New Quadratic Bent Functions in Polynomial Forms with Coefficients in Extension Fields

Chunming Tang, Yanfeng Qi, Maozhi Xu

***Abstract*—In this paper, we first discuss the bentness of a large class of quadratic Boolean functions in polynomial form $f(x) = \sum_{i=1}^{\frac{n}{2}-1} Tr_1^n(c_i x^{1+2^i}) + Tr_1^{n/2}(c_{n/2} x^{1+2^{n/2}})$, where $c_i \in GF(2^n)$ for $1 \leq i \leq \frac{n}{2}-1$ and $c_{n/2} \in GF(2^{n/2})$. The bentness of these functions can be connected with linearized permutation polynomials. Hence, methods for constructing quadratic bent functions are given. Further, we consider a subclass of quadratic Boolean functions of the form $f(x) = \sum_{i=1}^{\frac{m}{2}-1} Tr_1^n(c_i x^{1+2^{ei}}) + Tr_1^{n/2}(c_{m/2} x^{1+2^{n/2}})$, where $c_i \in GF(2^e)$, $n = em$ and m is even. The bentness of these functions are characterized and some methods for constructing new quadratic bent functions are given. Finally, for a special case: $m = 2^{v_0} p^r$ and $gcd(e, p-1) = 1$, we present the enumeration of quadratic bent functions.**

***Index Terms*—Bent function, Boolean function, linearized permutation polynomial, cyclotomic polynomial, semi-bent function**

I. Introduction

A bent function, whose Hamming distance to the set of all affine Boolean functions equals $2^{n-1} \pm 2^{\frac{n}{2}-1}$, is a Boolean function with even n variables from $GF(2^n)$ to $GF(2)$. Further, it has maximum nonlinearity and the absolute value of its Walsh transform has a constant magnitude [22]. Nonlinearity is an important property for a boolean function in cryptographic applications. Much research has been paid on bent functions [3], [4], [5], [6], [7], [10], [14], [17], [25]. Since bent functions with maximal nonlinearity have a close relationship with sequences, bent functions are often used in the construction of sequences with maximally linear complexity and low correlation[2], [8], [9], [15], [16], [21], [23]. Further, many applications of bent functions can be found in coding theory [18] and combinatorial design.

As another class of Boolean functions, semi-bent functions are also highly nonlinear. For an even integer n, the Walsh spectra of bent functions with n variables has the value $\pm 2^{\frac{n}{2}}$ while the Walsh spectra of semi-bent functions belongs to $\{0, \pm 2^{\frac{n+2}{2}}\}$. For an odd integer n, the Walsh spectra of semi-bent functions belongs to $\{0, \pm 2^{\frac{n+1}{2}}\}$. Khoo, Gong and Stinson [13], [14] 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 [6] 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 [17] applied techniques from [14] and considered the quadratic Boolean functions of the form

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

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 [25] considered the concrete constructions of bent functions of the form (1) and presented some enumeration results.

Hu and Feng [10] generalized results of Ma, Lee and Zhang [17] and studied the quadratic Boolean functions of the form

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

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

C. Tang is with School of Mathematics and Information, China West Normal University, Sichuan Nanchong, 637002, China. e-mail: tangchunming-math@163.com

Y. Qi is with LMAM, School of Mathematical Sciences, Peking University, Beijing, 100871, and Aisino corporation Inc., Beijing, 100097, China

M. Xu are with LMAM, School of Mathematical Sciences, Peking University, Beijing, 100871, China

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

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

where $c_i \in GF(2^n)$ for $1 \le i \le \frac{n}{2}-1$ and $c_{n/2} \in GF(2^{n/2})$. And we study the bentness of these functions from some specific linearized polynomials. Further, we generalize results in [10], [17] and study the bentness of quadratic Boolean functions of the form

$$f(x) = \sum_{i=1}^{\frac{m}{2}-1} Tr_1^n(c_i x^{1+2^{ei}}) + Tr_1^{n/2}(c_{m/2}x^{1+2^{n/2}}), \qquad (4)$$

where $c_i \in GF(2^e)$. Further, we gives some examples of new bent functions. And we construct new quadratic bent functions from known quadratic bent functions. Finally, we presents enumerations of bent functions of the form (4) 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).

The rest of the paper is organized as follows: Section 2 introduces some notations and backgrounds. Section 3 gives the description of bentness of quadratic Boolean functions considered in this paper and methods of constructing new bent functions. Section 4 enumerates the number of quadratic bent functions for special n. Finally, Section 5 makes a conclusion for this paper.

II. 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 $a, b \in GF(2^e)$.

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

$$f(x) = \sum_{i=0}^{\frac{n}{2}-1} Tr_1^n(c_i x^{1+2^i}) + Tr_1^{n/2}(c_{n/2}x^{1+2^{n/2}}), \qquad (5)$$

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

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

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

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

For a Boolean function $f(x)$ over $GF(2^n)$, the Hadamard transform is defined by

$$\hat{f}(\lambda) = \sum_{x \in GF(2^n)} (-1)^{f(x)+Tr_2^n(\lambda x)}, \lambda \in GF(2^n).$$

For a quadratic Boolean function $f(x)$ of the form (5) or (6), the distribution of the Hadamard transform can be described by the bilinear form

$$Q_f(x,y) = f(x+y) + f(x) + f(y). \qquad (7)$$

For the bilinear form Q_f, define

$$K_f = \{x \in GF(2^n) : Q_f(x,y) = 0, \forall y \in GF(2^n)\} \qquad (8)$$

and $k_f = dim_{GF(2)}(K_f)$. Then $2|(n-k_f)$. The distribution of the Hadamard transform values of $\hat{f}(\lambda)$ is given in the following theorem [11].

Theorem 2.1: Let $f(x)$ be a quadratic Boolean function of the form (5) or (6) and $k_f = dim_{GF(2)}(K_f)$, where K_f is defined in (8). The distribution of the Hadamard transform values of $f(x)$ is given by

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

Bent functions as an important class of Boolean functions are defined below.

Definition Let $f(x)$ be a Boolean function from $GF(2^n)$ to $GF(2)$. Then $f(x)$ is called a bent function if for any $\lambda \in GF(2^n)$, $\hat{f}(\lambda) \in \{2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}$.

Bent functions only exist in the case for even n. From Theorem 2.1, the following result on bent functions is given below.

Corollary 2.2: Let $f(x)$ be a quadratic function of the form (5) over $GF(2^n)$, then $f(x)$ is bent if and only if $K_f = \{0\}$, where K_f is defined in (8).

III. New construction of quadratic bent functions in polynomial forms

In this section, let n be even. We present the characterization of the bentness for quadratic Boolean functions and some methods for constructing bent functions.

