Almost Enumeration of eight-variable Bent Functions

Qingshu Meng*, Huanguo Zhang, Jingsong Cui, and Min Yang

Computer school, Wuhan university, Hubei, China 430072

Abstract. Bent functions are important cryptographic Boolean functions. In order to enumerate eight-variable bent functions, we solve the following three key problems. Firstly, under the action of $AGL(7,2)$, we almost completely classify $R(4,7)/R(2,7)$. Secondly, we construct all seven-variable *plateaued* functions from the orbits of $R(4,7)/R(2,7)$. Thirdly, we present a fast algorithm to expand *plateaued* function into bent functions. Based on the results above, it is feasible to enumerate eight-variable bent functions in practice.

Keywords: Cryptography, Reed-Muller Code, Affine Classification, Bent Functions
AMS Classification: 11B50,94A60

1 Introduction

Bent functions were discussed in [16, 6, 24] in the early 1970s. They are a special kind of Boolean functions whose Hamming distance to all affine Boolean functions are equal. Because of their nice cryptographic properties, such as the highest nonlinearity and the lowest autocorrelation, bent functions can be used in symmetric cipher in order to resist the differential cryptanalysis[1] and linear cryptanlysis[15]. Bent functions can also be used in spread communication [22, 21] and in error-correcting code[13]. For interest as a math problem and for their wide applications in many areas, bent functions have attracted a lot of research(for example, see[3, 4, 9] and references therein).

Despite their simple definition and extensive studies in the past 30 years, many questions about bent functions remain open. The space of Boolean functions is too huge and too complex. To enumerate, construct and classify bent functions are still open problems[13]. Only in up to 6 variables, all bent functions[24] are known. In 8 variables case, it is not clear. Even we don't consider functions with degree above 4 or functions containing affine functions, the number of Boolean functions we need to check is 2^{154}. Some known results are cubic bent functions[10], heuristic construction method[5] and some mathematical construction methods around the idea of partial spread of F_{2^n} or using fewer variables bent functions to produce more variables bent functions. Recently, Dobbertin and Leander [7] gave a toolkit to construct 8-variable bent functions.

In this paper, with the aim to enumerate 8-variable bent functions, we solve the following three key problems.

* email: mqseagle@yahoo.com

1. *classification of* $R(4,7)/R(2,7)$. The number of orbits of $R(4,7)/R(2,7)$ under the action of $AGL(7,2)$ is 68433. Using invariant theory, we get 68095 orbits, i.e., we almost classify $R(4,7)/R(2,7)$. There are still 338 orbits not found by us.
2. *construction of plateaued functions.* We construct all 7-variable *plateaued* functions using the 34049 orbits selected from the 68095 orbits.
3. *algorithm expanding plateaued functions into bent functions.* We give a fast algorithm to construct all bent functions that are expanded from one given *plateaued* function.

Based on the results above, it is feasible to enumerate 8-variable bent functions in practice. Because we don't classify $R(4,7)/R(2,7)$ completely, and in the missing $68433 - 68095 = 338$ orbits, there may exist some orbits that can be used to construct 8-variable bent functions too, our enumeration is an almost enumeration. However, our results are still very useful on several occasions. For example, it can be used to discover new properties of bent functions or disprove some conjectures about them. As many symmetric ciphers use 8 bits as basic computation unit, the designed 8-variable bent functions can used in symmetric cipher.

The rest of this paper is organized as follows. In Section 2, we discuss some related background. In Section 3, we discuss the classification of $R(4,7)/R(2,7)$. In Section 4, we discuss the construction of 7-variable *plateaued* functions. In Section 5, we discuss the algorithm expanding *plateaued* functions into bent functions. Finally a short conclusion is given in Section 6.

2 Preliminaries

The field of two elements is denoted by F_2, and the vector space over F_2 of dimension n is denote by F_2^n

A vector $s = (s_1, s_2, \cdots, s_n) \in F_2^n$ can be denoted by an integer t whose 2-adic expansion is the vector s. That is, the vector s and the integer t are isomorphic. In the rest of the paper, we would use an integer to represent a vector in brief if there is no confusion.

The set of all Boolean functions $F_2^n \to F_2$ is denote by p_n. A Boolean function can be written as

$$f(x) = \sum_{s=0}^{2^n-1} a_s x^s,$$

where $a_s \in F_2$ and $x^s = x_1^{s_1} x_2^{s_2} \cdots x_n^{s_n} \in p_n$. The degree of $f(x)$ is defined by

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

where $H(s)$ is the Hamming weight of the vector s.

Let

$$R(r,n) = \{f(x) | f(x) \in p_n, deg(f) \leq r\}$$

be the rth-order Reed-Muller code and for $s < r$, let $R(r,n)/R(s,n)$ be the set of all cosets of $R(s,n)$ in $R(r,m)$.

