A NEW CONSTRUCTION OF ROTATION SYMMETRIC BENT FUNCTIONS WITH MAXIMAL ALGEBRAIC DEGREE

SIHONG SU*

School of Mathematics and Statistics, Henan University
Kaifeng 475004, China

(Communicated by Zhengchun Zhou)

Abstract. In this paper, for any even integer \( n = 2m \geq 4 \), a new construction of \( n \)-variable rotation symmetric bent function with maximal algebraic degree \( m \) is given as

\[
 f(x_0, x_1, \ldots, x_{n-1}) = \bigoplus_{i=0}^{m-1} (x_i x_{m+i}) \oplus \bigoplus_{i=0}^{n-1} (x_i x_{i+1} \cdots x_{i+m-2} x_{i+2m+n}).
\]

whose dual function is

\[
 \tilde{f}(x_0, x_1, \ldots, x_{n-1}) = \bigoplus_{i=0}^{m-1} (x_i x_{m+i}) \oplus \bigoplus_{i=0}^{n-1} (x_i x_{i+1} \cdots x_{i+m-2} x_{i+2m+n-2}),
\]

where \( \pi_i = x_i \oplus 1 \) and the subscript of \( x \) is modulo \( n \).

1. Introduction

The subject of Boolean functions is well established and constitutes a cornerstone of cryptography and coding theory. Bent functions were introduced by Rothaus in 1976 [17]. A Boolean function is bent if it has maximal Hamming distance to the set of all the affine Boolean functions. Bent functions have been attracted much attention due to their important applications in cryptography, coding theory and sequence design [1, 5, 11, 12, 14, 15]. Bent functions always occur in pairs, that is, given a bent function one can always define its dual function which is again a bent function. Yet, computing the dual function of a given bent function is not an easy task in general [13].

It has been found recently that the class of rotation symmetric Boolean functions is extremely rich in terms of cryptographically significant Boolean functions. An \( n \)-variable Boolean function over the vector space \( \mathbb{F}_2^n \) which is invariant under the action of the cyclic group \( C_n \) is called rotation symmetric Boolean function. Rotation symmetric Boolean functions were introduced (with a different name, idempotents) in Papers [6, 7] and were studied under their now standard name in Paper [16]. In fact, such class of Boolean functions is of great interest since they need less space to be stored and allow faster computation of their Walsh-Hadamard transform [8, 10]. In recent years, the construction of rotation symmetric bent functions has become

---

2010 Mathematics Subject Classification: Primary: 58F15, 58F17; Secondary: 53C35.

Key words and phrases: Orbit, rotation symmetric Boolean function, Walsh-Hadamard transform, bent function, algebraic degree.

The author is supported by the National Natural Science Foundation of China (Grant No. 61502147) and the Excellent Youth Program of Henan University (Grant No. yqpy20170063).

* Corresponding author: Sihong Su (E-mail: sush@henu.edu.cn).
a hot topic. Any theoretic advancement in this direction can be used to find cryptographically significant functions on higher number of variables. Before 2015, only few constructions of rotation symmetric bent functions were known [3, 4, 9]. Further, the algebraic degrees of these rotation symmetric bent functions are not more than 4. For instance, in 2012, Gao et al. proved that the cubic rotation symmetric function $f(x_0, x_1, \cdots, x_{n-1}) = \bigoplus_{i=0}^{m-1} (x_i x_{m+i}) \oplus \bigoplus_{i=0}^{n-1} (x_i x_{i+1} + x_{i+m})$ is bent if and only if $\frac{m}{\gcd(m, n)}$ is odd [9], where $n = 2m$, $1 \leq t \leq m - 1$, $x_{i+m} = x_i + 1$, and the subscript of $x$ is modulo $n$. In 2017, a systematic constructions of $n$-variable rotation symmetric bent functions with any possible algebraic degree ranging from 2 to $n/2$ were proposed in Paper [18]. In Paper [19], the authors proposed a large group of bent functions with optimal algebraic degree and studied their dual bent functions.

In this paper, for any even integer $n \geq 4$, a new construction of $n$-variable rotation symmetric bent function with maximal algebraic degree $n/2$ is presented, whose dual function is also given.

The rest of this paper is organized as follows. In Section 2, some basic notations and definitions of Boolean functions and rotation symmetric bent functions are reviewed. In Section 3, the construction of $n$-variable rotation symmetric bent function with maximal algebraic degree $n/2$ is given. In Section 4, the dual function of the proposed rotation symmetric bent function is proposed, which also has maximal algebraic degree. Section 5 concludes this paper.

2. Preliminaries

Let $\mathbb{F}_2$ be the finite field with two elements, $n$ be a positive integer, and $\mathbb{F}_2^n$ be the $n$-dimensional vectorspace over $\mathbb{F}_2$. To avoid confusion, we denote the sum over $\mathbb{Z}$ by $+$ or $\sum$, and the sum over $\mathbb{F}_2$ by $\oplus$ or $\bigoplus$. Given a vector $x = (x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_2^n$, define its support as the set $\text{supp}(x) = \{0 \leq i < n \mid x_i = 1\}$, and its Hamming weight $\text{wt}(x)$ as the cardinality of its support, i.e., $\text{wt}(x) = |\text{supp}(x)|$.

