A Construction of Bent Functions with Optimal Algebraic Degree and Large Symmetric Group*

Wenying Zhang[1,3], Zhaohui Xing[1] and Keqin Feng[2]
1 School of Information Science and Engineering,
Shandong Normal University, Jinan 250014, China
2 Department of Mathematical Sciences, Tsinghua University,
Beijing, 100084, China,
3 Dept. Electrical Engineering (ESAT), KU Leuven and Imec, Leuven, 3001, Belgium
Email: wzhang@esat.kuleuven.be, kfeng@math.tsinghua.edu.cn

Abstract

We present a construction of bent function $f_{a,S}$ with $n = 2m$ variables for any nonzero vector $a \in \mathbb{F}_2^m$ and subset S of $\mathbb{F}_2^m$ satisfying $a + S = S$. We give the simple expression of the dual bent function of $f_{a,S}$. We prove that $f_{a,S}$ has optimal algebraic degree m if and only if $|S| \equiv 2(\text{mod}4)$. This construction provides series of bent functions with optimal algebraic degree and large symmetric group if a and S are chosen properly.

Keywords: Bent function, Algebraic degree, Symmetric group

1 Introduction

Let $\mathscr{B}_n = \{f = f(x_1, \cdots, x_n) : \mathbb{F}_2^n \to \mathbb{F}_2\}$ be the ring of Boolean functions with n variables. For each $f \in \mathscr{B}_n$, the Walsh transformation of f is $W_f : \mathbb{F}_2^n \to \mathcal{Z}$ defined by

$$W_f(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x\cdot y}, (y = (y_1, \cdots, y_n) \in \mathbb{F}_2^n),$$

where $x \cdot y = x_1y_1 + \cdots + x_ny_n \in \mathbb{F}_2$. f is called bent function if for all $y \in \mathbb{F}_2^n$,

$$W_f(y) = \pm 2^{\frac{n}{2}} = 2^{\frac{n}{2}}(-1)^{\widehat{f}(y)}.$$

Where $\hat{f} \in \mathscr{B}_n$ and called the dual of f. If f is a bent function then n is even and $\hat{f}$ is also a bent function. Bent functions were introduced by Rothaus [1] in 1976 and already studied by Dillon [2] in 1974 with their equivalent combinatorial objects: Hadamard difference sets in elementary 2-groups. Since then, bent functions have been extensively developed for their important applications in many aspects as cryptography(design of stream ciphers), coding theory, sequences with good correlation properties and graph theory.

Many constructions, primary and secondary, of bent functions has been found in past forty years (See book [3]). In the application on cryptography, we hope the bent function having large algebraic degree $deg(f)$. It is known that for any bent function f with $n = 2m$ variables, $deg(f) \leq m$. If $deg(f) = m$, f

*Supported by National Natural Science Foundation of China No.61272434,61672330,11571107,11471178 and 61602887

is called a bent function with optimal algebraic degree. We also hope f having large symmetric group in order to store the values of f with less space and allow faster computation of the Walsh transform. In this paper, a symmetry of f means a permutation σ of variables such that $f(x) = f(\sigma(x))$. More exactly speaking, we have the following definition.

Definition 1 *Let Σ_n be the group of all permutations on $\{1, 2, \cdots, n\}$. For $\sigma \in \Sigma_n, x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$, we define*

$$\sigma(x) = (x_{\sigma(1)}, \cdots, x_{\sigma(n)}) \in \mathbb{F}_2^n,$$

and for $f(x) \in \mathscr{B}_n$, we define $\sigma f \in \mathscr{B}_n$ by $(\sigma f)(x) = f(\sigma(x))$. It is known that if f is bent, then σf is bent. The symmetric group of $a \in \mathbb{F}_2^n$ is defined by

$$Sym(a) = \{\sigma \in \Sigma_n : \sigma(a) = a\}$$

The symmetric group of a Boolean function $f \in \mathscr{B}_n$ is defined by

$$Sym(f) = \{\sigma \in \Sigma_n : \sigma f = f\}.$$

We also call any subgroup of $Sym(f)$ as a symmetric group of f.

Let $\sigma = \begin{pmatrix} 1, 2, 3, \cdots, n-1, n \\ 2, 3, 4, \cdots, \quad n \quad, 1 \end{pmatrix} \in \Sigma_n$. A Boolean function $f \in \mathscr{B}_n$ is called rotation symmetric if $\sigma f = f$, namely $f(x_2, \cdots, x_n, x_1) = f(x_1, \cdots, x_n)$. Therefore, any rotation symmetric Boolean function $f \in \mathscr{B}_n$ have a symmetric group $< \sigma >$, a cyclic subgroup of Σ_n with size n. More general, for any $d \geq 1, f$ is called d-rotation symmetric if $\sigma^d(f) = f$. 1-rotation symmetric is just rotation symmetric.

