Title:

Homogeneous bent functions of degree n in $2n$ variables do not exist for $n \geq 3$

Author:

Tianbing Xia, Jennifer Seberry, Josef Pieprzyk, Chris Charnes

Mailing address:

Dr. Tianbing Xia,
Center for Computer Security Research,
School of IT and CS,
University of Wollongong,
Northfields Avenue, Wollongong,
NSW 2522
AUSTRALIA

Tel: +61 02 42213076
FAX: +61 02 42214329
E-mail: txia@uow.edu.au

Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$

Tianbing Xia[1], Jennifer Seberry[1], Josef Pieprzyk[2] and Chris Charnes[3]

[1] Centre for Computer Security Research,
University of Wollongong, NSW, Australia
Email: [txia, j.seberry]@uow.edu.au,

[2] Department of Computing,
Division of Information and Communication Sciences,
Macquarie University, NSW, Australia
Email: josef@ics.mq.edu.au,

[3] Computer Science and Software Engineering,
the University of Melbourne, VIC, Australia
Email: charnes@cs.mu.OZ.AU

Abstract

We prove that homogeneous bent functions $f : GF(2)^{2n} \rightarrow GF(2)$ of degree n do not exist for $n > 3$. Consequently homogeneous bent functions must have degree $< n$ for $n > 3$.

Keywords: Bent, Homogeneous, Difference sets

1 Motivation

components. while the Ever since Rothaus defined bent functions [6], there have been numerous investigations of different aspects of bent functions. Most studies have concentrated on the construction of bent functions (C. Carlet in [1] for instance). All known constructions produce bent functions whose algebraic normal form always contains at least one quadratic term. Note that quadratic bent functions are completely known (up to affine equivalence). The orbits of the group $GL(8, 2)$ acting on the cubic bent functions modulo the second degree Boolean funcions, were enumerated in [2]. The complete list of different cubic functions in 8 variables is given in [2]; note again that these cubic functions contain at least one quadratic term. The first example of cubic and homogeneous bent function in 6 variables was given in [5] (all 30 3-homogeneous bent functions of 6 variables are classified).

Rothaus [6] showed that bent functions in $2n$ variables exist only if their degree is less than or equal to n (All 2-homogeneous bent functions are classified).

In this paper we show that the homogeneity requirement influences the degree of bent functions. We prove that homogeneous bent functions of degree n in $2n$ variables do not exist. The proof uses a certain decomposition of a Menon difference set, which corresponds to any bent function. In particular, there is no homogeneous bent function of degree 4 in 8 Boolean variables. The only exceptions are the 3-homogeneous Boolean functions of 6 variables, and the 2-homogeneous Boolean functions of 4 variables.

2   Background

An element x of the binary field $GF(2) = \mathcal{Z}/2$ can be regarded as being an integer (either 0 or 1). We use $x \oplus y$ and $\bigoplus x_i$ to denote addition in $GF(2)$, and $x + y$ and $\sum x_i$ to denote addition in $\mathcal{Z}$. Let V_n be the set of all vectors with n binary coordinates, thus V_n contains 2^n vectors from $\alpha_0 = (0, 0, \ldots, 0)$ to $\alpha_{2^n-1} = (1, 1, \ldots, 1)$. The *weight* $W(x)$ of a vector $x \in V_n$ is defined as

$$W(x) = \sum_{i=1}^n x_i$$

where $x = (x_1, \ldots, x_n)$ and $x_i \in GF(2)$ for $i = 1, \ldots, n$. In other words, $W(x)$ gives the number of ones in the binary representation of the vector x. A *Boolean function* $f : V_n \to GF(2)$ assigns binary values to vectors from V_n.

For $x \in GF(2)$, we define $(-1)^x$ using the interpretation of x as an integer. We also use $\oplus$ to denote *inner* (or coordinatewise) addition on V_n, where coordinates are added in $GF(2)$. (This operations is also known as bit-by-bit XOR.)

