A NOVEL ALGORITHM ENUMERATING BENT FUNCTIONS*

Meng Qing-shu Yang min Zhang huan-guo
Cui jing-song

October 21, 2004

Abstract

By the relationship between the Walsh spectra at partial points and the Walsh spectra of its sub-functions, by the action of general linear group on the set of Boolean functions, and by the Reed-Muller transform, a novel method is developed, which can theoretically construct all bent functions. With this method, we enumerate all bent functions in 6 variables; in 8-variable case, our method is more efficient than the method presented by Clark though we still can not enumerate all bent functions; enumeration of all homogeneous bent functions of degree 3 in eight variables can be done in one minute by a P4 1.7G HZ computer; construction of homogenous bent function of degree 3 in 10 variables is efficient too; the nonexistence of homogeneous bent functions in 10 variables of degree 4 is proved.

Keywords: bent functions, Walsh transformation, Reed-Muller transform, group action.

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 [17] 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 communication). Many works [3, 4, 9, 17, 19, 20, 21] have been done in construction and classification of bent functions.

Recently, several papers [7, 15, 18] on homogeneous functions have been published. Qu, Seberry and Pieprzyk discussed homogeneous bent functions of degree 3 in [15]. For 6-variable Boolean functions, there are 20 monomials of degree 3, so there are 2^{20} homogeneous Boolean functions of degree 3. It is easy to check each one of all these 2^{20} functions to see if they are bent functions.

*email:mqseagle@sohu.com

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 [15], the following problems arise naturally: is there 8-variable and 10-variable homogeneous bent function of degree 3? In [7] 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 this paper, we mainly aim at construction of all homogenous bent functions in 8 variables of degree 3. and the construction of homogenous bent functions of degree in 10 variables. As there are $C_8^3 = 56$ monomials of degree 3 in 8 variables, so there are 2^{56} homogenous Boolean functions of degree 3 in 8 variables. Obviously it is infeasible to check one by one if they are bent functions. It is also impossible in 10 variables case. In order to make our construction possible, we first describe the relationship between the Walsh spectra of a Boolean function $f(x)$ at partial points and the Walsh spectra of its subfunctions. Another way to low the complexity is to classify the set of Boolean functions by an equivalent relationship. Two functions $f(x), g(x)$ are equivalent if there exists a matrix A in $GL(n, 2)$ such that $f(x) = g(Ax)$. If two functions are equivalent then the spectra of one function is the linearly rearranged spectra of the other function. That is, they have same Walsh spectra distribution without consideration of the order. With above two steps, a novel algorithm is given which theoretically can produce all bent functions. As application, we enumerate all homogenous bent function of degree 3 in 8 variables in only one minute in P4 1.7G HZ computer. And it is easy to construction homogenous bent functions of degree 3 in 10 variables. The nonexistence of homogenous bent functions of degree 4 in 10 variables is proved. we enumerate all bent functions in 6 variables, thus the number of functions is obtained, which will be useful in the studying of counting problem of bent functions.

The rest of the paper is organized as follows: in section 2 some basic definitions and notations are described. In section 3 the algorithm 1 is given and in section 4 some applications are given and finally a short conclusion is made in section 5.

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 $p_n = F_2[x_1, x_2, \cdots, x_n]/(x_1^2 - x_1, \cdots, x_n^2 - x_n)$

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 $a_s \in F_2^n$. 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. Denote by $AF(n)$ the set of functions with $deg(f) \leq 1$

Definition 1[17]. Let $f(x) : F_2^n \to F_2$ be a Boolean function, where $x = (x_1, x_2, \cdots, x_n)$, $w = (w_1, w_2, \cdots, w_n)$. 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

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

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

The transform is called the Walsh transform.

Definition 2[17]. Let $f(x), x \in F_2^n$ be Boolean function. If for any $w \in F_2^n, |s_{(f)}| = 2^{n/2}$, then $f(x)$ is called a bent function.

2.1 The Reed-Muller transform of Boolean functions

A Boolean function can be written as $f(x) = \sum_{s=0}^{2^n-1} a_s x^s$, where $a^s \in F_2^n$. Let $x = 0, 1, \cdots, 2^n - 1$, then:

$$[f(0), f(1), \cdots, f(2^n - 1)] = [a_0, a_1, \cdots, a_{2^n-1}]A_n,$$

where A_n can be defined recursively

$$A_0 = [1], A_n = \left[\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right] \otimes A_{n-1} = \left[\begin{array}{cc} A_{n-1} & A_{n-1} \\ 0 & A_{n-1} \end{array}\right].$$

By the form of A_n, there exists a fast algorithm to transform between the truth table of a Boolean function and its coefficients of its algebraic normal form. By the way, the matrix A_n is different from the Hadamard matrix H_n.

2.2 The action of general linear group on Boolean functions

Definition 3. Denote by $GL(n, 2)$ the set of all nonsingular matrix of order n, i.e. the general linear group. All permutation matrix of order n forms a group, denoted by $PL(n, 2)$. If the Hamming weight of every column and every row of a matrix is one, the matrix is called a permutation matrix. Obviously, $PL(n, 2)$ is a subgroup of $GL(n, 2)$.

Denote by $AGL(n, 2)$ the group $\{(A, b) | A \in GL(n, 2), b \in F_2^n\}$. The group operation is defined by

$$(A, u)(B, w) = (AB, A(w) + u)$$

$$(A,u)^{-1} = (A^{-1}, A^{-1}(u),$$

where $(A,u),(B,w) \in AGL(n,2)$.