The set of all nonsingular matrices of order n is denote by $GL(n,2)$, i.e. the general linear group. Denote by $AGL(n,2)$ the general affine group $\{(A,b)|A \in GL(n,2), b \in F_2^n\}$. The action of group $AGL(n,2)$ on Boolean functions is defined by:

$$\begin{array}{ll} c: \ p_n \rightarrow & p_n \\ by: f(x) \rightarrow f \circ c = f(xA+b) \end{array},$$

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

Two functions $f(x), g(x) \in R(r,n)/R(s,n)$ are called affinely equivalent if there exists $(A,b) \in AGL(n,2)$ such that $f(x) = g(xA+b) \bmod R(s,n)$. An invariant of $R(r,n)/R(s,n)$ is a mapping M from $R(r,n)/R(s,n)$ to a set such that $M(f) = M(g)$ holds for any two affinely equivalent functions $f(x), g(x) \in R(r,n)/R(s,n)$. If all functions with same invariant value are taken as one orbit, then invariant can be used to classify $R(r,n)/R(s,n)$. Suppose N is the number of distinct orbits of $R(r,n)/R(s,n)$ under the action of $AGL(7,2)$. If an invariant exactly takes N distinct values, then the set is already classified completely. In this case, the invariant is called a discriminant of $R(r,n)/R(s,n)$.

Definition 1. *[24] Let $f(x) \in p_n$, $x = (x_1, x_2, \cdots, x_n)$, $w = (w_1, w_2, \cdots, w_n)$, and*

$$w \cdot x = w_1x_1 + x_2w_2 + \cdots + x_nw_n \in F_2.$$

Define

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

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

The transform is called the Walsh transform.

Definition 2. *Define*

$$c_f(s) = \sum_{x=0}^{2^n-1} (-1)^{f(x)}(-1)^{f(x+s)}$$

as the autocorrelation function of $f(x)$, where $f(x) \in p_n, s \in F_2^n$.

Definition 3. *[24] Let $f(x) \in p_n, x \in F_2^n$ be Boolean function. If for any $w \in F_2^n, |s_{(f)}| = 2^{n/2}$, then $f(x)$ is called a bent function.*

Definition 4. *[26] For function $f(x) \in p_n$, if there exists an even integer r such that each $s^2_{(f)}(w)$ takes value of 2^{2n-r} or 0 only, then $f(x)$ is called a rth-order* plateaued *function.*

In this paper, we only care about the $(n-1)$th-order *plateaued* functions, and call it *plateaued* functions for brief.

3 Almost Classification of $R(4,7)/R(2,7)$

In this section, our main goal is to solve the first key problem: classification of $R(4,7)/R(2,7)$ under the action of $AGL(7,2)$. To this end, we introduce some basic transforms to Boolean functions, and corresponding invariants. With these invariants, we classify $R(4,6)/R(1,6)$ and $R(3,7)/R(1,7)$ first, then $R(4,7)/R(2,7)$.

3.1 Basic Transforms and Invariants

The basic transforms we will introduce include Walsh transform, autocorrelation function, decomposition, derivation and modification to truth table.

3.1.1 Walsh Transform and Autocorrelation Function

Proposition 1. *[23] Let $f(x), g(x) \in p_n$ be two functions such that $g(x) = f(xA+b) + lx$, where $A \in GL(n,2)$, b, $l \in F_2^n$, then for any $w \in F_2^n$,*

$$s_{(g)}(w) = (-1)^{(l+w)\cdot bA^{-1}} s_{(f)}((l+w)(A^{-1})^T).$$

Corollary 1. *[23] The distribution of absolute Walsh spectra of $f(x)$ is equal to that of $g(x)$.*

Proposition 2. *[23] Let $f(x), g(x) \in p_n$ be two functions such that $g(x) = f(xA+b) + lx$, where $A \in GL(n,2)$, b, $l \in F_2^n$, then for any $s \in F_2^n$,*

$$c_g(s) = (-1)^{l\cdot s} c_f(sA).$$

Corollary 2. *[23] The distribution of absolute autocorrelation function of $f(x)$ is equal to that of $g(x)$.*

3.1.2 Derivation

For any Boolean function $f(x) \in R(r,n)$, define its derivation function on direction $a \in F_2^n$ as $D_a(f) = f(x) + f(x+a)$.

Proposition 3. *[2]: Let $f(x) \in R(r,n)/R(r-1,n)$, then*

$$D_a(f \circ B) = (D_{aA} f) \circ B \ mod \ R(r-2,n),$$

where $B = (A,c) \in AGL(n,2)$.

