AAECC (2018) 29:197–208
https://doi.org/10.1007/s00200-017-0337-8

ORIGINAL PAPER

Two infinite classes of rotation symmetric bent functions with simple representation

Chunming Tang[1] · Yanfeng Qi[2] ·
Zhengchun Zhou[3] · Cuiling Fan[3]

Received: 30 October 2016 / Revised: 24 April 2017 / Accepted: 23 July 2017 /
Published online: 18 August 2017

Abstract In the literature, few n-variable rotation symmetric bent functions have been constructed. In this paper, we present two infinite classes of rotation symmetric bent functions on $\mathbb{F}_2^n$ of the two forms:

(i) $f(x) = \sum_{i=0}^{m-1} x_i x_{i+m} + \gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1})$,
(ii) $f_t(x) = \sum_{i=0}^{n-1}(x_i x_{i+t} x_{i+m} + x_i x_{i+t}) + \sum_{i=0}^{m-1} x_i x_{i+m} + \gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1})$,

where $n = 2m$, $\gamma(X_0, X_1, \ldots, X_{m-1})$ is any rotation symmetric polynomial, and $m/gcd(m, t)$ is odd. The class (i) of rotation symmetric bent functions has algebraic degree ranging from 2 to m and the other class (ii) has algebraic degree ranging from 3 to m. Moreover, the two classes of rotation symmetric bent functions are disjoint.

Keywords Bent functions · Rotation symmetric bent functions · The Maiorana–McFarland class of bent functions · Algebraic degree

✉ Chunming Tang
tangchunmingmath@163.com

Yanfeng Qi
qiyanfeng07@163.com

Zhengchun Zhou
zzc@swjtu.edu.cn

Cuiling Fan
fcl@swjtu.edu.cn

[1] School of Mathematics and Information, China West Normal University, Nanchong 637002, Sichuan, China

[2] School of Science, Hangzhou Dianzi University, Hangzhou 310018, Zhejiang, China

[3] School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China

Mathematics Subject Classification 06E75 · 94A60 · 11T23

1 Introduction

Boolean bent functions introduced by Rothaus [37] are an interesting combinatorial object with the maximum Hamming distance to the set of all affine functions. Such functions have been extensively studied because of their important applications in cryptography (stream ciphers [5]), sequences [33], graph theory [35], coding theory (Reed–Muller codes [13], two-weight and three-weight linear codes [1,17]), and association schemes [36]. A complete classification of bent functions is still elusive. Further, not only their characterization, but also their generation are challenging problems. Many papers on bent functions are devoted to the construction of bent functions [2–5,9,11,12,15,16,18,22–32,42].

Rotation symmetric Boolean functions, introduced by Pieprzyk and Qu [34], are invariant under circular translation of indices. Due to less space to be stored and allowing faster computation of the Walsh transform, they are of great interest. They can be obtained from idempotents (and vice versa) [19,20]. Characterizing and constructing rotation symmetric bent functions are difficult and have theoretical and practical interest. The dual of a rotation symmetric bent function is also a rotation symmetric bent function. In the literature, few constructions of bent idempotents have been presented, which are restricted by the number of variables and have algebraic degree no more than 4. See more rotation symmetric bent functions in [7,8,14,21,38–40].

Quadratic rotation symmetric bent functions have been characterized by Gao et al. [21]. They proved that the quadratic function

$$\sum_{i=1}^{m-1} c_i \left(\sum_{j=0}^{n-1} x_j x_{i+j} \right) + c_m \left(\sum_{j=0}^{m-1} x_j x_{m+j} \right)$$

is rotation symmetric bent if and only if the polynomial $\sum_{i=1}^{m-1} c_i (X^i + X^{n-i}) + c_m X^m$ is coprime with $X^n + 1$, where $c_i \in \mathbb{F}_2$. Stanica et al. [38] conjectured that there are no homogeneous rotation symmetric bent functions of algebraic degree greater than 2. The construction of rotation symmetric bent functions of algebraic degree greater than 2 is an interesting problem [6]. Charnes et al. [10] constructed homogeneous bent functions of algebraic degree 3 in 8, 10, and 12 variables by applying the machinery of invariant theory. Up to now, there are few known constructions of rotation symmetric bent functions. Gao et al. [21] constructed an infinite class of cubic rotation symmetric bent functions of the form

$$f_t(x_0, x_1, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} (x_i x_{i+t} x_{i+m} + x_i x_{i+t}) + \sum_{i=0}^{m-1} x_i x_{i+m},$$

where $1 \leq t \leq m - 1$ and $m/gcd(m, t)$ is odd. Carlet et al. [7] presented n-variable cubic rotation symmetric bent functions of the form