A. Bent functions and linearized permutation polynomials

In this subsection, we discuss the relationship of bentness of quadratic Boolean function of the form (3) with linearized permutation polynomials.

Theorem 3.1: The quadratic Boolean function

$$f(x) = \sum_{i=0}^{n-1} Tr_1^n(c_i x^{1+2^i}), c_i \in GF(2^n) \qquad (9)$$

is bent if and only if

$$L_f(x)=\sum_{i=1}^{n-1}(c_i+c_{n-i}^{2^i})x^{2^i} \tag{10}$$

is a linearized permutation polynomial, that is, $L_f(x)=0$ only has a solution 0.

Proof:

$$\begin{aligned}
f(x+y)=&\sum_{i=0}^{n-1}Tr_1^n(c_i(x+y)^{1+2^i})\\
=&\sum_{i=0}^{n-1}Tr_1^n(c_i(x+y)^1(x+y)^{2^i})\\
=&\sum_{i=0}^{n-1}Tr_1^n(c_ix^{1+2^i})+\sum_{i=0}^{n-1}Tr_1^n(c_iy^{1+2^i})\\
&+\sum_{i=0}^{n-1}Tr_1^n(c_ix^{2^i}y)+\sum_{i=0}^{n-1}Tr_1^n(c_iy^{2^i}x)\\
=&f(x)+f(y)+\sum_{i=0}^{n-1}Tr_1^n(c_ix^{2^i}y)+\sum_{i=0}^{n-1}Tr_1^n((c_iy^{2^i}x)^{2^{n-i}})\\
=&f(x)+f(y)+\sum_{i=1}^{n-1}Tr_1^n((c_i+c_{n-i}^{2^i})x^{2^i}y).
\end{aligned}$$

Then we have

$$\begin{aligned}
Q_f(x,y)=&f(x+y)+f(x)+f(y)\\
=&\sum_{i=1}^{n-1}Tr_1^n((c_i+c_{n-i}^{2^i})x^{2^i}y).
\end{aligned}$$

From Corollary 2.2, $f(x)$ is bent if and only if $\sum_{i=1}^{n-1}(c_i+c_i^{2^{n-i}})x^{2^i}=0$ has only a solution 0. Since $L_f(x)=\sum_{i=1}^{n-1}(c_i+c_i^{2^{n-i}})x^{2^i}$ is a linearized polynomial and can be seen as a linear transformation of $GF(2^n)$ over $GF(2)$, $L_f(x)=0$ has only a solution 0 if and only if $L_f(x)$ is a linearized permutation polynomial. This theorem follows. ■

The following theorem characterizes the bentness of quadratic Boolean functions of the form (3).

Theorem 3.2: Let $f(x)$ be a quadratic Boolean function defined by

$$f(x)=\sum_{i=1}^{\frac{n}{2}-1}Tr_1^n(c_ix^{1+2^i})+Tr_1^{n/2}(c_{n/2}x^{1+2^{n/2}}), \tag{11}$$

where $c_i\in GF(2^n)$ for $1\le i\le\frac{n}{2}-1$ and $c_{n/2}\in GF(2^{n/2})$. Then $f(x)$ is bent if and only if

$$L_f(x)=\sum_{i=1}^{\frac{n}{2}-1}(c_ix^{2^i}+c_i^{2^{n-i}}x^{2^{n-i}})+c_{n/2}x^{2^{n/2}} \tag{12}$$

is a linearized permutation polynomial, that is, $L_f(x)=0$ has only a solution 0.

Proof: Since $Tr_{n/2}^n(\cdot)$ is a surjective map from $GF(2^n)$ to $GF(2^{\frac{n}{2}})$, there exists $c'_{n/2}\in GF(2^n)$ satisfying $c_{n/2}=Tr_{n/2}^n(c'_{n/2})=c'_{n/2}+c'^{2^{n/2}}_{n/2}$. Then

$$f(x)=\sum_{i=1}^{\frac{n}{2}-1}Tr_1^n(c_ix^{1+2^i})+Tr_1^n(c'_{n/2}x^{1+2^{n/2}})$$

From Theorem 3.1,

$$L_f(x)=\sum_{i=1}^{\frac{n}{2}-1}(c_ix^{2^i}+c_i^{2^{n-i}}x^{2^{n-i}})+c_{n/2}x^{2^{n/2}}.$$

Hence, this theorem follows from the similar discussion of Theorem 3.1. ■

From Theorem 3.2, the bentness of quadratic Boolean functions depends on the corresponding linearized permutation polynomial (12). Hence, many results and techniques on linearized permutation polynomials, such as theories of non-commutative polynomials [19], [20], can be used to study quadratic bent functions. New results on linearized permutation polynomials can be found in [24]. So far, bent functions constructed of the form (11) generally satisfy that $c_i\in GF(2)$. We will present some bent functions with the form (11) with $c_i\in GF(2^n)\backslash GF(2)$ for some i.

Theorem 3.3: Let i be an integer satisfying $1\le i\le\frac{n}{2}-1$. Let $\alpha\in GF(2^n)^*$ and $n=2^{v_0}n_0$, where n_0 is odd. Let $f(x)$ be a quadratic Boolean function of the form

$$f(x)=Tr_1^n(\alpha x^{1+2^i}).$$

Then

(1) There exists $\alpha\in GF(2^n)$ making $f(x)$ bent if and only if $2^{v_0}\nmid i$.

(2) Let $2^{v_0}\nmid i$. Then $f(x)$ is bent if and only if α satisfies

$$\alpha^{(2^n-1)(2^{gcd(i,n)}-1)/(2^{gcd(2i,n)}-1)}=\alpha^{(2^n-1)/(2^{gcd(i,n)}+1)}\neq1.$$

In particular, let α be a primitive element in $GF(2^n)$, then $f(x)$ is bent.

