A new class of semi-bent quadratic Boolean functions

Chunming Tang[a], Yanfeng Qi[b,c]

[a]*School of Mathematics and Information, China West Normal University, Sichuan Nanchong, 637002, China*
[b]*LMAM, School of Mathematical Sciences, Peking University, Beijing, 100871, China*
[c]*Aisino Corporation Inc., Beijing, 100195, China*

Abstract

In this paper, we present a new class of semi-bent quadratic Boolean functions of the form $f(x) = \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} Tr_1^n(c_i x^{1+4^i})$ $(c_i \in \mathbb{F}_4, n = 2m)$. We first characterize the semi-bentness of these quadratic Boolean functions. There exists semi-bent functions only when m is odd. For the case: $m = p^r$, where p is an odd prime with some conditions, we enumerate the semi-bent functions. Further, we give a simple characterization of semi-bentness for these functions with linear properties of c_i. In particular, for a special case of p, any quadratic Boolean function $f(x) = \sum_{i=1}^{\frac{p-1}{2}} Tr_1^{2p}(c_i x^{1+4^i})$ over $\mathbb{F}_{2^{2p}}$ is a semi-bent function.

Keywords: Semi-bent function, Boolean function, m-sequence, cyclotomic polynomial, bent function

1. Introduction

A Boolean function is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Since finite fields have many rich structures and properties, we often study Boolean functions as functions from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$. Boolean functions with with low Walsh transform are of great interest because of their wide applications in cryptography and communications. For application in cryptography, these functions can resist linear cryptanalysis on block ciphers [11] and the fast correlation attack on stream ciphers [14]. As for application in communications, they can be used to design m-sequnces with low cross-correlation [6, 7].

Two classes of Boolean functions with low Walsh transform are bent functions and semi-bent functions. The maximum magnitude of the Walsh tranform of a Boolean function is at least $2^{n/2}$. When n is even, this lower bound can be reached. Such a Boolean function with this property is called a bent function [17], and the value of the Walsh transform belongs to $\{2^{n/2}, -2^{n/2}\}$. As for the odd n, the lower bound for the Walsh transform is still unknown in general [15, 16]. However, for quadratic Boolean functions with odd n, the lower bound is $2^{(n+1)/2}$ [13]. Such a Boolean function with the maximum magnitude $2^{(n+1)/2}$ is called a semi-bent function, and the value of the Walsh transform belongs to $\{0, \pm 2^{(n+1)/2}\}$. When n is even, a Boolean function with the maximum magnitude $2^{(n+2)/2}$ is called a semi-bent function [3], and the value of the Walsh transform belongs to $\{0, \pm 2^{(n+2)/2}\}$.

Gold [4] introduced the first family of m-sequences having low cross correlation from the semi-bent function $Tr_1^n(x^{1+2^i})$, where $2 \nmid n$ and $gcd(n,i) = 1$. Subsequently, Boztas and Kumar [2] proposed another class of semi-bent functions of the form $\sum_{i=1}^{\frac{n-1}{2}} Tr_1^n(x^{1+2^i})$.

Khoo, Gong and Stinson [9, 10] considered the quadratic Boolean function of the form

$$f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr_1^n(x^{1+2^i}),$$

where n is odd, $Tr_1^n(x)$ is the trace function from $GF(2^n)$ to $GF(2)$ and $c_i \in GF(2)$. They proved that $f(x)$ is semi-bent if and only if

$$gcd(c(x), x^n + 1) = x + 1,$$

where $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$.

Charpin, Pasalic and Tavernier [3] generalized Khoo et al.'s results to even n and considered quadratic functions of the form

$$f(x) = \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} c_i Tr_1^n(x^{1+2^i}), c_i \in GF(2).$$

When n is even, they proved that $f(x)$ is semi-bent if and only if

$$gcd(c(x), x^n + 1) = x^2 + 1,$$

where $c(x) = \sum_{i=1}^{\frac{n-2}{2}} c_i(x^i + x^{n-i})$. For odd n, they investigated the conditions for the semi-bent functions of $f(x)$ with three and four trace terms.

For further generalization, Ma, Lee and Zhang [12] applied techniques from [10] and considered the quadratic Boolean functions of the form

$$f(x)=\sum_{i=1}^{\frac{n-2}{2}} c_i Tr_1^n(x^{1+2^i})+Tr_1^{n/2}(x^{1+2^{\frac{n}{2}}}), \tag{1}$$

where $c_i \in GF(2)$ and $Tr_1^{n/2}(x)$ is the trace function from $GF(2^{\frac{n}{2}})$ to $GF(2)$. They proved that $f(x)$ is a bent function if and only if

$$gcd(c(x), x^n+1)=1,$$

where $c(x)=\sum_{i=1}^{\frac{n-2}{2}} c_i(x^i+x^{n-i})+x^{n/2}$. For some special cases of n, Yu and Gong [21] considered the concrete constructions of bent functions of the form (1) and presented some enumeration results.

Hu and Feng [5] generalized results of Ma, Lee and Zhang [12] and studied the quadratic Boolean functions of the form

$$f(x)=\sum_{i=1}^{\frac{m-2}{2}} c_i Tr_1^n(\beta x^{1+2^{ei}})+Tr_1^{n/2}(\beta x^{1+2^{\frac{n}{2}}}), \tag{2}$$

where $c_i \in GF(2)$, $n=em$, m is even and $\beta \in GF(2^e)$. They obtained that $f(x)$ is bent if and only if

$$gcd(c(x), x^m+1)=1,$$

where $c(x)=\sum_{i=1}^{\frac{m-2}{2}} c_i(x^i+x^{m-i})+x^{m/2}$. Further, they presented the enumerations of bent functions for some specified m. Note that $\beta \in GF(2^e)$, then $(\beta^{2^{e-1}})^{1+2^{ei}}=\beta^{2^e}=\beta$. The function $f(x)$ of the form (2) satisfies that

$$f(x)=\sum_{i=1}^{\frac{m-2}{2}} c_i Tr_1^n((\beta^{2^{e-1}}x)^{1+2^{ei}})+Tr_1^{n/2}((\beta^{2^{e-1}}x)^{1+2^{\frac{n}{2}}}),$$

where $c_i \in GF(2)$. From the transformation $x \longmapsto \beta^{2^{e-1}}x$, a bent function of the form (2) is changed into a bent function of the form (1). Actually, (2) does not introduce new bent functions.