If $n = 2m (m \geq 1)$, $\mathbb{F}_2^n$ can be viewed as $\mathbb{F}_2^m \times \mathbb{F}_2^m$ and any Boolean function $f \in \mathscr{B}_n$ can be expressed by $f(x, y) : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$, where $x, y \in \mathbb{F}_2^m$. For a permutation $\sigma \in \Sigma_m$, we define σf by

$$(\sigma f)(x, y) = f(\sigma(x), \sigma(y)). \tag{1}$$

Let $n = 2m (m \geq 1)$. It is known that the function $f(x) \in \mathscr{B}_n$ defined by

$$f = f(x, y) : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2, f(x, y) = x \cdot y = \sum_{i=1}^{m} x_i y_i, (x, y \in \mathbb{F}_2^m)$$

is a bent function, and $\hat{f} = f (self - dual)$. It is rotation symmetric since for

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix} \in \Sigma_n$$

$$\begin{aligned}(\sigma f)(x, y) = (\sigma f)(x_1, \cdots, x_m, y_1, \cdots, y_m) &= f(x_2, \cdots, x_m, y_1, y_2, \cdots, y_m, x_1) \\ &= x_2 y_2 + \cdots + x_m y_m + y_1 x_1 = x \cdot y = f(x, y).\end{aligned}$$

Moreover, each $\tau \in \Sigma_m$ is also a symmety of f since

$$(\tau f)(x, y) = f(\tau(x), \tau(y)) = \tau(x) \cdot \tau(y) = x \cdot y = f(x, y).$$

Therefore f has a big symmetric group generated by Σ_m and σ. On the other hand, the algebraic degree $deg(f) = 2$ is too small.

Many rotation symmetric bent functions with $deg(f) = 2$ have been found and it is stated in [12] that" any theoretic construction of rotation symmetric bent functions with algebraic degree larger than 2 is an interesting problem". Such bent functions f with $deg(f) = 3$ and 4 have been presented in [4, 5] and

[6] respectively. Recently, rotation symmetric and 2-rotation symmetric bent functions with any $deg(f)$ from 3 to $\frac{n}{2}$ have been constructed in [7, 8].

In this paper, we present a simple construction of bent function $f_{a,S}$ in $\mathscr{B}_n(n=2m, m\geq 2)$, where a is any nonzero vector in $\mathbb{F}_2^m$, S is any subset of $\mathbb{F}_2^m$ satisfying $a+S=S$ (Theorem 1). We show that the dual bent function $\hat{f}_{a,S}$ has a simple expression. We give a simple criterion on $f_{a,S}$ having optimal algebraic degree $deg(f_{a,S})=m$ (Theorem 3). We show that $Sym(a)\cap Sym(S)$ is a symmetric group of $f_{a,S}$(Theorem 4) which implies that $f_{a,S}$ has a large symmetric group if we choose suitable nonzero vector a and subset S of $\mathbb{F}_2^m$, such that $Sym(a)=\{\sigma\in\Sigma_m:\sigma(a)=a\}$ and $Sym(S)=\{\sigma\in\Sigma_m:\sigma(S)=S\}$ have a large intersection. We also construct a large class of $2l$-rotation symmetric bent function for all l(Theorem 5).

This paper is organized as following. We present the construction of bent function $f_{a,S}$, determine the dual bent function and show some relationship between our construction and some previous ones in section 2. We show a criterion for $deg(f_{a,S})=m$ in section 3. Finally, in section 4 we show that $Sym(a)\cap Sym(S)$ is a symmetric group of $f_{a,S}$ and give several examples of bent functions $f_{a,S}$ with optimal algebraic degree and large symmetric group, some of them are d-rotation symmetric for any even d. Section 5 is the conclusion.

2 Construction of Bent Function of $f_{a,S}$

In this section we fix the following notations:

$n=2m$ $(m\geq 2)$;

a : a nonzero vector in $\mathbb{F}_2^m$;

$H=H_a=\{0,a\}^{\perp}=\{v\in\mathbb{F}_2^m,:v\cdot a=0\}$, a hyperplane in $\mathbb{F}_2^m$;

S: a subset of $\mathbb{F}_2^m$ satisfying $a+S=S$. Thus S is a disjoint union of t cosets of $\{0,a\}$ in $(\mathbb{F}_2^m,+)$, $|S|=2t,\ t\geq 1$.

$\Omega=\Omega_{a,S}=\{(x,y)\in\mathbb{F}_2^m\times\mathbb{F}_2^m : x\in H, x+y\in S\}$.

I_U : the indicator function of a subset U in $\mathbb{F}_2^n$ defined by, for $x\in\mathbb{F}_2^n, I(x)=\begin{cases}1, & \text{if } x\in\ U\\ 0, & \text{otherwise}\end{cases}$.

Theorem 1 *The Boolean function $f_{a,S}\in\mathscr{B}_n$ defined by*

$$f_{a,S}(x,y):\mathbb{F}_2^m\times\mathbb{F}_2^m\to\mathbb{F}_2$$

$$f_{a,S}(x,y)=x\cdot y+I_\Omega=\begin{cases}x\cdot y+1, & \textit{if}\ \ (x,y)\in\ \Omega\\ x\cdot y, & \textit{otherwise}\end{cases}.$$

is a bent function and $\hat{f}_{a,S}(x,y)=f_{a,\hat{S}}(y,x)$, where $\hat{S}=S+1_m$ and $1_m=(1,1,\cdots,1)\in\mathbb{F}_2^m$.