$$f(x_0, x_1, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} x_i x_{i+r} x_{i+2r} + \sum_{i=0}^{2r-1} x_i x_{i+2r} x_{i+4r} + \sum_{i=0}^{m-1} x_i x_{i+m},$$

where $n = 2m = 6r$. Carlet et al. [8] proposed an infinite class of quartic rotation symmetric bent functions from two known semi-bent rotation symmetric functions by the indirect sum. Su and Tang [40] gave a class of n-variable rotation symmetric bent functions of any possible algebraic degree ranging from 2 to $n/2$ of the form

$$f(x) = \sum_{i=0}^{m-1} x_i x_{i+m} + \sum_{\delta \in A} \sum_{\beta' \boxplus \beta'' \in \mathcal{O}_m(\delta)} \prod_{i=0}^{m-1} x_i^{\beta'} x_{i+m}^{\beta''}, \tag{1}$$

where

- $\delta \in \mathbb{F}_2^m$.
- $\mathcal{O}_n(\delta)$ is the orbit of δ by cyclic shift.
- A is a subset of the representative elements of all the orbits $\mathcal{O}_m(\delta)$.
- $\beta' = (\beta'_0, \beta'_1, \ldots, \beta'_{m-1})$ and $\beta'' = (\beta''_0, \beta''_1, \ldots, \beta''_{m-1})$.
- $\boxplus$ denotes the sum over $\mathbb{Z}$.

These functions contain functions by Carlet et al. [7].

Motivated by the constructions of Gao et al. [21] and Su et al. [40], this paper constructs new rotation symmetric bent functions from some known rotation symmetric bent functions. We obtain two infinite classes of rotation symmetric bent functions which are equivalent to functions in the class of Maiorana–McFarland. Let $\gamma(X_0, X_1, \ldots, X_{m-1})$ be a rotation symmetric polynomial in $\mathbb{F}_2[X_0, X_1, \ldots, X_{m-1}]$, i.e., $\gamma(X_0, X_1, \ldots, X_{m-1}) = \gamma(X_1, \ldots, X_{m-1}, X_0)$. We obtain two classes of rotation symmetric bent functions of the form

$$f(x) = \sum_{i=0}^{m-1} x_i x_{i+m} + \gamma(x_0 + x_m, \ldots, x_{m-1} + x_m),$$

$$f_t(x) = \sum_{i=0}^{n-1} (x_i x_{i+t} x_{i+m} + x_i x_{i+t}) + \sum_{i=0}^{m-1} x_i x_{i+m} + \gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1}),$$

where $1 \le t \le m-1$ and $m/gcd(m,t)$ is odd. In fact, these bent functions belong to the Maiorana–McFarland class of bent functions. Moreover, the two classes of rotation symmetric bent functions are disjoint.

The rest of the paper is organized as follows. Section 2 introduces some basic notations of Boolean functions and rotation symmetric bent functions. Section 3 presents the constructed rotation symmetric bent functions. Section 4 proves main results on rotation symmetric bent functions. Section 5 makes a conclusion.

2 Preliminaries

Let $\mathbb{F}_2^n$ denote the n-dimensional vector space over the finite field $\mathbb{F}_2$. An n-variable Boolean function $f(x_0, x_1, \ldots, x_{n-1})$ is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. And $f(x_0, x_1, \ldots, x_{n-1})$ can be represented by a polynomial called its algebraic normal form (ANF):

$$f(x_0, x_1 \ldots, x_{n-1}) = \sum_{u \in \mathbb{F}_2^n} c_u \left(\prod_{i=0}^{n-1} x_i^{\beta_i} \right), \tag{2}$$

where $u = (\beta_0, \beta_1, \ldots, \beta_{n-1})$ and $c_u \in \mathbb{F}_2$. The number of variables in the highest order product term with nonzero coefficient is called its algebraic degree.

Definition 1 A Boolean function f over $\mathbb{F}_2^n$ or an algebraic normal form f in $\mathbb{F}_2[x_0, x_1, \ldots, x_{n-1}]$ is called rotation symmetric if for each input $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$, we have

$$f(x_1, x_2, \ldots, x_{n-1}, x_0) = f(x_0, x_1, \ldots, x_{n-1}).$$

The Walsh transform of a Boolean function calculates the correlations between the function and linear Boolean functions. The Walsh transform of f over $\mathbb{F}_2^n$ is

$$\mathcal{W}_f(b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+b\cdot x},$$

where $b = (b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_2^n$, $x = (x_0, x_1, \ldots, x_{n-1})$, and $b \cdot x = \sum_{i=0}^{n-1} x_i b_i$.

Definition 2 A Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is a bent function if $\mathcal{W}_f(b) = \pm 2^{n/2}$ for any $b \in \mathbb{F}_2^n$.

