AAECC (2019) 30:333–347
https://doi.org/10.1007/s00200-018-0376-9

ORIGINAL PAPER

New quadratic bent functions in polynomial forms with coefficients in extension fields

Dongmei Huang[1] · Chunming Tang[1] · Yanfeng Qi[2] · Maozhi Xu[3]

Received: 7 September 2017 / Revised: 5 November 2018 / Accepted: 12 December 2018 /
Published online: 1 January 2019

Abstract
In this paper, we first discuss the bentness of a large class of quadratic Boolean functions in polynomial form $f(x) = \sum_{i=1}^{n/2-1} \mathrm{Tr}_1^n(c_i x^{1+2^i}) + \mathrm{Tr}_1^{n/2}(c_{n/2} x^{1+2^{n/2}})$, where n is even, $c_i \in \mathrm{GF}(2^n)$ for $1 \le i \le n/2-1$ and $c_{n/2} \in \mathrm{GF}(2^{n/2})$. 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 $f(x) = \sum_{i=1}^{m/2-1} \mathrm{Tr}_1^n(c_i x^{1+2^{ei}}) + \mathrm{Tr}_1^{n/2}(c_{m/2} x^{1+2^{n/2}})$, where $n = em$, m is even, and $c_i \in \mathrm{GF}(2^e)$. The bentness of these functions is characterized and some methods for deriving new quadratic bent functions are given. Finally, when m and e satisfy some conditions, we determine the number of these quadratic bent functions.

Keywords Bent function · Boolean function · Linearized permutation polynomial · Cyclotomic polynomial · Semi-bent function

Mathematics Subject Classification 06E75 · 94A60

1 Introduction

A bent function, whose Hamming distance to the set of all affine Boolean functions equals $2^{n-1} \pm 2^{n/2-1}$, is a Boolean function with even n variables from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2)$. Further, it has maximum nonlinearity and the absolute value of its Walsh transform has a constant magnitude [24]. Nonlinearity is an important property for a

✉ Chunming Tang
tangchunmingmath@163.com

1 School of Mathematics and Information, China West Normal University, Nanchong 637002, Sichuan, China

2 School of Science, Hangzhou Dianzi University, Hangzhou 310018, Zhejiang, China

3 LMAM, School of Mathematical Sciences, Peking University, Beijing 100871, China

Boolean function in cryptographic applications. Bent functions have been extensively studied [3–7,10,15,18,27]. 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 [2,8,9,16,17,23,25]. Further, many applications of bent functions can be found in coding theory and combinatorial design [19].

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 have the value $\pm 2^{n/2}$ while the Walsh spectra of semi-bent functions are $\{0, \pm 2^{n/2+1}\}$. For an odd integer n, the Walsh spectra of semi-bent functions are $\{0, \pm 2^{(n+1)/2}\}$. The semi-bentness of quadratic Boolean functions of the form

$$f(x) = \sum_{i=1}^{\lfloor (n-1)/2 \rfloor} c_i \mathrm{Tr}_1^n \left(x^{1+2^i} \right), c_i \in \mathrm{GF}(2)$$

was studied [6,14,15]. Let $c(x) = \sum_{i=1}^{\lfloor (n-1)/2 \rfloor} c_i (x^i + x^{n-i})$. For odd n, $f(x)$ is semi-bent if and only if $\gcd(c(x), x^n + 1) = x + 1$. For even n, $f(x)$ is semi-bent if and only if $\gcd(c(x), x^n + 1) = x^2 + 1$.

For further generalization, Ma et al. [18] applied techniques from [15] and considered the quadratic Boolean functions of the form

$$f(x) = \sum_{i=1}^{n/2-1} c_i \mathrm{Tr}_1^n \left(x^{1+2^i} \right) + \mathrm{Tr}_1^{n/2} \left(x^{1+2^{n/2}} \right), \tag{1}$$

where $c_i \in \mathrm{GF}(2)$ and $\mathrm{Tr}_1^{n/2}(x)$ is the trace function from $\mathrm{GF}(2^{n/2})$ to $\mathrm{GF}(2)$. They proved that $f(x)$ is a bent function if and only if $\gcd(c(x), x^n + 1) = 1$, where $c(x) = \sum_{i=1}^{(n-2)/2} c_i (x^i + x^{n-i}) + x^{n/2}$. For some special cases of n, Yu and Gong [27] considered the concrete constructions of bent functions of the form (1) and presented some enumeration results.

