On the Systematic Constructions of Rotation Symmetric Bent Functions with Any Possible Algebraic Degrees

Sihong Su and Xiaohu Tang *

Abstract

In the literature, few constructions of n-variable rotation symmetric bent functions have been presented, which either have restriction on n or have algebraic degree no more than 4. In this paper, for any even integer $n = 2m \geq 2$, a first systemic construction of n-variable rotation symmetric bent functions, with any possible algebraic degrees ranging from 2 to m, is proposed.

Key words: Orbit, rotation symmetric function, Walsh transform, bent function, algebraic degree.

1 Introduction

Boolean bent functions were introduced by Rothaus in 1976 [13]. Let $\mathbb{F}_2$ be the finite field with two elements, $n > 0$ be a positive integer, and $\mathbb{F}_2^n$ be the n-dimensional vectorspace over $\mathbb{F}_2$. An n-variable Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is *bent* if it has maximal Hamming distance to the set of affine Boolean functions. Boolean bent functions have attracted much attention due to their important applications in cryptography [1, 4], coding theory and sequence design [8, 9, 11].

Boolean functions that are invariant under the action of cyclic rotation on the inputs are called rotation symmetric functions [12]. Such class of Boolean functions is of great interest since they need less space to be stored and allow faster computation of the Walsh transform. Further, it has been experimentally demonstrated that the class of rotation symmetric functions is extremely rich in terms of cryptographically significant Boolean functions. In particular, they allowed obtaining Boolean functions in odd numbers of variables beating the best known nonlinearities [7], and new bent functions (in even numbers of variables) [2, 3, 5, 6].

Throughout this paper, for $n = 2m$ we study the n-variable rotation symmetric bent functions. To avoid confusion, we denote the sum over $\mathbb{Z}$ by $+$, and the sum over $\mathbb{F}_2$ by $\oplus$. The quadratic Boolean function

$$f_0(x_0, \cdots, x_{n-1}) = \bigoplus_{i=0}^{m-1} x_i x_{m+i} \tag{1}$$

is the first class of rotation symmetric bent functions. According to experimental results, Stănică *et al.* conjectured that there is no homogeneous rotation symmetric bent function having algebraic degree greater than 2 [14]. Since then, large classes of homogeneous rotation symmetric functions seem to support the conjecture since all of them do not contain non-quadratic bent functions [10, 15].

As any theoretic advancement in this direction can be used to find cryptographically significant functions on higher number of variables, it was stated in [14] that any theoretic construction of rotation symmetric

bent functions with algebraic degree larger than 2 is an interesting problem. In the literature, the main method of constructing new rotation symmetric bent functions is to modify $f_0(x)$ in (1) [3, 6]. Up to now, only few constructions of rotation symmetric bent functions are known, whose algebraic degrees are all no more than 4. In [6], for $n = 2m$, Gao $et\ al.$ proved the cubic rotation symmetric function

$$f_t(x_0, \cdots, x_{n-1}) = \bigoplus_{i=0}^{m-1} x_i x_{m+i} \oplus \bigoplus_{i=0}^{n-1} \left(x_i x_{t+i} x_{m+i} \oplus x_i x_{t+i} \right)$$

is a rotation symmetric bent function if and only if $\frac{m}{\gcd(m,t)}$ is odd, where $1 \le t \le m-1$ and the subscript of x is modulo n. This is the first theoretical construction of rotation symmetric bent functions with algebraic degree lager than 2. Recently, another n-variable cubic rotation symmetric bent function

$$f(x_0, \cdots, x_{n-1}) = \bigoplus_{i=0}^{m-1} x_i x_{m+i} \oplus \bigoplus_{i=0}^{n-1} x_i x_{r+i} x_{2r+i} \oplus \bigoplus_{i=0}^{2r-1} x_i x_{2r+i} x_{4r+i},$$

where $n = 2m = 6r$, was presented in [3]. Later on, an infinite class of n-variable rotation symmetric bent functions with algebraic degree 4, where $n = 2m$ but not divisible by 4, was constructed from two known semi-bent rotation symmetric functions in m variables with complementary Walsh supports [2].

In this paper, we present a simple but generic construction of n-variable rotation symmetric bent functions still by the modification of the quadratic rotation symmetric bent function f_0 in (1). Unlike the previous modifications, our construction can provide n-variable rotation symmetric bent functions for any even integer n. Most notably, the proposed n-variable rotation symmetric bent functions can have any possible algebraic degree ranging from 2 to $n/2$. To the best of our knowledge, it is the first time to construct rotation symmetric bent functions of algebraic degree larger than 4 when $n \ge 10$.

The rest of this paper is organized as follows. In Section 2, some basic notations and definitions of Boolean functions, rotation symmetric bent functions in particular, are reviewed. In Section 3, a generic construction of n-variable rotation symmetric bent functions is proposed by modifying the support of the quadratic rotation symmetric bent function f_0 in (1). In Section 4, a flexible construction of n-variable rotation symmetric bent functions with any given algebraic degree from 2 to $n/2$ is presented. Finally, Section 5 concludes this paper.

