On the degree of homogeneous bent functions

Qing-shu Meng, Huan-guo Zhang, Min Yang, and Jing-song Cui

School of Computer,
Wuhan University, Wuhan 430072, Hubei, China
mqseagle@sohu.com

Abstract. It is well known that the degree of a $2m$-variable bent function is at most m. However, the case in homogeneous bent functions is not clear. In this paper, it is proved that there is no homogeneous bent functions of degree m in $2m$ variables when $m > 3$; there is no homogenous bent function of degree $m-1$ in 2m variables when $m > 4$; Generally, for any nonnegative integer k, there exists a positive integer N such that when $m > N$, there is no homogeneous bent functions of degree $m-k$ in $2m$ variables. In other words, we get a tighter upper bound on the degree of homogeneous bent functions. A conjecture is proposed that for any positive integer $k > 1$, there exists a positive integer N such that when $m > N$, there exists homogeneous bent function of degree k in $2m$ variables.
Keywords: cryptography, homogeneous bent functions, Walsh transform.

1 Introduction

Boolean functions have been of great interest in many fields of engineering and science, especially in cryptography. Boolean functions with highest possible nonlinearity are called bent functions, which was first proposed in [11] by Rothaus. As bent function has equal Hamming distance to all affine functions, it plays an important role in cryptography (in stream-ciphers, for instance), error correcting coding, and communication (modified into sequence used in CDMA[6]). Many works[5, 11, 1, 2, 13, 14] have been done in construction of bent functions and classification of bent functions.

Recently, several papers [10, 4, 12] on homogeneous functions have been published. Qu, Seberry and Pieprzyk discussed homogeneous bent functions of degree 3 in [10]. For 6-variable Boolean functions, there are 20 monomials of degree 3, so there are homogeneous Boolean functions of degree 3. It is easy to check each one of all these functions to see if they are bent functions. Using this method the authors gave all 30 homogeneous bent functions of degree 3. The authors also pointed out that the identified homogenous bent functions exhibited interesting combinatorial structure. From the paper [10], the following problems arise naturally: is there 8-variable and 10-variable homogeneous bent function of degree 3? The upper bound on the degree of $2m$-variable bent functions is m, which is a well-known result by Rothaus in [11]. Is it still true in homogeneous bent functions case? These two problems were solved in papers[4, 12]. In [4] by establishing the connection between invariant theory and the theory of bent function, Charnes, Rotteler and Beth gave some homogeneous bent functions of degree 3 in 8,10 and 12 variables with prescribed symmetry group action. And thus they proved the existence of homogeneous bent functions of degree 3 in $2m$ variables when $m > 2$. In [12] using difference sets it was proved that there exists no homogeneous bent function of degree m in $2m$ variables when $m > 3$. In other words, the upper bound on the degree of homogeneous bent function is at most $m - 1$. But we don't know whether or not that bound is a tight bound. Also we don't know whether or not there exist homogenous bent functions of other degree.

In this paper, the nonexistence of several kinds of homogeneous bent functions are proved and thus we get a tighter bound on the degree of homogeneous bent functions than the result in [12]. We first describe the relationship between the Walsh spectra of a Boolean function at partial points and the Walsh spectra of its sub-functions, and then describe a method to calculate the Hamming weight of the truth table of a homogenous Boolean function. Based on the just mentioned relationship and method, it is proved that there exists no homogeneous bent function of degree m in $2m$ variables when $m > 3$; there is no homogeneous bent function of degree $m - 1$ in $2m$ variables when $m > 4$; Generally for any nonnegative k, there exists a positive integer N such that when $m > N$, there is no homogeneous bent function of degree $m - k$ in $2m$ variables. And the relationship among the parameters k, N, m is given too. In other words, we get a tighter bound on the degree of homogeneous bent functions. To the problem that whether or not there exist homogeneous bent functions of other degree, we propose a conjecture that for any integer $k > 1$, there exists a positive integer N such that when $m > N$, there exist homogeneous bent functions of degree k in $2m$ variables.

The rest of the paper is organized as follows: in section 2 some basic definitions and notations is described. In section 3 the main results are given and finally a short conclusion is made in section 4.