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. Given a subset $T \subseteq \mathbb{F}_2^n$, the characteristic function of $T$ is defined as

$$\chi_T(x) = \begin{cases} 1, & x \in T, \\ 0, & x \in \mathbb{F}_2^n \setminus T. \end{cases}$$

Then, $\chi_T(x)$ is an $n$-variable Boolean function. The support of a Boolean function $f \in \mathcal{B}_n$ is defined as $\text{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$. Hence, $\text{supp}(\chi_T) = T$. In usual, a Boolean function $f \in \mathcal{B}_n$ is expressed as

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

where $c_\alpha$ is the coefficient of the term $x^\alpha = x_0^{\alpha_0} x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}}$ for the vectors $x = (x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_2^n$ and $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$. The expression of the Boolean function $f$ in (1) is called the algebraic normal form (ANF) of $f$. Further, the algebraic degree of the Boolean function $f$ in (1) is defined as

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

Especially, the Boolean functions of algebraic degree at most 1 are called affine functions.
Given a vector \( x = (x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_2^n \), define the left \( l \)-cyclic shift of \( x \) as 
\[
\rho^l_n(x) = (x_l, x_{l+1}, \cdots, x_{n-1+l}),
\]
where the integers \( l \geq 0 \) and \( 0 \leq i < n \). Herein and hereafter, the subscript of \( x \) is modulo \( n \). The orbit generated by a vector \( x \in \mathbb{F}_2^n \) is defined as 
\[
O_n(x) = \{ \rho^0_n(x), \rho^1_n(x), \cdots, \rho^{n-1}_n(x) \}.
\]
For example, it is easy to see that \( O_4(1,1,0,0) = \{(1,1,0,0), (0,1,1,0), (0,0,1,1), (1,0,0,1)\} \) and \( O_4(1,0,1,0) = \{(1,0,0,0), (0,1,0,1)\} \). Given a vector \( x \in \mathbb{F}_2^n \), the length of the orbit generated by \( x \) is defined as the cardinality of this orbit. For convenience, in this paper, given a subset \( T \) of \( \mathbb{F}_2^n \), we denote 
\[
O_n(T) = \bigcup_{x \in T} O_n(x).
\]

**Definition 2.1.** For a Boolean function \( f \in \mathcal{B}_n \), if \( f(\rho^l_n(x)) = f(x) \) holds for all inputs \( x \in \mathbb{F}_2^n \), then \( f \) is called an \( n \)-variable rotation symmetric Boolean function.

That is, rotation symmetric Boolean functions are invariant under the left cyclic shift of their inputs. As a consequence, given a vector \( \alpha \in \mathbb{F}_2^n \), the coefficients of the terms \( x^\beta \), \( \beta \in O_n(\alpha) \), in the ANF of an \( n \)-variable rotation symmetric Boolean function are all the same. Hence, when the ANF of an \( n \)-variable rotation symmetric Boolean function is given, we denote 
\[
O_n(x^\alpha) = \bigoplus_{\beta \in O_n(\alpha)} x^\beta
\]
in this paper for simplicity. For example, when \( n = 4 \), then \( O_4(x_0x_1) = x_0x_1 \oplus x_1x_2 \oplus x_2x_3 \oplus x_3x_0 \) and \( O_4(x_0x_2) = x_0x_2 \oplus x_1x_3 \).

The Walsh-Hadamard transform of a Boolean function \( f \in \mathcal{B}_n \) at the point \( \omega \in \mathbb{F}_2^n \) is defined as 
\[
W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \omega \cdot x},
\]
where \( \omega \cdot x = \bigoplus_{i=0}^{n-1} \omega_i x_i \) is the inner product of \( \omega = (\omega_0, \omega_1, \cdots, \omega_{n-1}) \) and \( x = (x_0, x_1, \cdots, x_{n-1}) \) over \( \mathbb{F}_2 \).

For any Boolean function \( f \in \mathcal{B}_n \), according to the well-known Parseval’s relation \([12]\), we know 
\[
\sum_{\omega \in \mathbb{F}_2^n} (W_f(\omega))^2 = 2^{2n},
\]
which indicates that \( \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| \geq 2^{n/2} \).

Indeed, bent function reaches the lower bound as follows.

**Definition 2.2.** If the Walsh-Hadamard transform of a Boolean function \( f \in \mathcal{B}_n \) satisfies \( W_f(\omega) = \pm 2^{n/2} \) for all \( \omega \in \mathbb{F}_2^n \), then \( f \) is called a bent function.

Obviously, an \( n \)-variable Boolean function is bent only if \( n \) is even. In addition, the algebraic degree of an \( n \)-variable bent function is at most \( n/2 \) for \( n \geq 4 \) \([2]\). It is known that bent functions occur in pair. In fact, given an \( n \)-variable bent function \( f \), we define its dual function, denoted by \( \tilde{f} \), when considering the signs of the values of the Walsh-Hadamard transform of \( f \), as 
\[
(-1)^{\tilde{f}(\omega)} = 2^{-n/2} W_f(\omega), \ \omega \in \mathbb{F}_2^n.
\]
Note that the dual function of a bent function is bent as well \([2]\).
From now on, for convenience, the following assumption and notations will be fixed all through this paper.

1. We assume $n = 2m \geq 4$ be an integer.
2. Given a vector $x \in \mathbb{F}_2^n$, we always denote $x = (x_0, x_1, \cdots, x_{n-1}) = (x', x_{m-2}, x_{m-1}, x'', x_{n-2}, x_{n-1})$, where $x' = (x_0, x_1, \cdots, x_{m-3})$ and $x'' = (x_m, x_{m+1}, \cdots, x_{n-3})$.
3. The all-zero (resp. all-one) vector of length $n$ is denoted by $0_n$ (resp. $1_n$).
4. We always denote $a = a \oplus 1$ for an entry $a \in \mathbb{F}_2$ and $x = x \oplus 1_n$ for a vector $x \in \mathbb{F}_2^n$.

3. Construction of rotation symmetric bent function with maximal algebraic degree

In this section, the method of constructing new $n$-variable rotation symmetric bent function is to choose a proper subset of $\mathbb{F}_2^n$ which is used to modify the support of a well-known quadratic Boolean function as

\[
f_0(x_0, x_1, \cdots, x_{n-1}) = O_n(x_0x_m) = \bigoplus_{i=0}^{m-1} x_i x_{m+i},
\]

which is the first kind of rotation symmetric bent function. And then, the ANF of the newly constructed $n$-variable rotation symmetric bent function will be given, which has the maximal algebraic degree $m$.