In [19], we generalized quadratic Boolean functions in [5, 12] and study Boolean functions of the form

$$f(x) = \sum_{i=1}^{\frac{m}{2}-1} Tr_1^n(c_i x^{1+2^{ei}}) + Tr_1^{n/2}(c_{m/2} x^{1+2^{n/2}}) \qquad (3)$$

where $n = em$, m is even and $c_i \in GF(2^e)$. And we proved that $f(x)$ is bent if and only if $gcd(c_f(x), x^m + 1) = 1$, where $c_f(x) = \sum_{i=1}^{\frac{m}{2}-1} c_i(x + x^{m-i}) + c_{m/2} x^{m/2}$. Then we presented enumerations of bent functions of the form (3) for the case $m = 2^{v_0} p^r$ and $gcd(e, p-1) = 1$, where $v_0 > 0$, $r > 0$, p is an odd prime satisfying $ord_p(2) = p - 1$ or $ord_p(2) = (p-1)/2$ ($(p-1)/2$ is odd).

In this paper, we consider quadratic Boolean functions of the form

$$f(x) = \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} Tr_1^n(c_i x^{1+4^i}),\ c_i \in \mathbb{F}_4 \qquad (4)$$

where $n = 2m$. Then $f(x)$ is semi-bent if and only if $gcd(c_f(x), x^m + 1) = x + 1$, where $c_f(x) = \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} c_i(x^i + x^{m-i})$. Further, for even m, $f(x)$ is not a semi-bent function. We give the enumeration of semi-bent functions for the case $m = 2^v p^r$, where p is not a Wieferich prime, $p \equiv 3 \mod 4$, $ord_p(2) = p - 1$ or $\frac{p-1}{2}$. The semi-bentness of $f(x)$ is characterized by conditions of coefficients c_i. In particular, any nonzero $f(x)$ is a semi-bent function for the case $m = p$, where p is an odd prime, $p \equiv 3 \mod 4$, $ord_p(2) = p - 1$ or $\frac{p-1}{2}$.

This paper is organized as follows. Section 2 introduces some notations and basic knowledge. Section 3 presents the class of semi-bent functions, enumerates the number of semi-bent functions and characterizes the semi-bentness for some cases. Section 4 concludes for this paper.

2. Preliminaries

In this section, some notations are given first. Let $GF(2^n)$ be the finite field with 2^n elements. Let $GF(2^n)^*$ be the multiplicative group of $GF(2^n)$. Let $e|n$, the trace function $Tr_e^n(x)$ from $GF(2^n)$ to $GF(2^e)$ is defined by

$$Tr_e^n(x) = x + x^{2^e} + \cdots + x^{2^{e(n/e-1)}}, \qquad x \in GF(2^n).$$

The trace function satisfies that

(1) $Tr_e^n(x^{2^e}) = Tr_e^n(x)$, where $x \in GF(2^n)$.

(2) $Tr_e^n(ax + by) = aTr_e^n(x) + bTr_e^n(y)$, where $x, y \in GF(2^n)$ and $a, b \in GF(2^e)$.

The Walsh transform of a Boolean function $f(x)$ is defined by

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\lambda x)}, \ \lambda \in \mathbb{F}_{2^n}. \tag{5}$$

The distribution of values of the Walsh transform can define bent functions and semi-bent functions.

Definition 2.1. A Boolean function $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$ is called a bent function if $\widehat{f}(\lambda) = \pm 2^{\frac{n}{2}}$ for all $\lambda \in \mathbb{F}_{2^n}$.

Obviously, bent functions do not exist for odd n.

Semi-bent functions are defined below for even n and odd n.

Definition 2.2. Let n be even. A Boolean function $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$ is called a semi-bent function if $\widehat{f}(\lambda) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ for all $\lambda \in \mathbb{F}_{2^n}$.

Definition 2.3. Let n be odd. A Boolean function $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$ is called a semi-bent function if $\widehat{f}(\lambda) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ for all $\lambda \in \mathbb{F}_{2^n}$.

A quadratic Boolean function can be represented by trace functions. When n is even, a quadratic Boolean function from $GF(2^n)$ to $GF(2)$ can be represented by

$$f(x) = \sum_{i=0}^{\frac{n}{2}-1} Tr_1^n(c_i x^{1+2^i}) + Tr_1^{n/2}(c_{n/2} x^{1+2^{n/2}}), \tag{6}$$

where $c_i \in GF(2^n)$ for $0 \leq i \leq \frac{n}{2}$ and $c_{n/2} \in GF(2^{\frac{n}{2}})$.

When n is odd, $f(x)$ can be represented by

$$f(x) = \sum_{i=0}^{\frac{n-1}{2}} Tr_1^n(c_i x^{1+2^i}), \tag{7}$$

where $c_i \in GF(2^n)$.

For a quadratic Boolean function $f(x)$ of the form (6) or (7), the distribution of the Walsh transform can be described by the bilinear form

$$Q_f(x, y) = f(x + y) + f(x) + f(y). \tag{8}$$

For the quadratic form Q_f, define

$$K_f = \{x \in GF(2^n) : Q_f(x, y) = 0, \forall y \in GF(2^n)\} \tag{9}$$

and $k_f = dim_{GF(2)}(K_f)$. Then $2|(n - k_f)$. The distribution of the Walsh transform values of $\hat{f}(\lambda)$ is given in the following theorem [7].

Theorem 2.4. *Let $f(x)$ be a quadratic Boolean function of the form (6) or (7) and $k_f = dim_{GF(2)}(K_f)$, where K_f is defined in (11). The distribution of the Walsh transform values of $f(x)$ is given by*

$$\hat{f}(\lambda) = \begin{cases} 0, & 2^n - 2^{n-k_f} \ times \\ 2^{\frac{n+k_f}{2}}, & 2^{n-k_f-1} + 2^{\frac{n-k_f}{2}-1} \ times \\ -2^{\frac{n+k_f}{2}}, & 2^{n-k_f-1} - 2^{\frac{n-k_f}{2}-1} \ times. \end{cases}$$

Corollary 2.5. *When n is even, a quadratic function $f(x)$ is a bent function if and only if $k_f = 0$, and $f(x)$ is a semi-bent function if and only if $k_f = 2$; When n is odd, $f(x)$ is a semi-bent function if and only if $k_f = 1$.*

The set $\mathcal{K}_f$ can also be described by the derivatives of f.

Definition 2.6. Let $f(x)$ be a Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Let $z \in \mathbb{F}_{2^n}$. The derivative of $f(x)$ with respect to z is the function $D_z f(x)$ defined by $D_z f(x) = f(x + z) + f(x)$.

z is called a linear structure of $f(x)$ if $D_z f(x)$ is constant. The set of all the linear structures is called the linear space of f. Precisely, $\mathcal{K}_f$ is exact the linear space of $f(x)$.