2 Preliminary

For each subset $s \subseteq \{1, 2, \cdots, n\}$, there exists a corresponding vector $s = (s_1, s_2, \cdots, s_n)$ of dimension n by letting $s_i = 1$ if element i is in s else letting $s_i = 0$. And a vector $(s_1, s_2, \cdots, s_n)$ can be denoted by a integer s whose 2-adic expansion is just the vector $(s_1, s_2, \cdots, s_n)$, where s_i take value 0 or 1. Obviously, the set, the vector and the integer are isomorphic. So in this paper, if confusion is not caused, we will use the three notations for description convenience. Denote by F_2 the Galois field with two elements $\{0, 1\}$ and denote by F_2^n the vector space over F_2. Denote by $p_n = F_2[x_n, x_{n-1}, \cdots, x_1]/(x_n^2 - x_n, \cdots, x_1^2 - x_1)$ the algebra of all functions $F_2^n \to F_2$. For each subset $s \subseteq \{1, 2, \cdots, n\}$, denote $\prod_{i \in s} x_i \in p_n$ by x^s. The algebraic normal form of a Boolean function $F_2^n \to F_2$ can be written as $f(x) = \sum_{s=0}^{2^n-1} a_s x^s$, where $a_s \in F_2$. The degree of $f(x)$ is defined by

$$\max_{s \in \{0,1,\cdots,2^n-1\}, a_s \neq 0} H(s),$$

where $H(s)$ is the Hamming weight of vector s. For simplicity, the Hamming weight of the truth table of a Boolean function is called the Hamming weight of the Boolean function.

A function $f(x) = \sum_{s=0}^{2^n-1} a_s x^s$, where $a_s = 0$ if $H(s) \neq r$, is called a homogeneous function of degree r.

Definition 1[11]. Let $f(x), x \in F_2^n$ be a Boolean function, where $x = (x_n, x_{n-1}, \cdots, x_1)$, $w = (w_n, w_{n-1}, \cdots, w_1)$. And $w \cdot x = w_1x_1 + x_2w_2 + \cdots + x_nw_n \in F_2$ is the dot production of w and x. Define

$$s_f(w) = \sum_{x \in F_2^n} f(x)(-1)^{w \cdot x}$$

be the Walsh spectrum of $f(x)$ at point w.

The transform is called the Walsh transform.

Definition 2[11]. Let $f(x), x \in F_2^n$ be a Boolean function. If for any $w \in F_2^n$, $|\sum_{x \in F_2^n}(-1)^{f(x)}(-1)^{w \cdot x}| = 2^{n/2}$, then $f(x)$ is called a bent function.

By definition 1 and 2, it is easy to get that f(x) is a bent function if and only if

$$s_f(0) = 2^{n-1} \pm 2^{n/2-1}, s_f(w) = \pm 2^{n/2-1} \qquad \text{for} \qquad w \neq 0.$$

3 The bound on the degree of homogeneous bent functions

Lemma 1 [7]. Let

$$f(x_n, x_{n-1}, \cdots, x_1) = \sum_{i=0}^{2^k-1} \delta_{a_i}(x') f_i(x''),$$

where $x' = (x_n, x_{n-1}, \cdots, x_{n-k+1})$, $x'' = (x_{n-k}, x_{n-k-1}, \cdots, x_1)$, $f_i(x'') : F_2^{n-k} \to F_2, i = 0, 1, \cdots, 2^k - 1$, the integer representation of $a_i \in F_2^k$ is i, $\delta_{a_i}(x') = \begin{cases} 1, & a_i = x' \\ 0, & a_i \neq x' \end{cases}$, then

$$\begin{aligned}&[s_f(a_0, w''), s_f(a_1, w''), \cdots, s_f(a_{2^k-1}, w'')]^T \\ &= H_k[s_{f_0}(w''), s_{f_1}(w''), \cdots, s_{f_{2^k-1}}(w'')]^T, \end{aligned} \tag{1}$$

where $w = (w', w''), w'' \in F_2^{n-k}$.

Remark: especially, in formula (1), let $w'' = 0$, then

$$\begin{aligned}&[s_f(a_0, 0), s_f(a_1, 0), \cdots, s_f(a_{2^k-1}, 0)]^T \\ &= H_k[s_{f_0}(0), s_{f_1}(0), \cdots, s_{f_{2^k-1}}(0)]^T. \end{aligned} \tag{2}$$

The spectrum $s_f(a_i, 0)$ is the Walsh spectrum of $f(x)$ at the point $(a_i, 0)$, while $s_{f_i}(0)$ is the Hamming weight of the sub-function $f_i(x'')$(here $f_i(x'')$ is called the sub-function of $f(x)$). The idea of this lemma can be found in several other papers [5, 1, 3] in different forms.