2 Preliminaries

Given a vector $x = (x_0, \cdots, x_{n-1}) \in \mathbb{F}_2^n$, define its support as the set $\mathrm{supp}(x) = \{0 \le i < n \,|\, x_i = 1\}$, and its Hamming weight $\mathrm{wt}(x)$ as the cardinality of its support, i.e., $\mathrm{wt}(x) = |\mathrm{supp}(x)|$.

In this paper, for simplicity, we do not distinguish the vector $x = (x_0, \cdots, x_{n-1}) \in \mathbb{F}_2^n$ and the integer $\sum_{i=0}^{n-1} x_i 2^i \in \{0, \cdots, 2^n - 1\}$ if the context is clear, since they are one-to-one corresponding. For any two vectors $x = (x_0, \cdots, x_{n-1}) \in \mathbb{F}_2^n$ and $y = (y_0, \cdots, y_{n-1}) \in \mathbb{F}_2^n$, if $x_i \le y_i$ for all $0 \le i < n$, then we say that y covers x and denote it by $y \succeq x$. According to Lucas formula, we have

$$\binom{y}{x} = 1 \pmod 2 \Longleftrightarrow y \succeq x. \tag{2}$$

Let $x = (x_0, \cdots, x_{n-1}) \in \mathbb{F}_2^n$. For two integers $l \ge 0$ and $0 \le i < n$, define the left l-cyclic shift version of vector x as $\rho_l^n(x) = \left(\rho_l^n(x_0), \cdots, \rho_l^n(x_{n-1}) \right)$ by

$$\rho_l^n(x_i) = x_{i+l},$$

where the subscript of x is modulo n. An orbit generated by a vector $x \in \mathbb{F}_2^n$ is defined as

$$O_n(x) = \left\{ \rho_0^n(x), \cdots, \rho_{n-1}^n(x) \right\}. \tag{3}$$

In other words, each orbit consists of all cyclic shifts of one vector in $\mathbb{F}_2^n$. Naturally, an orbit in $\mathbb{F}_2^n$ can be represented by its representative element which is the lexicographically first element belonging to the orbit. The set of the representative elements of all the orbits in $\mathbb{F}_2^n$ is denoted by $\mathbf{R}_n$. For example, $\mathbf{R}_4 = \{(0,0,0,0),(1,0,0,0),(1,1,0,0),(1,0,1,0),(1,1,1,0),(1,1,1,1)\}$.

An n-variable Boolean function is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. We denote by $\mathcal{B}_n$ the set of all the n-variable Boolean functions. A basic representation of a function $f \in \mathcal{B}_n$ is by the output of its truth table, i.e., a binary vector of length 2^n, as

$$f = [f(0), \cdots, f(2^n - 1)].$$

The support of f is defined as $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ and f is also said to be the characteristic function of the set $\mathrm{supp}(f)$. The Hamming weight of f is the cardinality of $\mathrm{supp}(f)$, i.e., $\mathrm{wt}(f) = |\mathrm{supp}(f)|$. It is easy to see that $\mathrm{supp}(f_0) = O_4(1,0,1,0) \cup O_4(1,1,1,0)$ and $\mathrm{wt}(f_0) = 6$ for f_0 in (1) when $n = 4$.

The most usual representation of a Boolean function $f \in \mathcal{B}_n$ is the algebraic normal form (ANF) as

$$f(x) = \bigoplus_{\alpha \in \mathbb{F}_2^n} c_\alpha x^\alpha, \ c_\alpha \in \mathbb{F}_2, \tag{4}$$

where c_α is the coefficient of the term $x^\alpha = x_0^{\alpha_0} \cdots x_{n-1}^{\alpha_{n-1}}$ for $x = (x_0, \cdots, x_{n-1})$ and $\alpha = (\alpha_0, \cdots, \alpha_{n-1})$ in $\mathbb{F}_2^n$. The algebraic degrees of the term x^α and the Boolean function f in (4) are respectively defined as $\deg(x^\alpha) = \mathrm{wt}(\alpha)$ and

$$\deg(f) = \max\{\mathrm{wt}(\alpha) \mid c_\alpha = 1, \alpha \in \mathbb{F}_2^n\}.$$

Specifically, the Boolean functions of degree at most 1 are called affine functions; the function f in (4) is called to be homogeneous if all the terms with nonzero coefficients in f have the same algebraic degree.