Proof: From the definition of $f(x)$,

$$L_f(x)=\alpha x^{2^i}+\alpha^{2^{n-i}}x^{2^{n-i}}.$$

From Theorem 3.2, we just consider the sufficient and necessary condition for

$$K_f=\{x\in GF(2^n):L_f(x)=0\}=\{0\}.$$

Since $x\mapsto x^{2^i}$ is an isomorphism for $GF(2^n)$, then $K_f=\{0\}$ if and only if $K_f^{2^i}=\{0\}$. Further,

$$\begin{aligned}
K_f^{2^i}=&\{x\in GF(2^n):\alpha^{2^i}x^{2^{2i}}+\alpha x=0\}\\
=&\{0\}\cup\{x\in GF(2^n):x^{2^{2i}-1}=(\frac{1}{\alpha})^{2^i-1}\}\\
=&\{0\}\cup K',
\end{aligned}$$

where $K'=\{x\in GF(2^n):x^{2^{2i}-1}=(\frac{1}{\alpha})^{2^i-1}\}$. Then $K_f^{2^i}=\{0\}$ if and only if $K'=\emptyset$, that is,

$$x^{2^{2i}-1}=(\frac{1}{\alpha})^{2^i-1},\quad x\in GF(2^n)$$

has no solution. Equivalently,

$$\begin{aligned}
(\frac{1}{\alpha})^{2^i-1}\notin&\{x^{2^{2i}-1}:x\in GF(2^n)^*\}\\
=&\{x^{gcd(2^{2i}-1,2^n-1)}:x\in GF(2^n)^*\}\\
=&\{x^{2^{gcd(2i,n)}-1}:x\in GF(2^n)^*\}.
\end{aligned}$$

That equals that

$$(\frac{1}{\alpha})^{(2^n-1)(2^i-1)/(2^{gcd(2i,n)}-1)} \neq 1,$$

or

$$(\frac{1}{\alpha})^{(2^n-1)(2^{gcd(i,n)}-1)/(2^{gcd(2i,n)}-1)} \neq 1. \qquad (13)$$

Note that

$$(2^{gcd(i,n)}-1) \mid (2^{gcd(2i,n)}-1) \mid (2^n-1).$$

There exists α satisfying (13) if and only if $(2^{gcd(i,n)}-1) < (2^{gcd(2i,n)}-1)$, that is, $gcd(i,n) < gcd(2i,n)$. Equivalently, $2^{v_0} \nmid i$. Hence, Result (1) follows. If $2^{v_0} \nmid i$, $f(x)$ is bent if and only if α satisfies (13). From $2^{v_0} \nmid i$,

$$gcd(2i,n) = 2 \cdot gcd(i,n).$$

Hence, Result (2) follows. ■

Theorem 3.4: Let $\alpha \in GF(2^n)^*$ and $(\alpha + \alpha^{-4}) \in GF(2^{n/2})$, the Boolean function

$$f(x) = Tr_1^n(x^{1+2^{n/2-2}}) + Tr_1^{\frac{n}{2}}((\alpha+\alpha^{-4})x^{1+2^{n/2}})$$

is bent if and only if $\alpha^{(2^n-1)/3} \neq 1$.

Proof: From the Boolean function $f(x)$,

$$L_f(x) = x^{2^{n/2-2}} + (\alpha+\alpha^{-4})x^{2^{n/2}} + x^{2^{n/2+2}},$$

After some transformation, the factorization of the linear transform $L_f(x)$ is

$$L_f(x) = T_{\alpha^{-4}}(T_\alpha(x^{2^{n/2-2}})),$$

where $T_\alpha(x) = x + \alpha x^{2^2}, T_{\alpha^{-4}}(x) = x + \alpha^{-4}x^{2^2}$. Since $x \mapsto x^{2^{n/2-2}}$ is an invertible linear transformation, $L_f(x)$ is invertible if and only if both $T_\alpha(x)$ and $T_{\alpha^{-4}}(x)$ are invertible. It is easily verified that both $T_\alpha(x)$ and $T_{\alpha^{-4}}(x)$ are invertible if and only if $\alpha^{(2^n-1)/3} \neq 1$. From Theorem 3.2, this theorem follows. ■

Remark (i) If $\frac{n}{2}$ is even, then $3|(2^{\frac{n}{2}}-1)$ and $3 \nmid (2^{\frac{n}{2}}+1)$. Let w be the largest integer satisfying $3^w|(2^{\frac{n}{2}}-1)$ and ζ_{3^w} be a primitive 3^w-th root of unity. Take

$$\alpha = \beta\zeta_{3^w}^i \qquad (14)$$

where $\beta \in GF(2^{\frac{n}{2}})$, $3 \nmid ord(\beta)$ and $3 \nmid i$. Then $(\alpha+\alpha^{-4}) \in GF(2^{n/2})$. It is easily verified that $\alpha^{(2^n-1)/3} \neq 1$. Hence, α satisfies Theorem 3.4 and $f(x)$ in Theorem 3.4 is a bent function.

(ii) If $\frac{n}{2}$ is odd, then $3|(2^{\frac{n}{2}}+1)$ and $3 \nmid (2^{\frac{n}{2}}-1)$. Let w be the largest integer satisfying $3^w|(2^{\frac{n}{2}}+1)$. Take

$$\alpha = (Tr_{n/2}^n u)^{3/5}u \qquad (15)$$

where $u \in GF(2^n)$, $u^{1+\frac{n}{2}} = 1$ and $3^w|ord(u)$. Note that $5 \nmid 2^{\frac{n}{2}}-1$ and $gcd(5, ord(Tr_{n/2}^n u)) = 1$. Then $(Tr_{n/2}^n u)^{3/5}$ is well defined. Since $3^w|ord(u)$, $u \notin GF(2^{\frac{n}{2}})$. Let $\lambda = u+u^{2^m}$, then the minimal polynomial of u over $GF(2^{\frac{n}{2}})$ is

$$u^2 + \lambda u + 1 = 0. \qquad (16)$$

Since $\lambda = Tr_{n/2}^n u \in GF(2^{\frac{n}{2}})$ and $3 \nmid (2^{\frac{n}{2}}-1)$, then α satisfies that $\alpha^{(2^n-1)/3} \neq 1$. From Identity (16),

$$\alpha + \alpha^{-4} = \lambda^{-\frac{12}{5}}(\lambda^4+\lambda^2+1) \in GF(2^{\frac{n}{2}}).$$

Hence, $f(x)$ defined in Theorem 3.4 is bent.

B. A subclass of quadratic bent functions

In this subsection, we will consider a special subclass of Boolean functions in (11). This subclass can be seen as a generalization of functions in [10], [17]. Let m be even and $n = me$ for this subsection.

Theorem 3.5: Let $f(x)$ be a Boolean function defined by

$$f(x) = \sum_{i=1}^{\frac{m}{2}-1} Tr_1^n(c_i x^{1+2^{ei}}) + Tr_1^{n/2}(c_{m/2}x^{1+2^{n/2}}) \qquad (17)$$

where $c_i \in GF(2^e)$, then $f(x)$ is bent if and only if $gcd(c_f(x), x^m+1) = 1$, where

$$c_f(x) = \sum_{i=1}^{\frac{m}{2}-1} c_i(x+x^{m-i}) + c_{m/2}x^{m/2}. \qquad (18)$$

In particular, if $f(x)$ is bent, then $c_{m/2} \neq 0$.