3.1 The nonexistence of homogeneous bent function of degree m in $2m$ variables when $m > 3$

Theorem 1[8]. Let $n = 2m$ be an even integer. When $m > 3$, there exists no homogeneous bent function of degree m in n variables.

This result can also be found in [12], but the method in [8] is completely different from [12]. Furthermore, with the method in [8], some profounder results can be obtained easily in the following parts. Here we list the result for completeness on upper bound of homogenous bent functions.

3.2 The nonexistence of homogeneous bent function of degree $m-1$ in $2m$ variables when $m > 4$

Lemma 2. If $f(x)$ is an n-variable homogeneous function of degree $n-2$, then the Hamming weight of the function is at most $n(n-1)/2 + n + 1$.

Proof: For an n-variable homogenous Boolean function, it can be written into the following form

$$f(x_n, x_{n-1}, \cdots, x_1) = \sum_{i=1}^{n(n-1)/2} c_i g_i(x),$$

where $c_i \in F_2$ and $\{g_i(x) | i = 1, 2, \cdots, n(n-1)/2\}$ is the set of all monomials of degree $n-2$ in n variables. Among the set $\{0, 1, \cdots, 2^n - 1\}$ from which x takes value, there are $C_n^{n-2} = n(n-1)/2$ elements with Hamming weight equal to $n-2$, and there are $C_n^{n-1} + C_n^n = n+1$ elements with Hamming weight above $n-2$. Now let x take values whose Hamming weight $\geq n-2$, compute the value of function $f(x)$. It is easy to see the Hamming weight of an n-variable homogeneous function of degree $n-2$ is at most $n(n-1)/2 + n + 1$.

Lemma 3[9]. There exists no homogeneous bent function of degree 4 in 10 variables.

The proof of this lemma is omitted here for brevity.

Theorem 2. Let $n = 2m$ be an even integer. When $m > 4$, there exists no homogeneous bent function of degree $m-1$.

Proof: On one hand, in formula (2), let $k = m-1$, the function $f(x)$ is divided into 2^{m-1} sub-functions of $m+1$ variables. When

$$s_f(a_0, 0) = 2^{n-1} - 2^{n/2-1},$$

and

$$s_f(a_i, 0) = -2^{n/2-1}, i = 1, 2, \cdots, 2^{m-1} - 1,$$

the spectrum

$$s_{f_0}(0) = \frac{1}{2^{m-1}} \sum_{i=0}^{2^{m-1}-1} s_f(a_i, 0) = 2^{m-1}$$

is the minimum value, which is also the minimum Hamming weight of the first sub-function by the remark of lemma 1.

On the other hand, by lemma 2, the Hamming weight of any $m+1$-variable homogeneous function of degree $m-1$ is at most $m(m+1)/2+m+2$. It is easy to see that when $m>5$ the following inequality holds:

$$2^{m-1} > m(m+1)/2 + m + 2. \tag{3}$$

That is, when $m>5$, all homogeneous functions of degree $m-1$ in $m+1$ variables cannot satisfy the necessary condition of a bent function. By lemma 3, there exists no homogeneous bent function of degree 4 in 10 variables. So the theorem is proved. End.

A more general result is described in the following theorem.

Theorem 3. For any nonnegative integer k, there exists a positive integer N such that when $m>N$, there exists no $2m$-variable homogeneous bent function of degree $m-k$.

Proof: On one hand, in formula (2) a $2m$-variable function can be divided into 2^{m-1} sub-functions in $m+1$ variables. Similar to the case in theorem 2, the Hamming weight of the first sub-function of a bent function is at least 2^{m-1}.

On the other hand, for any a $m+1$-variable homogeneous Boolean function of degree $m-k$, it can be written into

$$f(x) = \sum_{i=1}^{C_{m+1}^{m-k}} c_i g_i(x),$$

where $c_i \in F_2$ and $\{g_i(x)|i=1,2,\cdots,C_{m+1}^{m-k}\}$ is the set of all monomials of degree $m-k$ in $m+1$ variables. Among the set $\{0,1,\cdots,2^n-1\}$ from which x takes value, there are C_{m+1}^{m-k} elements with Hamming weight equal to $m-k$, and there are $C_{m+1}^{m-k+1}+C_{m+1}^{m-k+2}+\cdots+C_{m+1}^{m+1}$ elements with Hamming weight above $m-k$. Now let x takes the values whose Hamming weight $\geq m-k$, compute the value of function $f(x)$. It is easy to see the hamming weight of homogeneous functions of degree $m-k$ in $m+1$ variables is at most

$$C_{m+1}^{m-k} + C_{m+1}^{m-k+1} + \cdots + C_{m+1}^{m+1} = C_{m+1}^{0} + C_{m+1}^{1} + \cdots + C_{m+1}^{k+1}.$$