3. A new class of semi-bent quadratic Boolean functions

Let $n = 2m$. We consider quadratic Boolean functions of the form

$$f(x) = \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} Tr_1^n(c_i x^{4^i+1}), \quad c_i \in \mathbb{F}_4, (c_1, \cdots, c_{\frac{m-1}{2}}) \neq (0, \cdots, 0). \tag{10}$$

Let $\mathcal{Q}_m$ be the set of all the functions of the form (10). Let $\mathcal{SB}_m$ be the set of all the semi-bent functions in $\mathcal{Q}_m$.

3.1. Semi-bent quadratic Boolean functions

For a quadratic Boolean function defined by (10), the derivative with respect to $z \in \mathbb{F}_{2^n}$ is

$$\begin{aligned} D_z f(x) &= \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} Tr_1^n(c_i((x+z)^{4^i+1} + x^{4^i+1})) \\ &= \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} Tr_1^n(c_i(z^{4^i} + z^{4^{m-i}})x) + \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} Tr_1^n(c_i z^{4^i+1}). \end{aligned}$$

Then z is a linear structure of $f(x)$ if and only if $\sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} c_i(z^{4^i} + z^{4^{m-i}}) = 0$. We call $\sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} c_i(x^{4^i} + x^{4^{m-i}})$ the adjoint linear transformation of $f(x)$, which is denoted by $L_f(x)$. Then

$$\mathcal{K}_f = \{x \in \mathcal{K}_f : L_f(x) = 0\} = Ker(L_f(x)). \tag{11}$$

The following theorem presents the characterization of the semi-bentness of quadratic Boolean functions defined by (10).

Theorem 3.1. *Let $n = 2m$. A Boolean function defined by* (10) *is a semi-bent function if and only if $gcd(c_f(x), x^m + 1) = x + 1$, where*

$$c_f(x) = \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} c_i(x^i + x^{m-i}). \tag{12}$$

In particular, for even m, there is no semi-bent function of the form (10)*, that is, $\mathcal{SB}_m = \emptyset$.*

Proof. The adjoint linear transformation of $f(x)$ defined by (10) is

$$L_f(x) = \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} c_i(x^{4^i} + x^{4^{m-i}}).$$

Then $L_f(x)$ can be seen as a linear transformation from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ over $\mathbb{F}_4$. Take a regular element α of $\mathbb{F}_{2^n}$ over $\mathbb{F}_4$, that is, $\alpha, \alpha^4, \cdots, \alpha^{4^{m-1}}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_4$. The corresponding matrix of the linear transformation $L_f(x)$ under this basis is

$$M_f = \begin{bmatrix} 0 & c_1 & c_2 & \cdots & c_{m-1} \\ c_{m-1} & 0 & c_1 & \cdots & c_{m-2} \\ c_{m-2} & c_{m-1} & 0 & \cdots & c_{m-3} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ c_1 & c_2 & c_3 & \cdots & 0 \end{bmatrix}$$

where $c_{m-i} = c_i$ for $(1 \leq i \leq \lfloor \frac{m-1}{2} \rfloor)$ and $c_{m/2} = 0$ for even m. From Corollary 2.5 and $\mathcal{K}_f$ in (11), $f(x)$ is semi-bent if and only if the dimension of the kernel $Ker(L_f(x))$ over $\mathbb{F}_2$ is $dim_{\mathbb{F}_2}(Ker(L_f(x))) = 2$. Since $L_f(x)$ is also a linear transformation over $\mathbb{F}_4$, $dim_{\mathbb{F}_2}(Ker(L_f(x))) = 2$ if and only if $dim_{\mathbb{F}_4}(Ker(L_f(x))) = 1$ or the rank of M_f is $Rank(M_f) = m - 1$. Note that M_f is the generator matrix of a cyclic code over $\mathbb{F}_4$ with length m and generator polynomial $c_f(x)$. From theories of cyclic codes, $Rank(M_f) = m - deg(gcd(c_f(x), x^m + 1))$. Hence $f(x)$ is semi-bent if and only if $deg(gcd(c_f(x), x^m + 1)) = 1$. Obviously $deg(gcd(c_f(x), x^m + 1)) = 1$ if and only if $gcd(c_f(x), x^m + 1) = x + 1$.

When m is even,

$$\begin{aligned} c_f(x) = &\sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} c_i(x^i + x^{m-i}) = \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} c_i x^i (1 + x^{\frac{m}{2}-i})^2, \\ x^m + 1 = &(x^{\frac{m}{2}} + 1)^2, \end{aligned}$$

We obtain that $(x+1)^2 | gcd(c_f(x), x^m + 1)$ and $f(x)$ is not semi-bent.

Hence, this theorem follows. □

From Theorem 3.1, we just consider quadratic Boolean functions for odd m.

Corollary 3.2. *Let $n = 2m$, where m is odd. The quadratic Boolean function*

$$f(x) = Tr_1^n(cx^{4^i+1}), \quad c \in \mathbb{F}_4^*$$

is semi-bent if and only if $gcd(i, m) = 1$.

Proof. Note that $c_f(x) = c(x^i + c^{m-i})$. Then

$$gcd(c(x^i + x^{m-i}), x^m + 1) = gcd(x^{2i} + 1, x^m + 1) = x^{gcd(2i,m)} + 1.$$

Since m is odd, then $gcd(2i, m) = gcd(i, m)$. From Theorem 3.1, $f(x)$ is semi-bent if and only if $gcd(i, m) = 1$. □

3.2. The enumeration for semi-bent functions

For the enumeration of semi-bent functions, some notations are given first.

Definition 3.3. Let N be a positive integer and a be a positive integer coprime to N. The positive integer k is called the order of a module N if k is the least positive integer such that $N|(a^k-1)$. And k is denoted by $ord_N(a)$.

Lemma 3.4. *Let p be an odd prime. Then*

(1) *Let $ord_p(4)=s$ and $p\nmid \frac{4^s-1}{p}$, then $ord_{p^k}(4)=s_k=p^{k-1}s$.*

(2) *$ord_p(4)\neq p-1$. Further, $ord_p(4)=\frac{p-1}{2}$ if and only if $ord_p(2)=p-1$ or $ord_p(2)=\frac{p-1}{2}$ ($\frac{p-1}{2}$ is odd).*

Proof. (1) This can be obtained in [8].

(2) If $ord_p(4)=p-1$, then $ord_p(2)=p-1$ and $ord_p(4)=\frac{ord_p(2)}{gcd(2,ord_p(2))}=\frac{p-1}{2}$, which gives a contradiction. Hence $ord_p(4)\neq p-1$.