Proof: Since m is even and $e = \frac{n}{m}$ divides $\frac{n}{2}$, then $c_{\frac{m}{2}} \in GF(2^e) \subseteq GF(2^{\frac{n}{2}})$. Note that $Tr_{n/2}^n(\cdot)$ is surjective from $GF(2^n)$ to $GF(2^{\frac{n}{2}})$. Then there exists $c'_{m/2} \in GF(2^n)$ satisfying $c_{m/2} = Tr_{n/2}^n(c'_{m/2}) = c'_{m/2} + c'^{2^{n/2}}_{m/2}$. Hence,

$$f(x) = \sum_{i=1}^{\frac{m}{2}-1} Tr_1^n(c_i x^{1+2^{ei}}) + Tr_1^n(c'_{m/2}x^{1+2^{n/2}}).$$

From the similar proof of Theorem 3.1,

$$L_f(x) = \sum_{i=1}^{\frac{m}{2}-1} c_i(x^{2^{ei}} + x^{2^{e(m-i)}}) + c_{m/2}x^{2^{em/2}} = \sum_{i=1}^{m-1} a_i x^{2^{ei}},$$

where

$$a_i = \begin{cases} c_i, & 1 \leq i \leq m/2, \\ c_{m-i}, & m/2 < i \leq m-1. \end{cases}$$

Let $\alpha \in GF(2^n)$ be a regular element in $GF(2^e)$, that is, $\{\alpha, \alpha^{2^e}, \alpha^{2^{e \cdot 2}}, \ldots, \alpha^{2^{e(m-1)}}\}$ is a basis of $GF(2^n)$ over $GF(2^e)$, then the matrix associated with the linear transformation $L_f(x)$ under this basis is

$$A = \begin{bmatrix} 0 & a_1 & a_2 & \cdots & a_{m-1} \\ a_{m-1} & 0 & a_1 & \cdots & a_{m-2} \\ a_{m-2} & a_{m-1} & 0 & \cdots & a_{m-3} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_1 & a_2 & a_3 & \cdots & 0 \end{bmatrix}$$

Hence $L_f(x)$ is a linearized permutation polynomial if and only if A is non-singular. From the theory of cyclic codes in [1], A is non-sigular if and only if the dimension $m - gcd(0 + a_1x + a_2x^2, \cdots, a_{m-1}x^{m-1}, x^m - 1)$ of the cyclic code over $GF(2^e)$, generated by rows of A, is m, i.e. $gcd(c_f, x^m+1) = gcd(0 + a_1x + a_2x^2, \cdots, a_{m-1}x^{m-1}, x^m-1) = 1$. Finally, if $c_{m/2} = 0$, then $(x+1)|c_f(x)$.

Hence, this theorem follows. ■

Theorem 3.6: Let $m = 2^{v_0}$, where $v_0 \geq 1$. The Boolean function

$$f(x) = \sum_{i=1}^{\frac{m}{2}-1} Tr_1^n(c_i x^{1+2^{ei}}) + Tr_1^{n/2}(c_{m/2}x^{1+2^{n/2}}) \qquad (19)$$

is bent if and only if $c_{m/2} \neq 0$. Further, the number of bent functions with this form over $GF(n)$ is $(2^e-1)2^{e\frac{m-2}{2}}$.

Proof: Since $m = 2^{v_0}$, $x^m+1 = (x+1)^{2^{v_0}}$. Then $gcd(c_f(x), x^m+1) = 1$ if and only if $(x+1) \nmid c_f(x)$, that is, $c_f(1) \neq 0$. Note that $c_f(1) = c_{m/2}$. From Theorm 3.5, $f(x)$ is bent if and only if $c_{m/2} \neq 0$. From the random choice of $c_i \in GF(2^e)$ $(1 \leq i \leq \frac{m-2}{2})$, the number of bent functions is $(2^e-1)2^{e\frac{m-2}{2}}$. This theorem follows. ■

Theorem 3.7: Let $n = 2^{v_0}m_0$, where m_0 is odd. Let $\lambda \in GF(2^{2e})^*$ satisfying $\lambda + \frac{1}{\lambda} \in GF(2^e)^*$. Then the Boolean function

$$f(x) = Tr_1^n(x^{1+2^{ei}}) + Tr_1^{\frac{n}{2}}((\lambda + \frac{1}{\lambda})x^{1+2^{n/2}})$$

is bent if and only if $\lambda^{m_0/gcd(i,m_0)} \neq 1$.

Proof: From the definition of $f(x)$,

$$\begin{aligned} c_f(x) =&(x^i + x^{m-i}) + (\lambda + \frac{1}{\lambda})x^{m/2} \\ \equiv&(x^i + x^{-i}) + (\lambda + \frac{1}{\lambda}) \\ \equiv&\frac{x^{2i} + (\lambda + \frac{1}{\lambda})x^i + 1}{x^i} \\ \equiv&\frac{(x^i+\lambda)(x^i+\frac{1}{\lambda})}{x^i} \qquad \bmod x^{m_0}+1, \end{aligned}$$

Then $gcd(c_f(x), x^m+1) = 1$ if and only if $gcd(x^i+\lambda, x^{m_0}+1) = gcd(x^i+\frac{1}{\lambda}, x^{m_0}+1) = 1$. From $gcd(x^i+\lambda, x^{m_0}+1) = 1$, we have equivalently

$$\begin{aligned} \lambda \notin&\{x^i : x \in \overline{GF(2)}, x^{m_0} = 1\} \\ =&\{x : x \in \overline{GF(2)}, x^{m_0/gcd(i,m_0)} = 1\}, \end{aligned}$$

that is,

$$\lambda^{m_0/gcd(i,m_0)} \neq 1.$$

Similarly, $gcd(x^i + \frac{1}{\lambda}, x^{m_0}+1) = 1$ if and only if $\lambda^{-m_0/gcd(i,m_0)} \neq 1$. Note that $\lambda^{m_0/gcd(i,m_0)} \neq 1$ if and only if $\lambda^{-m_0/gcd(i,m_0)} \neq 1$. Hence, this theorem follows. ■

We will consider how to construct new quadratic bent functions from known quadratic bent functions.

Theorem 3.8: Let $c_i \in GF(2^e)$ for $1 \leq i \leq m/2$ and $\beta \in GF(2^e)^*$, then

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

is bent if and only if

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

is bent.