Denote by $G(n,2)$ the group of $\{(A,b)|A \in AGL(n,2), b \in AF(n)\}$. The group operation is defined by

$$(A,u)(B,w) = (AB, A(w)+U)$$

$$(A,u)^{-1} = (A^{-1}, A^{-1}(u)$$

The action of group G on Boolean functions is defined by:

$$\begin{array}{cc} c: & p_n \to p_n \\ by: & f(x) \to f(Ax)+b(x) \end{array} \quad ,$$

where $c = (A,b) \in G(n,2)$.

The action of group $AG(n,2)$ on the space F_2^n is defined by

$$\begin{array}{cc} c: & F_2^n \to F_2^n \\ by: & x \to Ax+b \end{array} \quad ,$$

where $c = (A,b) \in AG(n,2)$. As the groups $AG(n,2), GL(n,2), PL(n,2)$ are subgroups of $G(n,2)$, the action of $AGL(n,2), GL(n,2), PL(n,2)$ on the boolean functions is the special case of $G(n,2)$. The functions in the set $\{g(x)|g(x) = f(Ax), A \in G(n,2)\}$ are called one equivalent class. For detail see [11]. The spectra of $g(x)$ is just the linearly rearranged spectra of $f(x)$. That is, the function in one equivalent class have same Walsh spectra distribution. So, if one function in a equivalent class is a bent function, then all functions in the same equivalent class are bent functions too.

3 Algorithm

Lemma 1 [12]. Let

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=0}^{2^k-1} \delta_{a_i}(x') f_i(x''),$$

where $x' = (x_1, x_2, \cdots, x_k)$, $x'' = (x_{k+1}, x_{k+2}, \cdots, x_n)$, $f_i(x'') : F_2^{n-k} \to F_2, i = 0, 1, \cdots, 2^k-1$, 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

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

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

Corollary 1[12]. Let

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=0}^{2^k-1} \delta_{a_i}(x') f_i(x''),$$

where $x' = (x_1, x_2, \cdots, x_k)$, $x'' = (x_{k+1}, x_{k+2}, \cdots, x_n)$, $f_i(x'') : F_2^{n-k} \to F_2, i = 0, 1, \cdots, 2^k-1$, the integer representation of $a_i \in F_2^k$ is i, $\delta_{a_i}(x') = \left\{ \begin{array}{ll} 1, & a_i = x' \\ 0, & a_i \neq x' \end{array} \right.$, then

$$[s_{(f_0)}(w''), s_{(f_1)}(w''), \cdots, s_{(f_{(f_{2^k-1})})}(w'')]$$

$$= 2^{-k} H_k [s_{(f)}(a_0, w''), s_{(f)}(a_1, w''), \cdots, s_{(f)}(a_{2^k-1}, w'')].$$

especially, if $f(x)$ is bent and $w'' = 0$, then:

$$[s_{(f_0)}(0), s_{(f_1)}(0), \cdots, s_{(f_{(f_{2^k-1})})}(0)]$$

$$= 2^{n/2-k} H_k [(-1)^{\widetilde{f(a_0,0)}}, (-1)^{\widetilde{f(a_1,0)}}, \cdots, (-1)^{\widetilde{f(a_{2^k-1},0)}}]^T, \tag{2}$$

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

Remark to lemma 1 and corollary 1. In formula (1), let $w'' = 0$, then

$$[s_{(f)}(a_0, 0), s_{(f)}(a_1, 0), \cdots, s_{(f)}(a_{2^k-1}, 0)]$$

$$= H_k [s_{(f_0)}(0), s_{(f_1)}(0), \cdots, s_{(f_{2^k-1})}(0)]^T.$$

This result is proved in [5]. The first term in formula (2)

$$s_{(f_0)}(0) = 2^{n/2-k} \sum_{i=0}^{2^k-1} (-1)^{\widetilde{f(a_i,0)}},$$

which corresponds to theorem 5 in [2], a generalization of remark 6.1.14 of Dillon [9] and was proved by Carlet [3]. So the relationship between the spectra of a boolean function and the spectra of its subfunctions is already known, but here we give a general description.

Here the functions $f_i(x'')$ is called the subfunctions of function $f(x)$.

Corollary 2. If

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=0}^{2^k-1} \delta_{a_i}(x') f_i(x''),$$

is a bent function, then every spectrum $s_{(f_i)}(w'')$ can take the following $2^k + 1$ values:

$$\{(2^k - j)2^{n/2} - j2^{n/2}\}/2^k = (2^k - 2j)2^{n/2-k}, j = 0, 1, \cdots, 2^k.$$

All these values are called the k-th Granted-value.

Proof. Once $s_{(f)}(a_i, w), i = 0, 1, \cdots, 2^k - 1$ take one of the two possible values $\{\pm 2^{n/2}\}$, the value of $s_{(f_i)}(w), i = 0, 1, \cdots, 2^k - 1$ is fixed by formula (1). The number of different values the spectrum $s_{(f_i)}(w)$ can have only depends on the number of positive and negative values of $s_{(f)}(a_i, w), i = 0, 1, \cdots, 2^k - 1$. The corollary is proved.

