

Note

On the conjecture about the nonexistence of rotation symmetric bent functions *

Zhang Xiyong[†] Gao Guangpu

Zhengzhou Information Science and Technology Institute, PO Box 1001-745, Zhengzhou 450002, PRC

Abstract

In this paper, we describe a different approach to the proof of the nonexistence of homogeneous rotation symmetric bent functions. As a result, we obtain some new results which support the conjecture made in this journal, i.e., there are no homogeneous rotation symmetric bent functions of degree > 2 . Also we characterize homogeneous degree 2 rotation symmetric bent functions by using GCD of polynomials.

Keywords: *Boolean functions, Bent, Rotation-symmetric, Fourier Transform*

1 Motivation

Since the introduction in the seventies by Rothaus [1], bent functions have been intensively studied in the past three decades, and widely used in cryptography and error-correction coding due to their nice cryptographic and combinatoric properties. For example, the highest possible nonlinearity of bent functions can be used to resist the differential attack and the linear attack in symmetric cipher.

Recently, homogeneous rotation symmetric (Abbr. RotS) Boolean functions have attracted attentions (see [2, 3, 4]) because of their highly desirable property, i.e. they can be evaluated efficiently by re-using evaluations from previous iterations. Consequently, when efficient evaluation of the function (for example, design of some cryptographic algorithm, such as MD4 and MD5) is essential, these functions can serve as a good option.

It is natural to ask what kind of homogeneous RotS bent functions exist. In fact, homogeneous bent functions are of interest in literature [5, 6, 7, 8, 9, 10]. Stănică and Maitra [6, 7] studied RotS bent functions up to 10-variables. They enumerated all RotS bent functions in 8-variables. 4 · 3776 such functions of degree 2 were found. However, they couldn't find any homogeneous RotS bent functions of degree 3, 4 and 5 in 10 variables. Thus they made the following conjecture.

Conjecture 1.1 *There are no homogeneous rotation symmetric bent functions of degree > 2 .*

Let us summarize known results related to the above conjecture. Observing that bent functions are in fact Hadamard difference sets, Xia et al.[8] showed that there are no homogeneous bent functions of degree n in $2n$ variables for every $n > 3$. By using the relationship between the Fourier spectra of a Boolean function at partial points and the Fourier spectra of its sub-functions, Meng et al.[9] got a low bound of degree for homogeneous bent functions. From the view point of nonlinearity, Stănică [11] obtained the following nonexistence results (see Section 2 for the notation SANF of a Boolean function):

Theorem 1.2 *The following hold for a homogeneous RotS f of degree $d \geq 3$ in n variables:*

(i) *If the SANF of f is $x_1 \cdots x_d$, then f is not bent.*

*This work was supported by NSF of China with contract No. 60803154

[†]**Corresponding E-mail Address:** xiyong.zhang@hotmail.com

- (ii) If the SANF of f is $x_1 \cdots x_d + x_1 \cdots x_{d-1} x_{d+1}$, then f is not bent, assuming: $\frac{n-2}{4} > \lfloor \frac{n}{d} \rfloor$, if $n \not\equiv 1 \pmod{d}$; $\frac{n}{4} > \lfloor \frac{n}{d} \rfloor$, if $n \equiv 1 \pmod{d}$.
- (iii) If the SANF of f is $\mathbf{x}^{\mathbf{u}_1} + \cdots + \mathbf{x}^{\mathbf{u}_m}$, then f is not bent when $d_f < \frac{n/2-1}{\lfloor n/d \rfloor}$, where $d_f = \text{Max}_{i,j} \{j_2 - j_1 | u_{ij_1} = u_{ij_2} = 1, u_{ij} = 0 \text{ if } j_1 < j < j_2\}$.

In this paper we will introduce another method which may be more suitable for investigating homogeneous RotS bent functions. By using the rotation symmetric forms of RotS functions, we obtain more nonexistence results which are inaccessible by Theorem 1.2. For example our results imply that most homogeneous degree $d(\geq 3)$ RotS bent functions with SANF forms containing $x_1 \cdots x_d$ cannot exist. Also, we give an equivalent characterization of homogeneous degree 2 RotS bent functions by GCD of polynomials.