3.1. Construction of rotation symmetric Boolean function. Firstly, let’s define a subset of $\mathbb{F}_2^n$, which is used to construct new $n$-variable rotation symmetric bent function by modifying the support of the quadratic rotation symmetric bent function given in (3), as

\[
T = \{ x \in \mathbb{F}_2^n \mid x_{m-2} = x_{n-1}, x_{m-1} = x_{n-2} = 0, x'' = 0_m \}.
\]

For convenience, the subset $T$ in (4) can be written as $T = T_1 \cup T_2$, where

\[
\begin{cases}
T_1 = \{ x \in \mathbb{F}_2^n \mid x = (x', 0, 0, 0_m-2, 1, 0) \}, \\
T_2 = \{ x \in \mathbb{F}_2^n \mid x = (x', 1, 0, 0_m-2, 1, 1) \}.
\end{cases}
\]

Note that $T_1 \cap T_2 = \emptyset$. Further, it is easy to see that the number of the vectors in $T$ defined in (4) is equal to $2^{m-1}$ and the length of the orbit generated by each vector in $T$ is equal to $n$.

Using the subset $T$ of $\mathbb{F}_2^n$ in (4), we define an $n$-variable Boolean function as

\[
f(x) = \begin{cases}
f_0(x), & x \in O_n(T) \\
f_0(x), & x \in \mathbb{F}_2^n \setminus O_n(T)
\end{cases}
\]

where $f_0$ is the $n$-variable rotation symmetric bent function defined in (3).

In fact, by definition 2.1, we know the Boolean function $f$ in (6) is rotation symmetric since $f_0$ is rotation symmetric. So, we need to verify that the rotation symmetric Boolean function $f$ in (6) is bent, which will be done in the next subsection.
3.2. The bentness of the rotation symmetric Boolean function \( f \) defined in (6). In this subsection, we will verify the bentness of the rotation symmetric Boolean function \( f \) defined in (6).

Firstly, the following two conclusions will be used to compute the values of the Walsh-Hadamard transform of the rotation symmetric bent function \( f \) defined in (6).

Lemma 3.1. Given a vector \( \omega \in \mathbb{F}_2^n \), we have

\[
\sum_{x \in \mathbb{F}_2^{2n}} (-1)^\omega \cdot x = \begin{cases} 2^{m} & \omega = 0 \\ 0 & \text{otherwise} \end{cases}
\]

This is a well-known result. We omit the proof of this Lemma here.

Recall that a vector \( \omega \in \mathbb{F}_2^n \) can be represented as \( \omega = (\omega_0, \omega_1, \cdots, \omega_{n−1}) = (\omega', \omega_{m−2}, \omega_{m−1}, \omega'', \omega_{n−2}, \omega_{n−1}) \). Hence, given an integer \( l \in \{0, 1, \cdots, n−1\} \), we can get

\[
\rho_n^l(\omega) = (\rho_n^l(\omega_0), \rho_n^l(\omega_1), \cdots, \rho_n^l(\omega_{n−1}))
\]

\[
= (\omega_{n−l}, \omega_{n−l−1}, \cdots, \omega_{n−1−l})
\]

\[
= ((\rho_n^l(\omega))', \omega_{m−2−l}, \omega_{m−1−l}, (\rho_n^l(\omega))'', \omega_{n−2−l}, \omega_{n−1−l})
\]

which will be used in the next Lemma.

Lemma 3.2. Given a vector \( \omega \in \mathbb{F}_2^n \), we have

\[
\sum_{x \in \mathbb{O}_n(T)} (-1)^{f_0(x) \otimes \omega \cdot x} = 2^{m−1} \sum_{l \in \Delta} (-1)^{\omega_{n−2−l}},
\]

where \( f_0 \) is given in (3), \( T \) is given in (4), and

\[
\Delta = \{0 \leq l < n | (\rho_n^l(\omega))' = 0_{m−2}, \omega_{m−2−l} \neq \omega_{n−1−l} \}.
\]

Proof. Recall that the subset \( T \) in (4) can be written as \( T = T_1 \cup T_2 \) with \( T_1 \cap T_2 = \emptyset \), where \( T_1 \) and \( T_2 \) are defined in (5). Hence, we have

\[
\sum_{x \in \mathbb{O}_n(T)} (-1)^{f_0(x) \otimes \omega \cdot x}
\]

\[
= \sum_{x \in T_1} \sum_{0 \leq l < n} (-1)^{f_0(\rho_n^l(x)) \otimes \omega \cdot \rho_n^l(x)}
\]

\[
= \sum_{x \in T_1} \sum_{0 \leq l < n} (-1)^{f_0(\rho_n^l(x)) \otimes \omega \cdot \rho_n^l(x)} + \sum_{x \in T_2} \sum_{0 \leq l < n} (-1)^{f_0(\rho_n^l(x)) \otimes \omega \cdot \rho_n^l(x)}
\]

which will be discussed in the following two cases.

(1) If \( x \in T_1 \), then \( f_0(\rho_n^l(x)) = 0 \) for all \( 0 \leq l < n \) since \( f_0 \) is a rotation symmetric Boolean function and \( f_0(x) = 0 \). Hence, we have

\[
\sum_{x \in T_1} \sum_{0 \leq l < n} (-1)^{f_0(\rho_n^l(x)) \otimes \omega \cdot \rho_n^l(x)} = \sum_{x' \in \mathbb{F}_2^{m−2}} \sum_{0 \leq l < n} (-1)((\rho_n^l(\omega))', x' \otimes \omega_{n−2−l}),
\]