If $ord_p(2)=p-1$ or $ord_p(2)=\frac{p-1}{2}$ ($\frac{p-1}{2}$ is odd), then $ord_p(4)=\frac{ord_p(2)}{gcd(2,ord_p(2))}$ and $ord_p(4)=\frac{p-1}{2}$. If $ord_p(4)=\frac{p-1}{2}$, then $ord_p(2)=p-1$ or $\frac{p-1}{2}$. When $ord_p(2)=\frac{p-1}{2}$, $gcd(2,ord_p(2))=1$, that is, $\frac{p-1}{2}$ is odd. □

If p is not a Wieferich prime, then p satisfies $p\nmid\frac{4^s-1}{p}$. The definition of a Wieferich prime is given below.

Definition 3.5. Let p be a prime. Then p is called a Wieferich prime if $p|\frac{2^{p-1}-1}{p}$ [20].

Wieferich primes are rare. Between 1 and 17×10^{15}, there are only two Wieferich primes 1093 and 3511. Silverman [18] proved that there are infinite Wieferich primes if the abc conjecture holds.

The polynomial $c_f(x)$ for determining semi-bent functions has a close relation with self-reciprocal polynomials.

Definition 3.6. The reciprocal polynomial of a polynomial $h(x)$ of degree d is $x^dh(\frac{1}{x})$, denoted by $h^*(x)$. The polynomial $h(x)$ is called a self-reciprocal polynomial if $h^*(x)=h(x)$, that is, $h(x)=\sum_{i=0}^d a_ix^i$ with $a_i=a_{d-i}$.

Some results on self-reciprocal polynomials are given below.

Lemma 3.7. (1) *Let $A(x) = \sum_{i=0}^{n_1} a_i x^i$ be a self-reciprocal polynomial of degree n_1. Let $B(x) = \sum_{i=0}^{n_2} b_i x^i$ be a polynomial of degree n_2. Then $A(x)B(x)$ is a self-reciprocal polynomial of degree $n_1 + n_2$ if and only if $B(x)$ is a self-reciprocal polynomial.*

(2) *Let $A(x), g(x) \in \mathbb{F}_4[x]$. Let $A(x)$ be self-reciprocal and $g(x)$ be irreducible. Let $g(x)|A(x)$. Then $g^*(x)|A(x)$, where $g^*(x)$ is the reciprocal polynomial of $g(x)$. Further, if $g(x)$ is not self-reciprocal, then $\widetilde{g}(x)|A(x)$, where $\widetilde{g}(x) = g(x)g^*(x)$.*

Proof. (1) The reciprocal polynomial of $A(x)B(x)$ is $(A(x)B(x))^* = A^*(x)B^*(x)$. Since $A(x)$ is self-reciprocal, then $A(x) = A^*(X)$. Hence $A^*(x)B^*(x) = A(x)B(x)$ if and only if $B^*(x) = B(x)$.

(2) Since $g(x)|A(x)$, then $g^*(x)|A^*(x)$. Since $A(x)$ is self-reciprocal, then $g^*(x)|A(x)$.

Suppose $g(x)$ is not self-reciprocal. Since $g(x)$ is irreducible, $g^*(x)$ is also irreducible and $gcd(g(x), g^*(x)) = 1$. Then $g(x)g^*(x)|A(x)$. □

Two important classes of self-reciprocal polynomials are $x^N + 1$ and d-th cyclotomic polynomials $Q_d(x)$ [1, 8]. The d-th cyclotomic polynomial $Q_d(x)$, whose roots are primitive d-th roots of unity, is a monic polynomial of degree $\phi(d)$, where $\phi(\cdot)$ is Euler-totient function. The following lemma gives the factorization of cyclotomic polynomials.

Lemma 3.8. *Let p be an odd prime. Then*

(1) *Let $ord_{p^k}(4) = s_k$ and $t_k = \frac{p^k - p^{k-1}}{s_k}$, The p^k-th cyclotomic polynomial $Q_{p^k}(x)$ over $\mathbb{F}_4$ has the following monic irreducible factorization.*

$$Q_{p^k}(x) = h_1(x) \cdots h_{t_k}(x),$$

where $deg(h_i(x)) = s_k$ for $1 \leq i \leq t_k$. Further, if there exists l such that $p^k|(4^l + 1)$, then $h_i(x) = x^{s_k} h_i(\frac{1}{x})$, that is, $h_i(x)$ is self-reciprocal for any i. Otherwise, the factorization of $Q_{p^k}(x)$ is of the form

$$Q_{p^k}(x) = C h_1(x) h_1^*(x) \cdots h_{\frac{t_k}{2}}(x) h_{\frac{t_k}{2}}^*(x),$$

where $h_i^*(x) = x^{s_k} h_i(\frac{1}{x})$ for $1 \leq i \leq \frac{t_k}{2}$ and $C \in \mathbb{F}_4^*$.

(2) *Let $ord_p(4) = s$, $p \nmid \frac{4^s - 1}{p}$ and $t = \frac{p-1}{s}$. Then $Q_p(x)$ over $\mathbb{F}_4$ has the following monic irreducible factorization:*

$$Q_p(x) = h_1(x) \cdots h_t(x),$$

For any $k \geq 2$, $Q_{p^k}(x)$ over $\mathbb{F}_4$ has the irreducible factorization:

$$Q_{p^k}(x) = h_1(x^{p^{k-1}}) \cdots h_t(x^{p^{k-1}}).$$

(3) *Let p be a prime such that $p \equiv 3 \mod 4$, $ord_p(2) = p-1$ or $\frac{p-1}{2}$ ($\frac{p-1}{2}$ is odd). Then $Q_p(x)$ over $\mathbb{F}_4$ has the following monic irreducible factorization:*

$$Q_p(x) = Ch(x)h^*(x)$$

Suppose that $k \geq 2$. If p is not a Wieferich prime, $Q_{p^k}(x)$ over $\mathbb{F}_4$ has the irreducible factorization

$$Q_{p^k}(x) = Ch(x^{p^{k-1}})h^*(x^{p^{k-1}})$$

where $h^*(x)$ is the self-polynomial of $h(x)$ and $C \in \mathbb{F}_4^*$.

(4) $x^{p^k} + 1 = (x+1)Q_p(x) \cdots Q_{p^k}(x)$.

Proof. (1) From [8], $Q_{p^k}(x)$ over $\mathbb{F}_4$ has the following irreducible factorization

$$Q_{p^k}(x) = h_1(x) \cdots h_{t_k}(x).$$

From Lemma 3.7 $h_i^*(x)|Q_{p^k}(x)$. We just prove that if there exists l satisfying that $p^k|(4^l+1)$, then $h_i^*(x) = h_i(x)$; otherwise, $h_i^*(x) \neq h_i(x)$. Consider any $h_i(x)$. Let α be a root of $h_i(x)$. The reminding roots are $\{\alpha^{4^0}, \alpha^{4^1}, \cdots, \alpha^{4^{s_k-1}}\}$. Obviously, $h_i^*(x) = h_i(x)$ if and only if $h_i(\alpha^{-1}) = 0$, that is, there exists l such that $p^k|(4^l - (-1)) = 4^l + 1$. This results follows.