Proposition 4. *Let $f(x) \in R(r,n)/R(s,n)$, $B = (A,b) \in AGL(n,2)$, then*

$$D_a(f \circ B) = D_{aA}(f) \circ B \ mod \ R(s-1,n).$$

If M is an invariant of $R(r-1,n)/R(s-1,n)$, then

$$M(D_a(f \circ B)) = M(D_{aA}(f) \circ B).$$

Therefore,

$$\{M(D_a(f)) | a \in F_2^n\}$$

is an invariant of $R(r,n)/R(s,n)$.

Remark 1. Note that we use the invariant value $\{M(D_a(f))|a \in F_2^n\}$, instead of the invariant $\{M \circ D_a|a \in F_2^n\}$ itself, to denote an invariant. In the following parts, we use the value of an invariant, instead of the invariant itself, for convenience several times. The derivation function was used by Dillon[6] to prove the existence of bent functions not in family M[16], by Hou[12] in classification of $R(3,7)/R(2,7)$ and by Brier and Langevin[2] in classification of $R(3,9)/R(2,9)$. Proposition 4 is an extension of their results.

3.1.3 Decomposition

Let $f(x), g(x) \in R(r,n)$ be two functions such that $g(x) = f(xA+b) \bmod R(s,n)$, where $A \in GL(n,2), x = (x_1, \cdots, x_n), b = (b_1, b_2, \cdots, b_n) \in F_2^n$. If $f(x) = (x_1 + 1)f_0(x') + x_1 f_1(x')$, where $x' = (x_2, \cdots, x_n)$, then $g(x) = (x \cdot c_1 + b_1 + 1)f_0(x'') + (x \cdot c_1 + b_1)f_1(x'')$, where $c_1, c_2, \cdots, c_n$ are the columns of the matrix A, and $x'' = (x \cdot c_2 + b_2, \cdots, x \cdot c_n + b_n)$. Obviously, $f_0(x'), f_1(x')$ are affinely equivalent to $f_0(x''), f_1(x'')$ mod $R(s, n-1)$ respectively.

In general, we have:

Proposition 5. *Let $f(x),\ g(x) \in R(r,n)/R(s,n)$ be such that $g(x) = f(xA + b)$ mod $R(s,n)$, $(A,b) \in AGL(n,2)$. Let $f(x)$ be decomposed into two subfunctions: $f_{ax=0},\ f_{ax=1}$ on direction a, then $g(x)$ can be decomposed into two subfunctions $g_{cx=0},\ g_{cx=1}$ on direction c such that $\{f_{ax=0},\ f_{ax=1}\}$ are affinely equivalent to $\{g_{cx=0},\ g_{cx=1}\}$ modulo $R(s, n-1)$, where $c = aA^T$.*

Proof. If $f(x)$ is decomposed according to a vector a, i.e. according to $a \cdot x = 0$ or 1, then $g(x)$ can be decomposed according to $a \cdot (xA + b) = 0$ or 1.

Let $a = (a_1, \cdots, a_n)$, $x = (x_1, \cdots, x_n)$, $A = (C_1, \cdots, C_n)$, where $C_i, i = 1, \cdots, n$ is the columns of the matrix A, then we have

$$\begin{aligned} a \cdot (xA+b) &= a \cdot (x \cdot C_1, \cdots, x \cdot C_n) + a \cdot b \\ &= a_1(x \cdot C_1) + \cdots + a_n(x \cdot C_n) + a \cdot b \\ &= a_1(x_1 C_{1,1} + \cdots + x_n C_{n,1}) + \cdots + a_n(x_1 C_{1,n} + \cdots + x_n C_{n,n}) + a \cdot b \\ &= x_1(a_1 C_{1,1} + \cdots + a_n C_{1,n}) + \cdots + x_n(a_1 C_{n,1} + \cdots + a_n C_{n,n}) + a \cdot b\,. \\ &= x_1(a \cdot R_1) + \cdots + x_n(a \cdot R_n) + a \cdot b \\ &= x \cdot (a \cdot R_1, \cdots, a \cdot R_n) + a \cdot b \\ &= x \cdot (aA^T) + a \cdot b \end{aligned}$$

Because $a \cdot b \in F_2$ is a constant, we can decomposed $g(x)$ on direction $c = aA^T$.

Proposition 6. *If M is an invariant of $R(r, n-1)/R(s, n-1)$, then the set*

$$\{\{M(f_{ax=0}), M(f_{ax=1})\}|a \in F_2^n\}$$

is an invariant of $R(r,n)/R(s,n)$.

Remark 2. The basic idea of the decomposition of a function can be found early in Maiorana's paper[14], which made the classification of $R(6,6)/R(1,6)$ possible early in the 1990s. Recently, it was used by Brier and Langevin[2] to classify $R(3,9)/R(2,9)$.