A Boolean bent function only exists for even n. The algebraic degree of a bent function is no more than m for $n = 2m \geq 4$ and the algebraic degree of a bent function for $n = 2$ is 2.

Let σ be a permutation of $\mathbb{F}_2^n$ such that for any bent function f, $f \circ \sigma$ is also bent. Then $\sigma(x) = xA + b$, where A is an $n \times n$ nonsingular binary matrix over $\mathbb{F}_2$, xA is the product of the row-vector x and A, and $b \in \mathbb{F}_2^n$. All these permutations form an automorphism of the set of bent functions. Two functions $f(x)$ and $g(x) = f \circ \sigma(x)$ are called linearly equivalent. If $f(x)$ is bent and $L(x)$ is an affine function, then $f + L$ is also a bent function. Two functions f and $f \circ \sigma + L$ are called EA-equivalent. The completed version of a class is the set of all functions, which are EA-equivalent to the functions in the class.

Maiorana and McFarland [26] introduced independently a class of bent functions by concatenating affine functions. This class is called the Maiorana–McFarland class $\mathcal{M}$ of functions defined over $\mathbb{F}_2^m \times \mathbb{F}_2^m$ of the form

$$f(a, y) = y \cdot \pi(a) + h(a), \tag{3}$$

where $(a, y) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$, $\pi(a)$ is any mapping from $\mathbb{F}_2^m$ to $\mathbb{F}_2^m$, and $h(a)$ is any Boolean function on $\mathbb{F}_2^m$. Then f is bent if and only if π is bijective.

3 Two infinite classes of rotation symmetric bent functions

In this section, we only present two infinite classes of rotation symmetric bent functions. The proofs of the main results will be given in the next section.

Theorem 1 *Let $n = 2m$ and $\gamma(X_0, X_1, \ldots, X_{m-1}) \in \mathbb{F}_2[X_0, X_1, \ldots, X_{m-1}]$ be an algebraic normal form of algebraic degree d. Then the function*

$$f(x) = \sum_{i=0}^{m-1} x_i x_{i+m} + \gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1})$$

is a bent function. Further, if $\gamma(X_0, X_1, \ldots, X_{m-1})$ is rotation symmetric, then f is a rotation symmetric bent function. If $d \geq 2$, then f has algebraic degree d.

Example 1 Let $m = 6$. Then the function

$$f(x) = \sum_{i=0}^{5} x_i x_{i+6} + \prod_{i=0}^{5}(x_i + x_{i+6})$$

is a rotation symmetric bent function of algebraic degree 6.

Theorem 2 *Let $n = 2m$, t be an integer such that $1 \leq t \leq m - 1$ and $m/gcd(m, t)$ is odd, and $\gamma(X_0, X_1, \ldots, X_{m-1}) \in \mathbb{F}_2[X_0, X_1, \ldots, X_{m-1}]$ be an algebraic normal form. Then the function*

$$f_t(x) = \sum_{i=0}^{n-1}(x_i x_{i+t} x_{i+m} + x_i x_{i+t}) + \sum_{i=0}^{m-1} x_i x_{i+m} + \gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1})$$

is a bent function. Further, if $\gamma(X_0, X_1, \ldots, X_{m-1})$ is rotation symmetric of algebraic degree $d \geq 3$, then f is a rotation symmetric bent function of algebraic degree d.

Example 2 Let $m = 6$ and $t = 2$. Then the function

$$f_2(x) = \sum_{i=0}^{11}(x_i x_{i+2} x_{i+6} + x_i x_{i+2}) + \sum_{i=0}^{5} x_i x_{i+6} + \prod_{i=0}^{5}(x_i + x_{i+6})$$

is a rotation symmetric bent function of algebraic degree 6.

Example 3 Let m be an odd positive integer with $m \geq 3$ and $t = 1$. Then the function

$$f_1(x) = \sum_{i=0}^{2m-1} (x_i x_{i+1} x_{i+m} + x_i x_{i+1}) + \sum_{i=0}^{m-1} x_i x_{i+m} + \prod_{i=0}^{m-1} (x_i + x_{i+m})$$

is a rotation symmetric bent function with the greatest possible algebraic degree m.

The following lemma shows that the two classes of rotation symmetric bent functions constructed in Theorems 1 and 2 do not overlap.