(2) From Lemma 3.4 and Result (1), this result follows.

(3) Note that p satisfies that $ord_p(4) = \frac{p-1}{2}$ and $p \nmid \frac{4^s-1}{p}$. From Result (1) and Result (2), we just prove that $p \nmid (4^l+1)$ for any l. Otherwise, there exists l such that $p|(4^{2l}-1)$ and $\frac{p-1}{2}|2l$. Since $\frac{p-1}{2}$ is odd, $\frac{p-1}{2}|l$ and $p|(4^l-1)$. From $p|(4^l+1)$, $p|2$, that is, $p=2$, which contradicts that p is an odd prime. Hence, this result follows.

(4) This result can be obtained in [8]. □

Let m be an odd positive integer and $A(x)$ be a nonzero self-reciprocal polynomial. Let $\mathcal{SM}_m(A(x))$ be the set of polynomials $g(x) \in \mathbb{F}_4[x]$ such that

(i) $A(x)|g(x)$;

(ii) $deg(g(x)) = m - 1 - 2t(1 \leq t \leq \frac{m-1}{2})$;

(iii) $g^*(x) = g(x)$.

For convenience, we suppose that $0 \in \mathcal{SM}_m(A(x))$.

Let m be odd and $B(x)$ is a nonzero self-reciprocal polynoial. Let $\mathcal{SR}_m(B(x))$ be the set of polynomials $g(x) \in \mathbb{F}_4[x]$ such that

(i) $gcd(g(x), B(x)) = 1$;

(ii) $deg(g(x)) = m - 1 - 2t(1 \leq t \leq \frac{m-1}{2})$;

(iii) $g^*(x) = g(x)$.

Let $\mathcal{C}_m$ be the set of $c_f(x)$ satisfying that $gcd(c_f(x), x^m + 1) = x + 1$, where $f(x)$ is defined by (10).

Lemma 3.9. *Let notations be defined above. Then* $\#(\mathcal{C}_m) = \#(\mathcal{SR}_m(\frac{x^m+1}{x+1}))$.

Proof. To complete the proof, we just consider the bijection between $\mathcal{C}_m$ and $\mathcal{SR}_m(\frac{x^m+1}{x+1})$. Define a map

$$\begin{aligned} F : \mathcal{C}_m &\longrightarrow \mathcal{SR}_m(\frac{x^m+1}{x+1}) \\ c_f(x) &\longmapsto \frac{x^{-t}c_f(x)}{x+1} = \widetilde{c}_f(x). \end{aligned}$$

where t is the least positive integer such that $c_t \neq 0$ for $1 \leq t \leq \frac{m-1}{2}$.

We then verify the definition first. From the definition of $c_f(x)$, the integer t naturally exists. Let $c_i = c_{m-i}$ for $\frac{m+1}{2} \leq i \leq m-1$. Then

$$\widetilde{c}_f(x) = \frac{x^{-t}c_f(x)}{x+1} = \frac{1}{x+1}(c_{m-t}x^{m-2t} + c_{m-t-1}x^{m-2t-1} + \cdots + c_{t+1}x + c_t).$$

From Lemma 3.7, the polynomial $\widetilde{c}_f(x)$ is self-reciprocal of degree $deg(\widetilde{c}_f(x)) = m - 1 - 2t$. Hence, $\widetilde{c}_f(x)$ satisfies (ii) and (iii) in the definition of $\mathcal{SR}_m(\cdot)$. Finally, we just verify that $\widetilde{c}_f(x)$ satisfies (i).

$$\begin{aligned} gcd(\widetilde{c}_f(x), \frac{x^m+1}{x+1}) =& gcd((x+1)\widetilde{c}_f(x), x^m+1)/(x+1) \\ =& gcd(x^t(x+1)\widetilde{c}_f(x), x^m+1)/(x+1) \\ =& gcd(c_f(x), x^m+1)/(x+1) \\ =& 1. \end{aligned}$$

Hence, the map F is well defined.

Define another map

$$\begin{aligned} G : &\mathcal{SR}_m(\frac{x^m+1}{x+1}) \longrightarrow \mathcal{C}_m \\ &\widetilde{c}(x) \longrightarrow (x+1)x^t\widetilde{c}(x) = c(x), \end{aligned}$$

where $deg(\widetilde{c}(x)) = m-1-2t$. The map G is also well defined. Then we have

$$\begin{aligned} F(G(\widetilde{c}(x))) =&\widetilde{c}(x),\ \widetilde{c}(x) \in \mathcal{SR}_m(\frac{x^m+1}{x+1}), \\ G(F(c_f(x))) =&c_f(x),\ c_f(x) \in \mathcal{C}_m. \end{aligned}$$

Hence, this lemma follows. □

Lemma 3.10. (1) *Let $A(x)$ be a monic self-reciprocal polynomial of even degree d, where $0 \leq d \leq p^r - 3$. Then*

$$\#(\mathcal{SM}_{p^r}(A(x))) = 2^{p^r-1-d}.$$

If $d > p^r - 3$, then $\#(\mathcal{SM}_{p^r}(A(x))) = 1$.

(2) *Let p be not a Wieferich prime such that $p \equiv 3 \mod 4$, $ord_p(2) = p-1$ or $\frac{p-1}{2}$. Then*

$$\#(\mathcal{SR}_{p^r}(\frac{x^{p^r}+1}{x+1})) = 2^{p^r-1}\prod_{k=1}^{r}(1-(\frac{1}{2})^{p^k-p^{k-1}}).$$

Proof. (1) Let $g(x)$ be a nonzero polynomial. From Lemma 3.7, $g(x) \in \mathcal{SM}_{p^r}(A(x))$ if and only if $h(x) = \frac{g(x)}{A(x)}$ is a self-reciprocal polynomial of degree $deg(h(x)) \in \{0, 2, \cdots, p^r - 5 - d, p^r - 3 - d\}$. The number of self-reciprocal polynomials of $deg(h(x)) \in \{0, 2, \cdots, p^r - 5 - d, p^r - 3 - d\}$ is

$$3 + 3 \cdot 4^{\frac{2}{2}} + \cdots 3 \cdot 4^{\frac{p^r-5-d}{2}} + 3 \cdot 4^{\frac{p^r-3-d}{2}} = 2^{p^r-1-d} - 1.$$