3.1.4 The Modification of Truth Table

Definition 5. *[20] For Boolean function $f(x) \in p_n$, its 1-local connection functions $f_i(x)$ are defined by*

$$f_i(x) = \begin{cases} f(x) \quad , & x \neq i \\ f(x) + 1, & x = i \end{cases}, i = 0, 1, \cdots, 2^n - 1.$$

Proposition 7. *[8] Let $f(x), g(x) \in R(r, n)$ be such that $g(x) = f(xA + b) + lx$, then $g_j(x) = f_i(xA + b) + lx$, where $jA = (i + b), i = 0, 1, \cdots, 2^n - 1$.*

Proposition 8. *Let $f(x) \in R(r, n)$. If M is an invariant of $R(n, n)/R(1, n)$, then $\{M(f_i(x))|i \in F_2^n\}$ is an invariant of $R(r, n)/R(1, n)$.*

Remark 3. The purpose of the modification to truth table is to create many more couples of equivalent Boolean functions of the same equivalent relationship.

3.2 Classification of $R(4, 6)/R(1, 6)$

Based on the invariants above, we are able to classify $R(4, 6)/R(1, 6)$ under the action of $AGL(6, 2)$. The number of orbits of $R(4, 6)/R(1, 6)$ under the action of $AGL(6, 2)$ is 2499 due to Hou's work[11]. The classification can be done as follows:

1. *get the four orbits.* It is easy to get the four orbits of $R(2, 6)/R(1, 6)$. Due to Hou's work[12], the orbits of $R(2, 6)/R(1, 6)$ and $R(4, 6)/R(3, 6)$ are complementary. Therefore, the representative functions of the four orbits of $R(4, 6)/R(3, 6)$ can be written as
   (a) $f_0(x) = 0$,
   (b) $f_1(x) = x_3x_4x_5x_6$,
   (c) $f_2(x) = x_1x_2x_5x_6 + x_3x_4x_5x_6$,
   (d) $f_3(x) = x_1x_2x_3x_4 + x_1x_2x_5x_6 + x_3x_4x_5x_6$.
2. *classify the four cosets $f_i + R(3, 6)$.* Using derivation function, we classify the four cosets $f_i + R(3, 6), i = 0, \cdots, 3$ into 6,10,12,6 cosets of form $g_j + R(2, 6)$, $deg(g_j(x)) \leq 4$ respectively. The invariant of $R(3, 6)/R(1, 6)$ used in Proposition4 is the distribution of absolute Walsh spectra. What we do in this step is to check 4×2^{20} Boolean functions.
3. *classify the 34 cosets $g_i + R(2, 6)$.* Using the decomposition transform and modification transform, we classify the 34 cosets $g_i + R(2, 6), i = 0, 1, \cdots, 33$ into 2499 cosets of form $h_i(x) + R(1, 6)$, $deg(h_i(x)) \leq 4, i = 0, 1, \cdots, 2498$. The invariant of $R(4, 5)/R(1, 5)$ used in Proposition 6 is the distribution of absolute Walsh spectra and absolute autocorrelation function. The invariant of $R(6, 6)/R(1, 6)$ used in Proposition 8 is the distribution of absolute Walsh spectra and absolute autocorrelation function. In this step, we need to check 34×2^{15} Boolean functions.

3.3 Classification of $R(3,7)/R(1,7)$

We aim to classify $R(3,7)/R(1,7)$ in this subsection. The number of orbits of $R(3,7)/R(1,7)$ under the action of $AGL(7,2)$ is 179 due to Hou's work[11]. All these 179 orbits can be obtained as follows:

1. In [12], the 12 orbits of $R(3,7)/R(2,7)$ were given. Denote them by $f_i(x)+R(2,7)$, $i=0,1,\cdots,11$.
2. Using decomposition transform, the cosets $f_i(x)+R(2,7), i=0,1,\cdots,11$ can be classified into 4,8,19,10,20,6,7,29,12,39,10,15 cosets of form $g_i(x)+R(1,7)$ respectively. The invariant of $R(3,6)/R(1,6)$ used in Proposition 6 is the distribution of absolute Walsh spectra and absolute autocorrelation function.

3.4 Almost Classification of $R(4,7)/R(2,7)$

Due to Hou's result[12], the orbits of $R(4,7)/R(3,7)$ and $R(3,7)/R(2,7)$ are complementary. Because the 12 orbits of $R(3,7)/R(2,7)$ have been already given by Hou[12], the 12 orbits of $R(4,7)/R(3,7)$ are known too. We denote them by $g_i(x)+R(3,7),\ deg(g_i)=4,\ i=1,2,\cdots,12$. That is, $R(4,7)/R(2,7)$ can be firstly classified into 12 sets of forms: $g_i(x)+R(3,7)/R(2,7),\ i=1,2,\cdots,12$. We can classify the 12 sets one by one. For a given set, say $g_i(x)+R(3,7)/R(2,7)$, do the following steps.