Throughout the paper we use the following notations, where $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$;

- *inner product* of x and y defined as $x \odot y = x_1 y_1 \oplus \cdots \oplus x_n y_n = \bigoplus_{i=1}^n x_i y_i$.

- *concatenation* of vector $x \in V_n$ by a vector $y \in V_m$ is defined as $x \mid y = (x_1, \cdots, x_n, y_1, \cdots, y_m)$. The vector $x \mid y \in V_{n+m}$.

A Boolean function $f(x) : GF(2)^n \to GF(2)$, $x = (x_1, \cdots, x_n)$ has unique algebraic normal form defined as

$$f(x) = \bigoplus_{k=1}^n \left(\bigoplus_{1 \le i_1 < i_2 < \cdots < i_k \le n} a_{i_1 \cdots i_k} x_{i_1} \cdots x_{i_k} \right), \text{ where } a_{i_1 \cdots i_k} \in GF(2).$$

Each term $x_{i_1} \cdots x_{i_k}$ is a product of precisely k co-ordinates.

We define the group ring $\mathcal{Z}[V_n] = \sum_{x \in V_n} a(x)x$, $a(x) \in \mathcal{Z}$. Addition in $\mathcal{Z}[V_n]$ is given by the rule

$$\left(\sum_{x \in V_n} a(x)x \right) + \left(\sum_{x \in V_n} b(x)x \right) = \sum_{x \in V_n} (a(x) + b(x))x.$$

Multiplication in $\mathcal{Z}[V_n]$ is given by

$$\left(\sum_{x \in V_n} a(x)x \right) \left(\sum_{y \in V_n} b(y)y \right) = \sum_{z \in V_n} \left(\sum_{x \oplus y = z} a(x)b(y) \right) z.$$

For any subset $\mathcal{A}$ of V_n we define as $\sum_{x \in A} x \in \mathcal{Z}[V_n]$ and by abusing the notation we will denote it by $\mathcal{A}$. We denote zero element "0" in V_n by 1 in $\mathcal{Z}[V_n]$.

Next we define the difference between two sets.

Definition 1 *Given two sets $\mathcal{A}$, $\mathcal{B} \subset V_n$. The difference between two sets is*

$$\mathcal{A} - \mathcal{B} = \sum_{x \in \mathcal{A}, y \in \mathcal{B}} x \oplus y \in \mathcal{Z}[V_n].$$

(This is also called a multiset or a collection by various authors.) In particular, if $\mathcal{A} = \mathcal{B}$, the difference is denoted as

$$\triangle \mathcal{A} = \mathcal{A} - \mathcal{A}.$$

If $\mathcal{A} \neq \mathcal{B}$ then the following notation is useful

$$\triangle(\mathcal{A}, \mathcal{B}) = (\mathcal{A} - \mathcal{B}) + (\mathcal{B} - \mathcal{A}).$$

If $\mathcal{A} = \emptyset$, then

$$\triangle \emptyset = 0 \ and \ \triangle(\emptyset, \mathcal{B}) = 0.$$

where $\mathcal{B} \in V_n$.

By convention, for sets $\mathcal{A}$, $\mathcal{B} \subset V_n$, the difference $\mathcal{A} - \mathcal{B}$ is a set of vectors $x \oplus y$ where vectors x and y run through the sets $\mathcal{A}$ and $\mathcal{B}$, respectively.

Definition 2 *A Boolean function $f(x) : V_n \to GF(2)$ is bent if*

$$2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x) \oplus (\beta \odot x)} = \pm 1$$

for all $\beta \in V_n$.

It is known that each Boolean function $f : V_n \to GF(2)$ has its unique representation in the algebraic normal form. Homogeneity requires algebraic normal forms to contain only terms of the same degree.