Definition 1. *For a function $f \in \mathcal{B}_n$, if $f(\rho_l^n(x)) = f(x)$ holds for all inputs $x \in \mathbb{F}_2^n$ and integers $1 \leq l \leq n-1$, then f is called a rotation symmetric function. That is, rotation symmetric functions are invariant under cyclic rotation on inputs.*

The Walsh transform of an n-variable Boolean function f is an integer-valued function on $\mathbb{F}_2^n$, whose value at $\alpha \in \mathbb{F}_2^n$ is defined as

$$W_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \alpha \cdot x} \tag{5}$$

where $\alpha \cdot x = \alpha_0 x_0 \oplus \cdots \oplus \alpha_{n-1} x_{n-1}$ is the usual inner product of $\alpha = (\alpha_0, \cdots, \alpha_{n-1})$ and $x = (x_0, \cdots, x_{n-1})$. The nonlinearity of a function $f \in \mathcal{B}_n$ is given by $nl(f) = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |W_f(\alpha)|$.

Definition 2. *A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is said to be bent if $W_f(\alpha) = \pm 2^{\frac{n}{2}}$ for all $\alpha \in \mathbb{F}_2^n$.*

Obviously, an n-variable Boolean function is bent only if n is even. In addition, it is well known that the algebraic degree of an n-variable bent function is no more than m for $n = 2m \geq 4$, while the algebraic degree of a 2-variable bent function is 2.

The following result will be used in the computation of the values of the Walsh transform later.

Lemma 1. *Let a, b be two vectors over $\mathbb{F}_2^n$. Then,*

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{x \cdot (x \oplus a \oplus b)} = \begin{cases} 2^n, & a = \bar{b} \\ 0, & \text{otherwise} \end{cases}$$

where $\bar{b} = (b_0 \oplus 1, \cdots, b_{n-1} \oplus 1)$ for $b = (b_0, \cdots, b_{n-1})$.

Proof. For any two vectors $a, b \in \mathbb{F}_2^n$,

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{x \cdot (x \oplus a \oplus b)}$$

$$= \sum_{x \in \mathbb{F}_2^n} (-1)^{x \cdot ((1, \cdots, 1) \oplus a \oplus b)}$$

$$= \begin{cases} 2^n, & a = \bar{b} \\ 0, & \text{otherwise} \end{cases}$$

where the first identity holds since $x \cdot x = \mathrm{wt}(x) = x \cdot (1, \cdots, 1)$, and the second identity holds by the fact that $\sum_{y \in \mathbb{F}_2^n} (-1)^{\lambda \cdot y} = 2^n$ if $\lambda = 0$ and $\sum_{y \in \mathbb{F}_2^n} (-1)^{\lambda \cdot y} = 0$ if $\lambda \in \mathbb{F}_2^n \setminus \{0\}$. $\qquad \square$

From now on, we always assume $n = 2m \geq 2$. For a vector $x = (x_0, \cdots, x_{n-1}) \in \mathbb{F}_2^n$, we always denote $x' = (x_0, \cdots, x_{m-1})$, $x'' = (x_m, \cdots, x_{n-1})$, $x' \cdot x'' = x_0 x_m \oplus \cdots \oplus x_{m-1} x_{n-1}$, and $x' * x'' = x_0 x_m + \cdots + x_{m-1} x_{n-1}$. Obviously, $x' * x'' = 0$ if and only if $x_i x_{m+i} = 0$ for $0 \leq i \leq m - 1$. For simplicity, we use the notation $x' + x''$ for $x' \oplus x''$ satisfying $x' * x'' = 0$. This is to say, when $x' + x''$ is used in the rest of this paper, it always implies $x' * x'' = 0$.

3 A generic construction of rotation symmetric bent functions

In this section, we present a generic construction of rotation symmetric bent functions by modifying the support of $f_0(x)$ in (1).

Given a subset $T \subseteq \mathbb{F}_2^n$, define an n-variable Boolean function as

$$f(x) = \begin{cases} f_0(x) \oplus 1, & x \in T \\ f_0(x), & \text{otherwise} \end{cases} \tag{6}$$

where f_0 is given in (1). In order to construct an n-variable rotation symmetric bent function f in (6), it is crucial to choose a proper subset T of $\mathbb{F}_2^n$.

Firstly, we give a sufficient and necessary condition of T such that f in (6) is a rotation symmetric function.

Lemma 2. *The n-variable Boolean function f in (6) is a rotation symmetric function if and only if $O_n(x) \subseteq T$ for all $x \in T$.*

Proof. Recall that f_0 is a rotation symmetric function. Let $\chi_T(\cdot)$ be the characteristic function of T. Then, by Definition 1, f is a rotation symmetric function if and only if $\chi_T = f \oplus f_0$ is also a rotation symmetric function, which is equivalent to $\rho_l^n(x) \in T$ for all $x \in T$ and $1 \leq l < n$. This completes the proof by the definition of $O_n(x)$ in (3). $\qquad \square$

Secondly, we study a sufficient condition of T such that f is a bent function.

Lemma 3. *For any subset $\Gamma \subseteq \mathbb{F}_2^m$, if the subset*

$$T = \bigcup_{\gamma \in \Gamma} \{ x \in \mathbb{F}_2^n \mid x' \in \mathbb{F}_2^m, x'' = x' \oplus \gamma \}, \tag{7}$$

then the n-variable Boolean function f in (6) is a bent function.