Note that $0 \in \mathcal{SM}_{p^r}(A(x))$, then

$$\#(\mathcal{SM}_{p^r}(A(x))) = 2^{p^r-1-d}.$$

(2) From (3) in Lemma 3.8 and (2) in Lemma 3.7, $g(x) \in \mathcal{SR}_{p^r}(\frac{x^{p^r}+1}{x+1})$ if and only if $g(x) \in \mathcal{SM}_{p^r}(1)$ and $g(x) \notin \mathcal{SM}_{p^r}(Q_{p^k}(x))$ for $1 \leq k \leq r$. Note that if $1 \leq k_1 < \cdots < k_i \leq r$, then

$$\bigcap_{1\leq j\leq i} \mathcal{SM}_{p^r}(Q_{p^{k_j}}(x)) = \mathcal{SM}_{p^r}(\prod_{j=1}^{r} Q_{p^{k_j}}(x))$$

For convenience, let $d_k = deg(Q_{p^k}(x)) = p^k - p^{k-1}$. Then $deg(\prod_{j=1}^{r} Q_{p^{k_j}}(x)) = \sum_{j=1}^{r} d_{k_j}$. From Result (1) and the inclusion-exclusion principle,

$$\begin{aligned}
\#(\mathcal{SR}_{p^r}(\frac{x^{p^r}+1}{x+1})) =& 2^{p^r-1-0} + (-1)^1 \sum_{1\leq k_1 \leq r} 2^{p^r-1-d_{k_1}} \\
& + (-1)^2 \sum_{1\leq k_1<k_2\leq r} 2^{p^r-1-d_{k_1}-d_{k_2}} + \cdots \\
& + (-1)^i \sum_{1\leq k_1<\cdots<k_i\leq r} 2^{p^r-1-d_{k_1}-\cdots-d_{k_i}} + \cdots \\
& + (-1)^r 2^{p^r-1-d_1-\cdots-d_r} \\
=& 2^{p^r-1} \prod_{k=1}^{r} (1-(\frac{1}{2})^{d_k}) \\
=& 2^{p^r-1} \prod_{k=1}^{r} (1-(\frac{1}{2})^{p^k-p^{k-1}}).
\end{aligned}$$

Hence, this lemma follows. □

Theorem 3.11. *Let $n = 2m = 2p^r$, where $r \geq 1$, p is not a Wieferich prime, $p \equiv 3 \mod 4$, $ord_p(2) = p-1$ or $\frac{p-1}{2}$. Define the quadratic Boolean function*

$$f(x) = \sum_{i=1}^{\frac{p^r-1}{2}} Tr_1^n(c_i x^{4^i+1}), \quad c_i \in \mathbb{F}_4.$$

The number of semi-bent functions of the form $f(x)$ is

$$\#(\mathcal{SB}_{p^r}) = 2^{p^r-1} \prod_{k=1}^{r} (1-(\frac{1}{2})^{p^k-p^{k-1}}).$$

Proof. From Theorem 3.1,

$$\#(\mathcal{SB}_{p^r}) = \#(\mathcal{C}_{p^r}).$$

From Lemma 3.9,

$$\#(\mathcal{C}_{p^r}) = \#(\mathcal{SR}_{p^r}).$$

From Lemma 3.10,

$$\#(\mathcal{SB}_{p^r}) = 2^{p^r-1} \prod_{k=1}^{r} (1-(\frac{1}{2})^{p^k-p^{k-1}}).$$

□

Remark 3.12. If $r = 1$, it is not necessary that p is not a Wieferich prime in Theorem 3.11.

Corollary 3.13. *Let $n = 2m = 2p$, where $p \equiv 3 \mod 4$, $ord_p(2) = p - 1$ or $\frac{p-1}{2}$. The quadratic Boolean function defined by* (10) *is semi-bent, that is, $\mathcal{SB}_m = \mathcal{Q}_m$.*

Proof. Obviously, $\mathcal{SB}_m \subseteqq \mathcal{Q}_m$. From the definition of $\mathcal{Q}_m$,

$$\#(\mathcal{Q}_m) = 2^{p-1} - 1.$$

From Theorem 3.11,

$$\#(\mathcal{SB}_m) = 2^{p-1} - 1.$$

Hence,

$$\#(\mathcal{SB}_m) = \#(\mathcal{Q}_m),$$

that is,

$$\mathcal{SB}_m = \mathcal{Q}_m.$$

□

The reverse of Corollary 3.13 also holds.

Theorem 3.14. *Let $\mathcal{SB}_m = \mathcal{Q}_m$ for a positive integer m. Then m is an odd prime p such that $p \equiv 3 \mod 4$, $ord_p(2) = p - 1$ or $\frac{p-1}{2}$.*

Proof. From Theorem 3.1 and Corollary 3.2, m is an odd prime p.

We first prove that $ord_p(4) = \frac{p-1}{2}$. Suppose that $ord_p(4) = s < \frac{p-1}{2}$. Then $t = \frac{p-1}{s} > 2$.

(1) When s is even, then $p|(4^{\frac{s}{2}} + 1)$. From (1) in Lemma 3.8, we have the factorization

$$Q_p(x) = h_1(x) \cdots h_t(x),$$

where $h_i^*(x) = h_i(x)$ and $t = \frac{p-1}{s}$. We take

$$c(x) = (x + 1)x^{\frac{p-1-s}{2}} h_1(x).$$

(2) When s is odd, there does not exist l such that $p|(4^l + 1)$. From (1) in Lemma 3.8, we have the factorization

$$Q_p(x) = h_1(x)h_1^*(x) \cdots h_{\frac{t}{2}}(x)h_{\frac{t}{2}}^*(x),$$

where $deg(h_1(x)h_1(x)^*) = p-1-2\cdot\frac{p-1-2s}{2}$. We take

$$c(x) = (x+1)x^{\frac{p-1-2s}{2}}h_1(x)h_1(x)^*.$$

It can be verified that $c(x)$ has the form

$$c(x) = \sum_{i=1}^{\frac{p-1}{2}} c_i(x^i + x^{m-i}).$$

The quadratic Boolean function with respect to c_i is

$$f(x) = \sum_{i=1}^{\frac{p-1}{2}} Tr_1^{2p}(c_i x^{4^i+1}).$$

Hence, we have

$$\begin{aligned} gcd(c_f(x), x^p+1) =& gcd(c(x), x^p+1) \\ =&(x+1)gcd(\frac{c(x)}{x+1}, Q_p(x)) \\ =&\begin{cases} (x+1)h_1(x), & s \equiv 0 \mod 2 \\ (x+1)h_1(x)h_1^*(x), & s \equiv 1 \mod 2 \end{cases} \end{aligned}$$

From Theorem 3.1, $f(x) \notin \mathcal{SB}_m$, which contradicts that $\mathcal{SB}_m = \mathcal{Q}_m$.