Definition 3 *A Boolean function $f : V_n \to GF(2)$ is homogeneous of degree k if it can be represented as*

$$f(x) = \bigoplus_{1 \leq i_1 < \cdots < i_k \leq n} a_{i_1 \cdots i_k} x_{i_1} \cdots x_{i_k},$$

where $a_{i_1 \cdots i_k} \in GF(2)$ and $x = (x_1, \ldots, x_n)$. co-ordinates.

4

3 Difference Sets

Let $f : V_{2n+2} \to GF(2)$ be a Boolean function. For the function $f(x)$, one can determine the set

$$D = \{x \in V_{2n+2} | f(x) = 1\}.$$

and

$$\begin{aligned}
D_1 &= \{x \in V_{2n} | f(x, 0, 0) = 1\}, \\
D_2 &= \{x \in V_{2n} | f(x, 0, 1) = 1\}, \\
D_3 &= \{x \in V_{2n} | f(x, 1, 0) = 1\}, \\
D_4 &= \{x \in V_{2n} | f(x, 1, 1) = 1\}
\end{aligned} \tag{1}$$

where $x = (x_1, \ldots, x_{2n})$ is a binary vector. We introduce the following notation:

$$P_1 = (0, 0), \quad P_2 = (0, 1), \quad P_3 = (1, 0), \quad P_4 = (1, 1) \tag{2}$$

Clearly, the set D can be represented as

$$D = \bigcup_{i=1}^{4} (D_i \mid P_i) \tag{3}$$

where the set $D_i \mid P_i$ contains all vectors from D_i extended by the vector P_i for $i = 1, 2, 3, 4$. Consider the difference set $\triangle D$. ¿From the definition, we get

$$\begin{aligned}
\triangle D &= \sum_{x \in D; \ y \in D} x \oplus y = \sum_{x \in \bigcup_{i=1}^{4} (D_i | P_i); \ y \in \bigcup_{j=1}^{4} (D_j | P_j)} x \oplus y \\
&= \sum_{i,j=1}^{4} (D_i \mid P_i) - (D_j \mid P_j)
\end{aligned}$$

After rearranging the differences, we obtain

$$\triangle D = \sum_{i=1}^{4} \triangle (D_i \mid P_i) + \sum_{i=1}^{3} \sum_{j=i+1}^{4} \triangle ((D_i \mid P_i), (D_j \mid P_j)). \tag{4}$$

The minimum weights of the sets D_i can be identified with the minimum weights of their vectors and

$$t_i = \min_{x \in D_i} W(x) \text{ for } i = 1, 2, 3, 4. \tag{5}$$

Lemma 1 *Given a homogeneous function $f : V_{2n+2} \to GF(2)$ of degree $n + 1$ and its sets D_i, $i = 1, 2, 3, 4$, then*

$$t_1 \geq n + 1, \ \ t_2 \geq n, \ \ t_3 \geq n, \ \ t_4 \geq n - 1.$$

where t_i is defined by Equation (5).

Proof. Suppose $t_1 < n + 1$. This means that there is a vector $x = (x_1, \cdots, x_{2n}, 0, 0)$ whose weight $W(x) \leq n$. Then at most n co-ordinates x_i, $i = 1, \cdots, 2n$ take on the value 1. The remainder of the co-ordinates take on the value zero. However, since $f(x)$ is a homogeneous Boolean function of degree $n + 1$ over V_{2n+2}, each term of the function has precisely $n + 1$ co-ordinates and so each term of the function is zero. Hence $f(x) = 0$ which implies that $x \notin D_1$. This contradicts the definition of D_1 and therefore we conclude that $t_1 > n$. The proof for other cases is similar and is omitted. $\square$

Remark. This is true only if you adopt the convention that the minimum of the empty set is ∞. statements are hold.

4 Upper Bound on the Degree of Homogeneous Bent Functions

We prove the next theorem via difference sets as it arose during the study of Hadamard difference sets.