Algorithm 1

For any a function $f(x)\in g_i(x)+R(3,7)/R(2,7)$,

1. *invariant 1.* Based on vector a, the function $f(x)$ can be decomposed into two subfunctions $f_{ax=0}(x),\ f_{ax=1}(x)\in R(4,6)/R(2,6)$. Let $D^6_{4,2}$ be the discriminant of $R(4,6)/R(2,6)$ known from Subsection 3.2. Let
$$DE_a(f)=\{D^6_{4,2}(f_{ax=0}),D^6_{4,2}(f_{ax=1})\},$$
then the distribution
$$\{DE_a|a\in F_2^n,\ a\neq 0\}$$
is an invariant of $g_i(x)+R(3,7)/R(2,7)$.
2. *invariant 2.* Let $f_a(x)\in R(3,7)/R(1,7)$ be the derivation function of $f(x)$ on vector a. Let $D^7_{3,1}$ be the discriminant of $R(3,7)/R(1,7)$ known from Subsection 3.3, then the distribution $\{D^7_{3,1}(f_a)|a\in F_2^n,a\neq 0\}$ is an invariant of $g_i(x)+R(3,7)/R(2,7)$.
3. *final invariant.* The direct product of the above two invariants is also an invariant, denoted by IVT. We can use it to classify $g_i(x)+R(3,7)/R(2,7)$.

But Algorithm 1 is expensive in view of computation. It is not practical because we have to check 2^{35} functions in set $g_i(x)+R(3,7)/R(2,7)$. We give a more practical method.

Algorithm 2: Practical One

There are 35 monomials of degree 3 in $R(3,7)/R(2,7)$, and they can be represented as $x^s,\ H(s)=3$. They can be numbered as $0,1,\cdots,34$ according to the value of s, that is, x^s is numbered as 0 if the s is the least, and x^s is numbered as 34 if the s is the largest. With the description above, we divide the 35 monomials into two sets, named as $G1, G2$. $G1$ consist of the first 20 monomials and $G2$ consists of the rest 15 monomials. And denote by $FG1, FG2$ the set of homogeneous functions generated from $G1$, $G2$ respectively. The size of $FG1$, $FG2$ are 2^{20}, 2^{15} respectively.

For a given set $g_i(x) + R(3,7)/R(2,7)$,

1. classify the set $\{g_i(x) + m(x) | m(x) \in FG1\}$ using the invariant IVT, and denote by $RG1$ the set of orbits.
2. classify the set $\{h(x) + m(x) | h(x) \in RG1, m(x) \in FG2\}$ using the invariant IVT. The heuristic searching algorithm we use is given below. We denote by $RG2$ the set of representative functions of the orbits.
   Heuristic Searching

   ```
   for($h(x) \in RG1$)
   begin
       $neworbit = 0$;
       $count = 0$;
      for($m(x) \in FG2$)
      begin
          calculate the value of invariant $IVT(h(x) + m(x))$.
          if (the value of $IVT(h(x) + g(x))$ is new)
              then $neworbit + +$; and put $h(x) + g(x)$ in set RG2.
          $count + +$;
          if ($count > 1024$ and $neworbit == 0$) break out;
       end
   end
   ```

Using Algorithm 2, the 12 sets are classified. The second line of Table 1 lists the exact number of orbits we obtain. The sum of all these orbits is 68095. There are $68433 - 68095 = 338$ orbits not found by our algorithm. The ratio is $338/68433 \cong 0.49\%$. That is, we almost classified $R(4,7)/R(2,7)$ under the action of $AGL(7,2)$.

Table 1. The Number of Orbit of $g_i + R(3,7)/R(2,7)$ Under the Action of $AGL(7,2)$ and the Number of Reserved Orbits

g_i	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	sum
Num. of Fun.	12	63	285	474	694	185	121	6371	1013	33598	1302	23987	68095
Num. of Reserved Fun.	6	24	128	156	328	55	44	3306	501	16851	657	11993	34049

The reason we don't get all 68433 orbits is given below:

1. The invariant IVT used in Algorithm 1 may be not a discriminant of $g_i(x) + R(3,7)/R(2,7)$.

2. Even the invariant IVT is indeed a discriminant, out of the consideration on computation, we use a heuristic searching algorithm, not a exhaustive searching algorithm. Therefore, the heuristic searching algorithm can also lead to the loss of some orbits.

Beside the application in this paper, the almost classification of $R(4,7)/R(2,7)$ can be used to find the covering radius of $R(2,7)$ in $R(4,7)$.

4 construction of *plateaued* functions

In this section, we aim to solve the second key problem: construction of *plateaued* functions. To this end, we study the Walsh spectra properties of the subfunctions of bent function. We get some necessary conditions that the subfunctions of a bent function must satisfy. Based on the necessary conditions, we divide the 68095 orbits of $R(4,7)/R(2,7)$ into two sets. While one set can be used to construct 7-variable *plateaued* functions, the other set can't. When we finish the division, we also get all 7-variable *plateaued* functions.