Proof: We have

$$\begin{aligned} c_f(x) =& \sum_{i=1}^{\frac{m}{2}-1} c_i(x + x^{m-i}) + c_{m/2}x^{m/2}, \\ c_{f_\beta}(x) =&\beta(\sum_{i=1}^{\frac{m}{2}-1} c_i(x + x^{m-i}) + c_{m/2}x^{m/2}) = \beta c_f(x). \end{aligned}$$

Since $\beta \neq 0$, then

$$gcd(c_f(x), x^m+1) = gcd(c_{f_\beta}(x), x^m+1).$$

From Theorem 3.5, this theorem follows. ■

Remark This theorem can explain the relationship of bent functions presented by Hu and Feng[10] and bent functions constructed by Ma, Lee and Zhang [17].

Theorem 3.9: Let $c_i \in GF(2^e)$ for $1 \leq i \leq m/2$ and $\beta \in GF(2^e)$. Then

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

is bent if and only if

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

is bent.

Proof: We have

$$\begin{aligned} c_{f_+}(x) =&c_f(x) + \beta\sum_{i=1}^{\frac{m}{2}-1}(x^i + x^{m-i}) \\ =&c_f(x) + \beta(x^{m/2}+1)\sum_{i=1}^{\frac{m}{2}-1} x^i \end{aligned}$$

For any polynomial $g(x)$, $gcd(g(x), x^m+1) = 1$ if and only if $gcd(g(x), x^{m/2}+1) = 1$. Then

$$\begin{aligned} &gcd(c_{f_+}(x), x^{m/2}+1) \\ =&gcd(c_f(x) + \beta(x^{m/2}+1)\sum_{i=1}^{\frac{m}{2}-1} x^i, x^{m/2}+1) \\ =&gcd(c_f, x^{m/2}+1) \end{aligned}$$

Hence, this theorem follows. ■

From Theorem 3.9, we have a generalization of Theorem 5 in [10].

Corollary 3.10: Let m_0 be the largest odd integer dividing m. Let $1 \leq k \leq m/2-1$, $d \geq 1$, $\beta_1 \in GF(2^e)^*$ and $\beta_2 \in GF(2^e)$. The Boolean function

$$\begin{aligned} f(x) = &\sum_{i=1}^{m/2-1} Tr_1^n(\beta_2 x^{1+2^{ei}}) \\ &+ Tr_1^{\frac{n}{2}}(\beta_1 x^{1+2^{n/2}}) + \sum_{i=1}^{k} Tr_1^n(\beta_1 x^{1+2^{edi}}) \end{aligned}$$

is bent if and only if $gcd((2k+1)d, m_0) = gcd(d, m_0)$.

Proof: From Theorem 3.9 and Theorem 4 in [10], this theorem follows. ■

Theorem 3.11: Let $a_i, b_i \in GF(2^e)$ for $1 \leq i \leq m/2$. Two Boolean functions $f_1(x)$ and $f_2(x)$ are defined by

$$\begin{aligned} f_1(x) =& \sum_{i=1}^{\frac{m}{2}-1} Tr_1^n(a_i x^{1+2^{ei}}) + Tr_1^{n/2}(a_{m/2}x^{1+2^{n/2}}), \\ f_2(x) =& \sum_{i=1}^{\frac{m}{2}-1} Tr_1^n(b_i x^{1+2^{ei}}) + Tr_1^{n/2}(b_{m/2}x^{1+2^{n/2}}), \end{aligned}$$

Let $(\sum_{i=1}^{\frac{m}{2}-1} a_i(x+x^{m-i})+a_{m/2}x^{m/2})(\sum_{i=1}^{\frac{m}{2}-1} b_i(x+x^{m-i})+b_{m/2}x^{m/2})x^{m/2} \equiv \sum_{i=0}^{m-1} c_i x^i \mod x^m+1$, where $c_i \in GF(2^e)$. Let $a_0 = b_0 = 0$. Let $a_{m-j} = a_j, b_{m-k} = b_k$ for $m/2+1 \leq j,k \leq m$. Then

$$c_i = \sum_{\substack{j+k \equiv i+m/2 \mod m \\ 0 \leq j,k \leq m-1}} a_j b_k.$$

Further,

(1) $c_0 = 0$ and $c_{m-i} = c_i$ for $1 \leq i \leq m-1$;

(2) $f_{1*2}(x) = \sum_{i=1}^{\frac{m}{2}-1} Tr_1^n(c_i x^{1+2^{ei}}) + Tr_1^{n/2}(c_{m/2}x^{1+2^{n/2}})$ is bent if and only if both $f_1(x)$ and $f_2(x)$ are bent.

Proof: We have

$$\begin{aligned} c_0 = & \sum_{\substack{j+k \equiv m/2 \mod m \\ 0 \leq j,k \leq m-1}} a_j b_k \\ =& a_1 b_{m/2-1} + \cdots + a_{m/2-1}b_1 + a_{m/2}b_0 \\ & + a_{m/2+1}b_{m-1} + \cdots + a_{m-1}b_{m/2+1} \\ =& a_1 b_{m/2-1} + \cdots + a_{m/2-1}b_1 + a_{m/2} \cdot 0 \\ & + a_{m/2-1}b_1 + \cdots + a_1 b_{m/2-1} \\ =& 0. \end{aligned}$$

For $1 \leq i \leq m-1$,

$$\begin{aligned} c_{m-i} = & \sum_{\substack{j+k \equiv m/2-i \mod m \\ 0 \leq j,k \leq m-1}} a_j b_k \\ = & \sum_{\substack{j+k \equiv m/2-i \mod m \\ 0 \leq j,k \leq m-1}} a_{m-j} b_{m-k} \\ = & \sum_{\substack{(m-j)+(m-k) \equiv m/2+i \mod m \\ 0 \leq j,k \leq m-1}} a_{m-j} b_{m-k} \\ = & \sum_{\substack{j+k \equiv m/2+i \mod m \\ 0 \leq j,k \leq m-1}} a_j b_k \\ =& c_i. \end{aligned}$$

Hence, Result (1) follows. From the definition of $f_{1*2}(x)$,

$$c_{f_{1*2}}(x) = \sum_{i=0}^{m-1} c_i x^i.$$

Further,

$$c_{f_{1*2}}(x) \equiv c_{f_1}(x) \cdot c_{f_2}(x) \mod x^m+1.$$

Then

$$gcd(c_{f_{1*2}}(x), x^m+1) = gcd(c_{f_1}(x) \cdot c_{f_2}(x), x^m+1).$$

Hence, $gcd(c_{f_{1*2}}(x), x^m+1) = 1$ if and only if $gcd(c_{f_1}(x), x^m+1) = gcd(c_{f_1} \cdot c_{f_2}(x), x^m+1) = 1$. From Theorem 3.5, Result (2) follows. ■

Corollary 3.12: Let m_0 be the largest integer dividing m, then the Boolean function

$$\begin{aligned} f(x) =& Tr_1^n(x^{1+2^{ed_1}}) + Tr_1^n(x^{1+2^{ed_2}}) + Tr_1^n(x^{1+2^{e(d_1+d_2+m/2)}}) \\ & + Tr_1^n(x^{1+2^{e(d_1-d_2+m/2)}}) + Tr_1^{\frac{n}{2}}(x^{1+2^{n/2}}) \end{aligned}$$

is bent if and only if $gcd(3d_1, m_0) = gcd(d_1, m_0)$ and $gcd(3d_2, m_0) = gcd(d_2, m_0)$.