Proof. For $x,y\in\mathbb{F}_2^m$, the Walsh transformation of $f=f_{a,S}$ is,

$$\begin{aligned}W_f(x,y) &= \sum_{u,v\in\mathbb{F}_2^m}(-1)^{f(u,v)+u\cdot x+v\cdot y}\\ &= -\sum_{(u,v)\in\Omega}(-1)^{u\cdot v+u\cdot x+v\cdot y}+\sum_{(u,v)\notin\Omega}(-1)^{u\cdot v+u\cdot x+v\cdot y}\\ &= \sum_{u,v\in\mathbb{F}_2^m}(-1)^{u\cdot v+u\cdot x+v\cdot y}-2\sum_{(u,v)\in\Omega}(-1)^{u\cdot v+u\cdot x+v\cdot y}.\end{aligned}$$

The first summation is $2^m(-1)^{x\cdot y}$, the Walsh transformation of $g(u,v)=u\cdot v$. Therefore

$$W_f(x,y)=2^m(-1)^{x\cdot y}-2N,$$

where

$$
\begin{aligned}
N &= \sum_{(u,v)\in\Omega}(-1)^{u\cdot v+u\cdot x+v\cdot y} = \sum_{u\in H, z\in S}(-1)^{(u+y)\cdot(z+u)+u\cdot x} \qquad (z=u+v)\\
&= \sum_{u\in H, z\in S}(-1)^{u\cdot(z+y+x+u)+y\cdot z} = \sum_{z\in S}(-1)^{y\cdot z}\sum_{u\in H}(-1)^{u\cdot\ (z+x+y+1_m)} \qquad (\text{since } u\cdot u = u\cdot 1_m)\\
&= 2^{m-1}\sum_{z+x+y+1_m\in H^\perp=\{0,a\}, z\in S}(-1)^{y\cdot z} \qquad (2^{m-1}=|H|)\\
&= 2^{m-1}\sum_{z\in S, z\in\{x+y+1_m, x+y+1_m+a\}}(-1)^{y\cdot z}
\end{aligned}
$$

If $x+y+1_m \notin S$, then $\{x+y+1_m, x+y+1_m+a\}\cap S=\phi$ and N=0. Otherwise, $\{x+y+1_m, x+y+1_m+a\}\subseteq S$ and

$$
\begin{aligned}
N &= 2^{m-1}((-1)^{y\cdot(x+y+1_m)}+(-1)^{y\cdot(x+y+1_m+a)})\\
&= 2^{m-1}((-1)^{y\cdot x}+(-1)^{y\cdot(x+a)}) \quad (\text{since } y\cdot(y+1_m)=0).
\end{aligned}
$$

Therefore, if $x+y\notin \hat{S}(=S+1_m)$, then

$$W_f(x,y) = 2^m(-1)^{x\cdot y} - 2N = 2^m(-1)^{x\cdot y}.$$

If $x+y\in\hat{S}$, then

$$
\begin{aligned}
W_f(x,y) &= 2^m(-1)^{x\cdot y} - 2^m((-1)^{x\cdot y}+(-1)^{y\cdot x+y\cdot a})\\
&= 2^m(-1)^{y\cdot x+y\cdot a+1}\\
&= \begin{cases} 2^m(-1)^{y\cdot x+1}, & \text{if } y\cdot a=0 \text{ which means that } y\in H\\ 2^m(-1)^{y\cdot x}, & \text{otherwise.}\end{cases}
\end{aligned}
$$

Therefore f is a bent function and

$$\hat{f}(x,y) = \begin{cases} y\cdot x+1, & if\ y\in H\ and\ y+x\in\hat{S}\\ y\cdot x, & \text{otherwise.}\end{cases}$$

Namely, $\hat{f}(x,y) = f_{a,\hat{S}}(y,x)$ where $\hat{S}=S+1_m$ (remark that $a+S=S$ implies $a+\hat{S}=\hat{S}$). This completes the proof. ■

Now we show some relationship between some previous constructions and the construction given by Theorem 1. Our construction of $f_{a,S}$ belongs to the secondary construction where from Rothaus's bent function $f(x,y)=x\cdot y$, we give new bent function $f_{a,S}$ with the same number of variables as f. The vector a and the subset S of $\mathbb{F}_2^m$ can be chosen in much flexible way (just need $a\neq 0$ and $a+S=S$). One of secondary construction was given by Carlet[9] as following.

Lemma 1 *([9], also see [3] Theorem 6.0.1) Let E be a subspace of $\mathbb{F}_2^n$, $b\in\mathbb{F}_2^n$, $f\in\mathscr{B}_n$ be a bent function. Then $f^*=f+I_{b+E}$ is bent if and only if the following condition (*) holds.*

(*) For any $v\in\mathbb{F}_2^n\setminus E, f(x)+f(x+v)$ is balanced on $b+E$.

For the construction in Theorem 1, $f(x,y)=x\cdot y$, $(x,y\in\mathbb{F}_2^m, n=2m)$, $f^*=f+I_\Omega$, where $\Omega=\{(x,y): x\in H, , x+y\in S\}$. If Ω is a flat $b+E$ in $\mathbb{F}_2^n$, then for any $v\in\mathbb{F}_2^n\setminus E$, $v=(v_1,v_2)$ is a nonzero vector and the affine function

$$f(x,y)+f(x+v_1,y+v_2) = x\cdot y+(x+v_1)\cdot(y+v_2) = v_2\cdot x+v_1\cdot y+v_2\cdot v_1$$

is balanced on flat $\Omega=b+E$. Thus the condition (*) holds and the bentness of $f_{a,S}$ is derived by Lemma 1. But for many S, Ω is not a flat of $\mathbb{F}_2^n$. So Theorem 1 can provide some new bent functions.