2 Preliminaries

In this section we list some basic definitions and notations about homogeneous rotation symmetric Boolean functions and bent functions.

Let \mathbb{F}_2^n be the vector space of dimension n over the two element field \mathbb{F}_2 . A Boolean function $f(x_0, \dots, x_{n-1})$ in n variables is a map from \mathbb{F}_2^n to \mathbb{F}_2 . For $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{u} = (u_1, \dots, u_n) \in \mathbb{F}_2^n$. Denote $\mathbf{x}^{\mathbf{u}} = x_1^{u_1} \cdots x_n^{u_n}$. Then every Boolean function f is uniquely of the form $f(\mathbf{x}) = \sum_{\mathbf{u} \in \mathbf{U}_f} \mathbf{x}^{\mathbf{u}}$, where $\mathbf{U}_f \subseteq \mathbb{F}_2^n$. Let $|\mathbf{u}|$ be the Hamming weight of $\mathbf{u} \in \mathbb{F}_2^n$. The algebraic degree of f is defined to be $\text{Max}\{|\mathbf{u}| \mid \mathbf{u} \in \mathbf{U}_f\}$.

By $A\|B$ we mean the concatenation of two bit strings A and B . We use $\underbrace{1 \cdots 1}_l$ (respectively $\underbrace{0 \cdots 0}_l$) to represent 1 (respectively 0) string of length l , and $\underbrace{1 * \cdots * 1}_l$ to represent a bit string of length l , with the first and the last bit to be 1.

We define an operation \oplus over \mathbb{F}_2 to be $x \oplus y \in \mathbb{F}_2$ such that $x \oplus y = 0$ if and only if $x = 0$ and $y = 0$. \oplus can be extended to \mathbb{F}_2^n by this way: for $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, $\mathbf{x} \oplus \mathbf{y} = (\mathbf{x}_1 \oplus \mathbf{y}_1, \dots, \mathbf{x}_n \oplus \mathbf{y}_n)$. Let $1 \leq l \leq n$, the operation $\rho^l(\cdot)$ acting on \mathbb{F}_2^n is defined to be $\rho^l(x_1, \dots, x_n) = (x_{n-l+1}, x_{n-l+2}, \dots, x_n, x_1, \dots, x_{n-l})$, where $n+l = l$ if $l > 0$. The cycle length $l_{\mathbf{x}}$ of $\mathbf{x} \in \mathbb{F}_2^n$ is the least number l such that $\rho^l(\mathbf{x}) = \mathbf{x}$. Obviously $l_{\mathbf{x}} | n$ and $l_{\mathbf{x}} = l_{\rho(\mathbf{x})}$.

Definition 2.1 A Boolean function $f(\mathbf{x})$, is called rotation symmetric (Abbr. RotS) if

$$f(\mathbf{x}) = f(\rho(\mathbf{x})), \text{ for all } \mathbf{x} \in \mathbb{F}_2^n.$$

It is clear that a RotS function f is of the form

$$f(\mathbf{x}) = \sum_{1 \leq i \leq m} \sum_{0 \leq l \leq l_{\mathbf{u}_i} - 1} \mathbf{x}^{\rho^l(\mathbf{u}_i)},$$

where $m \geq 1$, $\mathbf{u}_i \in \mathbb{F}_2^n (1 \leq i \leq m)$. Since the existence of $\mathbf{x}^{\mathbf{u}_i}$ implies the existence of $\mathbf{x}^{\rho(\mathbf{u}_i)}$, we can represent a RotS function f by the so-called *short algebraic normal form* (Abbr. SANF) $\mathbf{x}^{\mathbf{u}_1} + \cdots + \mathbf{x}^{\mathbf{u}_m}$.

Definition 2.2 For a Boolean function $f(x)$, the Fourier transform of f at $\mathbf{c} \in \mathbb{F}_2^n$ is defined as

$$\hat{f}(\mathbf{c}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) + \mathbf{c} \cdot \mathbf{x}},$$

where \cdot is dot product of two vectors in \mathbb{F}_2^n .