Lemma 1 *Let $g(x_0, x_1, \ldots, x_{n-1})$ be a Boolean function on $\mathbb{F}_2^n$ or an algebraic normal form in $\mathbb{F}_2[x_0, x_1, \ldots, x_{n-1}]$ such that*

(1) *for any $0 \leq i \leq m-1$, $g(x_0, \ldots, x_i, \ldots, x_{i+m}, \ldots, x_{n-1}) = g(x_0, \ldots, x_{i+m}, \ldots, x_i, \ldots, x_{n-1})$;*
(2) *for any $0 \leq i \leq m-1$, $x_i x_{i+m}$ is not in the terms of g;*
(3) *g is rotation symmetric.*

Then there exists a rotation symmetric polynomial $\gamma(X_0, X_1, \ldots, X_{m-1}) \in \mathbb{F}_2[X_0, X_1, \ldots, X_{m-1}]$ such that

$$g(x_0, x_1, \ldots, x_{n-1}) = \gamma(x_0 + x_m, x_1 + x_{m+1}, \ldots, x_{m-1} + x_{2m-1}).$$

Proof If there exists $\gamma(X_0, X_1, \ldots, X_{m-1})$ such that

$$g(x_0, x_1, \ldots, x_{n-1}) = \gamma(x_0 + x_m, x_1 + x_{m+1}, \ldots, x_{m-1} + x_{2m-1}).$$

Since g is rotation symmetric, then $\gamma(X_0, X_1, \ldots, X_{m-1})$ is rotation symmetric.

Now we will give the proof by the induction on algebraic degree d of g, i.e, there exists such rotation symmetric polynomial γ from rotation symmetric $g(x)$ of algebraic degree d satisfying conditions (1) and (2).

(1) When $g = 0$ or $g = 1$, such γ obviously exists.
(2) When $d = 1$, such γ obviously exists.
(3) Suppose $d \geq 2$. From the conditions (1) and (2), there exists i such that

$$\begin{aligned} & g(x_0, x_1, \ldots, x_{n-1}) \\ & \quad = x_i g'(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{i+m-1}, x_{i+m+1}, \ldots, x_{n-1}) \\ & \qquad + x_{i+m} g''(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{i+m-1}, x_{i+m+1}, \ldots, x_{n-1}), \end{aligned}$$

where $g', g'' \in \mathbb{F}_2(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{i+m-1}, x_{i+m+1}, \ldots, x_{n-1})$. From the condition (1), we have $g' = g''$. From the induction of algebraic degree d, for g' and g'', there exists $\gamma'(X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_{m-1})$ such that

$$g' = g'' = \gamma'(x_0 + x_m, \ldots, x_{i-1} + x_{i+m-1}, x_{i+1} + x_{i+m+1}, \ldots, x_{m-1} + x_{2m-1}).$$

Take $\gamma(X_0, X_1, \ldots, X_m) = X_i \gamma'(X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_{m-1})$. Then

$$g(x_0, x_1, \ldots, x_{n-1}) = \gamma(x_0 + x_m, x_1 + x_{m+1}, \ldots, x_{m-1} + x_{2m-1}).$$

Hence, this lemma follows. □

Remark 1 Let $f(x)=\sum_{i=0}^{m-1}x_ix_{i+m}+g(x)$ defined in Eq. (1), where

$$g(x)=\sum_{\delta\in A}\sum_{\beta'\boxplus\beta''\in\mathcal{O}_m(\delta)}\prod_{i=0}^{m-1}x_i^{\beta'}x_{i+m}^{\beta''}.$$

We can verify that $g(x)$ satisfies all the three conditions in Lemma 1. There exists $\gamma\in\mathbb{F}_2[X_0,X_1,\ldots,X_{m-1}]$ such that

$$f(x)=\sum_{i=0}^{m-1}x_ix_{i+m}+\gamma(x_0+x_m,\ldots,x_{m-1}+x_{2m-1})$$

is bent. This shows that rotation symmetric bent functions constructed by Su and Tang [40] are contained in functions in Theorem 1. Let $h(x)=\sum_{i=0}^{n-1}(x_ix_{i+t}x_{i+m}+x_ix_{i+t})$. From Lemma 1, h can not be expressed as $h(x)=\gamma(x_0+x_m,\ldots,x_{m-1}+x_{2m-1})$ with $\gamma\in\mathbb{F}_2[X_0,X_1,\ldots,X_{m-1}]$ being a rotation symmetric polynomial. Thus, any function $f(x)$ constructed in Theorem 2 can not be written in $f(x)=\sum_{i=0}^{m-1}x_ix_{i+m}+\gamma(x_0+x_m,\ldots,x_{m-1}+x_{2m-1})$, where γ is a rotation symmetric polynomial in $\mathbb{F}_2[X_0,X_1,\ldots,X_{m-1}]$. Hence, the class of rotation symmetric bent functions constructed in Theorem 2 is completely disjoint from the one constructed in Theorem 1. In particular, any rotation symmetric bent functions in Theorem 2 are different from rotation symmetric bent functions constructed by Su and Tang [40].