Another interesting secondary construction was given by Carlet [10] and S. Mesnager [11] which shows that if f_1, f_2, f_3 are bent functions in $\mathscr{B}_n$ satisfying certain conditions, then $f_1f_2 + f_2f_3 + f_3f_1$ is also bent. We will show that our bent functions $f_i = f_{a,S_i}(i = 1, 2, 3)$ fit in this secondary construction: $f_1f_2 + f_2f_3 + f_3f_1$ is also bent without any extra conditions on a and $S_i(1 \le i \le 3)$. In fact, we have the following more general result. For Boolean functions $f_1, \cdots, f_N$ in $\mathscr{B}_n, 1 \le t \le N$, we denote the $t-$th elementary symmetric function of $f_1, \cdots, f_N$ by

$$\sigma_t(f_1, \cdots, f_N) = \sum_{\substack{A \subseteq \{1, \cdots, N\} \\ |A| = t}} \prod_{i \in A} f_i.$$

Theorem 2 *let $n = 2m(m \ge 3)$, a be a fixed nonzero vector in $\mathbb{F}_2^m$, S_i be the subsets of $\mathbb{F}_2^m$ such that $a + S_i = S_i, f_i = f_{a,S_i}, 1 \le i \le N$ be the bent functions in $\mathscr{B}_n$ given in Theorem 1. Let $1 \le t \le N$. If $\binom{N}{N-t}$ is odd and $\binom{N-j}{N-t}, 1 \le j \le t-1$, are even, then $\sigma_t(f_1, \cdots, f_N) \in \mathscr{B}_n$ is bent. Particularly (N=3 and $t = 2$), $f_1f_2 + f_2f_3 + f_3f_1$ is bent.*

Proof. Let $\Omega_i = \{(x, y) : x \cdot a = 0, x + y \in S_i\}, 1 \le i \le N$. Then $f_i(x, y) = x \cdot y + I_i(x, y)$, where $I_i(x, y) = I_{\Omega_i}(x, y)$ is the indicator function of Ω_i. For a subset A of $\{1, 2, \cdots, N\}, |A| = t$,

$$\begin{aligned} \prod_{i \in A} f_i(x, y) &= \prod_{i \in A} (x \cdot y + I_i(x, y)) \\ &= (x \cdot y)[1 + \sigma_1(I_i(x, y) : i \in A) + \cdots + \sigma_{t-1}(I_i(x, y) : i \in A)] + \prod_{i \in A} I_i(x, y). \end{aligned}$$

Therefore

$$\begin{aligned} \sigma_t(f_1, \cdots, f_N) &= \sum_{\substack{A \subseteq \{1, \cdots, N\} \\ |A| = t}} \prod_{i \in A} f_i \\ &= (x \cdot y)[\binom{N}{t} + \binom{N-1}{t-1}\sigma_1(I_1, \cdots, I_N) + \binom{N-2}{t-2}\sigma_2(I_1, \cdots, I_N) + \cdots \\ &+ \binom{N-(t-1)}{t-(t-1)}\sigma_{t-1}(I_1, \cdots, I_N)] + \sigma_t(I_1, \cdots, I_N). \end{aligned}$$

Since for each $j, 1 \le j \le t-1$, the number of subset $A(|A| = t)$ of $\{1, 2, \cdots, N\}$ containing a fixed subset of size j is $\binom{N-j}{t-j}$. By assumption,

$$\binom{N}{t} = \binom{N}{N-t} \equiv 1(\text{mod}2), \binom{N-j}{t-j} = \binom{N-j}{N-t} \equiv 0(\text{mod}2), 1 \le j \le t-1.$$

We get

$$\sigma_t(f_1, \cdots, f_N) = x \cdot y + \sigma_t(I_1, \cdots, I_N).$$

For $A \subseteq \{1, 2, \cdots, N\}, |A| = t$, it is easy to see that

$$\prod_{i \in A} I_i = \prod_{i \in A} I_{\Omega_{S_i}}(x, y) = I_{\Omega_{S(A)}}(x, y),$$

where $S(A) = \bigcap_{i \in A} S_i$. Remark that from $a + S_i = S_i$ we know that $a + S(A) = S(A)$. Then we have

$$\sigma_t(I_1, \cdots, I_N) = \sum_{\substack{A \subseteq \{1, \cdots, N\} \\ |A| = t}} \prod_{i \in A} I_i = \sum_{\substack{A \subseteq \{1, \cdots, N\} \\ |A| = t}} I_{\Omega_{S(A)}}(x, y) = I_{\Omega_{S(t)}}(x, y),$$

where $S(t)$ is the "Symmetric difference" of $\{S(A) : |A| = t\}$ defined by

$S(t) = \{v \in \mathbb{F}_2^m$: the number of $A, A \subseteq \{1, \cdots, N\}, |A| = t$ such that $v \in S(A)$ is odd $\}$.

From $a + S(A) = S(A)$ for each $A \subseteq \{1, \cdots, N\}, |A| = t$ we know that $a + S(t) = S(t)$. By Theorem 1,

$$\sigma_t(f_1, \cdots, f_N) = x \cdot y + \sigma_t(I_1, \cdots, I_N) = x \cdot y + I_{\Omega_{S(t)}}(x, y)$$

is bent. This completes the proof of Theorem 2. ■

Remark By the Lucas formula, it is not difficult to see that for $1 \leq t \leq N$, the conditions $2 \nmid \binom{N}{N-t}$ and $2|\binom{N-j}{N-t}$ for $1 \leq j \leq t-1$ hold if and only if $t = 2^m$ and $N = 2^{m+2}s + 2^{m+1} - 1$ where $s \geq 0$ and $m \geq 1$.