since \( \omega \cdot \rho_n^l(x) = \rho_n^{-l}(\omega) \cdot x = (\rho_n^{-l}(\omega))' \cdot x' \otimes \omega_{n−2−l} \).
(2) If \(x \in T_2\), then \(f_0(p'_n(x)) = 1\) for all \(0 \leq l < n\) since \(f_0\) is a rotation symmetric Boolean function and \(f_0(x) = 1\). Hence, similarly we have
\[
\sum_{x \in T_2} \sum_{0 \leq l < n} (-1)^{f_0(p'_n(x))} \cdot \omega \cdot p'_n(x)
\]
\[
\sum_{x \in T_2} \sum_{0 \leq l < n} (-1)^{f_0(p'_n(x))} \cdot \omega \cdot p'_n(x)
\]
\[
\sum_{x \in T_2} \sum_{0 \leq l < n} (-1)^{f_0(p'_n(x))} \cdot \omega \cdot p'_n(x)
\]
Combining (10) and (11), we have
\[
\sum_{x \in O_n(T)} (-1)^{f_0(x)} \cdot \omega \cdot x
\]
\[
\sum_{x \in O_n(T)} (-1)^{f_0(x)} \cdot \omega \cdot x
\]
\[
\sum_{x \in O_n(T)} (-1)^{f_0(x)} \cdot \omega \cdot x
\]
where the third identity holds by (7), and in the fourth identity we denote \(\Delta = \{0 \leq l < n \mid (\rho_n^{-l}(\omega))^\prime = 0_{m-2}, \omega_{m-2-l} \neq \omega_{n-1-l}\}\).

Note that, in the equation (8), if \(\Delta = \emptyset\) then we get \(\sum_{x \in O_n(T)} (-1)^{f_0(x)} \cdot \omega \cdot x = 0\).

In order to calculate the values of the Walsh-Hadamard transform of the rotation symmetric Boolean function \(f\) defined in (6), for any vector \(\omega \in F_2^n\) we should firstly determine the value of
\[
\delta_{\omega} = \sum_{l \in \Delta} (-1)^{(\omega_{m-1-l} \oplus \omega_{n-2-l}) \omega_{n-1-l}},
\]
where \(\Delta\) is given in (9).

The values of \(\delta_{\omega}\) in (12), \(\omega \in F_2^2\), will be determined in the following Lemma.

**Lemma 3.3.** Given a vector \(\omega \in F_2^2\), then \(\delta_{\omega} = 0\) or 2, where \(\delta_{\omega}\) is given in (12).

**Proof.** The values of \(\delta_{\omega}, \omega \in F_2^2\), will be discussed in the following three cases.

(1) If \(\Delta = \emptyset\), then \(\delta_{\omega} = 0\);

(2) If there exist an integer \(l_0 \in \Delta\) and \(\omega_{m-2-l_0} = 0\), i.e., \((\rho_n^{-l_0}(\omega))^\prime = 0_{m-2}\) and \(\omega_{n-1-l_0} = 1\), then the values of \(\delta_{\omega}\) will be discussed in the following four cases,

(2-1) If \((\omega_{m-1-l_0}, \omega_{n-2-l_0}) = (1, 1)\), i.e., \(\rho_n^{-l_0}(\omega) = (0_{m-2}, 0, 1, \omega_{m-l_0}, \cdots, \omega_{n-3-l_0}, 1, 1)\), then we know \(\Delta = \{l_0, l_0-1\}\), since \(\rho_n^{-l_0+1}(\omega) = (0_{m-2}, 1, \omega_{m-1-l_0-1}, \cdots, \omega_{n-4-(l_0-1)}, 1, 1, 0)\). Hence,
\[
\delta_{\omega} = (-1)^{(1 \oplus 1) \times 1} + (-1)^{(\omega_{m-l_0} \oplus 1) \times 0} = 2.
\]

(2-2) If \((\omega_{m-1-l_0}, \omega_{n-2-l_0}) = (1, 0)\), i.e., \(\rho_n^{-l_0}(\omega) = (0_{m-2}, 0, 1, \omega_{m-l_0}, \cdots, \omega_{n-3-l_0}, 0, 1)\), then the values of \(\delta_{\omega}\) will be discussed in the following two cases.
(2.2-1) If \((\omega_{m-1}, \cdots, \omega_{n-3-l_0}) = 0_{m-2}\), then \(\Delta = \{l_0, l_0 - 1, l_0 + m, l_0 + m - 1\}\), since \(\rho_n^{-l_0-m}(\omega) = \rho_n^{-l_0}(\omega) = (0_{m-2}, 0, 0, 0_m, 0, 0)\) and \(\rho_n^{-l_0+1}(\omega) = \rho_n^{-l_0-m+1}(\omega) = (0_{m-2}, 1, 0, 0_m, 0, 0)\). Hence,
\[
\delta_\omega = 2\[(−1)^{(1^0)0}1 + (−1)^{(0^1)0}0\] = 0.
\]
(2.2-2) If \((\omega_{m-1}, \cdots, \omega_{n-3-l_0}) \neq 0_{m-2}\), then we know \(\Delta = \{l_0, l_0 - 1\}\), since \(\rho_n^{-l_0+1}(\omega) = (0_{m-2}, 1, \omega_{m-1-\{l_0-1\}}, \cdots, \omega_{n-4-\{l_0-1\}}, 0, 1, 0)\). Hence,
\[
\delta_\omega = (−1)^{(1^0)0}1 + (−1)^{(0^1)0}0 = 0.
\]
(2-3) If \((\omega_{m-1-l_0}, \omega_{n-2-l_0}) = (0, 1)\), i.e., \(\rho_n^{-l_0}(\omega) = (0_{m-2}, 0, 0, \omega_{m-l_0}, \cdots, \omega_{n-3-l_0}, 1, 1)\), let \(\omega_{l'}-l_0\) be the first nonzero component in \(\rho_n^{-l_0}(\omega)\), where \(m \leq l' \leq n - 2\). Hence, we have \(\Delta = \{l_0, l_0 - l' + m - 2\}\), since \(\rho_n^{-l_0+l'+m-2}(\omega) = (0_{m-2}, 1, \omega_{m-1-l_0}, \cdots, \omega_{n-3-l_0}, 0, 0, 0)\). Hence,
\[
\delta_\omega = (−1)^{(0^1)1}0 + (−1)^{(1^0)0}0 = 0.
\]
(2-4) If \((\omega_{m-1-l_0}, \omega_{n-2-l_0}) = (0, 0)\), i.e., \(\rho_n^{-l_0}(\omega) = (0_{m-2}, 0, 0, \omega_{m-l_0}, \cdots, \omega_{n-3-l_0}, 0, 1)\), let \(\omega_{l'}-l_0\) be the first nonzero component in \(\rho_n^{-l_0}(\omega)\), where \(m \leq l' \leq n - 3\) or \(l' = n - 1\). Hence, we know \(\Delta = \{l_0, l_0 - l' + m + 2\}\), since \(\rho_n^{-l_0+l'+m-2}(\omega) = (0_{m-2}, 1, \omega_{m-1-l_0}, \cdots, \omega_{n-3-l_0}, 0, 0)\). Hence,
\[
\delta_\omega = (−1)^{(1^0)0}0 + (−1)^{(0^0)0}0 = 2.
\]
(3) If there exist an integer \(l_0 \in \Delta\) and \(\omega_{m-2-l_0} = 1\), i.e., \(\omega_{n-1-l_0} = 0\), then the values of \(\delta_\omega\) will be similarly discussed in the following four cases.