Hu and Feng [10] generalized results of Ma et al. [18] and studied the quadratic Boolean functions of the form

$$f(x) = \sum_{i=1}^{m/2-1} c_i \mathrm{Tr}_1^n \left(\beta x^{1+2^{ei}} \right) + \mathrm{Tr}_1^{n/2} \left(\beta x^{1+2^{n/2}} \right), \tag{2}$$

where $c_i \in \mathrm{GF}(2), n = em, m$ is even and $\beta \in \mathrm{GF}(2^e)$. They obtained that $f(x)$ is bent if and only if $\gcd(c(x), x^m + 1) = 1$, where $c(x) = \sum_{i=1}^{m/2-1} c_i (x^i + x^{m-i}) + x^{m/2}$. Further, they presented the number of bent functions for some specified m. Note that $\beta \in \mathrm{GF}(2^e)$, then $(\beta^{2^{e-1}})^{1+2^{ei}} = \beta^{2^e} = \beta$. The function $f(x)$ of the form (2) satisfies that

$$f(x) = \sum_{i=1}^{m/2-1} c_i \mathrm{Tr}_1^n \left(\left(\beta^{2^{e-1}} x \right)^{1+2^{ei}} \right) + \mathrm{Tr}_1^{n/2} \left(\left(\beta^{2^{e-1}} x \right)^{1+2^{n/2}} \right),$$

where $c_i \in \mathrm{GF}(2)$. 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

$$f(x) = \sum_{i=1}^{n/2-1} \mathrm{Tr}_1^n(c_i x^{1+2^i}) + \mathrm{Tr}_1^{n/2}\left(c_{n/2}x^{1+2^{n/2}}\right),$$

where n is even, $c_i \in \mathrm{GF}(2^n)$ for $1 \le i \le n/2-1$ and $c_{n/2} \in \mathrm{GF}(2^{n/2})$. We present the characterization of the bentness of these functions from some specific linearized polynomials. Further, we generalize results in [10,18] and characterize the bentness of quadratic Boolean functions of the form

$$f(x) = \sum_{i=1}^{m/2-1} \mathrm{Tr}_1^n\left(c_i x^{1+2^{ei}}\right) + \mathrm{Tr}_1^{n/2}\left(c_{m/2}x^{1+2^{n/2}}\right),$$

where $n = em$, m is even, and $c_i \in \mathrm{GF}(2^e)$. Further, some examples of bent functions are given. Methods for deriving new quadratic bent functions from known quadratic bent functions are presented. Finally, we determine the number of these bent functions 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 $\mathrm{ord}_p(2) = p-1$ or $\mathrm{ord}_p(2) = (p-1)/2$ ($(p-1)/2$ is odd).

The rest of the paper is organized as follows: Sect. 2 introduces some notations and background. Section 3 gives the description of bentness of quadratic Boolean functions considered in this paper and methods of deriving new bent functions. Section 4 enumerates the number of quadratic bent functions for a special case. Finally, Sect. 5 concludes this paper.

2 Preliminaries

In this section, some notations are given first. Let $\mathrm{GF}(2^n)$ be the finite field with 2^n elements. Let $\mathrm{GF}(2^n)^*$ be the multiplicative group of $\mathrm{GF}(2^n)$. Let $e|n$ and the trace function $\mathrm{Tr}_e^n(x)$ from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2^e)$ be defined by $\mathrm{Tr}_e^n(x) = \sum_0^{n/e-1} x^{2^{ei}}$, where $x \in \mathrm{GF}(2^n)$. The trace function satisfies that

(1) $\mathrm{Tr}_e^n(x^{2^e}) = \mathrm{Tr}_e^n(x)$, where $x \in \mathrm{GF}(2^n)$.
(2) $\mathrm{Tr}_e^n(ax+by) = a\mathrm{Tr}_e^n(x) + b\mathrm{Tr}_e^n(y)$, where $x, y \in \mathrm{GF}(2^n)$ and $a, b \in \mathrm{GF}(2^e)$.