At last, we find that the second construction given by Su and Tang [7] is very closed to our construction. Let $n = 2m \geq 4, \Gamma$ be any non-empty subset of $\mathbb{F}_2^m, \Omega' = \{(x, y) : x \in \mathbb{F}_2^m, x+y \in \Gamma\}$ and $f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ be the function defined by

$$f(x, y) \quad = \quad \begin{cases} x \cdot y + 1, & \text{if } (x, y) \in \Omega' \\ x \cdot y, & \text{otherwise.} \end{cases}$$

Su and Tang proved that $f(x, y)$ is a bent function ([7], Lemma 3). This construction is different from our construction in Theorem 1 since for $(x, y) \in \Omega'$, x can be any vector in $\mathbb{F}_2^m$, but for $(x, y) \in \Omega$ in our construction, x is taken from a hyperplane of $\mathbb{F}_2^m$.

3 The Optimality of Algebraic Degree $deg(f_{a,S})$

In this section we present a simple criterion on the bent function $f_{a,S} \in \mathscr{B}_n$ having optimal algebraic degree $\frac{n}{2}$.

Theorem 3 *Let $n = 2m, m \geq 3, f_{a,S}$ be the bent function given in Theorem 1 and $|S| = 2t (t \geq 1)$. Then $deg(f_{a,S}) = m$ if and only if t is odd.*

Proof. Firstly we need to get the polynomial expression of $f_{a,S}(x, y) = f_{a,S}(x_1, \cdots, x_m, y_1, \cdots, y_m)$ in $\mathbb{F}_2[x_1, \cdots, x_m, y_1, \cdots, y_m]/(x_i^2 - x_i, y_i^2 - y_i (1 \leq i \leq m))$. It is easy to see that for $x = (x_1, \cdots, x_m), y = (y_1, \cdots, y_m), a = (a_1, \cdots, a_m) \in \mathbb{F}_2^m$,

$$\begin{aligned} x \in H \quad &\Leftrightarrow \quad x \cdot a = 0 \Leftrightarrow a_1x_1 + \cdots + a_mx_m + 1 = 1. \\ x + y = v = (v_1, \cdots, v_m) \quad &\Leftrightarrow \quad (x_1 + y_1 + v_1 + 1) \cdots (x_m + y_m + v_m + 1) = 1 \end{aligned}$$

Therefore $f_{a,S}(x, y) = x \cdot y + g(x, y)$, where

$$\begin{aligned} g(x, y) \quad &= \quad \begin{cases} 1, & \text{if } x \in H \text{ and } x + y \in S \\ 0, & \text{otherwise.} \end{cases} \\ &= \quad (a_1x_1 + \cdots + a_mx_m + 1) \sum_{v=(v_1,\cdots,v_m)\in S} (x_1 + y_1 + v_1 + 1) \cdots (x_m + y_m + v_m + 1) \\ &= \quad \sum_{v \in S} h_v(x, y), \end{aligned} \tag{2}$$

where

$$h_v(x, y) = (a_1x_1 + \cdots + a_mx_m + 1)(x_1 + y_1 + v_1 + 1) \cdots (x_m + y_m + v_m + 1), v \in S. \tag{3}$$

From assumption $m \geq 3$ we know that $deg(f_{a,S}) = m$ if and only if $deg(g) = m$. Since $deg(f) \leq m$ for any bent function $f \in \mathscr{B}_n$, we know that $deg(g) = deg(f_{a,S}) \leq m$. The monomials of degree m are

$$x_I y_{\bar{I}} = \prod_{i \in I} x_i \prod_{j \in \bar{I}} y_j \quad (I \subseteq \{1, \cdots, m\}, \bar{I} = \{1, \cdots, m\} \setminus I).$$

Let $c_I \in \mathbb{F}_2$ be the coefficient of $x_I y_{\bar{I}}$ in the polynomial expression of $h_v(x, y)$ given by the right-hand side of (3). Then

$$\begin{aligned} c_I &= \text{the coefficient of } x_I \text{ in } (1 + \sum_{j \in I} a_j x_j) \prod_{i \in I} (x_i + v_i + 1) \\ &= 1 + \text{the coefficient of } x_I \text{ in } (\sum_{j \in I} a_j x_j) \prod_{i \in I} (x_i + v_i + 1). \end{aligned}$$

But

$$\begin{aligned} (\sum_{j \in I} a_j x_j) \prod_{i \in I} (x_i + v_i + 1) &= \sum_{j \in I} a_j (1 + v_j + 1) x_j \prod_{\substack{i \in I \\ i \neq j}} (x_i + v_i + 1) \\ &= \sum_{j \in I} a_j v_j x_j \prod_{\substack{i \in I \\ i \neq j}} (x_i + v_i + 1). \end{aligned}$$