(3-1) If \((\omega_{m-1-l_0}, \omega_{n-2-l_0}) = (1, 1)\), i.e., \(\rho_n^{-l_0}(\omega) = (0_{m-2}, 1, 1, \omega_{m-l_0}, \cdots, \omega_{n-3-l_0}, 1, 0)\), then we know \(\Delta = \{l_0, l_0 + 1\}\), since \(\rho_n^{-l_0+1}(\omega) = (0_{m-2}, 0, 0, 1, 1, \omega_{m+1-l_0}, \cdots, \omega_{n-2-l_0+1})\). Hence,
\[
\delta_\omega = \{(−1)^{(1^1)0}0 + (−1)^{(1^0)0}1\} = \begin{cases} 
0 & \text{if } \omega_{n-3-l_0} = 0, \\
2 & \text{if } \omega_{n-3-l_0} = 1.
\end{cases}
\]
(3-2) If \((\omega_{m-1-l_0}, \omega_{n-2-l_0}) = (1, 0)\), i.e., \(\rho_n^{-l_0}(\omega) = (0_{m-2}, 1, 1, \omega_{m-l_0}, \cdots, \omega_{n-3-l_0}, 0, 0)\), let \(\omega_{l'}-l_0\) be the last nonzero component in \(\rho_n^{-l_0}(\omega)\), where \(m - 1 \leq l' \leq n - 3\). It is easy to see that \(\Delta = \{l_0, l_0 - l' - 1\}\), since \(\rho_n^{-l_0+l'+1}(\omega) = (0_{m-2}, 0, 0, \omega_{m-1-l_0}, \cdots, \omega_{n-2-l_0-1})\). Hence,
\[
\delta_\omega = \{(−1)^{(1^0)0}0 + (−1)^{(0^0)0}0\} = \begin{cases} 
2 & \text{if } \omega_{l'-l_0} = 0, \\
0 & \text{if } \omega_{l'-l_0} = 1.
\end{cases}
\]
(3-3) If \((\omega_{m-1-l_0}, \omega_{n-2-l_0}) = (0, 1)\), i.e., \(\rho_n^{-l_0}(\omega) = (0_{m-2}, 1, 1, \omega_{m-1-l_0}, \cdots, \omega_{n-3-l_0}, 1, 0)\), then the values of \(\delta_\omega\) will be discussed in the following two cases.

(3-3-1) If \((\omega_{m-1-l_0}, \cdots, \omega_{n-3-l_0}) = 0_{m-2}\), then \(\Delta = \{l_0, l_0 + 1, l_0 + m, l_0 + m + 1\}\), since \(\rho_n^{-l_0+m}(\omega) = \rho_n^{-l_0}(\omega) = (0_{m-2}, 0, 0, 0_m, 0, 0)\) and \(\rho_n^{-l_0+1}(\omega) = \rho_n^{-l_0-m+1}(\omega) = (0_{m-2}, 0, 1, 0_m, 0, 1)\). Hence,
\[
\delta_\omega = 2[−(−1)^{(0^1)0}0 + (−1)^{(1^0)1}0] = 0.
\]

Advances in Mathematics of Communications Volume 13, No. 2 (2019), 253–265
Hence, the Walsh-Hadamard transform of \((13)\) is bent.

Theorem 3.4. The \(n\)-variable rotation symmetric Boolean function \(f\) defined in (6) is bent.

Proof. Recall that the values of the Walsh-Hadamard transform of the \(n\)-variable rotation symmetric bent function \(f_0\) in (3) are

\[
W_{f_0}(\omega) = (-1)^{f_0(\omega)} 2^m, \omega \in \mathbb{F}_2^n.
\]

Hence, the Walsh-Hadamard transform of \(f\) at any vector \(\omega \in \mathbb{F}_2^n\) is

\[
W_f(\omega) = \sum_{x \in \mathbb{F}_2^n \backslash O_n(T)} (-1)^{f_0(x) \oplus \omega \cdot x} + \sum_{x \in O_n(T)} (-1)^{f_0(x) \oplus \omega \cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f_0(x) \oplus \omega \cdot x} - 2 \sum_{x \in O_n(T)} (-1)^{f_0(x) \oplus \omega \cdot x} = (-1)^{f_0(\omega)} 2^m - 2^m \sum_{\ell \in \Delta} (-1)^{\omega_{n-2-\ell}} = (-1)^{f_0(\omega)} 2^m \left(1 - \sum_{\ell \in \Delta} (-1)^{\omega_{n-2-\ell} \oplus f_0(\omega)}\right) = (-1)^{f_0(\omega)} 2^m \left(1 - \sum_{\ell \in \Delta} (-1)^{\omega_{n-2-\ell} \oplus \omega_{m-2-l} \oplus \omega_{m-2-l} \oplus \omega_{m-1-l} \oplus \omega_{n-1-l}}\right) = (-1)^{f_0(\omega)} 2^m \left(1 - \sum_{\ell \in \Delta} (-1)^{\omega_{m-1-l} \oplus \omega_{n-2-l}} \omega_{n-1-l}\right) = (-1)^{f_0(\omega)} 2^m (1 - \delta_\omega)
\]

where \(\Delta\) is given in (9) and \(\delta_\omega\) is defined in (12), the third identity holds by (13) and \((8)\), the fifth identity holds since \(f_0(\omega) = f_0(\rho_n^{-l}(\omega))\) for \(0 \leq l < n\) by the definition of \(f_0\) in (3) and \((\rho_n^{-l}(\omega))' = (\omega_{n-1}, \omega_{n-1}, \ldots, \omega_{m-3} ) = 0_{m-2}\), the sixth identity holds since \(\omega_{m-2-\ell} \oplus 1 = \omega_{n-1-l}\).