Hence, $ord_p(4) = \frac{p-1}{2}$. Suppose that $p \not\equiv 3 \mod 4$, then $\frac{p-1}{2}$ is even. With the similar discussion, $p \not\equiv 3 \mod 4$ contradicts that $\mathcal{SB}_m = \mathcal{Q}_m$.

Hence, this theorem follows. □

3.3. The simpler characterization of semi-bentness

In this subsection, let p be not a Wieferich prime, $p \equiv 3 \mod 4$, $ord_p(2) = p-1$ or $\frac{p-1}{2}$. The following theorem presents a simpler characterization of semi-bent quadratic Boolean functions defined by (10).

Theorem 3.15. *Let $n = 2m$ and $m = p^r$, where $r \geq 2$, p is not a Wieferich prime, $p \equiv 3 \mod 4$, $ord_p(2) = p-1$ or $\frac{p-1}{2}$. The quadratic Boolean function $f(x)$ defined by* (10) *is semi-bent if and only if $(x^{p^{k-1}}+1)c_f(x) \not\equiv 0 \mod x^{p^k}+1$ for any $1 \leq k \leq r$.*

Proof. From (4) in Lemma 3.8,

$$gcd(c_f(x), x^{p^r}+1) = (x+1)gcd(c_f(x)/(x+1), \prod_{k=1}^{r} Q_{p^k}(x)).$$

From Lemma 3.1, $f(x)$ is semi-bent if and only if

$$gcd(c_f(x)/(x+1), \prod_{k=1}^{r} Q_{p^k}(x)) = 1.$$

Note that

$$(x+1) \nmid \prod_{k=1}^{r} Q_{p^k}(x),$$

Then

$$gcd(c_f(x)/(x+1), \prod_{k=1}^{r} Q_{p^k}(x)) = 1,$$

that is,

$$gcd(c_f(x), \prod_{k=1}^{r} Q_{p^k}(x)) = 1.$$

Equivalently, for any $1 \leq k \leq r$,

$$gcd(c_f(x), Q_{p^k}(x)) = 1.$$

From (3) in Lemma 3.8 and (2) in Lemma 3.7, $gcd(c_f(x), Q_{p^k}(x)) = 1$ if and only if

$$Q_{p^k}(x) \nmid c_f(x).$$

Since

$$gcd(x^{p^{k-1}}+1, Q_{p^{k}(x)}) = 1$$

and

$$(x^{p^{k-1}}+1) \cdot Q_{p^{k}(x)} = x^{p^k}+1,$$

$c_f(x) \not\equiv 0 \mod Q_{p^k}(x)$ is equivalent to

$$(x^{p^{k-1}}+1)c_f(x) \not\equiv 0 \mod x^{p^k}+1.$$

Hence, this theorem follows. □

Lemma 3.16. *Let $m = p^r$, where p is an odd prime. Let $c_f(x)$ be defined by* (12). Then

(1) For any $1 \leq k \leq r$, define

$$\begin{aligned} c_i =& c_{p^r-i}, \ (\frac{p^r+1}{2} \leq i \leq p^r - 1) \\ w_{i,k} =& \sum_{j=0}^{p^{r-k}-1} c_{i+jp^k}, \ (1 \leq i \leq p^k - 1). \end{aligned}$$

Then $w_{i,k} = w_{p^k-i,k}$ for any $1 \leq i \leq p^k - 1$. Further,

$$\begin{aligned} c_{f,k}(x) \equiv& c_f(x) \mod x^{p^k} + 1 \\ \equiv& \sum_{i=1}^{p^k-1} w_{i,k} x^i \equiv \sum_{i=1}^{(p^k-1)/2} w_{i,k}(x^i + x^{p^k-i}). \end{aligned}$$

(2) For $i = i_0 + jp^k$ and $0 \leq i_0 \leq p^k - 1$, define

$$\begin{aligned} w_{0,k} =& 0, \\ w_{i,k} =& w_{i_0,k}. \end{aligned} \tag{13}$$

Then

$$\begin{aligned} (x^{p^{k-1}} + 1)c_f(x) \equiv& (x^{p^{k-1}} + 1)c_{f,k}(x) \mod x^{p^k} + 1 \\ \equiv& \sum_{i=0}^{p^k-1} (w_{i,k} + w_{i-p^{k-1},k})x^i. \end{aligned}$$

(3) Let $w_{i,k}$ be defined above. Let

$$W_k = \begin{bmatrix} w_{0,k} & w_{1,k} & \cdots & w_{\frac{p^{k-1}-1}{2},k} & \cdots & w_{p^{k-1}-1,k} \\ w_{p^{k-1},k} & w_{p^{k-1}+1,k} & \cdots & w_{p^{k-1}+\frac{p^{k-1}-1}{2},k} & \cdots & w_{2p^{k-1}-1,k} \\ w_{2p^{k-1},k} & w_{2p^{k-1}+1,k} & \cdots & w_{2p^{k-1}+\frac{p^{k-1}-1}{2},k} & \cdots & w_{3p^{k-1}-1,k} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ w_{(\frac{p-1}{2})p^{k-1},k} & w_{(\frac{p-1}{2})p^{k-1}+1,k} & \cdots & w_{\frac{p^k-1}{2},k} & \cdots & w_{\frac{p^k-1}{2}+\frac{p^{k-1}-1}{2},k} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ w_{(p-1)p^{k-1},k} & w_{(p-1)p^{k-1}+1,k} & \cdots & w_{(p-1)p^{k-1}+\frac{p^{k-1}-1}{2},k} & \cdots & w_{p^k-1,k} \end{bmatrix}$$

Let $A_{i,k} = [A_{i,k}(0), A_{i,k}(1), \cdots, A_{i,k}(p-1)]'$ be the i-th column of W_k, that is,

$$W_k = \left[A_{0,k}, A_{1,k}, \cdots, A_{p^{k-1}-1,k}\right]. \tag{14}$$

Then

(i) For any $1 \leq i \leq p^{k-1}-1$ and $0 \leq j \leq p-1$, $A_{i,k}(j) = A_{p^{k-1}-i,k}(p-1-j)$;

(ii) For any $1 \leq i \leq p^{k-1}-1$, $A_{i,k}$ is constant if and only if $A_{p^{k-1}-i,k}$ is constant.