4.1 Walsh Spectra Properties of the Subfunctions

Definition 6. *Let*

$$f(x)=\sum_{i=0}^{2^k-1}\delta_i(x')f_i(x''),$$

where $x=(x',x'')$, $x'=(x_1,x_2,\cdots,x_k)$, $x''=(x_{k+1},x_{k+2},\cdots,x_n)$,

$$\delta_i(x')=\begin{cases}1,\ x'=i\\0,\ x'\neq i\end{cases},$$

then $f_i(x''), i=0,1,\cdots,2^k-1$ *are called the subfunctions of* $f(x)$.

The Walsh spectra properties of the subfunctions of bent function will be studied below.

Theorem 1. *[18]. Let*

$$f(x)=\sum_{i=0}^{2^k-1}\delta_i(x')f_i(x'')$$

defined as in Definition 6, then

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

$$=[s_{(f)}(0,w''),s_{(f)}(1,w''),\cdots,s_{(f)}(2^k-1,w'')]H_k/2^k, \qquad (1)$$

where $w=(w',w'')$, $w'\in F_2^k$, $w''\in F_2^{n-k}$, *and* H_k *is a Hadamard matrix.*

Corollary 3. *If*

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

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

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

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

Proof. In equation (1), once $s_{(f)}(i, w''), i = 0, 1, \cdots, 2^k - 1$ takes one of the two possible values $\{\pm 2^{n/2}\}$, the value of $s_{(f_0)}(w'')$ can be calculated uniquely. The number of different values the spectrum $s_{(f_0)}(w'')$ can take is determined by the number of positive values of $s_{(f)}(i, w''), i = 0, 1, \cdots, 2^k - 1$. Suppose the number of positive values of $s_{(f)}(i, w''), i = 0, 1, \cdots, 2^k - 1$ is j, then $s_{(f_0)}(w'')$ takes value $[(2^k - j)2^{n/2} - j2^{n/2}]/2^k = (2^k - 2j)2^{n/2-k}$. Let $j = 0, 1, \cdots, 2^k$, then $s_{(f_0)}(w'')$ takes $2^k + 1$ distinct values. Similarly, we can discuss $s_{(f_i)}(w'')$ for $i = 1, 2, \cdots, 2^k - 1$.

Let us consider the case $n = 8$. When $k = 1$, the set of the first-order Granted-value is $\{0, \pm 16\}$. When $k = 2$, the set of the second-order Granted-value is $\{0, \pm 8, \pm 16\}$. When $k = 3$, the set of the third-order Granted-value is $\{0, \pm 4, \pm 8, \pm 12, \pm 16\}$.

4.2 division of 68095 orbits into two sets

Corollary 3 can be used to check if a function is a bent function. For example, let $f(x) = (x_0 + 1)f_0(x') + x_0 f_1(x')$. Generally, we calculate the Walsh spectra of $f(x)$ and see if it is a bent function. Using Corollary 3, we calculate the Walsh spectra of $f_0(x)$ first and see if they take the first-order Granted-value. If the Walsh spectra of $f_0(x)$ doesn't take the first-order Granted-value, the function $f(x)$ can't be bent function. Obviously, much computation is saved.

In Section 3, $R(4, 7)/R(2, 7)$ is classified into 68095 orbits and the representative functions of all 68095 orbits are kept in $RG2$. With Corollary 3, we can check whether the 68095 functions could be expanded into bent functions easily. For any a function $f(x) \in RG2$, if there exists a function $g(x) \in R(2, 7)/R(1, 7)$ such that the Walsh spectra of $f(x) + g(x)$ take the first-order Granted-Value, then the function $f(x) \in RG2$ is reserved, otherwise $f(x)$ is discarded. In this way, we divide the 68095 functions into two sets. One set consists of reserved functions, denoted by HB. The other set consists of the discarded functions. The exact number of reserved functions is shown in Table 1. From Table 1, the size of HB is 34049. In this step, though there are 68095×2^{21} functions to be checked, we can do it efficiently using Corollary 3 or the fast searching algorithm in [19].

As the degree of 7-variable *plateaued* functions is no greater than 4 [26], we also get all 7-variable *plateaued* functions when we get the division.

5 Algorithm to Enumerate 8-variable Bent Functions

In this section we present a fast algorithm to construct all bent functions that are expanded from a given *plateaued* function.