For example, let $k = 1$, a bent function $f(x)$ is divided into two sub-functions $f_0(x''), f_1(x'')$. The Walsh spectra the two sub-functions can take are $0, \pm 2^{n/2}$. The two sub-functions is called complementary plateaued functions. Let $k = 2$, we get five values: $0, \pm 2^{n/2-1}, \pm 2^{n/2}$. Similarly we can let $k = 3, 4, \cdots, n/2 - 1$. Some properties in the case $k = 1, k = 2$ are discussed in [2, 6, 22].

Now we consider a concrete case: the number of variables $n = 8$, with $k = 1$, the set of the first Granted-value is $\{0, \pm 16\}$. With $k = 2$, the set of the 2nd Granted-value is $\{0, \pm 8, \pm 16\}$. With $k = 3$, the set of the 3rd Granted-value is $\{0, \pm 4, \pm 8, \pm 12, \pm 16\}$.

3.1 Algorithm 1: new construction of bent functions

Let $n = 2m$ be an even integer bigger than 4. in [17], Rothaus pointed out that the degree of a $2m$-variable bent function is at most m and that a function, which is the addition of a bent function and a affine linear function, is also a bent function. In order to obtain computation advantage, the affine linear function can be omitted. So a possible bent function can be written into $f(x) = \sum_{s=0}^{2^n-1} a_s x^s$, where $a_s = 0$ if $H(s) > m$ or $H(s) = 1$. Denote by B_n the set

$$\{f(x) = \sum_{s=0}^{2^{n-1}} a_s x^s | a_s = 0 \,\text{if}\, H(s) > m \,\text{or}\, H(s) = 1\} = \{f(x) = \sum_{i=0}^{2^k-1} \delta_{a_i}(x') f_i(x'')\},$$

denote by $B_{n,n-k,i}$ the set of the i-th $(n-k)$-variable subfuncitons $\{f_i(x'')\}$ of n-variable functions $f(x) \in B_n$.

1. Initialization. Let $k = m - 1, m - 2, \cdots, 1$. Compute the granted-value by the corollary 2. The 0th Granted-value set contains just one value $2^{n/2}$. Set $k = m - 1$;

2. For any a function in B_n, the function is divided into 2^k sub-functions. Used the Reed-Muller transform, compute the truth table of the first $(m+1)$-variable sub-function from its algebraic form. Use Walsh-Hadamard transform, compute the Walsh spectra from its truth table. Check if the Walsh spectra take values from the $(m-1)$-th Granted-value. If yes, reserve the sub-function, else discard the sub-function. The reserved sub-functions set is denoted by R_{m+1}.

3. Compute the Walsh spectra of the first $(n-k+1)$-variable subfunctions set

$$\{(x_{n-k+1} + 1) f_0(x') + x_{n-k+1} f_1(x') | f_0(x') \in R_{n-k}, f_1(x') \in B_{n,n-k,1}\},$$

and check one by one if they take values in the $(k-1)$-Granted -values. If yes, reserved it, else discard it. The set of the reserved functions is denoted by R_{n-k+1}.

4. $k = k - 1$, if $k = 0$, output the bent functions set R_n,end the program else goto step 3.

In practical application, k be any integer in set $\{m-1, m-2, \cdots, 1, 0\}$ according to computing convenience.

4 Applications

4.1 The enumeration of bent functions in 6 variables

The algorithm 1 theoretically can construct all bent functions. Practically, it is easy to construct all bent functions in 6 variables. The set of possible bent function in 6 variables is $B_6 = \{f(x)|x \in F_2^6, f(x) = \sum_{s=0}^{63} a_s x^s, a_s = 0$ if $H(s) > 3$ or $H(s) = 1\}$, So there are 2^{35} functions altogether. As 2^{35} is not a big number, you can compute the truth table from the algebraic normal form and get the Walsh spectra to see if they are bent functions. But it is time-consuming. With our algorithm, it is more efficient.

The set B_6 can also be expressed as the set:

$$\{\sum_{s=0}^{2^n-1} a_s x^s = \sum_{s=0}^{31} a_s x^s + \sum_{s=32}^{63} a_s x^s\},$$

and denote the first 5-variable sub-functions by

$$B_{6,5,0} = \{f_0(x')|f(x) = (x_6+1)f_0(x') + x_6 f_1(x'), f(x) \in B_6\},$$

and correspondingly $B_{6,5,1}$.

1. Set $k = 1$, the first granted-value set is $\{0, \pm 8\}$.

2. Check all functions in set $B_{6,5,0}$ by the first Granted-Value set, only 215706 functions are reserved, denoted by R_5.

3. Consider the set

$$\{(x_6+1)f_0(x') + x_6 f_1(x')|f_0(x') \in R_5, f_1(x') \in B_{6,5,1}\}.$$

Similarly, check if they satisfy the 0th Granted-value condition. There are 42386176 bent functions reserved. Denote the set of all these bent functions as R_6. Consider the following fact that if $f(x)$ is a bent function then for any affine function $l(x)$, $f(x)+l(x)$ is also a bent function. We get all bent functions in 6 variables:

$$\{f(x)|f(x) = g(x) + l(x), g(x) \in R_6, l(x) \in AF(6)\},$$

the cardinality of which is 128×42386176.

The number of bent functions in 6 variables is discussed in [1, 16, 10]. Adams and Tavares[1] estimated 48201728 as the number of bent function including linear based bent function and those constructed from four bent functions. 49774592 was estimated in [16] as the low bound of bent functions. Wang [10] gave a upper bound on the number of bent functions. Here the exact number of all 6-variable bent functions is given, which is helpful in studying the counting of bent function and further study of bent function. $N = 6$ maybe be the only case for which we can give the exact number of bent functions.