Therefore

$$c_I = \sum_{j \in I} a_j v_j + 1$$

and the coefficient of $x_I y_{\bar{I}}$ in (the polynomial expression of) $h_{v+a}(x, y)$ is $\sum_{j \in I} a_j (v_j + a_j) + 1$. For one pair $\{v, v + a\}$ in S, the coefficient of $x_I y_{\bar{I}}$ in $h_v(x, y) + h_{v+a}(x, y)$ is $\sum_{j \in I} [(a_j v_j + 1) + (a_j v_j + a_j + 1)] = \sum_{j \in I} a_j$, which is independent from v. There are t pairs of $\{v, v + a\}$ in S. Therefore the coefficient of $x_I y_{\bar{I}}$ in $g(x, y) = \sum_{v \in S} h_v(x, y)$ is $t \sum_{j \in I} a_j$. If t is even, then all coefficients of monomials $x_I y_{\bar{I}}$ with degree m in $g(x, y)$ are zero, which implies both $deg(f_{a,S})$ and $deg(g)$ are less than m. On the other hand, suppose that t is odd, from $0 \neq a = (a_1, \cdots, a_m) \in \mathbb{F}_2^m$ we know that there exits i such that $a_i = 1$. Choosing $I = \{i\}$, then the coefficient of $x_I y_{\bar{I}}$ in $g(x, y)$ is $t a_i = 1 \in \mathbb{F}_2$. Hence $deg(f_{a,S}) = deg(g) = m$. This completes the proof of Theorem 3. ■

4 The Symmetric Group of $f_{a,S}$ and Some Examples

Let Σ_m be the group of permutations on $\{1, 2, \cdots, m\}, m \geq 2, \sigma \in \Sigma_m$. For $a = (a_1, \cdots, a_m) \in \mathbb{F}_2^m$, $S \subseteq \mathbb{F}_2^m$, we define

$$\sigma(a) = (a_{\sigma(1)}, \cdots, a_{\sigma(n)}), \quad \sigma(S) = \{\sigma(v) : v \in S\}.$$

The symmetric group of a and S are defined by

$$Sym(a) = \{\sigma \in \Sigma_m : \sigma(a) = a\}, Sym(S) = \{\sigma \in \Sigma_m : \sigma(S) = S\}.$$

Let $n = 2m$. For $\sigma \in \Sigma_m$ and a Boolean function $f = f(x, y) \in \mathscr{B}_n (x, y \in \mathbb{F}_2^m)$, we define $\sigma f \in \mathscr{B}_n$ by

$$(\sigma f)(x, y) = f(\sigma(x), \sigma(y)).$$

Then $\{\sigma \in \Sigma_m : \sigma f = f\}$ is a symmetric group of f.

Theorem 4 *Let $n = 2m (m \geq 2), f_{a,S}(x, y)$ be the bent function in $\mathscr{B}_n$ defined in Theorem 1. Then $Sym(a) \cap Sym(S)$ is a symmetric group of $f_{a,S}$ and $\hat{f}_{a,S}$.*

Proof. Suppose that $\sigma \in G = Sym(a) \cap Sym(S)$. From $H = \{0, a\}^{\perp}$ we get $Sym(H) = Sym(a)$. By the definition, $f_{a,S}(x, y) = x \cdot y$ or $x \cdot y + 1$, $(\sigma f_{a,S})(x, y) = f_{a,S}(\sigma(x), \sigma(y)) = \sigma(x) \cdot \sigma(y) = x \cdot y$ or $x \cdot y + 1$. But

$$\begin{aligned} f_{a,S}(x, y) = x \cdot y + 1 \quad & \Leftrightarrow x \in H \text{ and } x + y \in S \\ & \Leftrightarrow \sigma(x) \in H \text{ and } \sigma(x) + \sigma(y) = \sigma(x + y) \in S \text{ (since } \sigma \in Sym(H) \cap Sym(S)) \\ & \Leftrightarrow f_{a,S}(\sigma(x), \sigma(y)) = \sigma(x) \cdot \sigma(y) + 1 = x \cdot y + 1. \end{aligned}$$

Therefore, $\sigma(f_{a,S}) = f_{a,S}$ and then, $Sym(a) \cap Sym(S)$ is a symmetric group of $f_{a,S}$.

Finally, $\hat{f}_{a,S}(x, y) = f_{a,\hat{S}}(y, x)$ where $\hat{S} = S + \mathtt{1}_m$. It is easy to see that $Sym(S) = Sym(\hat{S})$. Therefore $Sym(a) \cap Sym(S) = Sym(a) \cap Sym(\hat{S})$ is also a symmetric group of $\hat{f}_{a,S}$. This completes the proof of Theorem 4. ■

The following results show that our construction (Theorem 1) can produce several d-rotation symmetric bent functions for all even d.

Theorem 5 *Let $n = 2m \geq 4, f_{a,S}(x, y)$ be the bent function in $\mathscr{B}_n$ constructed in Theorem 1, and $g_{a,S}(z) \in \mathscr{B}_n$ is defined by*

$$g_{a,S}(z) = g_{a,S}(z_1, z_2, \cdots, z_n) = f_{a,S}(z_1, z_3, \cdots, z_{2m-1}, z_2, z_4, \cdots, z_{2m}).$$

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & m-1 & m \\ 2 & 3 & 4 & \cdots & m & 1 \end{pmatrix} \in \Sigma_m$, and $1 \leq l \leq \frac{m}{2} - 1$. If $\sigma^l(a) = a$ and $\sigma^l(S) = S$, then $g_{a,S}(z)$ is a $2l$-rotation symmetric bent function.