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

$$f(x) = \sum_{i=0}^{n/2-1} \mathrm{Tr}_1^n\left(c_i x^{1+2^i}\right) + \mathrm{Tr}_1^{n/2}\left(c_{n/2}x^{1+2^{n/2}}\right), \tag{3}$$

where $c_i \in \mathrm{GF}(2^n)$ for $0 \le i \le n/2-1$ and $c_{n/2} \in \mathrm{GF}(2^{n/2})$.

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

$$f(x) = \sum_{i=0}^{(n-1)/2} \mathrm{Tr}_1^n \left(c_i x^{1+2^i} \right), \tag{4}$$

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

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

$$\hat{f}(\lambda) = \sum_{x \in \mathrm{GF}(2^n)} (-1)^{f(x)+\mathrm{Tr}_1^n(\lambda x)}, \lambda \in \mathrm{GF}(2^n).$$

For a quadratic Boolean function $f(x)$ of the form (3) or (4), the distribution of the Hadamard transform can be described by the quadratic form

$$Q_f(x, y) = f(x + y) + f(x) + f(y).$$

For the quadratic form Q_f, define

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

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

Theorem 1 [6,11] *Let $f(x)$ be a quadratic Boolean function of the form (3) or (4) and $k_f = dim_{\mathrm{GF}(2)}(K_f)$. The distribution of the Hadamard transform values of $f(x)$ is given by*

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

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

Definition 1 Let $f(x)$ be a Boolean function from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2)$. Then $f(x)$ is called a bent function if for any $\lambda \in \mathrm{GF}(2^n)$, $\hat{f}(\lambda) \in \{2^{n/2}, -2^{n/2}\}$.

Bent functions only exist in the case of even n. From Theorem 1, the following result on bent functions is given below.

Corollary 1 *Let $f(x)$ be a quadratic function of the form (3) over $\mathrm{GF}(2^n)$, then $f(x)$ is bent if and only if $K_f = \{0\}$.*

3 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.

3.1 Bent functions and linearized permutation polynomials

In this subsection, we discuss the relationship between bentness of quadratic Boolean function and linearized permutation polynomials. From Theorem 1 and Corollary 1, we have the following well known result.

Theorem 2 [6,11] *The quadratic Boolean function*

$$f(x) = \sum_{i=0}^{n-1} \mathrm{Tr}_1^n \left(c_i x^{1+2^i} \right), c_i \in \mathrm{GF}(2^n)$$

is bent if and only if $L_f(x) = \sum_{i=1}^{n-1} (c_i + c_{n-i}^{2^i}) x^{2^i}$ *is a linearized permutation polynomial, i.e.,* $L_f(x) = 0$ *only has a solution 0.*

The following corollary as a direct consequence of Theorem 2 characterizes the bentness of quadratic Boolean functions.

Corollary 2 *Let* $f(x)$ *be a quadratic Boolean function defined by*

$$f(x) = \sum_{i=1}^{n/2-1} \mathrm{Tr}_1^n \left(c_i x^{1+2^i} \right) + \mathrm{Tr}_1^{n/2} \left(c_{n/2} x^{1+2^{n/2}} \right), \tag{5}$$

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

$$L_f(x) = \sum_{i=1}^{n/2-1} \left(c_i x^{2^i} + c_i^{2^{n-i}} x^{2^{n-i}} \right) + c_{n/2} x^{2^{n/2}} \tag{6}$$

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

From Corollary 2, the bentness of quadratic Boolean functions depends on the corresponding linearized permutation polynomial (6). Hence, many results and techniques on linearized permutation polynomials, such as theories of non-commutative polynomials [21,22], can be used to study quadratic bent functions. New results on linearized permutation polynomials can be found in [26]. So far, bent functions constructed of the form (5) generally satisfy that $c_i \in \mathrm{GF}(2)$. We will present some bent functions with the form (5) with $c_i \in \mathrm{GF}(2^n) \backslash \mathrm{GF}(2)$ for some i. From Corollary 2, the following corollary characterizes a class of monomial bent functions, which is a special case of Theorem 2 in [12].