Definition 2.3 A Boolean function $f(\mathbf{x})$ is called bent if

$$|\hat{f}(\mathbf{c})| = 2^{n/2} \text{ for all } \mathbf{c} \in \mathbb{F}_2^n.$$

It is well-known that if $f(x_1, \dots, x_n)$ is bent, then n must be even, and the algebraic degree of f is upper-bounded by $n/2$.

Let $f(\mathbf{x}) = \mathbf{x}^{\mathbf{u}_1} + \dots + \mathbf{x}^{\mathbf{u}_m}$, define

$$h_f(\mathbf{u}) = \sum_{\substack{0 \leq t_1, \dots, t_m \leq 1 \\ t_1 \mathbf{u}_1 \oplus \dots \oplus t_m \mathbf{u}_m = \mathbf{u}}} (-2)^{t_1 + \dots + t_m}.$$

It is not difficult to deduce that

$$\widehat{f}(\mathbf{c}) = (-1)^{|\mathbf{c}|} \cdot \sum_{\mathbf{u} \succ \mathbf{c}} 2^{n-|\mathbf{u}|} h_f(\mathbf{u}),$$

where \succ is a partial order on \mathbb{F}_2^n such that $(u_1, \dots, u_n) \succ (v_1, \dots, v_n)$ if $u_i = v_i$ or $(u_i, v_i) = (1, 0)$. We also have the inverse formula:

$$h_f(\mathbf{u}) = (-1)^{|\mathbf{u}|} \cdot 2^{|\mathbf{u}|-n} \cdot \sum_{\mathbf{c} \succ \mathbf{u}} \widehat{f}(\mathbf{c}).$$

By the above formulas and Definition 2.3, one can prove that

Lemma 2.4 [12, 13] *Let n be even and $f(\mathbf{x}) = \mathbf{x}^{\mathbf{u}_1} + \dots + \mathbf{x}^{\mathbf{u}_m}$. Then f is bent if and only if*

$$v_2(h_f(\mathbf{u})) \begin{cases} = n/2 & \text{if } \mathbf{u} = \mathbf{1}, \\ > |\mathbf{u}| - n/2 & \text{if } \mathbf{u} \neq \mathbf{1}. \end{cases}$$

where $v_2(\cdot)$ is the 2-adic order function, $\mathbf{1}$ represents the vector $(1, \dots, 1) \in \mathbb{F}_2^n$.

3 The result

Let f be a RotS function of homogeneous degree d , SANF of f is $\sum_{1 \leq i \leq m} \mathbf{x}^{\mathbf{u}_i}$, where $\mathbf{u}_i = (u_{i1}, u_{i2}, \dots, u_{in})$, $u_{i1} = 1$, and $|\mathbf{u}_i| = d$.

We assume

$$\begin{aligned} D_i &= \text{Max}\{j | u_{ij} = 1, 1 \leq j \leq n\}, 1 \leq i \leq m, \\ D_1 &= \text{Min}\{D_i | 1 \leq i \leq m\}. \end{aligned}$$

Theorem 3.1 *Let f be a RotS bent function of homogeneous degree $d \geq 3$, the SANF of f is $\sum_{1 \leq i \leq m} \mathbf{x}^{\mathbf{u}_i}$, and $\mathbf{u}_1 = A_l \| \underbrace{0 \dots 0}_{n-D_1} \| B_{D_1-l} \| \underbrace{0 \dots 0}_{D_1-l}$, where $A_l = \underbrace{1 * \dots * 1}_l$, $B_{D_1-l} = \underbrace{1 * \dots * 1}_{D_1-l}$. If for all $1 \leq i \leq m$, $\mathbf{u}_i \neq A_l \| \underbrace{0 \dots 0}_{D_i-D_1} \| B_{D_1-l} \| \underbrace{0 \dots 0}_{n-D_i}$ and $\mathbf{u}_i \neq B_{D_1-l} \| \underbrace{0 \dots 0}_{n-kD_1} \| A_l \| \underbrace{0 \dots 0}_{kD_1-D_1}$, where $kd < n$, then*

$$k \cdot (d-1) < \frac{n}{2}.$$

Proof. Let

$$\mathbf{u}_0 = \mathbf{u}_1 \oplus \rho^{D_1}(\mathbf{u}_1) \oplus \dots \oplus \rho^{(k-1)D_1}(\mathbf{u}_1),$$

where $kd < n$.

