such that

$$\begin{aligned}\langle r, s_1 \oplus s_2 \rangle &= c_1 \oplus c_2, \\ \langle r, s_1 \oplus s_3 \rangle &= c_1 \oplus c_3.\end{aligned}$$

The lemma is proved. □

3 The property of quadratic Boolean functions

Definition 1. Function $h : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ is called *affine* if $h(x) = Ax \oplus b$ for some $m \times n$ matrix A and $b \in \mathbb{Z}_2^m$.

Let us prove the main result.

Theorem 1. Let $f : \mathbb{Z}_2^{2k} \rightarrow \mathbb{Z}_2$ satisfy the property (*). Then $\deg f \leq 2$.

Proof. Without loss of generality we suppose that f may be represented in the following way:

$$f(x, y) = \langle x, \pi(y) \rangle \oplus \varphi(y), \quad (1)$$

where $\pi : \mathbb{Z}_2^k \rightarrow \mathbb{Z}_2^k$, $\varphi : \mathbb{Z}_2^k \rightarrow \mathbb{Z}_2$. Indeed, if Boolean function satisfies the property (*) then there exists an affine subspace L of dimension k such that f is affine on $a \oplus L$ for any $a \in \mathbb{Z}_2^{2k}$. So, we can choose an affine transform that maps L to $L_{(0, \dots, 0)}^k$; then each $a \oplus L$ will be mapped to L_y^k , where $y \in \mathbb{Z}_2^k$, therefore, the function obtained will be affine on all L_y^k , i.e. it will be equal to $\langle a_y, x \rangle \oplus \langle b_y, y \rangle \oplus c_y$ for some $a_y, b_y \in \mathbb{Z}_2^k$ and $c_y \in \mathbb{Z}_2$. So, if $\pi(y) = a_y$ and $\varphi(y) = \langle b_y, y \rangle \oplus c_y$, we will get a function in the form (1) which is affine equivalent to f .

Note that representation (1) is similar to McFarland construction [3], more precisely, f is a bent function from McFarland class if and only if π is one-to-one function.

The statement $\deg f \leq 2$ for function with representation (1) is equivalent to the following:

1. π is an affine function,
2. $\deg \varphi \leq 2$.

Let us prove the first condition.

We use the mathematical induction by k . For $k = 1$ the statement is obvious. Suppose that for $1, \dots, k-1$ the condition is true. Show that it is true for k .

Consider values of function f for all x such that $x_i = 0$ for some $i \in \{1, \dots, k\}$. For simplicity suppose that $i = k$, i.e. $x_k = 0$. Let $y \in \mathbb{Z}_2^k$, denote by $\overline{y}$ the vector y without the last coordinate, so, $\overline{y} \in \mathbb{Z}_2^{k-1}$; also denote by $\overline{\pi}(y)$ the vector $\overline{\pi(y)}$. It is obvious that there exist different $s_1, s_2 \in \mathbb{Z}_2^k$ such that $\overline{\pi}(s_1) = \overline{\pi}(s_2)$. Therefore, according to lemma 2 function f is affine on $L_{(0,s_1)}^{k-1} \cup L_{(0,s_2)}^{k-1}$. Also by the property (*) function f is also affine on any shift of $L_{(0,s_1)}^{k-1} \cup L_{(0,s_2)}^{k-1}$, so, by lemma 2

$$\overline{\pi}(s_1 \oplus y) = \overline{\pi}(s_2 \oplus y) \quad \forall y \in \mathbb{Z}_2^k,$$

it is equivalent to

$$\overline{\pi}(y) = \overline{\pi}(s_1 \oplus s_2 \oplus y) \quad \forall y \in \mathbb{Z}_2^k.$$

Let $s = s_1 \oplus s_2$. Since $s_1 \neq s_2$, there exists a nonzero coordinate of s . For simplicity suppose that it is the last coordinate. Then

$$\overline{\pi}(\overline{y}, 1) = \overline{\pi}(\overline{y} \oplus \overline{s}, 0).$$

By induction we note that $\overline{\pi}(\overline{y}, 0)$ is affine, therefore

$$\overline{\pi}(\overline{y}, y_k) = \overline{\pi}(\overline{y}, 0) \oplus y_k \cdot (\overline{\pi}(\overline{s}, 0) \oplus \overline{\pi}(\mathbf{0}, 0)),$$

where $\mathbf{0}$ is zero element of $\mathbb{Z}_2^{k-1}$. Thus, $\overline{\pi}(y)$ is affine function. Since we could fix any x_i , π is also affine. So, the first point is proved.