Remark 2 From the proof of Lemma 1, it is observed that a Boolean function $g(x_0,\ldots,x_{2m-1})$ on $\mathbb{F}_2^{2m}$ can be written as $g=\gamma(x_0+x_m,\ldots,x_{m-1}+x_{2m-1})$ with $\gamma\in\mathbb{F}_2[X_0,X_1,\ldots,X_{m-1}]$ if and only if the following two conditions hold

(1) for any permutation σ over $\{0,1,\ldots,2m-1\}$ with $\{\sigma(i),\sigma(i+m)\}=\{i,i+m\}$, where $0\le i\le m-1$, $g(x_0,\ldots,x_{2m-1})=g(x_{\sigma(0)},\ldots,x_{\sigma(2m-1)})$;

(2) for any $0\le i\le m-1$, x_ix_{i+m} is not in the terms of g.

For any boolean function $g(x_0,\ldots,x_{2m-1})$ on $\mathbb{F}_2^{2m}$ and $i\in\{0,1,\ldots,2m-1\}$, let D_ig be the functions defined as

$$D_ig(x_0,\ldots,x_{2m-1})=g(x_0,\ldots,x_i+1,\ldots,x_{2m-1})+g(x_0,\ldots,x_i,\ldots,x_{2m-1}).$$

Then, one has the following proposition.

Proposition 1 *Let $g(x_0,\ldots,x_{2m-1})$ be a Boolean function on $\mathbb{F}_2^{2m}$. Then, $g=\gamma(x_0+x_m,\ldots,x_{m-1}+x_{2m-1})$ with $\gamma\in\mathbb{F}_2[X_0,X_1,\ldots,X_{m-1}]$ if and only if $D_ig=D_{i+m}g$ for any $i\in\{0,1,\ldots,m-1\}$.*

Proof First, assume $g=\gamma(x_0+x_m,\ldots,x_{m-1}+x_{2m-1})$. Then,

$$\begin{aligned}D_{i+m}g(x_0,\ldots,x_{2m-1})&=\gamma(x_0+x_m,\ldots,x_i+x_{i+m}+1,\ldots,x_{m-1}+x_{2m-1})\\&\quad+\gamma(x_0+x_m,\ldots,x_i+x_{i+m},\ldots,x_{m-1}+x_{2m-1})\\&=D_ig(x_0,\ldots,x_{2m-1}).\end{aligned}$$

Conversely, assume $D_i g = D_{i+m} g$. Then, for any $i \in \{0, 1, \ldots, m-1\}$, there exist Boolean functions A_i, B_i, C_i and D_i, whose values are completely independent with x_i and x_{i+m} such that

$$g(x_0, \ldots, x_{2m-1}) = A_i x_i x_{i+m} + B_i x_i + C_i x_{i+m} + D_i. \tag{4}$$

Thus, $D_{i+m} g(x_0, \ldots, x_{2m-1}) = A_i x_i + C_i$ and $D_i g(x_0, \ldots, x_{2m-1}) = A_i x_{i+m} + B_i$. One gets $A_i = 0$ and $B_i = C_i$ from $D_i g = D_{i+m} g$. By Eq. (4), one has

$$g(x_0, \ldots, x_{2m-1}) = B_i (x_i + x_{i+m}) + D_i.$$

Hence, the function g satisfies the conditions (1) and (2) in Remark 2, which completes the proof.

4 Proofs

In this section, we give the proofs of our main results on rotation symmetric bent functions. We first give the following lemma on rotation symmetric functions.

Lemma 2 *Let $\gamma \in \mathbb{F}_2[X_0, \ldots, X_{m-1}]$, then $g(x_0, \ldots, x_{2m-1}) = \gamma(x_0+x_m, \ldots, x_{m-1} + x_{2m-1})$ over $\mathbb{F}_2^{2m}$ is rotation symmetric if and only if $\gamma(X_0, \ldots, X_{m-1})$ over $\mathbb{F}_2^m$ is rotation symmetric.*

Proof If $\gamma(X_0, \ldots, X_{m-1})$ over $\mathbb{F}_2^m$ is rotation symmetric, then

$$\begin{aligned} g(x_1, \ldots, x_m, x_{m+1} \ldots, x_0) &= \gamma(x_1 + x_{m+1}, \ldots, x_0 + x_m) \\ &= \gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1}) \\ &= g(x_0, \ldots, x_{m-1}, x_m, \ldots, x_{2m-1}). \end{aligned}$$

Thus, $\gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1})$ is rotation symmetric.