4.2 The enumeration of homogeneous bent functions of degree 3 in 8 variables

The case in 8 variables is not as the case in 6 variables. As there are $C_8^4 + C_8^3 + C_8^2$ monomials in 8 variables, all possible bent functions in 8 variables is 2^{154}. Our numerical experiment shows it is impossible to enumerate all bent functions in 8 variables with our algorithm 1 though it is more efficient to construct bent functions than the heuristic method in[8]. After all 2^{154} is a too big number. But we can restrict the algebraic normal form of Boolean function that we can get some special kind of bent functions in 8 variables, for example, homogenous bent functions. We first search for homogenous bent functions of degree 4 in 8 variables. In the algorithm 1, let $k = 3$, unlucky enough, no function is reserved in set R_5. This lead us to think that there exists no homogenous bent function of degree m in 2m variables with $m > 3$. This is a result in [18, 13]. Further, we get a more general result that for any integer $k > 2$, there exists a integer N such that with $m > N$, there exists no homogenous bent function of degree $m - k$ in $2m$ variables [14]. As there exists no homogenous bent function of degree 4, we turn to construct homogenous bent function of degree 3 in 8 variables. The existence already had been solved by Charnes[7]. Here we want to enumerate all homogenous bent functions of degree 3 in 8 variables.

Though there are $2^{C_8^3} = 2^{56}$ homogenous functions, it is still possible to enumerate all 8-variable 3-degree homogenous bent functions using the algorithm 1 directly, but it is time-consuming!

In order to enumerate all homogenous bent functions efficiently, a modification to the algorithm 1 is necessary.

Algorithm 2. Let $n = 2m$ be an even integer bigger than 4. All possible bent functions can be written into $f(x) = \sum_{s=0}^{2^n-1} a_s x^s$, where $a_s = 0$ if $H(s) > m$ or $H(s) = 1$. Denote by B_n the set

$$\{f(x) = \sum_{s=0}^{2^{n-1}} a_s x^s\} = \{f(x) = \sum_{i=0}^{2^k-1} \delta_{a_i}(x') f_i(x'')\}.$$

Denote by $B_{n,n-k,i}$ the corresponding set of the ith $(n-k)$-variable subfuncitons $\{f_i(x'')\}$ of the n-variable functions $f(x) \in B_n$.

1. Initialization. Let $k = m-1, m-2, \cdots, 1$. Compute the k-th Granted-value by the corollary 2. Set $k = m - 1$.

2. For any function in B_n, the function is divided into 2^k sub-functions. Used the Reed-Muller transform, compute the truth table of the first $(m+1)$-variable subfunction from its algebraic form. Use Walsh transform, compute the Walsh spectra from its truth table. Check if the Walsh spectra take values in the $(m-1)$-th Granted-value. If yes, reserve the subfunction, else discard

the subfunction. The reserved subfunctions set is denoted by R_{m+1}. Classify the set R_{m+1} by the action of permutation group $PL(m+1,2)$ (or group G) on the set R_{m+1}, and denote by ER_{m+1} the set of equivalent classes.

3.Compute the Walsh spectra of the first $(n-k+1)$-variable subfunctions set $\{(x_{n-k+1}+1)f_0(x')+x_{n-k+1}f_1(x')|f_0(x') \in ER_{n-k}, f_1(x') \in B_{n,n-k,1}\}$, and check one by one if they take values in the $(k-1)$-th Granted-values. If yes, reserved it, else discard it. The set of the reserved functions is denoted by R_{n-k+1}. Classify the set R_{n-k+1} by the action of permutation group $PL(n-k+1,2)$ (or group G), and denote by ER_{n-k+1} the set of equivalent classes.

4.$k=k-1$, if $k=0$, output the bent functions in the sets R_n, end the program else goto step3.

With the algorithm 2, all homogenous bent functions can be enumerated. The set of all the homogenous Boolean functions of degree 3 in 8 variables is

$$\{f(x) = \sum_{s=0}^{s=255} a_s x^s | a_s = 0 \quad \text{if} \quad H(s) \neq 3\}$$

$= \{f(x) = (x_8+1)(x7+1)f_0(x')+(x_8+1)x_7f_1(x')+x_8(x_7+1)f_2(x')+x_8x_7f_3(x')\}$ There are 2^{20} subfunctions in the set $B_{8,6,0}$, 2^{15} in $B_{8,6,1}$, 2^{15} in $B_{8,6,2}$, and 2^6 in $B_{8,6,3}$.

1.Let $k=2$, by the corollary 2, the set of 2nd Granted-values is $\{0, \pm 8, \pm 16\}$, and $k=1$, the set of 1st Granted-values is $\{0, \pm 16\}$.

2.Noticing that there are 2^{20} homogeneous functions in the set of $B_{8,6,0}$. By Reed-Muller transformation and Walsh transformation, the spectra of $f_0(x'')$ in $B_{8,6,0}$ can be got. Sieved by the set of 2nd Granted-Value $\{0, \pm 8, \pm 16\}$, only 95370 sub-functions are reserved. Under the action of permutation group $PL(6,2)$, only 181 equivalent classes are reserved. That is, the cardinality of the set ER_6 is 181.