Corollary 3 *Let* i *be an integer satisfying* $1 \le i \le n/2 - 1$. *Let* $\alpha \in \mathrm{GF}(2^n)^*$ *and* $n = 2^{v_0} n_0$, *where* n_0 *is odd. Let* $f(x) = \mathrm{Tr}_1^n(\alpha x^{1+2^i})$. *Then*

(1) *there exists* $\alpha \in \mathrm{GF}(2^n)$ *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*

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

In particular, let α be a primitive element in $\mathrm{GF}(2^n)$*, 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 Corollary 2, f is bent if and only if

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

Since $x \mapsto x^{2^i}$ is an isomorphism for $\mathrm{GF}(2^n)$, then $K_f = \{0\}$ if and only if $K_f^{2^i} = \{x \in \mathrm{GF}(2^n) : \alpha^{2^i} x^{2^{2i}} + \alpha x = 0\} = \{0\}$. Then $K_f^{2^i} = \{0\}$ if and only if $\alpha \notin \Gamma = \{z^{2^{i+1}} : z \in \mathrm{GF}(2^n)\}$ [12]. Note that $\mathrm{GF}(2^n)\backslash\Gamma \neq \emptyset$ if and only if $\gcd(2^i + 1, 2^n - 1) > 1$. From Lemma 11.1 in [20], $\gcd(2^i + 1, 2^n - 1) > 1$ if and only if $\gcd(2i, n) = 2 \cdot \gcd(i, n)$. Equivalently, $2^{v_0} \nmid i$. Hence, Result (1) follows. We have $\alpha \notin \Gamma$ if and only if $\alpha^{(2^n-1)/\gcd(2^i+1,2^n-1)} \neq 1$. Note that $\gcd(2^i + 1, 2^n - 1) = \frac{\gcd(2^{2i}-1,2^n-1)}{\gcd(2^i-1,2^n-1)} = 2^{\gcd(i,n)} + 1$. Hence, Result (2) follows. □

Theorem 3 *Let* $\alpha \in \mathrm{GF}(2^n)^*$ *and* $(\alpha + \alpha^{-4}) \in \mathrm{GF}(2^{n/2})$*, the Boolean function* $f(x) = \mathrm{Tr}_1^n(x^{1+2^{n/2-2}}) + \mathrm{Tr}_1^{n/2}((\alpha+\alpha^{-4})x^{1+2^{n/2}})$ *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 $T_\alpha(x) = x + \alpha x^{2^2}$ and $T_{\alpha^{-4}}(x) = x + \alpha^{-4}x^{2^2}$. 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 Corollary 2, this theorem follows. □

Remark 1 (i) If $n/2$ is even, then $3|(2^{n/2} - 1)$ and $3 \nmid (2^{n/2} + 1)$. Let w be the largest integer satisfying $3^w|(2^{n/2}-1)$ and ζ_{3^w} be a primitive 3^w-th root of unity. Take $\alpha = \beta\zeta_{3^w}^i$, where $\beta \in \mathrm{GF}(2^{n/2})$, $3 \nmid \mathrm{ord}(\beta)$ and $3 \nmid i$. Obviously, $\zeta_{3^w} \in \mathrm{GF}(2^{n/2})$ and $\alpha \in \mathrm{GF}(2^{n/2})$. Then $(\alpha+\alpha^{-4}) \in \mathrm{GF}(2^{n/2})$. It is easily verified that $\alpha^{(2^n-1)/3} \neq 1$. Hence, α satisfies Theorem 3 and $f(x)$ in Theorem 3 is a bent function.