Prove that $\deg \varphi \leq 2$. Since π is affine, we without loss of generality suppose that $\pi(y) = (y_1, \dots, y_r, A(y_1, \dots, y_r))$ for some matrix A of dimension $k-r$ (due to affine equivalence).

Using induction by k we have: for $k = 1$ and $k = 2$ the statement is obvious. Suppose that for $1, \dots, k-1$ the statement is true. Prove that $\deg \varphi \leq 2$ for k .

Consider values of function f for all x such that $x_{k-1} = 0$ and $x_k = 0$. Then according to lemma 3 the function f is affine on $U = L_{(0,0,0)}^{k-2} \cup L_{(0,0,1)}^{k-2} \cup L_{(0,1,0)}^{k-2} \cup L_{(0,1,1)}^{k-2}$ if and only if

$$\varphi(\mathbf{0}, 0, 0) \oplus \varphi(\mathbf{0}, 0, 1) \oplus \varphi(\mathbf{0}, 1, 0) \oplus \varphi(\mathbf{0}, 1, 1) = \mathbf{0}. \quad (2)$$

Since $\deg(\varphi(y) \oplus y_{k-1}y_k) \leq 2$ if and only if $\deg \varphi \leq 2$, it is sufficient to prove only one inequality. So, without loss of generality the equality (2) is true. Therefore, from the property (*) and lemma 3 it follows that

$$\varphi(y, 0, 0) \oplus \varphi(y, 0, 1) \oplus \varphi(y, 1, 0) \oplus \varphi(y, 1, 1) = \mathbf{0} \quad \forall y \in \mathbb{Z}_2^{k-2}.$$

Reduce φ by last two variables:

$$\begin{aligned} \varphi(y, u, v) &= (u \oplus 1)(v \oplus 1)\varphi(y, 0, 0) \oplus (u \oplus 1)v\varphi(y, 0, 1) \oplus \\ &\quad u(v \oplus 1)\varphi(y, 1, 0) \oplus uv\varphi(y, 1, 1). \end{aligned}$$

Therefore,

$$\begin{aligned}\varphi(y, u, v) &= (\varphi(y, 0, 0) \oplus \varphi(y, 0, 1) \oplus \varphi(y, 1, 0) \oplus \varphi(y, 1, 1))uv \oplus \\ &(\varphi(y, 0, 0) \oplus \varphi(y, 1, 0))u \oplus (\varphi(y, 0, 0) \oplus \varphi(y, 0, 1))v \oplus \varphi(y, 1, 1) = \\ &(\varphi(y, 0, 0) \oplus \varphi(y, 1, 0))u \oplus (\varphi(y, 0, 0) \oplus \varphi(y, 0, 1))v \oplus \varphi(y, 1, 1).\end{aligned}$$

As far as by induction $\deg \varphi(y, y_{k-1}, 0) \leq 2$ and $\deg \varphi(y, 0, y_k) \leq 2$, we have

$$\begin{aligned}\deg(\varphi(y, 0, 0) \oplus \varphi(y, 1, 0)) &\leq 1, \\ \deg(\varphi(y, 0, 0) \oplus \varphi(y, 0, 1)) &\leq 1.\end{aligned}$$

Also by induction $\deg \varphi(y, 1, 1) \leq 2$. So, $\deg \varphi \leq 2$. The theorem is proved. □

References

- [1] *Kolomeec N. A., Pavlov A. V.* Properties of Bent functions that are on the minimal possible distance // Discrete Applied Mathematics. — 2009. — No 4. — P. 5–20. (in Russian).
- [2] *Logachev O. A., Salnikov A. A., Yaschenko V. V.* Boolean functions in coding theory and cryptology. — Moscow : MCCME, 2004. — 470 p. (in Russian).
- [3] *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory, Ser. A. — 1973. — V. 15. — 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.* Nonlinear Boolean functions: bent functions and their generalizations // Saarbrücken: LAP LAMBERT Academic Publishing, 2011. — 180 P. — ISBN: 978-3-8433-0904-2. (In Russian)