Because $|\mathbf{u}_i| = d$ for all $1 \leq i \leq m$, we deduce that

$$\text{Min} \left\{ \sum_{1 \leq i \leq m, 1 \leq j \leq n} e_{ij} \mid \bigoplus_{1 \leq i \leq m} \bigoplus_{1 \leq j \leq n-1} e_{ij} \rho^j(\mathbf{u}_i) = \mathbf{u}_0, e_{ij} = 0, 1 \right\} = k.$$

Since for all $1 \leq i \leq m$, $\mathbf{u}_i \neq A_l \| \underbrace{0 \dots 0}_{D_i-D_1} \| B_{D_1-l} \| \underbrace{0 \dots 0}_{n-D_i}$ and $\mathbf{u}_i \neq B_{D_1-l} \| \underbrace{0 \dots 0}_{n-kD_1} \| A_l \| \underbrace{0 \dots 0}_{kD_1-D_1}$,

the only solution such that $\text{Min} \left\{ \sum_{1 \leq i \leq m, 1 \leq j \leq n} e_{ij} \right\} = k$ for the equation

$$\bigoplus_{1 \leq i \leq m} \bigoplus_{1 \leq j \leq n-1} e_{ij} \rho^j(\mathbf{u}_i) = \mathbf{u}_0, e_{ij} = 0, 1,$$

is

$$\mathbf{u}_0 = \mathbf{u}_1 \oplus \rho^{D_1}(\mathbf{u}_1) \oplus \cdots \oplus \rho^{(k-1)D_1}(\mathbf{u}_1).$$

Hence we get $v_2(h_f(\mathbf{u}_0)) = k$. Since $kd < n$, $\mathbf{u}_0 \neq \mathbf{1}$. By Theorem 2.4, we have

$$v_2(h_f(\mathbf{u}_0)) = k > |\mathbf{u}| - \frac{n}{2} = kd - \frac{n}{2},$$

and thus $k \cdot (d-1) < \frac{n}{2}$. ■

The above theorem implies nonexistence of many RotS bent functions. For example, we get

Proposition 3.2 *For a RotS function f of homogeneous degree $d \geq 3$, the following nonexistence results hold,*

- (1) *If the SANF $\sum_{1 \leq i \leq m} \mathbf{x}^{\mathbf{u}_i}$ of f contains $\mathbf{x}^{\mathbf{u}_1} = x_1 \cdots x_d$, and $\mathbf{u}_i (2 \leq i \leq m)$ is not of the form $\underbrace{1 \cdots 1}_l \underbrace{0 \cdots 0}_{D_i-d} \underbrace{1 \cdots 1}_{d-l} \underbrace{0 \cdots 0}_{n-D_i}$, then f is not bent.*
- (2) *If the SANF of f is $x_1 \cdots x_d + x_1 \cdots x_{d-1}x_{d+1}$, then f is not bent.*
- (3) *Suppose the SANF of f be $x_1x_{2+n_1}x_{3+n_1+n_2}$ and $n = q(D+n_0) + r + (n_1+1)$, where $n_1, n_2 \geq 0, n_0 = \text{Max}\{n_1, n_2\}, D = n_1 + n_2 + 3, q \geq 1, 0 \leq r < D + n_0$. If $q(D - n_0 - 1) \geq r + n_1 + 1$, then f is not bent.*

Proof.

(1) If $d \nmid n$. Let $n = qd + r, 0 < r < d, q \geq 2$.

Since $\mathbf{x}^{\mathbf{u}_1} = x_1 \cdots x_d$, and $\mathbf{u}_i (2 \leq i \leq m)$ is not of the form $\underbrace{1 \cdots 1}_l \underbrace{0 \cdots 0}_{D_i-d} \underbrace{1 \cdots 1}_{d-l} \underbrace{0 \cdots 0}_{n-D_i}$, using

Theorem 3.1, we have

$$k \cdot (d-1) < \frac{n}{2}, \quad 1 \leq k \leq \lfloor \frac{n}{d} \rfloor.$$

Let $k = \lfloor \frac{n}{d} \rfloor = q$. Thus $qd < 2q + r < 2q + d$, which produces $d < 2 + \frac{2}{q-1}$.