Proposition 1 *Given a Boolean bent function $f : V_{2n+2} \to GF(2)$ (not necessary homogeneous) and sets D_i for $i = 1, 2, 3, 4$ defined for the bent function $f(x)$ by Formula (1). Let k_i denote the cardinality of the sets D_i (or $k_i = |D_i|$) for $i = 1, 2, 3, 4$. Then*

1. three of k_1, k_2, k_3, k_4 are equal and the remaining one is different, and

2. $\min(k_1, k_2, k_3, k_4) \geq 2^{2n-1} - 2^n$.

Proof. Define $T = \sum_{x \in V_{2n+2}} x$ which is the set of all vectors from V_{2n+2} and denote the vector $(0, \cdots, 0) \in V_{2n+2}$ as θ. The function $f(x)$ is bent if and only if the set $D = \{x \in V_{2n+2} | f(x) = 1\}$ is a difference set with parameters $(v, k, \lambda) = (2^{2n+2}, 2^{2n+1} \pm 2^n, 2^{2n} \pm 2^n)$ (see Kumar, Scholtz and Welch [3]). That is

$$\triangle D = (k - \lambda)\theta + \lambda T = 2^{2n}\theta + (2^{2n} \pm 2^n)T \tag{6}$$

On the other hand, from equation (4), we have

$$
\begin{aligned}
\triangle D \quad = \quad & (\sum_{i=1}^{4} \triangle D_i) \mid P_1 \\
& + (\triangle(D_1, D_2) + \triangle(D_3, D_4)) \mid P_2 \\
& + (\triangle(D_1, D_3) + \triangle(D_2, D_4)) \mid P_3 \\
& + (\triangle(D_1, D_4) + \triangle(D_2, D_3)) \mid P_4
\end{aligned}
\tag{7}
$$

If we compare (6) with (7), we get the following system of equations (see M. Xia [8] for details)

$$\sum_{i=1}^{4} \triangle D_i = 2^{2n}\theta' + \lambda T'$$

6

$$\triangle(D_1, D_2) + \triangle(D_3, D_4) = \lambda T' \tag{8}$$
$$\triangle(D_1, D_3) + \triangle(D_2, D_4) = \lambda T'$$
$$\triangle(D_1, D_4) + \triangle(D_2, D_3) = \lambda T'$$

where θ' is the zero vector in V_{2n} and $T' = \sum_{x \in V_{2n}} x$. We count the number of terms on both sides of (8) and obtain the following equations:

$$k_1^2 + k_2^2 + k_3^2 + k_4^2 = 2^{2n} + \lambda 2^{2n} \tag{9}$$
$$2k_1 k_2 + 2k_3 k_4 = \lambda 2^{2n}$$
$$2k_1 k_3 + 2k_2 k_4 = \lambda 2^{2n}$$
$$2k_1 k_4 + 2k_2 k_3 = \lambda 2^{2n}$$

Without loss of generality, we assume

$$k_1 \le k_2 \le k_3 \le k_4.$$

¿From (9), (10), (10) and (10) we get

$$(k_1 - k_2)^2 + (k_3 - k_4)^2 = 2^{2n},$$
$$(k_4 - k_1)(k_3 - k_2) = 0, \tag{10}$$
$$(k_2 - k_1)(k_4 - k_3) = 0.$$

Thus $k_1 = k_2 = k_3 < k_4$ or $k_1 < k_2 = k_3 = k_4$. This completes the part (1) of the proof.

We assume that k_1, k_2, k_3 equal k and k_4 equals to k'. Now equation (10) gives us

$$k - k' = \pm 2^n. \tag{11}$$

The cardinality of the set D is the sum of numbers of vectors in D_1, D_2, D_3, D_4, so

$$3k + k' = 2^{2n+1} \pm 2^n. \tag{12}$$

First we suppose the right side of the equation (12) is $2^{2n+1} - 2^n$. Then $\lambda = 2^{2n} - 2^n$. From (11) and (12) we get

$$k = 2^{2n-1} \text{ and } k' = 2^{2n-1} - 2^n,$$
$$\text{or} \tag{13}$$
$$k = 2^{2n-1} - 2^{n-1} \text{ and } k' = 2^{2n-1} + 2^{n-1}.$$