3.Consider the set $\{(x_7+1)f_0(x')+x_7f_1(x')|f_0(x') \in ER_6, f_1(x') \in B_{8,6,1}\}$, the cardinality of which is 181×2^{15}. Similarly, get the spectra of them, Sieved by the set of 1st-Granted-Value $\{0, \pm 16\}$, only 3540 sub-functions in R_7 are reserved and by action of permutation group $PL(7,2)$ only 251 sub-functions are reserved in ER_7. Let $k=1$.

4.Consider the set $\{(x_8+1)f_0(x')+x_8f_1(x')|f_0(x') \in ER_7, f_1(x') \in B_{8,7,1}\}$, the cardinality of which is 251×2^{21}. Check if they are bent functions. Only 722 bent functions are reserved, and by the action of permutation group $PL(8,2)$, there are 14 equivalent classes in ER_8. See the appendix 1.

Now we say we already construct all homogenous bent functions of degree 3 in 8 variables. This can be seen from the following two facts.

Fact 1. Denote by B_n a set of Boolean functions of n variables(or the r-order Reed-Muller code R(r,n)), denote

$$B_{n,n-1,0} = \{f_0(x')|f(x) = (x_n+1)f_0(x') + x_nf_1(x'), f(x) \in B_n, x' \in F_2^{n-1}\}$$

and respectively $B_{n,n-1,1}$. Classify the set $B_{n,n-1,0}$ under the action of permutation group $PL(n-1,2)$(or group G) into ER_{n-1}, and define a set

$$B' = \{f(x)|f(x) = (x_n+1)f_0(x')+x_nf_1(x'), f_0(x') \in ER_{n-1}, f_1(x') \in B_{n,n-1,1}\}.$$

Then the numbers of equivalent classes of B' and B_n under the action of $PL(n,2)$ (or group G) is equal.

Proof. For any a given function $f(x) = (x_n + 1)h_1(x') + x_n f_1(x') \in B_n$, there exists a function $h_2(x') \in ER_{n-1}$ and $A \in PL(n-1,2)$ such that

$$h_1(x') = h_2(Ax').$$

Then the funciton $f(x)$ is in set

$$\{(x_n + 1)h_2(x'A) + x_n f_1(x'A) | f_1(x') \in B_{n,n-1,1}\},$$

which is transformed by A from the set

$$\{(x_n + 1)h_2(x') + x_n f_1(x') | f_1(x') \in B_{n,n-1,1}\} \subseteq B'.$$

That is, for any a function in B_n can be transformed into the set B' by the action of $PL(n-1,2)$. So the conclusion is proved.

Fact 2. If $f(x) = g(Ax)$, then the two functions have same Walsh distribution without consideration of the order. So if a function in one equivalent class satisfies the Granted-value condition, then all functions in the same class can satisfy too.

From all these 14 functions, we get a set $\{f(xA) | f(x) \in ER_8, A \in PL(8,2)\}$, the cardinality of which is 293760. So there are 293760 homogeneous bent functions, which is all homogeneous bent function in 8 variables. This can be done in one minute in a p4 1.7GHZ computer.

The correctness can also be verified by the following easy experiment. Use the algorithm 2 to construct all homogenous bent functions of degree 3 in 6 variables. Denote by B_6 the set of all 2^{20} homogenous Boolean functions. Let $k = 1$, the 1st Granted-value set is $\{0, \pm 8\}$. Sieve the 2^{10} functions in the set $B_{6,5,0}$, we get 15 functions in R_5, and by the action of $PL(5,2)$, only 1 function is reserved in ER_5. Sieve all 1×2^{10} functions in the set $\{(x_6 + 1)f_0(x') + x_6 f_1(x') | f_0(x') \in R_5, f_1(x') \in B_{6,5,1}\}$ by the 0th Granted-value, only 2 functions are reserved. The 2 functions can be classified into 1 function under the action of $PL(6,2)$ in set ER_6. Consider the set $\{f(xA) | f(x) \in ER_6, A \in PL(6,2)\}$, the cardinality of which is 30. This result verifies the correctness of algorithm 2 and the correctness of our result in 8 variables case.

4.3 The construction of homogenous bent functions of degree 3 in 10 variables

As there are too many 3-degree homogeneous bent functions in 10 variables, only some type of bent functions are given here. If you like, you can construct as many as possible.

In corollary 2, let $k = 2$, similar to the case in 8-variable, we get the set R_8. The first function in appendix 1, denoted by $f_0(x)$, is in the set. Similarly we get a set $\{(x_9 + 1)f_0(x) + x_9 f_1(x) | f_1(x) \in B_{10,8,1}\}$, the cardinality of which is 2^{28}, sieved by the set of the first Granted-Value, only 19200 sub-functions are reserved in R_9. Now get a set $\{(x_{10}+1)f_0(x')+x_{10}f_1(x')|f_0(x') \in R_9, f_1(x') \in B_{10,9,1}\}$, the cardinality of which is 19200×2^{36}. Check if they are bent functions. It is efficient to construct bent functions, but it is hard to enumerate, after all 19200×2^{36} is a big number. Our experiment constructs a lot of homogeneous bent functions, which are expanded by $f_0(x')$. By the limitation of space, only two examples are listed in appendix 2.

Here we don't classify the set R_9 because the cardinality of $PL(9,2)$ is $9! = 362880$, classification a set of cardinality 19200 with a group of cardinality 362880 is a time-consuming task.