(1.1) If $q = 2$, then $d < 2 + \frac{2}{q-1} = 4$, so the only choice for d is $d = 3$. By again $qd < 2q + r$, we have $r > 3$, conflicting with $r < d = 3$.

(1.2) If $q = 3$, then $d < 2 + \frac{2}{q-1} = 3$, conflicting with $d \geq 3$.

(1.3) If $q \geq 4$, then $d < 2 + \frac{2}{q-1} < 3$, conflicting with $d \geq 3$.

If $d|n$, let $n = qd, q \geq 2$. We choose $k = \lfloor \frac{n}{d} \rfloor - 1 = q - 1$. Similarly using Theorem 3.1, we have

$$(q-1) \cdot (d-1) < \frac{n}{2} = \frac{qd}{2},$$

which produces $d < 2 + \frac{2}{q-2}$.

(1.4) If $q = 2$, then $n = 2d$. We choose another

$$\mathbf{u}_0 = \mathbf{u}_1 \oplus \rho^{d-1}(\mathbf{u}_1) = \underbrace{1 \cdots 1}_{n-1} \parallel 0.$$

Similarly we get $v_2(h_f(\mathbf{u}_0)) = 2$. By Theorem 2.4, $v_2(h_f(\mathbf{u}_0)) = 2 > |\mathbf{u}_0| - n/2 = n-1 - n/2$. Therefore $n < 6$. So $d = n/2 < 3$, conflicting with $d \geq 3$.

(1.5) If $q = 3$, then $d < 2 + \frac{2}{q-2} = 4$. Thus $d = 3$ and $n = qd = 9$. Obviously this is impossible since a bent function of n variables can exist for even n .

(1.6) If $q \geq 4$, then $d < 2 + \frac{2}{q-2} < 3$, conflicting with $d \geq 3$.

(2) Denote $\mathbf{u}_1 = \underbrace{1 \cdots 1}_d \parallel \underbrace{0 \cdots 0}_{n-d}$, $\mathbf{u}_2 = \underbrace{1 \cdots 1}_{d-1} \parallel 0 \parallel \underbrace{0 \cdots 0}_{n-d-1}$, then the SANF of f is $\mathbf{x}^{\mathbf{u}_1} + \mathbf{x}^{\mathbf{u}_2}$.

If $n \neq 0, 1 \pmod d$, let $n = qd + r$, $1 < r < d$, $q \geq 2$. We choose

$$\mathbf{u}_0 = \mathbf{u}_1 \oplus \rho^{D_1}(\mathbf{u}_1) \oplus \cdots \oplus \rho^{(q-1)D_1}(\mathbf{u}_1) = \underbrace{1 \cdots 1}_{qd} \underbrace{0 \cdots 0}_r,$$

and it is easy to see that $v_2(h_f(\mathbf{u}_0)) = q$.

Using Theorem 3.1, we obtain $q \cdot (d-1) < \frac{n}{2}$, and thus $qd < 2q + r < 2q + d$. The remaining discussions are the same as (1.1), (1.2) and (1.3).

If $n \equiv 0 \pmod d$, let $n = qd$, $q \geq 2$. We choose

$$\mathbf{u}_0 = \mathbf{u}_1 \oplus \rho^{D_1}(\mathbf{u}_1) \oplus \cdots \oplus \rho^{(q-2)D_1}(\mathbf{u}_1) = \underbrace{1 \cdots 1}_{(q-1)d} \underbrace{0 \cdots 0}_d.$$

Similarly by Theorem 3.1 we get $d < 2 + \frac{2}{q-2}$. We discuss the inequality in three cases: $q = 2$, $q = 3$ and $q \geq 4$. The proof for the cases $q = 3, 4$ are the same as (1.5), (1.6) respectively.