The proof is finished by Definition 2.2 and Lemma 3.3.

We have finished the proof.
3.3. The ANF of the Rotation Symmetric Bent Function $f$ Defined in (6).

In this subsection, we will compute the ANF of the $n$-variable rotation symmetric bent function $f$ defined in (6).

Next conclusion tells us that we can interchange $\bigoplus$ and $\prod$ when we compute the ANF of the $n$-variable rotation symmetric bent function $f$ defined in (6).

**Lemma 3.5.** Given a nonempty set $T = T_0 \times T_1 \times \cdots \times T_{n-1}$ with $T_i \subseteq \mathbb{F}_2$ for $0 \leq i < n$, we have

$$\bigoplus_{\alpha \in T} \prod_{i=0}^{n-1} (x_i \oplus \alpha_i) = \prod_{i=0}^{n-1} \left[ \bigoplus_{\alpha_i \in T_i} (x_i \oplus \alpha_i) \right].$$

**Proof.** In fact, by a direct calculation, we have

$$\bigoplus_{\alpha \in T} \prod_{i=0}^{n-1} (x_i \oplus \alpha_i)$$

$$= \bigoplus_{(\alpha_0, \alpha_1, \cdots, \alpha_{n-1}) \in T_0 \times T_1 \times \cdots \times T_{n-1}} \left( \bigoplus_{\alpha_0 \in T_0} \prod_{i=0}^{n-1} (x_i \oplus \alpha_i) \right)$$

$$= \bigoplus_{(\alpha_0, \alpha_1, \cdots, \alpha_{n-1}) \in T_0 \times T_1 \times \cdots \times T_{n-1}} \left[ \left( \bigoplus_{\alpha_0 \in T_0} (x_0 \oplus \alpha_0) \right) \prod_{i=1}^{n-1} (x_i \oplus \alpha_i) \right]$$

$$= \left( \bigoplus_{\alpha_0 \in T_0} (x_0 \oplus \alpha_0) \right) \bigoplus_{(\alpha_1, \cdots, \alpha_{n-1}) \in T_1 \times \cdots \times T_{n-1}} \prod_{i=1}^{n-1} (x_i \oplus \alpha_i)$$

Repeat the above steps, the proof is finished. \(\square\)

For example, let $n = 4$ and $T = \{0\} \times \{1\} \times \{0,1\} \times \{0,1\}$. Then the left hand side of the equation in (15) is equal to

$$\bigoplus_{\alpha \in T} \prod_{i=0}^{n-1} (x_i \oplus \alpha_i) = x_0(x_1 \oplus 1) [x_2x_3 \oplus x_2(x_3 \oplus 1) \oplus (x_2 \oplus 1)x_3 \oplus (x_2 \oplus 1)(x_3 \oplus 1)] = x_0(x_1 \oplus 1)$$

and the right hand side of the equation in (15) is equal to

$$\prod_{i=0}^{n-1} \left[ \bigoplus_{\alpha_i \in T_i} (x_i \oplus \alpha_i) \right] = x_0(x_1 \oplus 1)[x_2 \oplus (x_2 \oplus 1)]x_3 \oplus (x_3 \oplus 1) = x_0(x_1 \oplus 1)$$

Now, we begin to compute the ANF of the $n$-variable rotation symmetric bent function $f$ defined in (6).

**Theorem 3.6.** The ANF of the $n$-variable rotation symmetric bent function $f$ defined in (6) is

$$f(x) = f_0(x) \oplus O_n(x_0x_1 \cdots x_{m-2} x_m),$$

where $f_0$ is given in (3).
Proof. In order to calculate the ANF of the \( n \)-variable rotation symmetric bent function \( f \) defined in (6), we only need to calculate the characteristic function of \( O_n(T) \) with \( T \) given in (4), since \( f(x) = f_0(x) \oplus \chi O_n(T)(x) \).

In fact, given a vector \( \alpha = (\alpha_0, \alpha_1, \cdots, \alpha_{n-1}) \in T \) in (4), we know \( \alpha_i \in \mathbb{F}_2 \) for \( 0 \leq i \leq m - 3 \), \( \alpha_{m-2} = \alpha_{n-1} \in \mathbb{F}_2 \), \( \alpha_i = 0 \) for \( m - 1 \leq i \leq n - 3 \), and \( \alpha_{n-2} = 1 \). Hence,

\[
\chi_T(x) = \bigoplus_{\alpha \in T} \prod_{i=0}^{n-1} (\overline{x_i} \oplus \alpha_i)
= \left( \prod_{i=0}^{m-3} \left( \bigoplus_{\alpha_i \in \mathbb{F}_2} (\overline{x_i} \oplus \alpha_i) \right) \right) (x_{m-2} \oplus x_{n-1} \oplus 1) \left( \prod_{i=m-1}^{n-3} \overline{x_i} \right) x_{n-2}
= (x_{m-2} \oplus x_{n-1} \oplus 1) \left( \prod_{i=m-1}^{n-3} \overline{x_i} \right) (x_{n-2} \oplus 1)
= \left( \prod_{i=m-2}^{n-2} \overline{x_i} \right) \left( x_{m-2} x_{n-2} \oplus x_{n-2} x_{n-1} \oplus x_{n-2} x_{m-2} \oplus x_{n-2} x_{n-1} \oplus 1 \right)
= \left( \prod_{i=m-2}^{n-2} \overline{x_i} \right) \left( \prod_{i=m-1}^{n-1} \overline{x_i} \right) \left( \prod_{i=m-2}^{n-2} \overline{x_i} \right) \left( \prod_{i=m-1}^{n-1} \overline{x_i} \right) x_{n-1}
\]