Proof. Substituting f to the definition of the Walsh transform in (5), we have

$$
\begin{aligned}
W_f(\alpha) &= \sum_{x \in \mathbb{F}_2^n \setminus T} (-1)^{f_0(x) \oplus \alpha \cdot x} + \sum_{x \in T} (-1)^{f_0(x) \oplus 1 \oplus \alpha \cdot x} \\
&= \sum_{x \in \mathbb{F}_2^n} (-1)^{x' \cdot x'' \oplus \alpha' \cdot x' \oplus \alpha'' \cdot x''} - 2 \sum_{x \in T} (-1)^{x' \cdot x'' \oplus \alpha' \cdot x' \oplus \alpha'' \cdot x''} \\
&= \sum_{x'' \in \mathbb{F}_2^m} (-1)^{\alpha'' \cdot x''} \sum_{x' \in \mathbb{F}_2^m} (-1)^{(x'' \oplus \alpha') \cdot x'} - 2 \sum_{\gamma \in \Gamma} \sum_{x' \in \mathbb{F}_2^m} (-1)^{x' \cdot (x' \oplus \gamma) \oplus \alpha' \cdot x' \oplus \alpha'' \cdot (x' \oplus \gamma)} \\
&= (-1)^{\alpha' \cdot \alpha''} 2^m - 2 \sum_{\gamma \in \Gamma} (-1)^{\alpha'' \cdot \gamma} \sum_{x' \in \mathbb{F}_2^m} (-1)^{x' \cdot (x' \oplus \gamma \oplus \alpha' \oplus \alpha'')} \\
&= \begin{cases} (-1)^{1 + \alpha' \cdot \alpha''} 2^m, & \text{if } \alpha' \oplus \alpha'' = \overline{\gamma} \text{ for a } \gamma \in \Gamma \\ (-1)^{\alpha' \cdot \alpha''} 2^m, & \text{otherwise} \end{cases}
\end{aligned}
$$

where the fourth identity comes from the fact that $\sum_{y \in \mathbb{F}_2^m} (-1)^{\lambda \cdot y} = 2^m$ if $\lambda = 0$ and $\sum_{y \in \mathbb{F}_2^m} (-1)^{\lambda \cdot y} = 0$ if $\lambda \in \mathbb{F}_2^m \setminus \{0\}$, the last identity follows from Lemma 1. $\qquad \square$

The following result is immediate from Lemmas 2 and 3.

Theorem 1. *The n-variable Boolean function defined in (6) is a rotation symmetric bent function if the subset $T \subseteq \mathbb{F}_2^n$ satisfies (7) and $O_m(\gamma) \subseteq \Gamma$ for all $\gamma \in \Gamma$.*

Proof. According to (7), $x = (x_0, \cdots, x_{n-1}) \in T$ if and only if $x_{i+m} = x_i \oplus \gamma_i$, i.e., $x_{l+i+m} = x_{l+i} \oplus \gamma_{l+i}$, for all $0 \le i < n$ and $1 \le l < n$, where $\gamma = (\gamma_0, \cdots, \gamma_{m-1}) \in \Gamma$. Then, given $1 \le l < n$, $\rho_l^n(x) = (x_l, \cdots, x_{l+n-1}) \in T$ if and only if $\rho_l^m(\gamma) = (\gamma_l, \cdots, \gamma_{l+m-1}) \in \Gamma$, i.e., $O_n(x) \subseteq T$ if and only if $O_m(\gamma) \subseteq \Gamma$. Hence, f in (6) is a rotation symmetric bent function by Lemmas 2 and 3. $\qquad \square$

In what follows, we investigate the ANF of the function proposed in Theorem 1. To do so, it is sufficient to determine the ANF of the characteristic function χ_T.

Given a $\gamma \in \mathbf{R}_m$, define

$$
T_\gamma = \bigcup_{\delta \in O_m(\gamma)} \left\{ x \in \mathbb{F}_2^n \,\middle|\, x' \in \mathbb{F}_2^m, x'' = x' \oplus \delta \right\}. \tag{8}
$$

It is easy to see that the subset T_γ of $\mathbb{F}_2^n$ in (8) satisfies:

P1 $T_\alpha \cap T_\beta = \emptyset$ if $\alpha \ne \beta$, where $\alpha, \beta \in \mathbf{R}_m$.