4.4 The nonexistence of homogeneous bent function of degree 4 in 10 variables

We need a result by Hou[20] on the relationship between the bentness and the coefficients of a Boolean function first.

Lemma 2[20]. Let $f = \sum_{v \subset \{1,2,\cdots,2t\}} a_v x^v) \in P_{2t}(t \geq 2)$ be a bent function, where $x^v = \prod_{i \in v} x_i \in P_n$ for a subset $v \subset \{1,2,\cdots,n\}$. For a given integer $l \geq 1$ and for a given subset $s \subset \{1,2,\cdots,2t\}$.

If

$$2t > |s| \geq max\{l+t, (l-1)degf+1\}$$

or

$$2t = |s| \geq max\{l+t+1, (l-1)degf+1\},$$

then the following equation holds:

$$\sum_{\substack{\{s_1, s_2, \cdots, s_l\} \\ s_1, \cdots, s_l \subset s \quad \text{distinct} \\ s_1 \bigcup \cdots \bigcup s_l = s}} a_{s_1} \cdots a_{s_l} = 0. \tag{3}$$

This is a necessary condition for a function being a bent function.

If $l = 2$, $t = 5$, and $deg(f) = 4$, then $|s| \geq max\{7, 5\} = 7$.

Use the algorithm 1, we have:

1. Let $k = 4$, by corollary 2, compute the set of the 4th Granted-value$\{\pm 4k|k = 0, 1, \cdots, 8\}$, $k = 3$, the set of the 3rd granted-value is $\{\pm 8k|k = 0, 1, 3, 4\}$, $k = 2$, the set of the 2nd granted-value is $\{0, \pm 16, \pm 32\}$.

2. $k = 4$, sieved the set $B_{10,6,0}$ by the 4th granted-value, and classify the set R_6 by the action of permutation $PL(6,2)$, only there are 14 equivalent classes reserved in ER_6. $k = 3$, sieve the set $\{(x_7+1)f_0(x')+x_7f_1(x')|f_0(x') \in ER_6, f_1(x') \in B_{10,6,1}\}$ by the 3rd granted -value, we get a set R_7 and classify it into ER_7. Only 95 functions is left in ER_7.

3. When $k = 2$, consider the set $\{(x_8+1)f_0(x')+x_8f_1(x')|f_0(x') \in ER_7, f_1(x') \in B_{10,7,1}\}$. Sieve the set by the 2nd Granted-Value, and the result set is R_8. Check functions in R_8 by the coefficients condition as follows. In lemma 2, let $t = 5, deg(f) = 4$, $l = 2$, then $|s| > 6$, the equation (3) holds. Let s be

$$\{1,2,3,4,5,6,7\}, \{1,2,3,4,5,6,8,\}, \{1,2,3,4,5,7,8\}, \{1,2,3,4,6,7,8\},$$

$$\{1,2,3,5,6,7,8\},\{1,3,4,5,6,7,8\},\{2,3,4,5,6,7,8\},\{1,2,3,4,5,6,7,8\}.$$

And check if all functions in set

$$\{(x_8+1)f_0(x')+x_8f_1(x')|f_0(x')\in ER_7, f_1(x')\in B_{10,7,1}\}$$

satisfy the equation (3). If the formula holds, reserve the function, else discard it.

Sieved by the Granted-Value and the coefficients condition, no 8-variable sub-function is reserved. That means that there exists no homogeneous bent function of degree 4 in 10 variables.

5 Conclusion

In this paper, by the relationship between the Walsh spectra at partial points and the Walsh spectra of its sub-functions, and by the well known Reed-Muller transformation, an algorithm is developed to construct bent functions, which theoretically can construct all bent functions. By the action of permutation group on Boolean functions, we get an improved algorithm 2. With the algorithm 2, all homogenous bent functions of degree 3 in 8 variables are enumerated; it is efficient to construct 3-degree homogenous bent functions in 10 variables as many as you want; the nonexistence of 4-degree homogenous bent function in 10 variables is proved. Use the algorithm 1 or 2, we get all bent functions in 6 variables. In 8-variable case, it is hard to enumerate all bent functions though it is efficient to construct bent functions. The enumeration of 8-variable bent functions is still under research.

References

[1] Adams, E. Tavares, Generating and counting binary bent functions, ieee Trans.on I.T. Vol 36,No.5, 1170-1173, 1990.

[2] A. Canteaut, P.Charpin, Decompsing bent functions. IEEE,transaction on Information Theory. Vol.49,No.8 ,2004-2019,2003

[3] C. Carlet. Two new classes of bent functions, Advance in cryptology-eurocrypt'93, LNCS765. 77-101, 1994.

[4] C. Carlet, Generalized partial spreads, ieee Trans.on I.T. Vol 41,No.5, 1482-1487, 1995.

[5] C. Carlet and P. Sarkar, Spectral domain analysis of correlation immune and resilient Boolean functions", Finite Fields and Applications (journal) Vol.l8, 120-130. 2002

[6] C. Carlet, Partially- bent funcitons, proceeding of crypto'92,advance in cryptology 92, LNCS 740, springer-verlag,280-291,1993.

[7] C. Charnes, M. Rotteler, T. Beth. Homogeneous bent functions, invariants, and designs. Designs, Codes and Cryptography. Kluewer Acdemmic publishers,2002, Vol.26, pp 139-154.