where the second identity holds by Lemma 3.5 and since

\[
\bigoplus_{\alpha_{m-2} = \alpha_{n-1} \in \mathbb{F}_2} (x_{m-2} \oplus \alpha_{m-2})(x_{n-1} \oplus \alpha_{n-1})
= x_{m-2} x_{n-1} \oplus x_{m-2} x_{n-1}
= x_{m-2} \oplus x_{n-1} \oplus 1
\]

and the third identity holds since \( \bigoplus_{\alpha_i \in \mathbb{F}_2} (\overline{x_i} \oplus \alpha_i) = (x_i \oplus 0 \oplus 1) \oplus (x_i \oplus 1 \oplus 1) = 1 \) for all \( 0 \leq i \leq m - 3 \).

Since \( O_n \left( \prod_{i=m-2}^{n-2} \overline{x_i} \right) = O_n \left( \prod_{i=m-1}^{n-1} \overline{x_i} \right) \) and \( O_n \left( \prod_{i=m-2}^{n-2} \overline{x_i} \right) = O_n \left( \prod_{i=m-1}^{n-1} \overline{x_i} \right) \), we know

\[
\chi_{O_n(T)}(x) = O_n(\chi_T(x))
= O_n \left( \left( \prod_{i=m-1}^{n-3} \overline{x_i} \right) x_{n-1} \right)
= O_n \left( \left( \prod_{i=0}^{m-2} \overline{x_i} \right) x_m \right)
\]

The proof is finished. \( \square \)

In fact, there is another rotation symmetric bent function which has the similar ANF as the rotation symmetric bent function given in Theorem 3.6.

**Corollary 1.** The \( n \)-variable rotation symmetric Boolean function

\[
g(x) = f_0(x) \oplus O_n(x_0 x_1 \cdots x_{m-2} \overline{x_m})
\]

is bent.
is also bent, and the support of $O_n(x_0x_1\cdots x_{m-2}x_m)$ is $\{x \mid x \in O_n(T)\}$, where $f_0$ is given in (3) and $T$ is given in (4).

Proof. From Theorem 3.6 we know the $n$-variable rotation symmetric Boolean function

$$f(x) = f_0(x) \oplus O_n(x_0x_1\cdots x_{m-2}x_m)$$

is bent. Let $y_i = x_i^1$ for $0 \leq i < n$. Then, let

$$h(y) = f(x) = f_0(y) \oplus O_n(y_0y_1\cdots y_{m-2}y_m)$$

$$= \bigoplus_{i=0}^{m-1} (y_i + 1)(y_m+i + 1) \oplus O_n(y_0y_1\cdots y_{m-2}y_m)$$

$$= \bigoplus_{i=0}^{m-1} y_iy_{m+i} \oplus \bigoplus_{i=0}^{n-1} y_i \oplus m \oplus O_n(y_0y_1\cdots y_{m-2}y_m)$$

$$= f_0(y) \oplus O_n(y_0y_1\cdots y_{m-2}y_m) \oplus \bigoplus_{i=0}^{n-1} y_i \oplus m$$

which is a rotation symmetric bent function. Hence, $g(y) = h(y) \oplus \bigoplus_{i=0}^{n-1} y_i \oplus m$ is a rotation symmetric bent function since $\bigoplus_{i=0}^{n-1} y_i \oplus m$ is a rotation symmetric affine function. \qed

4. The dual function of the rotation symmetric bent function $f$ defined in (6)

In this section, we study the dual function of the rotation symmetric bent function $f$ defined in (6).

Define a subset of $\mathbb{F}_2^n$ as

$$\bar{T} = \{x \in \mathbb{F}_2^n \mid x_{m-2} = x_{n-1}, (x_{m-1}, x''_{n-2}) = (1, 0_{m-1})\}.$$  \hspace{1cm} (16)

Similarly, the subset $\bar{T}$ in (16) can be written as $\bar{T} = \bar{T}_1 \cup \bar{T}_2$, where

$$\bar{T}_1 = \{x \in \mathbb{F}_2^n \mid x = (x', 0, 1, 0_{m-2}, 0, 0)\},$$

$$\bar{T}_2 = \{x \in \mathbb{F}_2^n \mid x = (x', 1, 1, 0_{m-2}, 0, 1)\}.$$

Then, by a direct verification it is easy to know the following conclusion holds.

Corollary 2. Given a vector $\omega \in \mathbb{F}_2^n$, then $\delta_\omega = 2$ if and only if $\omega \in O_n(\bar{T})$, where $\delta_\omega$ is given in (12) and $\bar{T}$ is defined in (16).

Theorem 4.1. The dual function of the rotation symmetric bent function $f$ defined in (6) is

$$\bar{f}(x) = \begin{cases} \bar{f}_0(x), & x \in O_n(\bar{T}) \\ f_0(x), & x \in \mathbb{F}_2^n \setminus O_n(\bar{T}) \end{cases}$$

where $f_0$ is given in (3) and $\bar{T}$ is defined in (16).
Proof. On one hand, given a vector $\omega \in \mathbb{F}_2^n$, by (14) we know the value of the Walsh-Hadamard transform of $f$ at $\omega$ is $W_f(\omega) = 2^m(-1)^{f_0(\omega)}(1 - \delta_\omega)$, where $\delta_\omega$ is given in (12) and the value of $\delta_\omega$ is equal to 0 or 2. On the other hand, by (2) we know the dual function of $f$, denoted by $\tilde{f}$, should satisfy $W_f(\omega) = 2^m(-1)^{\tilde{f}_0(\omega)}$, where $\omega \in \mathbb{F}_2^n$. Which gives

$(-1)^{\tilde{f}(\omega)} = \begin{cases} \frac{1}{2}
(-1)^{f(\omega)}, & \delta_\omega = 2, \\
(-1)^{f(\omega)}, & \delta_\omega = 0. \end{cases}$

The proof is finished by Corollary 2.