Proof. Suppose that $\sigma^l(a) = a$ and $\sigma^l(S) = S$. By Theorem 4 we know that $(\sigma^l f_{a,S})(x, y) = f_{a,S}(x, y)$. Then we get

$$\begin{aligned} g_{a,S}(z_{2l+1}, z_{2l+2}, \cdots, z_{2l}) \quad & = f_{a,S}(z_{2l+1}, z_{2l+3}, \cdots, z_{2l-1}, z_{2l+2}, z_{2l+4}, \cdots, z_{2l}) \\ & = f_{a,S}(\sigma^l(x), \sigma^l(y)) \ (x = (z_1, z_3, \cdots, z_{2m-1}), y = (z_2, z_4, \cdots, z_{2m})) \\ & = (\sigma^l f_{a,S})(x, y) = f_{a,S}(x, y) = g_{a,S}(z_1, z_2, \cdots, z_m), \end{aligned}$$

which means that $g_{a,S}(z)$ is $2l$-rotation symmetric. ■

At the end of this section, we show some examples of bent functions $f_{a,S}$ and their dual bent function $\hat{f}_{a,S}$ with optimal algebraic degree and large symmetric group by choosing a and S properly.

Example 1 *Let a be any nonzero vector in $\mathbb{F}_2^m (m \geq 3), S = \{0, a\}$. Then*

$$f_{a,S}(x, y) \quad = \quad \begin{cases} x \cdot y + 1, & \text{if } x \cdot a = 0 \text{ and } \ y = x \text{ or } x + a \\ x \cdot y, & \text{otherwise.} \end{cases}$$

$$\hat{f}_{a,S}(x, y) \quad = \quad f_{a,S+\mathtt{1}_m}(y, x) = \begin{cases} x \cdot y + 1, & \text{if } y \cdot a = 0 \text{ and } \ x = y + \mathtt{1}_m \text{ or } y + a + \mathtt{1}_m \\ x \cdot y, & \text{otherwise.} \end{cases}$$

By Theorem 1, 3, 4, we know that $f_{a,S}$ and $\hat{f}_{a,S}$ are bent functions in $\mathscr{B}_n, n = 2m$ with optimal algebraic degree and $Sym(a)$ is a symmetric group for both of them. Particularly, if $a = \mathtt{1}_m$, then $f_{\mathtt{1}_m,S}$ and $\hat{f}_{\mathtt{1}_m,S}$ have a large symmetric group $Sym(\mathtt{1}_m) = \Sigma_m$.

Example 2 *Let $a = 1_m \in \mathbb{F}_2^m, m \geq 3$, $S_j = \{v \in \mathbb{F}_2^m : wt_H(v) = i\}, 0 \leq i \leq m$, where $wt_H(v)$ is the Hamming weight of v. It is easy to see that $1_m + S = S_{m-i}$. Let I be the subset of $\{0, 1, \cdots, [\frac{m-1}{2}]\}$ and*

$$S_I = \bigcup_{i \in I} (S_i \cup S_{m-i}).$$

Then $1_m + S_I = S_I$ *and* $|S_I| = \sum_{i\in I}(\binom{m}{i} + \binom{m}{m-i}) = 2\sum_{i\in I}(\binom{m}{i})$. *From* $Sym(S_i) = \Sigma_m$ *we get* $Sym(S_I) = \Sigma_m = Sym(1_m)$. *Therefore if* $\sum_{i\in I}\binom{m}{i}$ *is odd, then* f_{1_m,S_I} *is bent function in* $\mathscr{B}_n, n = 2m$ *with optimal algebraic degree and have* Σ_m *as a symmetric group. Taking* $I = \{0\}$ *and* $S = S_I = \{0, 1_m\}$, *we get the bent function* $f_{1_m,S}$ *in example 1.*

The following example shows that our construction can provide many self-dual bent functions under some conditions on N and t.

Example 3 *Let* $n = 2m, m \geq 3, a$ *be any nonzero vector in* $\mathbb{F}_2^m$ *with even* $wt_H(a)$, $H = \{v \in \mathbb{F}_2^m : v \cdot a = 0\}$. *Then* $a \in H$ *and* $1_m \in H$ *since* $a \cdot a = 1_m \cdot a = wt_H(a)$. *Let* S *be an union of several cosets of* $\{0, a, 1_m, 1_m + a\}$ *in* H *(if* $a = 1_m$, *then* $\{0, a, 1_m, 1_m + a\} = \{0, 1_m\}$*). Then* $a + S = 1_m + S = S$. *By Theorem 1,* $f_{a,S}$ *is a bent function in* $\mathscr{B}_n$ *and*

$$\hat{f}_{a,S}(x, y) = f_{a,S+1_m}(y, x) = f_{a,S}(y, x).$$

Moreover, for $x, y \in \mathbb{F}_2^m$, *from* $S \subseteq H$ *we know that* $x \in H$ *and* $x + y \in S \Leftrightarrow y \in H$ *and* $x + y \in S$.

Therefore $\hat{f}_{a,S}(x, y) = f_{a,S}(y, x) = f_{a,S}(x, y)$ *which means that* $f_{a,S}$ *is self-dual. If* $a = 1_m \in \mathbb{F}_2^m, m$ *is even and* S *is an union of odd number of cosets of* $\{0, 1_m\}$ *in* H, *then* $f_{a,S}$ *has optimal algebraic degree.*

The last example shows that our construction can provide d- rotation symmetric bent functions for each even $d \geq 2$.