Theorem 2. *[24] Let $f(x) \in p_n$ be a bent function. $\widetilde{f(x)}$ be such that $s_{(f)}(w) = 2^{n/2}(-1)^{\widetilde{f(x)}}$, then $\widetilde{f(x)}$ is a bent function, and is called the dual function of f(x).*

Corollary 4. *Let $f(x) = (x_1+1)f_0(x'') + x_1 f_1(x'') \in p_n$ be a bent function, then the size of $\{w'' | s_{(f_0)}(w'') = 0,\ w'' = 0, \cdots, 2^{n-1}-1\}$ is 2^{n-2}.*

Proof. If $f(x)$ is a bent function, then $f_0(x'')$ is a *plateaued* function. The Walsh spectra of $f_0(x'')$ take value $0, \pm 2^{n/2}$. Denote by m the size of $\{w'' | s_{(f_0)}(w'') = \pm 2^{(n+1)/2},\ w'' = 0, \cdots, 2^{n-1}-1\}$, then due to Parseval's equation, $m \times 2^n = 2^{2(n-1)}$. We get $m = 2^{n-2}$. In other words, the size of $\{w'' | s_{(f_0)}(w'') = 0,\ w'' = 0, \cdots, 2^{n-1}-1\}$ is 2^{n-2}.

Algorithm 3

Let $f(x) = (x_1+1)f_0(x') + x_1 f_1(x'), x = (x_1, x_2, \cdots, x_8)$, be a bent function. By [26], the two subfunctions are called complementary *plateaued* functions. The distribution of their Walsh spectra would be of the following forms respectively:

$$\overbrace{a,\cdots,a}^{n_1},\overbrace{b,\cdots,b}^{n_2},\overbrace{a\cdots,a}^{n_3},\cdots \tag{2}$$

$$\overbrace{b,\cdots,b}^{n_1},\overbrace{a',\cdots,a'}^{n_2},\overbrace{b\cdots,b}^{n_3},\cdots, \tag{3}$$

where $a = \pm 16$, $a' = \pm 16$, $b = 0$ and $n_i, i = 1, 2, \cdots$, are nonnegative integers. The spectra sequence of $f(x)$, denote by S, is of form like

$$\overbrace{a,\cdots,a}^{n_1},\overbrace{a',\cdots,a'}^{n_2},\overbrace{a\cdots,a}^{n_3},\cdots,\overbrace{a,\cdots,a}^{n_1},\overbrace{-a',\cdots,-a'}^{n_2},\overbrace{a,\cdots,a}^{n_3},\cdots \tag{4}$$

In above sequence, if 0 is substituted for 16 and 1 for -16, then the sequence resulted from the substitution should be a truth table of another bent function by Theorem 2. Given a *plateaued* function(i.e. a is known), to expand it into bent functions is to determine the value of a'. Because the number of a' is 64 by Corollary 4, usually it is hard to determine. But using Corollary 3 we can do it.

1. Substitute 1 for $a = 16$ and -1 for $a = -16$ in sequence S.
2. The length of the sequence S is 256. The sequence S can be divided into 8 blocks of equal length. Suppose there are m_1, m_2, m_3, m_4 a's in the first, second, third and fourth block respectively, where $m_1 + m_2 + m_3 + m_4 = 64$. The $5-8$th blocks is determined by the $1-4$th blocks respectively due to formula (4). For each of the 8 blocks, substitute -1 or 1 for unknown a', then each block becomes a polarized truth table of a 5-variable Boolean function. We check if the Walsh spectra of each block take the 3rd-order Granted-value. If they do take the 3rd-order Granted-value, then the substitution

is right, otherwise the substitution is not proper and should be discarded. The number of substitutions in this step is $2^{m_1} + 2^{m_2} + 2^{m_3} + 2^{m_4}$. After this step, suppose there are N_1, N_2, N_3, N_4 substitutions are reserved for the 1-4th blocks respectively.

3. Divide the sequence S into 4 blocks of equal length, each of which is then a truth table of a 6-variable Boolean function. There are $N_1 \times N_2$ substitutions in the first block, and $N_3 \times N_4$ substitutions in the second block. The third and the fourth block is determined by the first and second block respectively due to formula (4). For each of the four blocks, we check if the Walsh spectra take the second-order Granted-value. Suppose there are M_1, M_2 substitutions are reserved in first and second block respectively.
4. Divide the sequence S into 2 blocks of equal length, each of which is then a truth table of a 7-variable Boolean function. There are $M_1 \times M_2$ substitutions in the first block. The second block is determined by the first block. For the two blocks, we check if the Walsh spectra take the first-order Granted-value. Suppose there are M substitutions are reserved. Now for the M substitutions, we check if the sequence S is a bent function.

The dual function of sequence S is the bent function we obtain.

6 Conclusion

In this paper, we present a practical method to enumerate 8-variable bent functions. Because we don't classify $R(4,7)/R(2,7)$ completely, and in the small number of missing orbits there may exist orbits that can be used to construct bent function too, our enumeration is an almost enumeration. However, our results are still very useful. For example, they can be used to discover new properties of bent functions or disprove some conjectures about them. For the purpose of being processed by 8-bit CPU, many symmetric ciphers use 8 bits as basic computing unit. The designed 8-variable bent functions can used in symmetric cipher.