Conversely, let $g(x_0, \ldots, x_{2m-1})$ be rotation symmetric. Set $x_i = X_i$ for $0 \le i \le m-1$ and $x_i = 0$ for $m \le i \le 2m-1$.Then,

$$\begin{aligned} \gamma(X_1, \ldots, X_0) &= \gamma(x_1 + x_{m+1}, \ldots, x_0 + x_m) \\ &= g(x_1, \ldots, x_m, x_{m+1}, \ldots, x_0) \\ &= g(x_0, \ldots, x_{m-1}, x_m, \ldots, x_{2m-1}) \\ &= \gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1}) \\ &= \gamma(X_0, \ldots, X_{m-1}). \end{aligned}$$

Thus, $\gamma(X_0, \ldots, X_{m-1})$ is rotation symmetric. □

4.1 The proof of Theorem 1

For any function γ on $\mathbb{F}_2^m$, the function

$$f_0(a, y) = \sum_{i=0}^{m-1} y_i a_i + \gamma(a_0, a_1, \ldots, a_{m-1})$$

is a bent function on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ in the Maiorana–McFarland class $\mathcal{M}$ of functions defined in Eq. (3). Take the nondegenerate linear transform on $f_0(a, y)$ as

$$\begin{aligned} y_i &= x_i, \\ a_i &= x_i + x_{i+m}, \end{aligned}$$

where $0 \le i \le m-1$. We have a bent function

$$\begin{aligned} f_1(x_0, x_1, \ldots, x_{n-1}) &= \sum_{i=0}^{m-1} x_i(x_i + x_{i+m}) + \gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1}) \\ &= \sum_{i=0}^{m-1} x_i x_{i+m} + \gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1}) + \sum_{i=0}^{m-1} x_i. \end{aligned}$$

Since $\sum_{i=0}^{m-1} x_i$ is a linear function, then $f(x) = f_1 + \sum_{i=0}^{m-1} x_i$ is a bent function. Since Lemma 2, if γ is a rotation symmetric polynomial in $\mathbb{F}_2[X_0, X_1, \ldots, X_{m-1}]$, then $f(x)$ is also rotation symmetric.

If $\gamma(X_0, X_1, \ldots, X_{m-1})$ has algebraic degree d, then $\gamma(x_0+x_m, \ldots, x_{m-1}+x_{2m-1})$ has algebraic degree d. If $d \ge 3$, then the algebraic degree of f is d. Otherwise, f has algebraic degree less than 2. Thus, f has algebraic degree 2 since f is bent. Hence, Theorem 1 follows.

4.2 The proof of Theorem 2

In order to prove Theorem 2, we first recall some notations and results in [21]. Define the sets

$$\begin{aligned} E &= \{x \in \mathbb{F}_2^n : x_i + x_{i+m} = 1 \text{ for } 0 \le i \le m-1\} \\ &= \{(y_0, \ldots, y_{m-1}, 1 + y_0, \ldots, 1 + y_{m-1}) \in \mathbb{F}_2^n : (y_0, \ldots, y_{m-1}) \in \mathbb{F}_2^m\} \end{aligned}$$

and

$$\begin{aligned} W &= \{x \in \mathbb{F}_2^n : x_i = 0 \text{ for } m \le i \le n-1\} \\ &= \{(a_0, \ldots, a_{m-1}, 0, \ldots, 0) \in \mathbb{F}_2^n : (a_0, \ldots, a_{m-1}) \in \mathbb{F}_2^m\}. \end{aligned}$$

Then

$$\mathbb{F}_2^n = \bigcup_{a \in W} (a + E).$$

Thus, for any $x \in \mathbb{F}_2^n$, there exists a unique pair (a, y) ($a \in W$ and $y \in E$), such that $x = a + y$. Furthermore, if $x = (x_0, x_1, \ldots, x_{n-1})$, then

$$\begin{aligned} y &= (x_m + 1, x_{m+1} + 1, \ldots, x_{n-1} + 1, x_m, x_{m+1}, \ldots, x_{n-1}) \\ a &= (x_0 + x_m + 1, x_1 + x_{m+1} + 1, \ldots, x_{m-1} + x_{n-1} + 1, 0, 0, \ldots, 0). \end{aligned} \tag{5}$$

Gao et al. [21] proved that $F_t(x) = \sum_{i=0}^{n-1}(x_i x_{i+t} x_{i+m} + x_i x_{i+t}) + \sum_{i=0}^{m-1} x_i x_{i+m}$ can be expressed in Maiorana–McFarland's form

$$F_t(x) = F_t(a + y) = \pi(a) \cdot y + h_0(a), \tag{6}$$

where $a \in W$, $y \in E$,$h_0(a) = \sum_{i=m-t}^{m-1} a_i a_{i+t}$, and $\pi(a) = (\pi_0(a), \pi_1(a), \ldots, \pi_{m-1}(a), 0, 0, \ldots, 0)$ with $\pi_i(a) = a_i a_{(i+t) \bmod m} + a_{(i+t) \bmod m} + a_{(i+m-t) \bmod m}$. Since $m/gcd(m, t)$ is odd, then from Gao et al. [21][Proof in Theorem 1], $a \mapsto (\pi_0(a), \pi_1(a), \ldots, \pi_{m-1}(a), 0, 0, \ldots, 0)$ is a permutation of W. Then $F_t(x)$ is a bent function.