Proof. (1) From $c_f(1) = 0$,

$$\begin{aligned} c_{f,k}(x) \equiv& c_f(x) \mod x^{p^k}+1 \\ \equiv& c_1 x + c_2 x^2 + \cdots + c_{p^k-1}x^{p^k-1} + \\ & c_{1+p^k}x + c_{2+p^k}x^2 + \cdots + c_{p^k-1+p^k}x^{p^k-1} + \cdots + \\ & c_{1+(p^{r-k}-1)p^k}x + c_{2+(p^{r-k}-1)p^k}x^2 + \cdots + c_{p^k-1+(p^{r-k}-1)p^k}x^{p^k-1} \\ \equiv& (\sum_{j=0}^{p^{r-k}-1} c_{1+jp^k})x + (\sum_{j=0}^{p^{r-k}-1} c_{2+jp^k})x^2 + \cdots + (\sum_{j=0}^{p^{r-k}-1} c_{p^k-1+jp^k})x^{p^k-1} \\ \equiv& \sum_{i=1}^{p^k-1} w_{i,k}x^i. \end{aligned}$$

Note that $w_{i,k} = w_{p^k-i,k}$. Then this result obviously follows.

(2) From the definition of $w_{i,k}$, this result follows.

(3) From the definition of $A_{i,k}(j)$,

$$\begin{aligned} A_{i,k}(j) =& w_{i+jp^{k-1},k}, \\ A_{p^{k-1}-i,k}(p-1-j) =& w_{p^{k-1}-i+(p-1-j)p^{k-1},k} = w_{p^k-(i+jp^{k-1}),k}. \end{aligned}$$

From $w_{i,k} = w_{p^k-i,k}$, Result (i) follows. From Result (i), Result (ii) follows. □

Theorem 3.17. *Let $n = 2m = 2p^r$, where $r \geq 2$, p is not a Wieferich prime, $p \equiv 3 \mod 4$, $ord_p(2) = p-1$ or $\frac{p-1}{2}$. The quadratic Boolean function $f(x)$ defined by (10) is semi-bent if and only if for any $1 \leq k \leq r$, there exists $0 \leq i \leq \frac{p^{k-1}-1}{2}$ such that $A_{i,k}$ is not constant, where $A_{i,k}$ is defined in (14).*

Proof. From Theorem 3.15, $f(x)$ is semi-bent if and only if for any $1 \leq k \leq r$,

$$(x^{p^{k-1}} + 1)c_f(x) \not\equiv 0 \mod x^{p^k} + 1.$$

From (2) in Lemma 3.16, that is equivalent to that there exists $0 \leq i \leq p^k - 1$ such that $w_{i,k} + w_{i-p^{k-1},k} \neq 0$. For $i = i_0 + jp^{k-1}$ and $0 \leq i_0 \leq p^{k-1} - 1$, $w_{i,k} + w_{i-p^{k-1},k} \neq 0$ is equivalent to

$$A_{i_0,k} = [w_{i_0,k}, w_{i_0+p^{k-1},k}, \cdots, w_{i_0+(p-1)p^{k-1},k}]'$$

is not constant. From (3) in Lemma 3.16, this theorem follows. □

4. Conclusion

This paper presents a new class of semi-bent quadratic Boolean functions with even variable n. For some special cases, the number of semi-bent functions is enumerated and the simpler characterization of semi-bentness is given. The techniques used in this paper can be utilized into the study of generalized bent functions and generalized semi-bent functions.

Acknowledgment

This work was supported by the Natural Science Foundation of China (Grant No.10990011 & No. 61272499). Yanfeng Qi also acknowledges support from Aisino Corporation Inc.

References

[1] E. R. Berlekamp, Algebraic Coding Theory , revised ed. Laguna Hills, CA: Aegean Park, 1984.

[2] S. Boztas and P. V. Kumar, "Binary sequences with Gold-like correlation but larger linear span," IEEE Trans. Inf. Theory , vol. 40, pp. 532-537, 1994.

[3] 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, Dec. 2005.

[4] R. Gold, “Maximal recursive sequences with 3-valued recursive crosscorrelation functions, ”IEEE Trans. Inf. Theory, vol. 14, no. 1, pp. 154-156, Jan. 1968.

[5] H. Hu, D. Feng, “On quadratic bent functions in polynomial forms,” IEEE Trans. Inform. Theory 53(2007) 2610-2615.

[6] T. Helleseth, ”Correlation of m-sequences and related topics,” in Sequences and Their Applications, Springer, 1998, pp. 49-66.

[7] T. Helleseth and P. V. Kumar, “Sequences with low correlation,” in Handbook of Coding Theory, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: North-Holland, 1998, vol. II, pp. 1765-1853.

[8] R. Lidl and H. Niederreiter, “Finite fields, ”in Encyclopedia of Mathematics and its Applications. Reading, MA: Addison-Wesley, 1983, vol. 20.

[9] K. Khoo, G. Gong, and D. R. Stinson, “A new family of Gold-like sequences,”in Proc. IEEE Int. Symp. Inf. Theory, Lausanne, Switzerland,Jun./Jul. 2002, p. 181.

[10] K. Khoo, G. Gong, and D. R. Stinson, “A new characterization of semibent and bent functions on finite fields, ”Des. Codes. Cryptogr. , vol. 38, no. 2, pp. 279-295, Feb. 2006.

[11] M. Matsui,”Linear cryptanalysis method for DES cipher. Proceedings of EUROCRYPT’93,” Lecture Notes in Computer Science765, pp. 386-397, 1994.

[12] W. Ma, M. Lee, and F. Zhang, “A new class of bent functions,”IEICE Trans. Fundamentals, vol. E88-A, no. 7, pp. 2039-2040, Jul. 2005.

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

[14] W. Meier and O. Staffelbach,”Fast correlation attacks on stream ciphers,” Advances in Cryptology, EUROCRYPT’88, Lecture Notes in Computer Science 330, pp. 301-314, 1988.

[15] N.J Patterson and D.H. Wiedemann,“The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276,” IEEE Transactions on Information Theory29(1983), 354-356.

[16] N.J Patterson and D.H. Wiedemann,“Correction to “The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276”,”IEEE Transactions Information Theory 36(1990), 443.

[17] O. S. Rothaus, “On bent functions,”J. Combin. Theory A, vol. 20, pp. 300-305, 1976.

[18] J. Silverman, “Wieferich’s criterion and the abc-conjecture,” J. Number Theory 30 (2) (1988) 226-237.

[19] C. Tang,Y. Qi,and M. Xu,“New quadratic bent functions in polynomial forms with coefficients in extension fields,” IACR Cryptology ePrint Archive 2013: 405 (2013).

[20] A. Wieferich, “Zum letzten Fermat’Schen Theorem,” J. Reine Angew. Math., 136(1909), 293-302.

[21] N. Y. Yu and G. Gong, “Constructions of quadratic bent functions in polynomial forms, ”IEEE Trans. Inf. Theory, vol. 52, no. 7, pp. 3291-3299, Jul. 2006.