Theorem 4.2. The ANF of the $n$-variable rotation symmetric bent function $\tilde{f}$ in (17) is

$$\tilde{f}(x) = f_0(x) \oplus O_n(x_0x_1\cdots x_{m-2}x_{n-2}),$$

where $f_0$ is given in (3).

Proof. We only need to verify that the characteristic function of $O_n(\tilde{T})$ is

$$\chi_{O_n(\tilde{T})}(x) = O_n(x_0x_1\cdots x_{m-2}x_{n-2}),$$

where $\tilde{T}$ is given in (16).

Similarly to the proof of Theorem 3.6, by Lemma 3.5 and by the definition of $\tilde{T}$, we have

$$\chi_{\tilde{T}}(x) = \prod_{i=m}^{n-2} x_i \left( x_{m-1} \oplus 1 \right) \left( x_{m-2} \oplus x_{n-1} \oplus 1 \right)$$

= \prod_{i=m}^{n-2} x_i \left( x_{m-1} x_{m-2} \oplus x_{m-1} x_{n-1} \oplus x_{m-1} x_{m-2} \oplus x_{n-1} \oplus 1 \right)

= \prod_{i=m}^{n-2} x_i \oplus \left( \prod_{i=m}^{n-1} x_i \right) \oplus \left( \prod_{i=m}^{n-2} x_i \right) \oplus \left( \prod_{i=m}^{n-1} x_i \right) \oplus \left( \prod_{i=m}^{n-2} x_i \right) \left( x_{m-2} \oplus 1 \right)

Since

$$\chi_{O_n(\tilde{T})}(x) = O_n(\chi_{\tilde{T}}(x)) = O_n(x_0x_1\cdots x_{m-2}x_{n-2}),$$

the proof is finished.

By a direct calculation, we have the following conclusion.

Corollary 3. The dual function of the $n$-variable rotation symmetric bent function in Corollary 1 is

$$\tilde{g}(x) = f_0(x) \oplus O_n(x_0x_1\cdots x_{m-2}x_{n-2}),$$

where $f_0$ is given in (3).

5. Conclusion

In this paper, for any even integer $n = 2m \geq 4$, we give a new construction of $n$-variable rotation symmetric bent function with maximal algebraic degree and very simple ANF. Further, its dual function is also given.
The author would like to thank the associate editor and the anonymous reviewers for their constructive comments and suggestions which improved the quality of the paper.

REFERENCES

[1] A. Canteaut and P. Charpin, Decomposing Bent functions, IEEE Trans. Inf. Theory, 49 (2003), 2004–2019.
[2] C. Carlet, Boolean functions for cryptography and error correcting codes, in Boolean Models and Methods (eds. Y. Crama and P. L. Hammer), Cambridge, U.K.: Cambridge Univ. Press, (2010), 257–397.
[3] 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, 127 (2014), 161–175.
[4] C. Carlet, G. Gao and W. Liu, Results on constructions of rotation symmetric bent and semi-bent functions, in Sequences and Their Applications–SETA 2014, Springer International Publishing, Switzerland, 8865 (2014), 21–33.
[5] P. Charpin, E. Pasalic and C. Tavernier, On bent and semi-bent quadratic Boolean functions, IEEE Trans. Inf. Theory, 51 (2005), 4286–4298.
[6] É. Filiol and C. Fontaine, Highly nonlinear balanced Boolean functions with a good correlation-immunity, in EUROCRYPT 1998, (eds. K. Nyberg), Springer, Heidelberg, 1403 (1998), 475–488.
[7] C. Fontaine, On some cosets of the first-order Reed-Muller code with high minimum weight, IEEE Trans. Inf. Theory, 45 (1999), 1237–1243.
[8] S. Fu, L. Qu, C. Li and B. Sun, Balanced rotation symmetric Boolean functions with maximum algebraic immunity, IET Inf. Secur., 5 (2011), 93–99.
[9] G. Gao, X. Zhang, W. Liu and C. Carlet, Constructions of quadratic and cubic rotation symmetric bent functions, IEEE Trans. Inf. Theory, 58 (2012), 4908–4913.
[10] S. Kavut, S. Maitra and M. Yücel, Search for Boolean functions with excellent profiles in the rotation symmetric class, IEEE Trans. Inf. Theory, 53 (2007), 1743–1751.
[11] A. Lempel and M. Cohn, Maximal families of bent sequences, IEEE Trans. Inf. Theory, 28 (1982), 865–868.
[12] F. MacWilliams and N. Sloane, The Theory of Error-Correcting Codes, Amsterdam, The Netherlands, North-Holland, 1977.
[13] S. Mesnager, Several new infinite families of bent functions and their duals, IEEE Trans. Inf. Theory, 60 (2014), 4397–4407.
[14] S. Mesnager, Bent Functions, Springer International Publishing Switzerland, 2016.
[15] J. Olsen, R. Scholtz and L. Welch, Bent-function sequences, IEEE Trans. Inf. Theory, 28 (1982), 858–864.
[16] J. Pieprzyk and C. Qu, Fast hashing and rotation-symmetric functions, J. Univ. Comput. Sci., 5 (1999), 20–31.
[17] O. Rothaus, On ‘bent’ functions, J. Comb. Theory, Series A, 20 (1976), 300–305.
[18] S. Su and X. Tang, Systematic constructions of rotation symmetric bent functions, 2 rotation symmetric bent functions, and bent idempotent functions, IEEE Trans. Inf. Theory., 63 (2017), 4658–4667.
[19] W. Zhang, Z. Xing and K. Feng, A construction of bent functions with optimal algebraic degree and large symmetric group, preprint, Cryptology ePrint Archive, : Submission 2017/229.

Received for publication March 2018.

E-mail address: sush@henu.edu.cn