Example 1. *If $n = 4$, the vector sets T_γ, $\gamma \in \mathbf{R}_2$, are given in Table 1.*

Table 1: The vector sets T_γ for $\gamma \in \mathbf{R}_2$

γ	T_γ
$(0,0)$	$O_4(0,0,0,0) \cup O_4(1,0,1,0) \cup O_4(1,1,1,1)$
$(1,0)$	$O_4(1,0,0,0) \cup O_4(1,1,1,0)$
$(1,1)$	$O_4(1,1,0,0)$

Since $O_m(\gamma) \subseteq \Gamma$ for all $\gamma \in \Gamma$, then we can write Γ as $\Gamma = \bigcup_{\gamma \in \mathbf{R}_m \cap \Gamma} O_m(\gamma)$ and then

$$
T = \bigcup_{\gamma \in \mathbf{R}_m \cap \Gamma} T_\gamma.
$$

By P1, we have

$$\chi_T(x) = \bigoplus_{\gamma \in \mathbf{R}_m \cap \Gamma} \chi_{T_\gamma}(x) \tag{9}$$

where $\chi_T(\cdot)$ is the characteristic function of T. Therefore, we study the ANF of the function χ_{T_γ} firstly.

Lemma 4. *The ANF of the n-variable characteristic function of T_γ in* (8) *is*

$$\chi_{T_\gamma}(x) = \bigoplus_{\delta \in O_m(\gamma)} \bigoplus_{\beta' + \beta'' \succeq \delta} x^\beta \tag{10}$$

$$= \bigoplus_{\substack{\delta \in \mathbf{R}_m \\ \delta \succeq \gamma}} c_\delta \bigoplus_{\beta' + \beta'' \in O_m(\delta)} x^\beta \tag{11}$$

where $c_\delta \in \{0,1\}$ with $c_\gamma = 1$.

Proof. First of all, we prove (10) in two special cases: $\gamma = \mathbf{0}_m$ and $\gamma = \mathbf{1}_m$ where $\mathbf{0}_m$ and $\mathbf{1}_m$ respectively denote the all-zero and all-one vector of length m.

According to the definition of characteristic function, we have

$$
\begin{aligned}
\chi_{T_{\mathbf{1}_m}}(x) &= \bigoplus_{(b_0,\cdots,b_{m-1})\in\mathbb{F}_2^m} \prod_{i=0}^{m-1} (x_i \oplus b_i \oplus 1)(x_{m+i} \oplus b_i) \\
&= \prod_{i=0}^{m-1} \Big(\bigoplus_{b_i\in\{0,1\}} (x_i \oplus b_i \oplus 1)(x_{m+i} \oplus b_i) \Big) \\
&= \prod_{i=0}^{m-1} (x_i \oplus x_{m+i}) \\
&= \bigoplus_{\substack{0\leq i<m \\ \beta_i,\beta_{m+i}\in\mathbb{F}_2,\beta_i+\beta_{m+i}=1}} \prod_{i=0}^{m-1} x_i^{\beta_i} x_{m+i}^{\beta_{m+i}}
\end{aligned} \tag{12}
$$

and

$$
\begin{aligned}
\chi_{T_{\mathbf{0}_m}}(x) &= \bigoplus_{(b_0,\cdots,b_{m-1})\in\mathbb{F}_2^m} \prod_{i=0}^{m-1} (x_i \oplus b_i \oplus 1)(x_{m+i} \oplus b_i \oplus 1) \\
&= \prod_{i=0}^{m-1} \Big(\bigoplus_{b_i\in\{0,1\}} (x_i \oplus b_i \oplus 1)(x_{m+i} \oplus b_i \oplus 1) \Big) \\
&= \prod_{i=0}^{m-1} (x_i \oplus x_{m+i} \oplus 1) \\
&= \bigoplus_{\substack{0\leq i<m \\ \beta_i,\beta_{m+i}\in\mathbb{F}_2,\beta_i+\beta_{m+i}\in\{0,1\}}} \prod_{i=0}^{m-1} x_i^{\beta_i} x_{m+i}^{\beta_{m+i}}
\end{aligned} \tag{13}
$$

Then, based on (12) and (13), we are able to get

$$\chi_{T_\gamma}(x)$$

$$= \bigoplus_{\substack{(b_0,\cdots,b_{m-1})\in\mathbb{F}_2^m \\ \delta=(\delta_0,\cdots,\delta_{m-1})\in O_m(\gamma)}} \prod_{i=0}^{m-1}(x_i\oplus b_i\oplus 1)(x_{m+i}\oplus b_i\oplus\delta_i\oplus 1)$$

$$= \bigoplus_{\substack{(b_0,\cdots,b_{m-1})\in\mathbb{F}_2^m \\ \delta\in O_m(\gamma)}} \prod_{i\in\mathrm{supp}(\delta)}(x_i\oplus b_i\oplus 1)(x_{m+i}\oplus b_i) \prod_{i\in\mathrm{zeros}(\delta)}(x_i\oplus b_i\oplus 1)(x_{m+i}\oplus b_i\oplus 1)$$

$$= \bigoplus_{\delta\in O_m(\gamma)}\left(\bigoplus_{\substack{i\in\mathrm{supp}(\delta) \\ \beta_i,\beta_{m+i}\in\mathbb{F}_2,\beta_i+\beta_{m+i}=1}}\prod_{i\in\mathrm{supp}(\delta)}x_i^{\beta_i}x_{m+i}^{\beta_{m+i}}\right)\left(\bigoplus_{\substack{i\in\mathrm{zeros}(\delta) \\ \beta_i,\beta_{m+i}\in\mathbb{F}_2,\beta_i+\beta_{m+i}\in\{0,1\}}}\prod_{i\in\mathrm{zeros}(\delta)}x_i^{\beta_i}x_{m+i}^{\beta_{m+i}}\right)$$