If $q = 2$, then $n = 2d$. We choose

$$\mathbf{u}_0 = \mathbf{u}_1 \oplus \rho^{d-2}(\mathbf{u}_1) = \underbrace{1 \cdots 1}_{2d-2} \parallel 00.$$

It is easy to see that $v_2(h_f(\mathbf{u}_0)) = 2$. By Theorem 2.4, we get $v_2(h_f(\mathbf{u}_0)) = 2 > 2d - 2 - n/2$. Thus $d < 4$. Since $d \geq 3$, we have $d = 3, n = 6$. However, RotS function over 6 variables with the SANF form $x_1x_2x_3 + x_1x_2x_4$ can be verified to be non-bent.

The remaining case is $n \equiv 1 \pmod d$. Assume $n = qd + 1$. We choose

$$\mathbf{u}_0 = \mathbf{u}_1 \oplus \rho^{D_1}(\mathbf{u}_1) \oplus \cdots \oplus \rho^{(q-2)D_1}(\mathbf{u}_1) = \underbrace{1 \cdots 1}_{(q-1)d} \underbrace{0 \cdots 0}_{d+1}.$$

Similarly we get $d < 2 + \frac{1}{q-2}$. If $q > 2$, then $d < 3$, a contradiction to $d \geq 3$. If $q = 2$, then $n = 2d + 1$. However, a Boolean functions in odd number variables cannot be bent.

(3) Denote $\mathbf{u}_1 = 1 \parallel \underbrace{0 \cdots 0}_{n_1} \parallel 1 \parallel \underbrace{0 \cdots 0}_{n_2} \parallel 1 \parallel \underbrace{0 \cdots 0}_{n-D}$, then the SANF of f is $\mathbf{x}^{\mathbf{u}_1}$.

Since $n = q(D + n_0) + r + (n_1 + 1)$ and $q \geq 1$, we see that $n - (n_1 + 1) \geq D + n_0$. Let $\mathbf{u}_2 = \bigoplus_{0 \leq i \leq n_0-1} \rho^i(\mathbf{u}_1)$, i.e.

$$\begin{aligned} \mathbf{u}_2 &= \underbrace{1 \cdots 0}_{n_1} \underbrace{0 \cdots 1}_{n_2} \underbrace{0 \cdots 0}_{n-D} \oplus \\ &\quad \underbrace{0 \cdots 1}_{n_1} \underbrace{1 \cdots 0}_{n_2} \underbrace{0 \cdots 0}_{n-D-1} \oplus \\ &\quad \vdots \\ &\quad \underbrace{0 \cdots 0}_{n_0} \underbrace{1 \cdots 0}_{n_1} \underbrace{0 \cdots 0}_{n_2} \underbrace{1 \cdots 0}_{n-D-n_0} \underbrace{0 \cdots 0}_{n-D-n_0} \\ &= \underbrace{1 \cdots 1}_{D+n_0} \parallel \underbrace{0 \cdots 0}_{n-D-n_0}. \end{aligned}$$

Let

$$\begin{aligned} \mathbf{u}_0 &= \bigoplus_{0 \leq i \leq k-1} \rho^{i(D+n_0)}(\mathbf{u}_2) \\ &= \underbrace{1 \cdots 1}_{D+n_0} \parallel \cdots \parallel \underbrace{1 \cdots 1}_{D+n_0} \parallel \underbrace{0 \cdots 0}_{n-k(D+n_0)} \\ &= \underbrace{1 \cdots 1}_{k(D+n_0)} \parallel \underbrace{0 \cdots 0}_{n-k(D+n_0)}, \end{aligned}$$

where $1 \leq k \leq \lfloor \frac{n-n_1-1}{D+n_0} \rfloor$. It is not difficult to see that $v_2(h_f(\mathbf{u}_0)) = k(n_0 + 1)$.