Let $f_t(x) = F_t(x) + \gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1}) = \sum_{i=0}^{n-1}(x_i x_{i+t} x_{i+m} + x_i x_{i+t}) + \sum_{i=0}^{m-1} x_i x_{i+m} + \gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1})$, where $\gamma \in \mathbb{F}_2[X_0, X_1, \ldots, X_{m-1}]$. From Eq. (5), for any $\gamma \in \mathbb{F}_2[X_0, X_1, \ldots, X_{m-1}]$, there exists a function h_1 on W such that $\gamma(x_0 + x_m, \ldots, x_{m-1} + x_{2m-1}) = h_1(a)$. Then, from Eq. (6), we can express f_t in the form

$$f_t(x) = f_t(a + y) = \pi(a) \cdot y + (h_0(a) + h_1(a)).$$

Hence, $f_t(x)$ is a bent function. From Lemma 2, if γ is a rotation symmetric polynomial in $\mathbb{F}_2[X_0, X_1, \ldots, X_{m-1}]$, then $f_t(x)$ is also rotation symmetric. Obviously, if γ has algebraic degree $d \geq 3$, then f is also a function of algebraic degree d. Hence, Theorem 2 follows.

Remark 3 From the proofs of Theorems 1 and 2, bent functions in both theorems are in the completed Maiorana–McFarland class of bent functions.

5 Conclusion

In this paper, we propose a systematic method for constructing n-variable rotation symmetric bent functions from some functions in the Maiorana–McFarland class. One class of rotation symmetric bent functions has algebraic degree ranging from 2 to m and the other class has algebraic degree ranging from 3 to m.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant Nos. 11401480, 11531002, 11371138). C. Tang also acknowledges support from 14E013, CXTD2014-4, and the Meritocracy Research Funds of China West Normal University. Y. Qi also acknowledges support from Zhejiang provincial Natural Science Foundation of China (LQ17A010008 and LQ16A010005). The work of Z. Zhou and C. Fan was supported by the Sichuan Provincial Youth Science and Technology Fund under Grant 2016JQ0004, and in part by National Cryptography Development Fund under Grant MMJJ20170119.

References

1. Calderbank, R., Kantor, W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. **18**(2), 97–122 (1986)
2. Canteaut, A., Charpin, P., Kyureghyan, G.: A new class of monomial bent functions. Finite Fields Their Appl. **14**(1), 221–241 (2008)
3. Carlet, C.: Two new classes of bent functions. In: EUROCRYPT (Lecture Notes in Computer Science), vol. 765, pp. 77–101. Springer, New York (1994)
4. Carlet, C.: A construction of bent function. In: Proc. 3rd Int. Conf. Finite Fields and Appl., pp. 47–58 (1996)
5. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge Univ. Press, Cambridge (2010)
6. Carlet, C.: Open problems on binary bent functions. In: Open Problems in Mathematics and Computational Science, pp. 203–241 (2014)
7. Carlet, C., Gao, G., Liu, W.: Results on constructions of rotation symmetric bent and semi-bent functions. In: SETA 2014, Springer International Publishing Switzerland, 2014, vol. 8865, Lecture Notes in Computer Science, pp. 21–33 (2014)
8. Carlet, C., Gao, G., Liu, W.: A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions. J. Comb. Theory Ser. A **127**, 161–175 (2014)
9. Carlet, C., Mesnager, S.: On Dillons class H of bent functions, Niho bent functions and O-polynomials. J. Comb. Theory Ser. A **118**(8), 2392–2410 (2011)
10. Charnes, C., Rotteler, M., Beth, T.: Homogeneous bent functions, invariants, and designs. Des. Codes Cryptogr. **26**(1–3), 139–154 (2002)
11. Charpin, P., Gong, G.: Hyperbent functions, Kloosterman sums and Dickson polynomials. In: Proc. ISIT, pp. 1758–1762 (2008)
12. Charpin, P., Kyureghyan, G.: Cubic monomial bent functions: a subclass of M. SIAM J. Discrete Math. **22**(2), 650–665 (2008)
13. Cohen, G., Honkala, I., Litsyn, S., Lobstein, A.: Covering Codes. North Holland, Amsterdam (1997)
14. Dalai, D.K., Maitra, S., Sarkar, S.: Results on rotation symmetric bent functions. Discrete Math. **309**, 2398–2409 (2009)
15. Dillon, J.: Elementary Hadamard difference sets. Ph.D. dissertation, Netw. Commun. Lab., Univ. Maryland, College Park, MD, USA (1974)
16. Dillon, J.F., Dobbertin, H.: New cyclic difference sets with Singer parameters. Finite Fields Their Appl. **10**(3), 342–389 (2004)
17. Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015)
18. Dobbertin, H., Leander, G., Canteaut, A., Carlet, C., Felke, P., Gaborit, P.: Construction of bent functions via Niho power functions. J. Comb. Theory Ser. A **113**(5), 779–798 (2006)
19. Fontaine, C.: On some cosets of the first-order Reed–Muller code with high minimum weight. IEEE Trans. Inf. Theory **45**, 1237–1243 (1999)
20. Filiol, E., Fontaine, C.: Highly nonlinear balanced Boolean functions with a good correlationimmunity. In: Proceedings of EUROCRYPT98. Lecture Notes in Computer Science, vol. 1403, pp. 475–488 (1998)
21. Gao, G., Zhang, X., Liu, W., Carlet, C.: Constructions of quadratic and cubic rotation symmetric bent functions. IEEE Trans. Inf. Theory **58**(7), 4908–4913 (2012)
22. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions (Corresp.). IEEE Trans. Inf. Theory **14**(1), 154–156 (1968)