$$= \bigoplus_{\delta\in O_m(\gamma)}\left(\bigoplus_{\substack{\beta_i,\beta_{m+i}\in\mathbb{F}_2,1\le i\le m \\ \beta_i+\beta_{m+i}=1,i\in\mathrm{supp}(\delta) \\ \beta_i+\beta_{m+i}\in\{0,1\},i\in\mathrm{zeros}(\delta)}}x^\beta\right)$$

$$= \bigoplus_{\delta\in O_m(\gamma)}\bigoplus_{\beta'+\beta''\succeq\delta}x^\beta$$

where $\mathrm{zeros}(x)=\{0\le i<n\,|\,x_i=0\}$ for $x=(x_0,\cdots,x_{n-1})\in\mathbb{F}_2^n$ and the third identity follows from (12) and (13).

Next we prove (11). Note the fact that $x\succeq\rho_k^m(\gamma)$ if and only if $\rho_{m-k}^m(x)\succeq\gamma$ for any $x\in\mathbb{F}_2^m$ and $0\le k<m$. Therefore, by the definition of $O_n(x)$ in (3) we have $\{x\in\mathbb{F}_2^m\,|\,x\succeq\delta,\delta\in O_m(\gamma)\}=\{x\in\mathbb{F}_2^m\,|\,x\in O_m(\delta),\delta\succeq\gamma,\delta\in\mathbf{R}_m\}$. Then, we can rewrite (10) as

$$\chi_{T_\gamma}(x)=\bigoplus_{\substack{\delta\in\mathbf{R}_m \\ \delta\succeq\gamma}}\bigoplus_{\beta'+\beta''\in O_m(\delta)}c_\beta x^\beta \tag{14}$$

where $c_\beta=c'_\beta\,(\mathrm{mod}\,2)$ and c'_β is the number of the term x^β that appears in the right hand side of (10), i.e., $c'_\beta=|\{\delta|\beta'+\beta''\succeq\delta,\delta\in O_m(\gamma)\}|$. Still by the above fact, we have that c'_β is a constant for all $\beta'+\beta''\in O_m(\delta)$, which is denoted by c'_δ for convenience, clearly $c'_\gamma=1$. Then we arrive at (11) from (14) where $c_\delta=c'_\delta\,(\mathrm{mod}\,2)$ and $c_\gamma=c'_\gamma\,(\mathrm{mod}\,2)=1$. $\qquad\square$

Example 2. *When $n=4$, the ANFs of $\bigoplus_{\beta'+\beta''\succeq\delta}x^\beta$ and $\bigoplus_{\beta'+\beta''\in O_m(\delta)}x^\beta$, $\delta\in\mathbb{F}_2^2$, are given in Table 2.*

Table 2: The ANFs of $\bigoplus_{\beta'+\beta''\succeq\delta}x^\beta$, $\bigoplus_{\beta'+\beta''\in O_m(\delta)}x^\beta$, $\delta\in\mathbb{F}_2^2$

δ	$\bigoplus_{\beta'+\beta''\succeq\delta}x^\beta$	$\bigoplus_{\beta'+\beta''\in O_m(\delta)}x^\beta$
$(0,0)$	$1\oplus\bigoplus_{i=0}^{3}(x_i\oplus x_ix_{i+1})$	1
$(1,0)$	$x_0\oplus x_2\oplus\bigoplus_{i=0}^{3}x_ix_{i+1}$	$\bigoplus_{i=0}^{3}x_i$
$(0,1)$	$x_1\oplus x_3\oplus\bigoplus_{i=0}^{3}x_ix_{i+1}$	$\bigoplus_{i=0}^{3}x_i$
$(1,1)$	$\bigoplus_{i=0}^{3}x_ix_{i+1}$	$\bigoplus_{i=0}^{3}x_ix_{i+1}$

Applying Lemma 4 to (9), we have

7

Theorem 2. *For the rotation symmetric bent function given in Theorem 1, its ANF is*

$$f_0(x) \oplus \bigoplus_{\gamma \in \mathbf{R}_m \cap \Gamma} \bigoplus_{\delta \in O_m(\gamma)} \bigoplus_{\beta' + \beta'' \succeq \delta} x^\beta.$$

As mentioned before, $n/2$ is the maximal algebraic degree of the n-variable bent function, which is usually of particular interest.

Corollary 1. *For the rotation symmetric bent function given in 1, the algebraic degree arrives at the maximal value $n/2$ if and only if the size $|\Gamma|$ of Γ is odd.*

4   Rotation symmetric bent functions of any possible algebraic degree

In this section, we study a flexible construction of n-variable rotation symmetric bent functions of any prescribed algebraic degree from 2 to $n/2$. We begin from a very useful linear combination of the n-variable characteristic functions $\chi_{T_\gamma}(x)$ in (11).