[8] J.A.Clark,S. Jacob, S. Matria,P. Stanica. Almost boolean functions: the design of boolean fucntions by spectral inversion. Computational Intelligence, Volume 20, Number 3,446-458, 2004

[9] J. F. Dillon. Elementary Hadmard Difference Sets. Ph. D, Dissertation, Unv. Maryland, 1974.

[10] Ling Wang, Jianzhou Zhang, A best possible computable upper bound on bent functions. Journal of uest of China.Vol.33,No.2,113-115,2004.

[11] Maiorana J. A. A classification of the cosets of the Reed-Muller code R(1,6). Mathematics of Computation, 1991, 57(195): 403-414.

[12] Qing-shu Meng, Huan-guo Zhang,Zhang-yi Wang,etc. Designing bent functions using evolving computing. to appear in acta electronica sinica, No.11,2004.

[13] Qingshu Meng, Huanguo Zhang, etc. A simple proof for the nonexistence of homogenous bent function of degee m in $2m$ variables with $m > 3$. Submitted to Journal of WUhan university.

[14] Qingshu Meng, Huanguo Zhang, Min Yang, Jingsong Cui, On the degree of homogenous bent functions. submitted to discrete applied mathematics.

[15] Qu Chengxin, J. Seberry, J.Pieprzyk. Homogeneous bent functions. Discrete Applied Mathematics. 102, 133-139, 2000.

[16] J. Seberry, Xian-mo Zhang, Constructions of bent functions from two known bent functions journal of combinatorcs. 9,21-35,1994.

[17] Rothaus. O. S., On "Bent" functions, J. Combin. Theory Ser. A.20, 300-305,1976.

[18] 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, 127-132, 2004.

[19] Xiang-dong Hou, Results on bent functions. Journal of combinatorial theory, series A 80,232-246,1997.

[20] Xiang-dong Hou, On the coefficients of binary bent functions. proceeding of the American mathematical society, Vol 128,No.4, 987-996, 1999.

[21] Xiang-dong Hou, cubic bent funcitons. Discrete mathematics, Vol.189,149-161,1998.

[22] Yuliang Zheng, Xianmo Zhang, Relationships between bent functions and complementary plateaued functions, proc. 2nd inter. Conf. Information security and cryptology, LNCS 1787,60-75,1999.

Appendix1 The algebraic normal forms of homogeneous bent functions of degree 3 in 8 variables, and denote $x_0x_1x_2$ by x_{012}.

1.$x_{023} + x_{123} + x_{014} + x_{025} + x_{135} + x_{235} + x_{045} + x_{245} + x_{016} + x_{026} + x_{126} + x_{236} + x_{046} + x_{246} + x_{346} + x_{356} + x_{456} + x_{027} + x_{037} + x_{047} + x_{147} + x_{347} + x_{157} + x_{257} + x_{357} + x_{457} + x_{067} + x_{367}$

2.$x_{012} + x_{013} + x_{023} + x_{015} + x_{125} + x_{035} + x_{145} + x_{245} + x_{016} + x_{136} + x_{046} + x_{146} + x_{346} + x_{156} + x_{256} + x_{037} + x_{237} + x_{047} + x_{247} + x_{347} + x_{257} + x_{357} + x_{267} + x_{467}$

3.$x_{012} + x_{013} + x_{023} + x_{015} + x_{125} + x_{035} + x_{145} + x_{245} + x_{016} + x_{136} + x_{046} + x_{146} + x_{346} + x_{156} + x_{256} + x_{027} + x_{237} + x_{047} + x_{247} + x_{347} + x_{057} + x_{357} + x_{457} + x_{067} + x_{267} + x_{367} + x_{567}$

4.$x_{023} + x_{123} + x_{014} + x_{025} + x_{125} + x_{035} + x_{135} + x_{045} + x_{145} + x_{245} + x_{016} + x_{026} + x_{126} + x_{036} + x_{136} + x_{236} + x_{046} + x_{056} + x_{156} + x_{356} + x_{017} + x_{027} + x_{127} + x_{037} + x_{137} + x_{237} + x_{047} + x_{247} + x_{057} + x_{157} + x_{357} + x_{457} + x_{267} + x_{467} + x_{567}$

5.$x_{012} + x_{013} + x_{123} + x_{014} + x_{024} + x_{025} + x_{125} + x_{235} + x_{045} + x_{145} + x_{016} + x_{136} + x_{236} + x_{046} + x_{246} + x_{056} + x_{156} + x_{256} + x_{456} + x_{027} + x_{127} + x_{037} + x_{137} + x_{237} + x_{057} + x_{157} + x_{357} + x_{457} + x_{067} + x_{167} + x_{267} + x_{467}$

6.$x_{012} + x_{013} + x_{123} + x_{014} + x_{024} + x_{025} + x_{125} + x_{035} + x_{135} + x_{235} + x_{045} + x_{145} + x_{245} + x_{016} + x_{026} + x_{126} + x_{036} + x_{236} + x_{046} + x_{146} + x_{056} + x_{156} + x_{356} + x_{017} + x_{027} + x_{037} + x_{137} + x_{237} + x_{147} + x_{057} + x_{157} + x_{257} + x_{457} + x_{167} + x_{267} + x_{367} + x_{567}$