Let $k = \lfloor \frac{n-n_1-1}{D+n_0} \rfloor = q$. By Theorem 2.4, we have $v_2(h_f(\mathbf{u}_0)) = q(n_0 + 1) > |\mathbf{u}_0| - n/2$, which implies $q(D - n_0 - 1) < r + n_1 + 1$. It follows that f is not bent if $q(D - n_0 - 1) \geq r + n_1 + 1$. ■

Remark 3.3 Note that the above nonexistence results could not be obtained by Theorem 1.2. For example, the nonexistence of homogeneous RotS bent functions with SANF $x_1 \cdots x_d + x_1 \cdots x_{d-1}x_{d+1}$ could not be proven by Theorem 1.2.

Remark 3.4 We remark that the statement “prove the nonexistence of homogeneous RotS bent functions of degree ≥ 3 on a single cycle (i.e. the SANF is $\mathbf{x}^{\mathbf{u}}$ for some \mathbf{u})” in [14] is incorrect. The proof is based on the assumption that all RotS functions of a single cycle are affinely equivalent to RotS functions with SANF $x_1x_2 \cdots x_d$. In fact there are many RotS functions of a single cycle that are not affinely equivalent to $x_1x_2 \cdots x_d$.

In the following we will give a characterization of homogeneous RotS bent function of degree 2. First recall two basic results about bent functions and circulant matrixes. A circulant matrix over \mathbb{F}_2 is of the form

$$\begin{pmatrix} \mathbf{a}_1 \\ \rho(\mathbf{a}_1) \\ \vdots \\ \rho^{n-1}(\mathbf{a}_1) \end{pmatrix},$$

where $\mathbf{a}_1 = (a_{11}, \dots, a_{1n}) \in \mathbb{F}_2^n$. So a circulant matrix can be represented by its first row \mathbf{a}_1 . Further a circulant matrix over \mathbb{F}_2 can be represented by the polynomial $\sum_{1 \leq j \leq n} a_{1j}x^{j-1} \in \mathbb{F}_2[x]$.

Lemma 3.5 Quadratic Boolean function $f(x_1, \dots, x_n) = \sum_{1 \leq i < j \leq n} a_{ij}x_i x_j + \sum_{1 \leq i \leq n} b_i x_i$ is bent if and only if the matrix $(a_{ij})_{n \times n}$ is nonsingular, where $a_{ij} = a_{ji} \in \mathbb{F}_2, a_{ii} = 0, 1 \leq i, j \leq n$.

Lemma 3.6 Circulant matrix $(a_{ij})_{n \times n}$ over \mathbb{F}_2 is nonsingular if and only if the polynomials $\sum_{1 \leq j \leq n} a_{1j}x^{j-1}$ and $x^n + 1$ are relatively prime, i.e. $\text{GCD}(\sum_{1 \leq j \leq n} a_{1j}x^{j-1}, x^n + 1) = 1$.

It can be verified that $\sum_{1 \leq i \leq n} x_i x_{e-1+i}$ with $e > n/2$ is in fact equal to $\sum_{1 \leq i \leq n} x_i x_{n-e+1+i}$ with $n - e + 2 \leq n/2 + 1$. So we can assume a homogeneous RotS function of degree 2 has SANF form $x_1x_{e_1} + \dots + x_1x_{e_m}$, where $2 \leq e_1 < e_2 < \dots < e_m \leq n/2 + 1, m \leq n/2$. Obviously, the associated matrix $(a_{ij})_{n \times n}$ of f is circulant, with the first row (a_{11}, \dots, a_{1n}) such that

$$a_{11} = 0, a_{1e_i} = a_{1(n+2-e_i)} = 1, 1 \leq i \leq m, \text{ and } a_{1j} = 0 \text{ if } j \neq e_i \text{ or } n+2-e_i.$$

Thus the corresponding polynomial is $\sum_{1 \leq i \leq m} (x^{e_i-1} + x^{n+1-e_i})$, where $x^{e_i-1} + x^{n+1-e_i}$ is assumed to be $x^{n/2}$ if $e_i - 1 = n + 1 - e_i = n/2$. By Lemma 3.5 and Lemma 3.6, we have