Lemma 5. *For each $\delta \in \mathbf{R}_m$, there exists an nonempty subset $A_\delta \subseteq \mathbf{R}_m$ such that*

$$\bigoplus_{\beta' + \beta'' \in O_m(\delta)} x^\beta = \bigoplus_{\gamma \in A_\delta} \chi_{T_\gamma}.$$

Proof. List all the vectors in $\mathbf{R}_m$ according to the Hamming weight firstly and the lexicographic order secondly as

$$\mathbf{R}_m = \{\alpha_1, \cdots, \alpha_{|\mathbf{R}_m|}\}$$

i.e., $\alpha_i \not\succeq \alpha_j$ if $i < j$. Then, by (11) we have

$$\left(\chi_{T_{\alpha_1}}, \cdots, \chi_{T_{\alpha_{|\mathbf{R}_m|}}}\right) = \left(\bigoplus_{\beta' + \beta'' \in O_m(\alpha_1)} x^\beta, \cdots, \bigoplus_{\beta' + \beta'' \in O_m(\alpha_{|\mathbf{R}_m|})} x^\beta\right) \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ * & 1 & \ddots & & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ * & & \ddots & 1 & 0 \\ * & * & \cdots & * & 1 \end{pmatrix}$$

Since the matrix is a lower triangular matrix of full rank, each $\bigoplus_{\beta' + \beta'' \in O_m(\delta)} x^\beta$ can be expressed as a linear combination of $\chi_{T_{\alpha_1}}, \cdots, \chi_{T_{\alpha_{|\mathbf{R}_m|}}}$. $\square$

Based on Lemma 5, we can construct n-variable rotation symmetric bent function f with any algebraic degree $2 \leq \deg(f) \leq n/2$.

Theorem 3. *For any element $\delta \in \mathbf{R}_m$ with $\mathrm{wt}(\delta) \geq 2$, the function*

$$f_0(x) \oplus \left(\bigoplus_{\beta' + \beta'' \in O_m(\delta)} x^\beta\right)$$

is a rotation symmetric bent function with algebraic degree $\deg(f) = \mathrm{wt}(\delta)$, where f_0 is given in (1).

Proof. The bent property of f is a direct consequence of (9), Theorem 2, and Lemma 5. And $\deg(f) = \mathrm{wt}(\delta)$ comes the fact that $\deg(x^\beta) = \mathrm{wt}(\beta) = \mathrm{wt}(\delta)$ for all $\beta' + \beta'' \in O_m(\delta)$.

$\square$

By means of Theorem 3, we are able to construct more n-variable rotation symmetric bent functions by flexibly assembling some $\bigoplus_{\beta'+\beta''\in O_m(\delta)} x^\beta$.

Theorem 4. *For any nonempty subset $A \subseteq \mathbf{R}_m$, the function*

$$f_0(x) \oplus \bigoplus_{\delta \in A} \left(\bigoplus_{\beta'+\beta'' \in O_m(\delta)} x^\beta \right)$$

is a rotation symmetric bent function, where f_0 is given in (1).

Example 3. *In [3], for $n = 2m = 6r$, Carlet et al. constructed an n-variable cubic rotation symmetric bent function as*

$$f(x) = f_0(x) \oplus \bigoplus_{i=0}^{n-1} x_i x_{r+i} x_{2r+i} \oplus \bigoplus_{i=0}^{2r-1} x_i x_{2r+i} x_{4r+i}$$

where $f_0(x)$ is given by (1). According to Theorem 1 in [3], we know that $f(x)$ can be rewritten as

$$f(x) = f_0(x) \oplus \bigoplus_{\beta'+\beta'' \in O_m(\delta)} x^\beta$$

where $\delta \in \mathbf{R}_m$ such that $\mathrm{supp}(\delta) = \{0, r, 2r\}$. In other words, the cubic rotation symmetric bent function in [3] is a simple case of our construction.

Finally, we demonstrate a class of rotation symmetric bent functions by setting

$$\Gamma_i^{(m)} \quad = \bigcup_{\gamma \in \mathbf{R}_m,\, \mathrm{wt}(\gamma)=i} T_\gamma \tag{15}$$

where T_γ is given in (8) and $0 \le i < m$.

Lemma 6. *The ANF of the n-variable characteristic function of $\Gamma_i^{(m)}$ in (15) can be expressed as*

$$\chi_{\Gamma_i^{(m)}}(x) = \bigoplus_{j \succeq i} \bigoplus_{\substack{\mathrm{wt}(\alpha)=j \\ \alpha'*\alpha''=0}} x^\alpha$$

for all $0 \le i \le m$.