23. Leander, G.: Monomial bent functions. IEEE Trans. Inf. Theory **52**(2), 738–743 (2006)
24. Leander, G., Kholosha, A.: Bent functions with 2r Niho exponents. IEEE Trans. Inf. Theory **52**(12), 5529–5532 (2006)
25. Li, N., Helleseth, T., Tang, X., Kholosha, A.: Several new classes of bent functions from Dillon exponents. IEEE Trans. Inf. Theory **59**(3), 1818–1831 (2013)
26. McFarland, R.L.: A family of noncyclic difference sets. J. Comb. Theory Ser. A **15**(1), 1–10 (1973)
27. Mesnager, S.: A new family of hyper-bent Boolean functions in polynomial form. In: Parker, M.G. (ed.) Cryptography and Coding (Lecture Notes in Computer Science), vol. 5921, pp. 402–417. Springer, Berlin (2009)
28. Mesnager, S.: Hyper-bent Boolean functions with multiple trace terms. In: Hasan, M., Helleseth, T. (eds.) Arithmetic of Finite Fields (Lecture Notes in Computer Science), vol. 6087, pp. 97–113. Springer, Berlin (2010)
29. Mesnager, S.: Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. IEEE Trans. Inf. Theory **57**(9), 5996–6009 (2011)
30. Mesnager, S.: A new class of bent and hyper-bent Boolean functions in polynomial forms. Des. Codes Cryptogr. **59**(1–3), 265–279 (2011)
31. Mesnager, S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inf. Theory **60**(7), 4397–4407 (2014)
32. Mesnager, S., Flori, J.P.: Hyper-bent functions via Dillon-like exponents. IEEE Trans. Inf. Theory **59**(5), 3215–3232 (2013)
33. Olsen, J.D., Scholtz, R.A., Welch, L.R.: Bent-function sequences. IEEE Trans. Inf. Theory **28**(6), 858–864 (1982)
34. Pieprzyk, J., Qu, C.: Fast Hashing and rotation symmetric functions. J. Univ. Comput. Sci. **5**, 20–31 (1999)
35. Pott, A., Tan, Y., Feng, T.: Strongly regular graphs associated with ternary bent functions. J. Comb. Theory Ser. A **117**(6), 668–682 (2010)
36. Pott, A., Tan, Y., Feng, T., Ling, S.: Association schemes arising from bent functions. Des. Codes Cryptogr. **59**(1–3), 319–331 (2011)
37. Rothaus, O.: On bent functions. J. Comb. Theory Ser. A **20**(3), 300–305 (1976)
38. Stanica, P., Maitra, S.: Rotation symmetric Boolean functions-count and cryptographic properties. Discrete Appl. Math. **156**, 1567–1580 (2008)
39. Stanica, P., Maitra, S., Clark, J.: Results on rotation symmetric bent and correlation immune Boolean functions. In: Proceedings of Fast Software Encryption 2004. Lecture Notes in Computer Science, vol. 3017, pp. 161–177 (2004)
40. Su, S., Tang, X.: On the systematic constructions of rotation symmetric bent functions with any possible algebraic degrees. arXiv:1505.02875
41. Xu, G., Cao, X., Xu, S.: Several new classes of Boolean functions with few Walsh transform values. arXiv:1506.04886v1
42. Yu, N.Y., Gong, G.: Construction of quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory **52**(7), 3291–3299 (2006)