Example 4 *Let* $n = 2m, m = ls$. *For a vector* $v = (v_1, v_2, \cdots, v_l) \in \mathbb{F}_2^l$, *let* $\tau(v) = (v_2, v_3, \cdots, v_l, v_1)$. *The period of* v *is the least positive integer* p *such that* $\tau^p(v) = v$. *Let* $c, c_\lambda (1 \leq \lambda \leq t)$ *be nonzero vectors in* $\mathbb{F}_2^l$ *such that the period of* c_λ *is* l, *and* $\bigcup_{\lambda=1}^{t}\bigcup_{i=0}^{l-1}\tau^i(c_\lambda)A$ *is a disjoint union of* tl *cosets of* $A = \{0, c\}$ *in* $\mathbb{F}_2^l$. *(For example, we take* $c = (1, \cdots, 1) \in \mathbb{F}_2^l, (l \geq 3), c_1 = (1, 0 \cdots, 0), t = 1$ *). Let* $a = \underbrace{(c, c, \cdots, c)}_{s} \in \mathbb{F}_2^m, a_\lambda = \underbrace{(c_\lambda, c_\lambda, \cdots, c_\lambda)}_{s} \in \mathbb{F}_2^m$. *Then for* $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & m-1 & m \\ 2 & 3 & 4 & \cdots & m & 1 \end{pmatrix} \in \Sigma_m, S = \bigcup_{\lambda=1}^{t}\bigcup_{i=0}^{l-1}\sigma^i(a_\lambda)B$ *is a disjoint union of* tl *cosets of* $B = \{0, a\}, |\, S \,| = 2tl$. *It is easy to see that* $\sigma^l(a) = a$ *and* $\sigma^l(S) = S$. *By Theorem 5,* $g_{a,S}(x, y)$ *is a* $2l$*-rotation symmetric bent function. Moreover, if* tl *is odd, then* $deg(g_{a,S}) = m$.

5 Conclusions

In this paper, a large number of bent Functions with optimal algebraic degree and large symmetric group are given. We present a new construction of bent function $f_{a,S}$ in $\mathscr{B}_n(n = 2m, m \geq 2)$ by flipping the famous bent function $f(x, y) = x \cdot y$ on the direct product of $H = \{0, a\}^\perp$ and $S \subseteq \mathbb{F}_2^m, a + S = S$. The vector a and set S can be chosen in much flexible way. And the dual bent function $\hat{f}_{a,S}$ has a simple expression. Most surprisingly, elementary symmetric functions $\sigma_t(f_1, \cdots, f_N)$ based on $f_i = f_{a,S_i}$ are also bent functions. We propose a simple criterion on $f_{a,S}$ having optimal algebraic degree $deg(f_{a,S}) = m$ and show that $Sym(a) \cap Sym(S)$ is a symmetric group of $f_{a,S}$. Furthermore, our construction can produce several d-rotation symmetric bent functions for all even d. Besides the strict demonstration of the correctness of our construction, we also give some examples of that bent functions $f_{a,S}$ and their dual bent functions.

References

[1] O. S. Rothaus. On bent Functions. Journal of Combinatorial Theory, Series A vol.20(3): 300-305,1976.

[2] Dillon, J.F. Elementary hadamard difference sets. Ph.D. Thesis, University of Maryland, College Park, 1974.

[3] S. Mesnager. Bent functions. Springer International Publishing Switzeland, 2016.

[4] C. Carlet, G. Gao, and W. Liu, A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions. Journal of Combinatorial Theory, Series A, vol.127(1): 161-175, 2014.

[5] G. Gao, X. Zhang, W. Liu, and C. Carlet, Constructions of quadratic and cubic rotation symmetric bent functions. IEEE Transactions on Information Theory, vol.58(7):4908-4913, 2012.

[6] C. Carlet, G. Gao, and W. Liu, Results on constructions of rotation symmetric bent and semi-bent functions. In SETA 2014, Springer International Publishing Switzerland, 2014, Lecture Notes in Computer Science, vol.8865: pp. 21-33, 2014

[7] S. Su and X. Tang. Systematic Constructions of Rotation Symmetric Bent Functions, 2-Rotation Symmetric Bent Functions, and Bent Idempotent Functions. To appear in IEEE Transactions on Information Theory 2017. DOI 10.1109/TIT.2016.2621751.

[8] C. Tang, Y. Qi, Z. Zhou, C. Fan. Two infinite classes of rotation symmetric bent functions with simple representation. arXiv preprint arXiv:1508.05674, 2015.

[9] C. Carlet. Two New Classes of Bent Functions. EUROCRYPT 1993 Lecture Notes in Computer Science, vol.765: pp.77-101, 1994.

[10] C. Carlet. On Bent and Highly Nonlinear Balanced/Resilient Functions and Their Algebraic Immunities. In AAECC 2006, Lecture Notes in Computer Science, vol.3857: pp.1-28, 2006.

[11] S. Mesnager. Several New Infinite Families of Bent Functions and Their Duals. IEEE Transactions on Information Theory, 60(7):4397-4407, 2014.

[12] D. K. Dalai, S. Maitra, S.Sarkar. Results on rotation symmetric bent functions. Discrete Math. vol.309: pp.2398-2409, 2009.