7.$x_{012} + x_{013} + x_{123} + x_{014} + x_{024} + x_{025} + x_{125} + x_{035} + x_{135} + x_{235} + x_{045} + x_{145} + x_{245} + x_{016} + x_{026} + x_{126} + x_{036} + x_{236} + x_{046} + x_{146} + x_{246} + x_{346} + x_{056} + x_{156} + x_{356} + x_{017} + x_{027} + x_{037} + x_{137} + x_{237} + x_{147} + x_{247} + x_{347} + x_{057} + x_{157} + x_{257} + x_{457} + x_{167} + x_{267} + x_{367} + x_{567}$

8.$x_{012} + x_{013} + x_{123} + x_{014} + x_{024} + x_{025} + x_{125} + x_{035} + x_{135} + x_{235} + x_{045} + x_{345} + x_{016} + x_{026} + x_{036} + x_{136} + x_{236} + x_{046} + x_{146} + x_{246} + x_{056} + x_{156} + x_{256} + x_{037} + x_{137} + x_{237} + x_{147} + x_{247} + x_{347} + x_{157} + x_{257} + x_{357} + x_{457} + x_{067} + x_{167} + x_{267}$

9.$x_{012} + x_{013} + x_{123} + x_{014} + x_{024} + x_{025} + x_{125} + x_{035} + x_{135} + x_{235} + x_{045} + x_{345} + x_{016} + x_{026} + x_{036} + x_{136} + x_{236} + x_{046} + x_{146} + x_{246} + x_{056} + x_{156} + x_{256} + x_{017} + x_{027} + x_{127} + x_{037} + x_{237} + x_{347} + x_{057} + x_{157} + x_{357} + x_{167} + x_{267} + x_{367} + x_{467} + x_{567}$

10.$x_{012} + x_{013} + x_{123} + x_{014} + x_{024} + x_{025} + x_{125} + x_{035} + x_{135} + x_{235} + x_{045} + x_{345} + x_{016} + x_{026} + x_{036} + x_{136} + x_{236} + x_{046} + x_{246} + x_{056} + x_{156} + x_{256} + x_{456} + x_{017} + x_{027} + x_{127} + x_{037} + x_{237} + x_{147} + x_{347} + x_{057} + x_{157} + x_{357} + x_{457} + x_{167} + x_{267} + x_{367} + x_{467} + x_{567}$

11.$x_{012} + x_{013} + x_{123} + x_{014} + x_{024} + x_{015} + x_{025} + x_{035} + x_{135} + x_{235} + x_{045} + x_{145} + x_{345} + x_{016} + x_{126} + x_{036} + x_{136} + x_{236} + x_{256} + x_{356} + x_{017} + x_{027} + x_{127} + x_{037} + x_{237} + x_{047} + x_{247} + x_{347} + x_{157} + x_{257} + x_{357} + x_{457} + x_{167} + x_{267}$

12.$x_{012} + x_{013} + x_{123} + x_{014} + x_{024} + x_{034} + x_{015} + x_{235} + x_{045} + x_{145} + x_{245} + x_{345} + x_{016} + x_{026} + x_{126} + x_{036} + x_{146} + x_{246} + x_{056} + x_{156} + x_{256} + x_{356} + x_{017} + x_{127} + x_{237} + x_{047} + x_{147} + x_{247} + x_{157} + x_{257} + x_{357} + x_{457} + x_{067} + x_{267} + x_{467} + x_{567}$

13.$x_{012} + x_{013} + x_{023} + x_{123} + x_{024} + x_{124} + x_{034} + x_{134} + x_{015} + x_{125} + x_{035} + x_{235} + x_{045} + x_{145} + x_{245} + x_{345} + x_{016} + x_{026} + x_{126} + x_{136} + x_{046} + x_{017} + x_{027} + x_{137} + x_{237} + x_{047} + x_{147} + x_{247} + x_{347} + x_{057} + x_{157} + x_{257} + x_{357} + x_{067} + x_{167} + x_{367} + x_{467}$

14.$x_{012}+x_{013}+x_{023}+x_{123}+x_{024}+x_{124}+x_{034}+x_{134}+x_{015}+x_{125}+x_{035}+x_{235}+x_{045}+x_{145}+x_{245}+x_{345}+x_{126}+x_{136}+x_{046}+x_{246}+x_{056}+x_{017}+x_{027}+x_{137}+x_{237}+x_{047}+x_{147}+x_{247}+x_{347}+x_{057}+x_{157}+x_{257}+x_{357}+x_{367}+x_{567}$

Appendix2.The truth tables of homogeneous bent functions of degree 3 in 10 variables. From left to right, each hexadecimal character is expanded into four bits. The first bit of the expanded bits string is the value of the function with input 0, and so on.

1).00061117053f4e74171e5caa12d8fcc9055672de3cacee8147e46ac97ee1099617
225366121b0c05003a1edb05fcbeb874eba9c94d1135963659b1de0f5cd281121b3
03942883af0505628d1ffc522e7712dca69e282fc6366ca872b0a65b1de5f65d7ed0f
f6dd241d28cf05b2bbc533a5354b24369a7d2eb2d20666de7d3093

2).00061117053f4e74171e5caa12d8fcc9055672de3cacee8147e46ac97ee1099617
225366121b0c05003a1edb05fcbeb874eba9c94d1135963659b1de0f5cd281003a1
12b639a28d171443af0ede403f539a94e2166cab4e7e282cfaf42e135967e77c5cc1d
d7fc360f09ee1793a9d712217d03a07e1ef966fa56822e5a357817