Some immediate results of this paper are useful too. For example, the almost classification of $R(4,7)/R(2,7)$ can be used to find the covering radius of $R(2,7)$ in $R(4,7)$; Covering radius is useful in coding and in cryptography. The 7-variable *plateaued* functions obtained can be used to construct *plateaued* functions in more variables by Corollary 2 in paper[25].

References

1. E. Bihama, A.Shamir,Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology, Vol.4, No.1, 3-72, 1991.
2. E. Brier, P. Langevin, Classification of Boolean Cubic Forms in Nine Variables, 2003 IEEE Information Theory Workshop, 179-182, 2003.
3. C. Carlet. Two new classes of bent functions, Advance in cryptology-eurocrypt'93, 1994, LNCS765, 77-101.

4. C. Carlet, Generalized partial spreads, ieee Trans.on I.T. 1995, Vol 41,No.5, 1482-1487.
5. J.A.Clark, S.Jacob, S. Matria,P. Stanica. Almost Boolean Functions: the Design of Boolean Fucntions by Spectral Inversion. Computational Intelligence, 2004, Vol. 20, No. 3, 446-458.
6. J. F. Dillon. Elementary Hadamard Difference Sets. in Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing, F.Hoffman et al.(Eds), Utilitas Math, 237-249, 1975.
7. H. Dobbertin, G. Leander, Cryptographer's Toolkit for Construction 8-bit Bent Functions, http://eprint.iacr.org, 2005/089.
8. J. FULLER, and W. MILLAN, Linear Redundancy in S-box, In: Fast Software Encryption, LNCS 2887, Springer-Verlag, 74-86, 2003.
9. X. Hou, On the Coefficients of Binary Bent Functions. Proceeding of the American Mathematical Society, 1999, Vol. 128, No.4, 987-996.
10. X. Hou, Cubic Bent Functions, Discrete Mathematics, 189, 149-161, 1998.
11. X. Hou, $AGL(m, 2)$ Acting on $R(r, m)/R(s, m)$, Journal of Algebra, 171, 921-938, 1995.
12. X. Hou, $GL(m, 2)$ Acting on $R(r, m)/R(r - 1, m)$, Discrete Mathematics, 149, 99-122, 1996.
13. F. J. Macwillams, J. A. Solane, The theory of Error-correcting Codes. North-holland publishing company, Amsterdam, 1978.
14. J.A. Maiorana, A Classification of the Cosets of the Reed-Muller Code $R(1, 6)$, Mathematic Computation, 57, 1991, 403-414.
15. M. Matsui, Linear Cryptanalysis Method for DES Cipher. LNCS 765, Eurocrypt93, 386-397, 1994.
16. R.L.McFarland, A Family of Noncyclic Difference Sets, Journal of Combinatorics(series A) 15, 1-10, 1973.
17. Q. Meng, M. Yang, H. Zhang,Y.Liu, Analysis of Affinely Equivalent Boolean Functions, The First Workshop on Boolean Functions and Application on Cryptography, also available at http://eprint.iacr.org, 2005/025.
18. Q. Meng, H. Zhang,Z. Wang, et al. Designing Bent Functions Using Evolving Computing. Acta electronica sinica, No.11, 1901-1903, 2004.
19. Q. Meng, H. Zhang, M. Yang, et al. A Novel Algorithm Enumerating Bent Functions. http://eprint.icar.org, 2004/274.
20. W. Millan, A. Clark, E. Dawson, Smart Hill Climbing Finds Better Boolean Functions. in Proceeding of the Workshop on Selected Areas in Cryptology 1997,Ottawa,Canada, 50-63, 1997.
21. J.D. Olsen, R.A. Scholtz, L.R.Welch, Bent-function Sequences, IEEE Transaction on Information Theory, 1982, Vol.28, No.6, 858-864.
22. K. G. Paterson, Sequences for OFDM and Multi-code CDMA: Two Problems in Algebraic Coding Theory, in T.Helleseth, P.V. Kumar and K.Yang editors, Proceedings of Sequence and Their Applications, SETA01, Springer-verlag, London, 46-71, 2002.
23. B. Preneel, Analysis and Design of Cryptographic Hash Functions, Ph.D thesis, KU Leuven(Belgium),February 1993.
24. O. S. Rothaus, On "Bent" Functions, J. Combin. Theory Ser. A.20,1976, 300-305.
25. X. Zeng, L. Hu. A Composition Construction of Bent-like Boolean Functions from Quadratic Polynomials. http://eprint.iacr.org, 2003/204.
26. Y. Zheng, X. Zhang, Relationships between Bent Functions and Complementary plateaued Functions, Proceedings of the 2nd International Conference on Information Security and Cryptology, LNCS 1787, 60-75, 1999.