When

$$2^{m-1} > C_{m+1}^{0} + C_{m+1}^{1} + \cdots + C_{m+1}^{k+1}, \tag{4}$$

there exists no homogenous bent function. For any given nonnegative integer k, it is easy to prove that there exists an integer N such that when $m>N$, the formula (4) holds. That is, all homogeneous functions cannot satisfy the necessary condition of a bent function. End.

Remark:

1). Let $k=2$, there exists $N=8$, such that when $m>8$, there exists no $2m$-variable homogeneous bent function of degree $m-2$. Similarly k can take values $3,4,\cdots$. Obviously, in the case of homogeneous bent function, the upper bound of degree is not fixed, but varies according to the number of variables. That is, the degree bound of homogeneous bent function is more complex than the case of bent functions.

2). We also should notice that the parameter N obtained by formula (4) is not tight. This can be seen from the following fact: for $k = 1$, by formula (4), we get $N = 5$, but by theorem 2, we get $N = 4$. Thus other method, like the method in [9], is needed if we want to obtain a tight bound. Naturally or intuitively, we conjecture that for any integer $k > 1$, there exists an integer N such that when $m > N$, there exist $2m$-variable homogeneous bent functions of degree k.

4 Conclusion

In this paper, we get several results on the nonexistence of homogeneous bent functions of special kinds. In other words, we get tighter bound on the degree of homogenous bent functions than the result in paper [12]. However the exact upper bound is still under research. Intuitively we proposed a conjecture that for any integer $k > 1$, there exists a positive integer N such that when $m > N$, there exist homogeneous bent functions of degree k in $2m$ variables. To prove this conjecture, we plan to construct a homogeneous bent function of degree 4 first and then to prove the conjecture.

References

1. C. Carlet. Two new classes of bent functions, Advance in cryptology-eurocrypt'93(LNCS765),1994. 77-101.
2. C. Carlet, Generalized partial spreads, IEEE Trans.on I.T. Vol 41,No.5, 1995. 1482-1487.
3. C. Carlet, P. Sarkar. Spectral domain analysis of correlation immune and resilient Boolean functions, Finite Fields and Applications (journal) Vol.l8, 2002.120-130.
4. C. Charnes, M. Rotteler, T. Beth. Homogeneous bent functions, invariants, and designs. Designs, Codes and Cryptography. Kluewer Acdemmic publishers, Vol.26,2002. 139-154.
5. J. F. Dillon. Elementary Hadmard Difference Sets. Ph. D. Dissertation, Unv. Maryland, 1974.
6. J.D.Olsen, R.A.Scholtz, L.R.Welch. Bent-function sequences, IEEE Trans. on I.T., Vol. IT-28, No.6,1982.. 858-864.
7. Qing-shu Meng, Huan-guo Zhang,Zhang-yi Wang, et al. Designing bent functions using evolving computing. to appear in acta electronica sinica, No.11,2004.
8. Qing-shu Meng, Huan-guo Zhang, Zhong-ping Qing,et al. A simple proof for the nonexistence of homogenous bent function of degee m in $2m$ variables with $m > 3$. to appear in Wuhan university Journal of Natural Sciences.
9. Qing-shu Meng, Min Yang, Huan-guo Zhang, et al. An novel algorithm enumerating bent functions, http://eprint.iacr.org,2004/274.
10. Chengxin Qu, J. Seberry, J.Pieprzyk. Homogeneous bent functions. Discrete Applied Mathematics. 102, 2000.133-139.
11. Rothaus. O. S., On "bent" functions, Journal of Combinatorial Theory,series A 20, 1976.300-305.
12. Tianbing Xia, J. Seberry, J.Pieprzyk, C. Charnes. Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$, Discrete Applied Mathematics. 142, 2004.127-132.

13. Xiang-dong Hou, Results on bent functions. Journal of Combinatorial Theory, series A 80,1997.232-246.
14. Xiang-dong Hou, Cubic bent funcitons. Discrete Mathematics, Vol.189,1998.149-161.