Proof: From Theorem 3.11 and Theorem 4 in [10], this corollary follows. ■

IV. The enumeration for bent functions in case $m = 2^{v_0}p^r$ and $gcd(e, p-1) = 1$

In this section, we will consider the enumeration of bent functions in (17). In [10], [25], cyclotomic polynomials and their factorization are used in the enumeration. Our method can be generalized for general cases. Before the enumeration, some knowledge on monic self-reciprocal polynomials is given first.

Definition The reciprocal polynomial $g^*(x)$ of a polynomial $g(x)$ of degree n is defined by $g^*(x) = x^n g(1/x)$. A polynomial is called self-reciprocal if it coincides with its reciprocal polynomial.

Lemma 4.1: Let $A(x) = \sum_{i=0}^{n_1} a_i x^i$ be a monic self-reciprocal polynomial of degree n_1 and $B(x) = \sum_{i=0}^{n} b_i x^i$ be a polynomial of degree n_2. Then $A(x)B(x)$ is a monic self-reciprocal polynomial of degree n_1+n_2 if and only if $B(x)$ is a monic self-reciprocal polynomial.

Proof: Let $C(x) = A(x)B(x) = \sum_{i=0}^{n_1+n_2} c_i x^i$. Suppose $B(x)$ is a monic self-reciprocal polynomial, then $c_0 = a_0 b_0 = a_{n_1} b_{n_2} = c_{n_1+n_2} = 1$. For $0 < k < n_1+n_2$,

$$\begin{aligned} c_{n_1+n_2-k} = & \sum_{i+j=n_1+n_2-k} a_i b_j \\ = & \sum_{i+j=n_1+n_2-k} a_{n_1-i} b_{n_2-j} \\ = & \sum_{(n_1-i)+(n_2-j)=k} a_{n_1-i} b_{n_2-j} \\ = & \sum_{i+j=k} a_i b_j \\ =& c_k. \end{aligned}$$

Hence $C(x)$ is a monic self-reciprocal polynomial of degree n_1+n_2.

On the other hand, suppose that $C(x)$ is a monic self-reciprocal polynomial. From $a_0 b_0 = c_0 = 1$ and $a_{n_1} b_{n_2} = c_{n_1+n_2} = 1$, $b_0 = 1$ and $b_{n_2} = 1$. If $B(x)$ is not monic self-reciprocal, there exists an integer k satisfying that $0 < k < n_2$, $b_k \neq b_{n_2-k}$ and $b_{k-1} = b_{n_2-(k-1)}, \cdots, b_0 = b_{n_2}$. Then

$$\begin{aligned} 0 =& c_k - c_{n_1+n_2-k} \\ =& (a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0) \\ & - (a_{n_1} b_{n_2-k} + a_{n_1-1} b_{n_2-(k-1)} + \cdots + a_{n_1-k} b_{n_2}) \\ =& (a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0) \\ & - (a_0 b_{n_2-k} + a_1 b_{k-1} + \cdots + a_k b_0) \\ =& b_k - b_{n_2-k}, \end{aligned}$$

The result $b_k = b_{n_2-k}$ contradicts the supposition of k. Hence, $B(x)$ is a monic self-reciprocal polynomial.

This theorem follows. ■

Lemma 4.2: Let $A(x), g(x) \in GF(2^e)[x]$ and $A(x)$ be monic self-reciprocal. Let $g(x)$ be irreducible and $g(x)|A(x)$, 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: If $g(x)$ is self-reciprocal, $g^*(x) = g(x)$, the results obviously hold.

Suppose that $g(x)$ is not self-reciprocal. From $g(x)|A(x)$, $g^*(x)|A^*(x) = A(x)$. Then $g^*(x)|A(x)$. Since $g(x)$ is irreducible, $gcd(g(x), g^*(x)) = 1$ and $g(x)g^*(x)|A(x)$. Hence, this lemma follows. ■

Corollary 4.3: Let $A(x) \in GF(2^e)[x]$ be a monic self-reciprocal polynomial. Then $A(x)$ has the following factorization.

$$\begin{aligned} A(x) =& g_1(x)g_1^*(x)\cdots g_s(x)g_s^*(x)g_{s+1}(x)\cdots g_{s+t}(x) \\ =& \widetilde{g}_1(x)\cdots \widetilde{g}_s(x)\widetilde{g}_{s+1}(x)\cdots \widetilde{g}_{s+t}(x), \end{aligned} \tag{20}$$

where $g_i(x), g_j^*(x)$ $(1 \leq i \leq s+t, 1 \leq j \leq s)$ are irreducible. $g_i(x)$ is not self-reciprocal for $1 \leq i \leq s$ and $\widetilde{g}_i(x) = g_i(x)g_i^*(x)$, where $g_i^*(x)$ is the reciprocal polynomial of $g_i(x)$. $g_i(x)$ is self-reciprocal for $s+1 \leq i \leq s+t$ and $\widetilde{g}_i(x) = g_i(x)$.

Proof: From Lemma 4.1 and Lemma 4.2, this corollary follows. ■

Let the monic self-reciprocal polynomial $A(x) \in GF(2^e)[x]$ without duplicate factors have the following factorization of the form (20).

$$A(x) = \widetilde{g}_1(x)\cdots \widetilde{g}_s(x)\widetilde{g}_{s+1}(x)\cdots \widetilde{g}_{s+t}(x), \tag{21}$$

where $\widetilde{g}_i(x)$ is self-reciprocal. Further, suppose $\widetilde{g}_i(x)$ is monic. Then $n_i = deg(\widetilde{g}_i(x))$ $(1 \leq i \leq s+t)$ is even. For a positive even integer k, let $\mathfrak{R}_k$ be a set of polynomial $C(x) \in GF(2^e)[x]$, where $C(x)$ satisfies the following conditions.

(i) $deg(C(x)) \leq k$ and $deg(C(x))$ is even;

(ii) $C(x)$ is monic self-reciprocal;

(iii) $gcd(C(x), x+1) = 1$.