(ii) If $n/2$ is odd, then $3|(2^{n/2} + 1)$ and $3 \nmid (2^{n/2} - 1)$. Let w be the largest integer satisfying $3^w|(2^{n/2} + 1)$. Take $\alpha = (\mathrm{Tr}_{n/2}^n(u))^{3/5}u$, where $u \in \mathrm{GF}(2^n)$, $u^{1+n/2} = 1$ and $3^w|\mathrm{ord}(u)$. Note that $5 \nmid 2^{n/2} - 1$ and $\gcd(5, \mathrm{ord}(\mathrm{Tr}_{n/2}^n(u))) = 1$. Then $(\mathrm{Tr}_{n/2}^n(u))^{3/5}$ is well defined. Since $3^w|\mathrm{ord}(u)$, $u \notin \mathrm{GF}(2^{n/2})$. Let $\lambda = \mathrm{Tr}_{n/2}^n(u) = u + u^{2^{n/2}} \in \mathrm{GF}(2^{n/2})$, then the minimal polynomial of u over $\mathrm{GF}(2^{n/2})$ is

$$u^2 + \lambda u + 1 = 0. \tag{7}$$

Since $3 \nmid (2^{n/2}-1)$, then α satisfies that $\alpha^{(2^n-1)/3} \neq 1$. From Identity (7), $\alpha+\alpha^{-4} = \lambda^{-12/5}(\lambda^4 + \lambda^2 + 1) \in \mathrm{GF}(2^{n/2})$. Hence, $f(x)$ defined in Theorem 3 is bent.

The following proposition makes a supplement to Theorem 3.

Table 1 $N_m (1 \le m \le 10)$

m	1	2	3	4	5	6	7	8	9	10
N_m	1	3	3	15	11	47	43	175	171	751

Proposition 1 *Let $b \in \mathrm{GF}(2^{n/2})$. If $b \notin \{\alpha + \alpha^{-4} : \alpha \in \mathrm{GF}(2^n)\}$. Then the Boolean function $f(x) = \mathrm{Tr}_1^n(x^{1+2^{n/2-2}}) + \mathrm{Tr}_1^{n/2}(bx^{1+2^{n/2}})$ is bent.*

Proof From the Boolean function $f(x)$, we have $L_f(x) = x^{2^{n/2-2}} + bx^{2^{n/2}} + x^{2^{n/2+2}}$. Then $L_f(x)$ is invertible if and only if $T(x) = x^{4^2} + b^{x^4} + x$ is invertible over $\mathrm{GF}(x^n)$. Suppose that $T(x)$ is not invertible. Then there exists $\alpha \in \mathrm{GF}(2^n)$ such that $T(\alpha) = 0$, i.e., $\alpha^{15} + b\alpha^3 + 1 = 0$. Hence, $b = (\alpha^{-3}) + (\alpha^{-3})^4$, which makes a contradiction. Then this proposition holds. □

Let $n = 2m$, $\mathcal{N}_M = \mathrm{GF}(2^m)\backslash\{x^{12} + \frac{1}{x^3} : x \in \mathrm{GF}(2^m)^*\}$, and $N_m = \#\mathcal{N}_m$. From Theorem 3 and Proposition 1, the Boolean function $f(x) = \mathrm{Tr}_1^n(x^{1+2^{n/2-2}}) + \mathrm{Tr}_1^{n/2}(bx^{1+2^{n/2}})$ is bent if and only if $b \in \mathcal{N}_m$, where $b \in \mathrm{GF}(2^m)$.

Example 1 Let $n = 2m = 20$. Let $\mathrm{GF}(2^n) = \mathrm{GF}(2)(\alpha)$, where α satisfies that $\alpha^{20} + \alpha^{10} + \alpha^9 + \alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha + 1 = 0$. Take $b = \alpha^{878425}$. Then $b \in \mathrm{GF}(2^m)$, $b^{10} + b^7 + b^6 + b^5 + b^4 + b^3 + b^2 + b + 1 = 0$ and $b \in \mathcal{N}_m$. Then $f(x) = \mathrm{Tr}_1^{20}(x^{1+2^8}) + \mathrm{Tr}_1^{10}(bx^{1+2^{10}})$ is bent.