In this case

$$\min(k_1, k_2, k_3, k_4) = \min(k, k') \ge 2^{2n-1} - 2^n. \tag{14}$$

When the right side of the equation (12) is $2^{2n+1} + 2^n$, then $\lambda = 2^{2n} + 2^n$. ¿From (11) and (12) we have

$$k = 2^{2n-1} + 2^{n-1} \text{ and } k' = 2^{2n-1} - 2^{n-1},$$
$$\text{or} \tag{15}$$
$$k = 2^{2n-1} \text{ and } k' = 2^{2n-1} + 2^n.$$

Equation (14) holds as well. This proves part (2) and completes the proof of our proposition. $\qquad\square$

Theorem 1 *Let $f : V_{2n+2} \rightarrow GF(2)$ be a homogeneous Boolean function of degree $n+1$ and let $n \geq 3$. Then $f(x)$ is not bent.*

Proof. Suppose $f(x)$ is a bent function. Then the set $D = \{x|f(x) = 1\}$ is a difference set with parameters $(2^{2n+2}, 2^{2n+1} \pm 2^n, 2^{2n} \pm 2^n)$ [3]. Moreover,

$$D = \bigcup_{i=1}^{4} (D_i \mid P_i)$$

where the sets D_i are defined by Equation (1). ¿From Lemma 1 we know that the minimum weight of vectors in D_1 (denoted as t_1) is $t_1 \geq n + 1$. ¿From Proposition (1), we know the number of vectors in D_1 (denoted as k_1) is $k_1 \geq 2^{2n-1} - 2^n$. Consider the following set

$$D_0 = \{(x_1, \cdots, x_{2n}) \in V_{2n} | W(x) \geq n + 1\}.$$

It is obvious that $D_0 \supset D_1$. We denote the number of elements in D_0 by k_0. Clearly $k_0 \geq k_1$. But

$$
\begin{aligned}
k_0 &= \sum_{i=1}^{n} \binom{2n}{n+i} = \frac{1}{2}\left(\sum_{i=0}^{2n} \binom{2n}{i} - \binom{2n}{n}\right) \\
&= \frac{1}{2}\left(2^{2n} - \binom{2n}{n}\right) = 2^{2n-1} - \frac{1}{2}\binom{2n}{n}.
\end{aligned}
$$

It is easy to prove that $2^{n+1} < \binom{2n}{n}$ for any integer $n \geq 3$. Hence we can establish the following relation

$$k_0 < 2^{2n-1} - 2^n \leq k_1.$$

This leads to the contradiction which also completes the proof. $\square$

References

[1] C. Carlet, Two new classes of bent functions, *Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science*, Springer-Verlag, pp. 77-101, 1993.

[2] X. Hou, Cubic bent functions, *Discrete Mathematics*, 189, pp. 149-161, 1998.

[3] P. V. Kumar, R. A. Scholtz and L. R. Welch, Generalized bent functions and their properties, *Journal of Combinatorial Theory*, Ser. A, 40, pp. 90-107, 1985.

[4] J. Pieprzyk, C. Qu. Fast hashing and rotation-symmetric functions. *Journal of Universal Computer Science*, vol. 5, No. 1, pp. 20-31, 1999.

[5] C. Qu, J. Seberry, J. Pieprzyk, Homogeneous bent functions, *Applied Discrete Mathematics – Special Coding Theory Collection*, vol. 102, pp. 133-139, 2000.

[6] O. S. Rothaus, On "bent" functions, *Journal of Combinatorial Theory*, Ser. A, 20, pp. 300-305, 1976.

[7] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, 28, pp. 656-715, 1949.

[8] M. Xia, Some infinite classes of special Williamson matrices and difference sets, *Journal of Combinatorial Theory*, Ser. A, 61, pp. 230-242, 1992.

criterion, 1990.

Govaerts,

functions,

characteristics,