Proof. By (9), (10) and (15), we have

$$
\begin{aligned}
\chi_{\Gamma_i^{(m)}}(x) \quad &= \bigoplus_{\substack{\gamma \in \mathbf{R}_m \\ \mathrm{wt}(\gamma)=i}} \chi_{T_\gamma}(x) \\
&= \bigoplus_{\substack{\gamma \in \mathbf{R}_m \\ \mathrm{wt}(\gamma)=i}} \bigoplus_{\delta \in O_m(\gamma)} \bigoplus_{\beta'+\beta'' \succeq \delta} x^\beta \\
&= \bigoplus_{\mathrm{wt}(\delta)=i} \bigoplus_{\beta'+\beta'' \succeq \delta} x^\beta \\
&= \bigoplus_{j=i}^{m} \left[\binom{j}{i} \bigoplus_{\substack{\mathrm{wt}(\beta)=j \\ \beta'*\beta''=0}} x^\beta \right] \\
&= \bigoplus_{j \succeq i} \bigoplus_{\substack{\mathrm{wt}(\beta)=j \\ \beta'*\beta''=0}} x^\beta
\end{aligned}
$$

where the fourth identity holds since given any vector $\beta \in \mathbb{F}_2^n$ with $\mathrm{wt}(\beta) = j$ for $i \le j \le m$, satisfying $\beta' + \beta'' \succeq \delta$, we have that

9

- $\operatorname{wt}(\beta) = \operatorname{wt}(\beta' + \beta'')$;

- the number of distinct δ with $\operatorname{wt}(\delta) = i$ satisfying $\beta' + \beta'' \succeq \delta$ is $\binom{j}{i}$,

and the last identity holds by Lucas formula in (2). □

From Theorem 1, Lemma 6, (9) and (15), we obtain the following theorem.

Theorem 5. *For any set $\Gamma_i^{(m)}$ in (15), the function $f_0(x) \oplus \bigoplus\limits_{j \succeq i} \bigoplus\limits_{\substack{\operatorname{wt}(\alpha)=j \\ \alpha' * \alpha'' = 0}} x^\alpha$ is a rotation symmetric bent function with algebraic degree $\deg(f) = m$, where f_0 is given in (1).*

5 Conclusion

In this paper, for $n = 2m$, we proposed a systematic method for constructing n-variable rotation symmetric bent functions with any given possible algebraic degrees ranging from 2 to m.

References

[1] A. Canteaut and P. Charpin, "Decomposing Bent functions," IEEE Trans. Inf. Theory, vol. 49, no. 8, pp. 2004-2019, 2003.

[2] 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," J. Comb. Theory, Ser. A, vol. 127, pp. 161-175, 2014.

[3] 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, vol. 8865, Lecture Notes in Computer Science, pp. 21-33.

[4] P. Charpin, E. Pasalic, and C. Tavernier, "On Bent and semi-bent quadratic Boolean functions," IEEE Trans. Inf. Theory, vol. 51, no.12, pp. 4286-4298, 2005.

[5] D. Dalai, S. Maitra, and S. Sarkar, "Results on rotation symmetric bent functions," Discr. Math., vol. 309, no. 8, pp. 2398-2409, 2009.

[6] G. Gao, X. Zhang, W. Liu, and C. Carlet, "Constructions of quadratic and cubic rotation symmetric bent functions," IEEE Trans. Inf. Theory, vol. 58, no. 7, pp. 4908-4913, 2012.

[7] S. Kavut, S. Maitra and M.D. Ycel, "Search for Boolean functions with excellent profiles in the rotation symmetric class," IEEE Trans. Inf. Theory, vol. 53, no. 5, pp. 1743-1751, 2007.

[8] A. Lempel and M. Cohn, "Maximal families of bent sequences," IEEE Trans. Inf. Theory, vol. 28, no. 6, pp. 865-868, 1982.

[9] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North-Holland, 1977.

[10] Q. Meng, L. Chen, and F. Fu, "On homogeneous rotation symmetric bent functions," Discr. Appl. Math., vol. 158, no. 10, pp. 1111-1117, 2010.

[11] J.D. Olsen, R.A. Scholtz, and L.R. Welch, "Bent-function sequences," IEEE Trans. Inf. Theory, vol. 28, no. 6, pp. 858-864, 1982.

[12] J. Pieprzyk and C. Qu, "Fast hashing and rotation-symmetric functions," J. Univ. Comput. Sci., vol. 5, pp. 20-31, 1999.

[13] O. Rothaus, "On 'bent' functions," J. Comb. Theory, Series A, vol. 20, no. 3, pp. 300-305, 1976.

[14] P. Stănică and S. Maitra, "Rotation symmetric Boolean Functions-Count and Cryptographic Properties," Discr. Appl. Math., vol. 156, pp. 1567-1580, 2008.

[15] P. Stănică, "On the nonexistence of homogeneous rotation symmetric bent Boolean functions of degree greater than two," Proceedings of the NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security, IOS Press, Amsterdam, pp. 214-218, 2008.