For an even integer $h > deg(A(x))$, define $\mathfrak{P}_h(A(x))$ as a set

$$\mathfrak{P}_h(A(x)) = \{C(x) \in \mathfrak{R}_h : gcd(C(x), A(x)) = 1\}. \tag{22}$$

Then we have the enumeration for $\#(\mathfrak{R}_k)$ and $\#(\mathfrak{P}_h(A(x)))$.

Lemma 4.4: Let notations be defined above, then

$$\begin{aligned} \#(\mathfrak{R}_k) =& 2^{e\frac{k}{2}}, \\ \#(\mathfrak{P}_h(A(x))) =& 2^{e\frac{h}{2}} \prod_{i=1}^{s+t}(1-(\frac{1}{2^e})^{\frac{n_i}{2}}). \end{aligned}$$

Proof: Note that the monic self-reciprocal polynomial $x^{2i} + a_{2i-1}x^{2i-1} + \cdots + a_i x^i + \cdots + a_1 x^1 + 1$ of even degree is coprime to $x+1$ if and only if $a_i \neq 0$. From the definition of $\mathfrak{R}_k$, the numbers of polynomials of degree $0, 2, 4, 6, \cdots, k$ in $\mathfrak{R}_k$ are $1, (2^e-1), (2^e-1)(2^e)^1, (2^e-1)(2^e)^2, \cdots, (2^e-1)(2^e)^{\frac{k}{2}-1}$ respectively. Hence,

$$\begin{aligned} \#(\mathfrak{R}_k) =& 1 + (2^e-1) + (2^e-1)(2^e)^1 + (2^e-1)(2^e)^2 \\ & + \cdots + (2^e-1)(2^e)^{\frac{k}{2}-1} \\ =& 2^{e\frac{k}{2}}. \end{aligned}$$

To enumerate $\mathfrak{P}_h(A(x))$, we introduce the auxiliary set

$$\mathfrak{M}_h(i_1, i_2, \cdots, i_k) = \{C(x) \in \mathfrak{R}_h : \prod_{j=1}^{k} \widetilde{g}_{i_j}(x)|C(x)\},$$

where $1 \leq k \leq s+t$ and $1 \leq i_1 < i_2 < \cdots < i_k \leq s+t$.

From Lemma 4.1, for any $C(x) \in \mathfrak{M}_h(i_1, i_2, \cdots, i_k)$, $C(x)$ can be uniquely represented by $C(x) = C'(x)\prod_{j=1}^{k}\widetilde{g}_{i_j}(x)$, where $C'(x) \in \mathfrak{R}_{h-n_{i_1}-\cdots-n_{i_k}}$. Then

$$\#(\mathfrak{M}_h(i_1, i_2, \cdots, i_k)) = \#(\mathfrak{R}_{h-n_{i_1}-\cdots-n_{i_k}}).$$

Since $A(x)$ has no duplicate factors, $gcd(\widetilde{g}_i(x), \widetilde{g}_j(x)) = 1$ $(i \neq j)$ and $deg(\widetilde{g}_i(x))$ is even. Then $gcd(\widetilde{g}_i(x), x+1) = 1$. From the inclusion-exclusion principle,

$$\begin{aligned} & \#(\mathfrak{P}_h(A(x))) \\ =& \#(\mathfrak{R}_h) - \sum_{1\leq i_1 \leq s+t} \#(\mathfrak{M}_h(i_1)) + \sum_{1\leq i_1 < i_2 \leq s+t} \#(\mathfrak{M}_h(i_1, i_2)) \\ & + (-1)^{s+t}\#(\mathfrak{M}_h(1, 2, \cdots, s+t)) \\ =& \#(\mathfrak{R}_h) + \sum_{k=1}^{s+t}(-1)^k \sum_{1\leq i_1<i_2<\cdots<i_k\leq s+t} \#(\mathfrak{M}_h(i_1, i_2, \cdots, i_{s+t})) \\ =& \#(\mathfrak{R}_h) + \sum_{k=1}^{s+t}(-1)^k \sum_{1\leq i_1<i_2<\cdots<i_k\leq s+t} \#(\mathfrak{R}_{h-n_{i_1}-\cdots-n_{i_k}}) \\ =& 2^{e\frac{h}{2}} + \sum_{k=1}^{s+t}(-1)^k \sum_{1\leq i_1<i_2<\cdots<i_k\leq s+t} 2^{e\frac{h-n_{i_1}-n_{i_2}\cdots-n_{i_k}}{2}} \\ =& 2^{e\frac{h}{2}}(1 + \sum_{k=1}^{s+t}(-1)^k \sum_{1\leq i_1<i_2<\cdots<i_k\leq s+t} 2^{-e\frac{n_{i_1}+n_{i_2}\cdots+n_{i_k}}{2}}) \\ =& 2^{e\frac{h}{2}} \prod_{k=1}^{s+t}(1-(\frac{1}{2^e})^{\frac{n_i}{2}}). \end{aligned}$$

Hence, this lemma follows. ■

Now we consider the enumeration of bent functions. Let $m = 2^{v_0}p^r$ and $gcd(e, p-1) = 1$, where $v_0 > 0$, $r > 0$ and p is an odd prime satisfying $ord_p(2) = p-1$ or $ord_p(2) = (p-1)/2((p-1)/2$ is odd). We first discuss the factorization of $x^{p^r}+1$ over $GF(2^e)$, which is connected with cyclotomic polynomials [12]. The d-th cyclotomic polynomial $Q_d(x)$, whose roots are primitive d-th roots of unity, is a monic polynomial of order d and degree $\phi(d)$, where $\phi(\cdot)$ is Euler-totient function.

Lemma 4.5: Let notations be defined above.

(1) If $gcd(e, p-1) = 1$, then $ord_p(2^e) = ord_p(2)$.

(2) $)x^{p^r}+1$ has no duplicate factors.

(3) For any $i \geq 1$, $Q_{p^i}(x)$ is a monic self-reciprocal polynomial of even degree.

(4) Let $i \geq 1$. If $ord_p(2) = p-1$, $Q_{p^i}(x)$ is irreducible over $GF(2^e)$. If $ord_p(2) = \frac{p-1}{2}$ is odd, then $Q_{p^i}(x) = g_i(x)g_i^*(x)$, where $g_i(x), g_i^*(x) \in GF(2^e)$ are monic irreducible polynomials and $g_i^*(x)$ is the reciprocal polynomial of $g_i(x)$.

(5) $x^{p^r}+1 = (x+1)Q_p(x)\cdots Q_{p^r}(x)$ and $\frac{x^{p^r}+1}{x+1}$ is a monic self-reciprocal polynomial.

(6) If $ord_p(2) = p-1$ or $ord_p(2) = (p-1)/2$ $((p-1)/2$ is odd), then $\frac{x^{p^r}+1}{x+1} = Q_p(x)\cdots Q_{p^r}(x)$ is a factorization in the form of (20) or (21).