Theorem 3.7 Homogeneous RotS function f of degree 2 described as above is bent if and only if

$$\text{GCD}(\sum_{1 \leq i \leq m} (x^{e_i-1} + x^{n+1-e_i}), x^n + 1) = 1.$$

Remark 3.8 A necessary condition for $\text{GCD}(\sum_{1 \leq i \leq m} (x^{e_i-1} + x^{n+1-e_i}), x^n + 1) = 1$ is $x^{n/2}$ should be contained in $\sum_{1 \leq i \leq m} (x^{e_i-1} + x^{n+1-e_i})$, i.e. the SANF of f must contain $x_1x_{n/2+1}$. For example, all homogeneous degree 2 RotS bent functions in 8-variables are (expressed in SANF forms, see [7]):

$$\begin{aligned} & x_1x_5; \quad x_1x_2 + x_1x_5; \quad x_1x_3 + x_1x_5; \quad x_1x_4 + x_1x_5; \quad x_1x_2 + x_1x_3 + x_1x_5; \\ & x_1x_2 + x_1x_4 + x_1x_5; \quad x_1x_3 + x_1x_4 + x_1x_5; \quad x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5. \end{aligned}$$

4 Conclusion

In this paper, we presented a different method suitable for the existence problem of homogeneous rotation symmetric bent functions, which led to some new results, and may be used to prove the nonexistence of most homogeneous rotation symmetric bent functions with degree > 2 once their SANFs are given. Since the conjecture is only partially proved, we expect a fully proof with the aid of our proposed method.

References

- [1] O.S.Rothaus, On bent functions, *Journal of Combinatorial Theory Series A*, 20(1976)300-305.
- [2] J.Pieprzyk and C.X.Qu, Fast hashing and rotation symmetric functions, *Journal of Universal Computer Science*, 5(1)(1999)20-31.
- [3] T.W.Cusick and P.Stănică, Fast evaluation, weights and nonlinearity of rotation-symmetric functions, *Discrete Mathematics*, 258(2002) 289-301.
- [4] S.Kavut, S.Maitra and M.D.Yucel, Search for Boolean functions with excellent profiles in the rotation symmetric class, *IEEE Transaction on Information Theory*, 53(5)(2007)1743-1751.
- [5] C.Charnes, Rötteler, and T.Beth, Homogeneous bent functions, invariants, and designs, *Designs, Codes and Cryptography*(special issue dedicated to Ron Mullin), 26(1-3)(2002)139-154.
- [6] P.Stănică and S.Maitra, Rotation symmetric Boolean functions- Count and cryptographic properties, in: R. C. Bose Centenary Symposium on Discrete Mathematics and Applications, December 2002, Electronic Notes in Discrete Mathematics, Elsevier, Volume 15(2002).
- [7] P.Stănică and S.Maitra, Rotation symmetric Boolean functions- Count and cryptographic properties, *Discrete Applied Mathematics*, 156(2008) 1567-1580.
- [8] T.Xia, J.Seberry, J.Pieprzyk, C.Charnes, Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$, *Discrete Applied Mathematics*, 142(2004) 127-132.
- [9] Q.Meng, H.Zhang, M.Yang, J.Cui, On the degree of homogeneous bent functions, *Discrete Applied Mathematics*, 155(2007)665-669.
- [10] D.K.Dalai, S.Maitra and S.Sarkar, Results on rotation symmetric bent functions, *Discrete Mathematics*, 309(8)(2009)2398-2409.
- [11] P.Stănică, On the nonexistence of bent rotation symmetric Boolean functions of degree greater than two, Proceedings of NATO Advanced Studies Institute (Boolean Functions in Cryptology and Information Security - NATO Science for Peace and Security), Ed. O.A. Logachev, (2008)214-218 .
- [12] X.D.Hou, p -Ary and q -ary versions of certain results about bent functions and resilient functions, *Finite Fields and Their Applications*, 10(2004)566-582.
- [13] C.Carlet, P.Guillot, Bent resilient functions and the numerical normal form, in: Codes and Association Schemes, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., American Mathematical Society, Providence. RI, 56(2001)87-96.
- [14] P.Stănică, S.Maitra and J.A.Clark, Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions, in: B. Roy and W. Meier (Eds.), *Fast software Encryption 2004*, Lecture Notes in Computer Science, Volume 3017(2004)161-177.