Proof: (1) This can be obtained by the fact that $GF(p)^*$ is a cylic group of order $p-1$.

(2) Since $gcd(x^{p^r}+1,(x^{p^r}+1)') = gcd(x^{p^r}+1, x^{p^r-1}) = 1$, then $x^{p^r}+1$ has no duplicate factors.

(3) From its definition, $Q_{p^i}(x)$ is monic and of even degree $\phi(p^i) = p^{i-1}(p-1)$. $Q_{p^i}(x)$ is self-reciprocal, which can be found in [1].

(4) This can be obtained in [6].

(5) The factorization of $x^{p^r}+1$ can be found in [1]. $\frac{x^{p^r}+1}{x+1}$ is obviously monic. The self-reciprocal property of $\frac{x^{p^r}+1}{x+1}$ can be obtained from Lemma 4.1.

(6) From Result (5) and (4), this result can be obtained. ■

From Theorem 3.5, the Boolean function in (17) is bent if and only if the polynomial $c_f(x)$ in (18) is coprime to x^m+1. There exists an integer k satisfying that $1 \leq k \leq m/2$, $c_k \neq 0$ and $c_{k-1} = \cdots = c_1 = 0$. Then we have

$$\begin{aligned} c_f(x) =& c_k x^k (x^{m-2k} + \frac{c_{k+1}}{c_k} x^{m-2k-1} + \cdots + \frac{c_{m/2}}{c_k} x^{m/2-k} \\ &+ \cdots + \frac{c_{k+1}}{c_k} x^1 + 1) \\ =& c_k x^k C(x). \end{aligned}$$

Hence $gcd(c_f(x), x^m+1) = 1$ if and only if $gcd(C(x), x^m+1) = 1$. Note that $x^m+1 = (x^{p^r}+1)^{2^{v_0}}$. Equivalently, $gcd(C(x), x^{p^r}+1) = 1$, that is, $C(x) \in \mathfrak{P}_{m-2}(\frac{x^{p^r}+1}{x+1})$. Since $c_k \in GF(2^e)^*$, the number of bent function of the form (17) is

$$\#(GF(2^e)^*)\#(\mathfrak{P}_{m-2}(\frac{x^{p^r}+1}{x+1})). \quad (23)$$

Hence, we have the following theorem.

Theorem 4.6: Let $m = 2^{v_0}p^r$, where $v_0 \geq 1$, $r \geq 1$ and p satisfies that $ord_p(2) = p-1$ or $ord_p(2) = \frac{p-1}{2}$ ($\frac{p-1}{2}$ is odd). Let $gcd(e, p-1) = 1$. Define the Boolean function

$$f(x) = \sum_{i=1}^{\frac{m}{2}-1} Tr_1^n(c_i x^{1+2^{ei}}) + Tr_1^{n/2}(c_{m/2} x^{1+2^{n/2}}) \quad (24)$$

where $c_i \in GF(2^e)$. The number of bent functions of this form is

$$(2^e-1)2^{e\frac{m-2}{2}} \prod_{i=1}^{r} (1 - (\frac{1}{2^e})^{\frac{p^i-p^{i-1}}{2}}).$$

Proof: From Result (6) in Lemma 4.5,

$$\frac{x^{p^r}+1}{x+1} = Q_p(x) \cdots Q_{p^r}(x)$$

is the factorization of $\frac{x^{p^r}+1}{x+1}$ in the form (21) and $n_i = \phi(p^i) = p^i - p^{i-1}$ $(1 \leq i \leq r)$. From Lemma 4.4

$$\#(\mathfrak{P}_{m-2}(\frac{x^{p^r}+1}{x+1})) = 2^{e\frac{m-2}{2}} \prod_{i=1}^{r} (1 - (\frac{1}{2^e})^{\frac{p^i-p^{i-1}}{2}}). \quad (25)$$

From Identity (23), the number of bent functions defined in (24) is

$$(2^e-1)2^{e\frac{m-2}{2}} \prod_{i=1}^{r} (1 - (\frac{1}{2^e})^{\frac{p^i-p^{i-1}}{2}}).$$

Hence, this theorem follows. ■

V. Conclusion

In this paper, we present the relationship of quadratic Boolean functions with linearized permutation polynomials. A large class of quadratic bent functions is discussed and studied. Some quadratic bent functions are constructed. Further, new quadratic bent functions can be constructed from known quadratic bent functions. Finally, for special n, we present the construction and enumeration of quadratic bent functions. Our technique can be used in the study of 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] A. Canteaut and P. Charpin, “Decomposing bent functions,”IEEE Trans. Inf. Theory, vol. 49, no. 8, pp. 2004-2019, Aug. 2003.

[4] C. Carlet, “A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction,”in Advances in Cryp- tology-CRYPTO 2002 . Berlin, Germany: Springer-Verlag, 2002, vol. 2442, Lecture Notes in Computer Science, pp. 549-564.

[5] C. Carlet, P. Charpin, and V. A. Zinoviev, “Codes, bent functions and permutations suitable for DES-like cryptosystem, ”Des. Codes. Cryptogr. , vol. 15, pp. 125-156, 1998.

[6] 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.

[7] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit,“Construction of bent functions via Niho power functions,”J. Comb. Theory , ser. A, vol. 113, pp. 779-798, 2006.

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

[9] S. W. Golomb and G. Gong, “Signal design for good correlation-for wireless communication,”in Cryptography and Radar. Cambridge, U.K.: Cambridge Univ. Press, 2005.

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

[11] 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.

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

[13] 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.

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

[15] S. H. Kim and J. S. No, ”New families of binary sequences with low correlation, ”IEEE Trans. Inf. Theory , vol. 49, no. 11, pp. 3059-3065, Nov. 2003.

[16] A. Lempel and M. Cohn, “Maximal families of bent sequences,”IEEE Trans. Inf. Theory, vol. 28, pp. 865-868, Nov. 1982.

[17] 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.

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

[19] O. Ore, ”Theory of non-commutative polynomials,” Ann. of Math. 34 (1933) 480C508.

[20] O. Ore, ”On a special class of polynomials,” Trans. Amer. Math. Soc. 35 (1933) 559C584.

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

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

[23] P. Udaya,“Polyphase and frequency hopping sequences obtained from finite rings, ”Ph.D. dissertation, Indian Inst. Technol., Dep. Elect. Eng., Kanpur, India, 1992.

[24] B. Wu, Z. Liu, “Linearized polynomials over finite fields revisited,” Finite Fields Appl. 22 (2013) 79-100.

[25] 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.