When $1 \le m \le 10$, from the computer program, we have the following table of values of N_m (Table 1).

3.2 A subclass of quadratic bent functions

In this subsection, let $n = me$ and m be even. we will consider a special subclass of Boolean functions in (5). This subclass can be seen as a generalization of functions in [10,18,27] and contains more bent functions.

Theorem 4 *Let $f(x)$ be a Boolean function defined by*

$$f(x) = \sum_{i=1}^{m/2-1} \mathrm{Tr}_1^n\left(c_i x^{1+2^{ei}}\right) + \mathrm{Tr}_1^{n/2}\left(c_{m/2} x^{1+2^{n/2}}\right), \tag{8}$$

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

$$c_f(x) = \sum_{i=1}^{m/2-1} c_i\left(x + x^{m-i}\right) + c_{m/2} x^{m/2}. \tag{9}$$

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 $c_{m/2} \in \mathrm{GF}(2^e) \subseteq \mathrm{GF}(2^{n/2})$. Note that $\mathrm{Tr}_{n/2}^n(\cdot)$ is surjective from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2^{n/2})$. Then there exists $c'_{m/2} \in \mathrm{GF}(2^n)$ satisfying $c_{m/2} = \mathrm{Tr}_{n/2}^n(c'_{m/2}) = c'_{m/2} + c'^{2^{n/2}}_{m/2}$. Hence, $f(x) = \sum_{i=1}^{m/2-1} \mathrm{Tr}_1^n(c_i x^{1+2^{ei}}) + \mathrm{Tr}_1^n(c'_{m/2} x^{1+2^{n/2}})$. From the similar proof of Theorem 2, $L_f(x) = \sum_{i=1}^{m/2-1} c_i (x^{2^{ei}} + x^{2^{e(m-i)}}) + c_{m/2} x^{2^{em/2}} = \sum_{i=1}^{m-1} a_i x^{2^{ei}}$, where $a_i = \begin{cases} c_i, & 1 \le i \le m/2, \\ c_{m-i}, & m/2 < i \le m-1. \end{cases}$

Let $\alpha \in \mathrm{GF}(2^n)$ be a regular element in $\mathrm{GF}(2^e)$, i.e., $\{\alpha, \alpha^{2^e}, \alpha^{2^{e\cdot 2}}, \ldots, \alpha^{2^{e(m-1)}}\}$ is a basis of $\mathrm{GF}(2^n)$ over $\mathrm{GF}(2^e)$, 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 $m - \gcd(0 + a_1 x + a_2 x^2, \ldots, a_{m-1} x^{m-1}, x^m - 1)$ of the cyclic code over $\mathrm{GF}(2^e)$, generated by rows of A, is m, i.e. $\gcd(c_f, x^m + 1) = \gcd(0 + a_1 x + a_2 x^2, \ldots, a_{m-1} x^{m-1}, x^m - 1) = 1$. Finally, if $c_{m/2} = 0$, then $(x+1) | c_f(x)$.

Hence, this theorem follows. □

Example 2 Let $m = 10$, $e = 3$, and $n = 30$. Let $\mathrm{GF}(2^3) = Gf(2)(\beta)$, where $\beta^3 + \beta + 1 = 0$. Let $c_1 = \beta^5$, $c_2 = \beta^5$, $c_3 = \beta^4$, $c_4 = \beta^3$, and $c_5 = \beta^5$. Then $c_f(x) = \sum_1^4 c_i (x^i + x^{10-i}) + c_5 x^5$ and $\gcd(c_f(x), x^5 + 1) = 1$. From Theorem 4, the Boolean function $f(x) = \sum_{i=1}^4 \mathrm{Tr}_1^{30}(c_i x^{1+8^i}) + \mathrm{Tr}_1^{15}(c_5 x^{1+2^{15}})$ is bent. And the number of such bent functions is 28224. This can be verified by the computer program.

Corollary 4 *Let $m = 2^{v_0}$, where $v_0 \ge 1$. The Boolean function of the form (8) is bent if and only if $c_{m/2} \ne 0$. Further, the number of bent functions with this form is $(2^e - 1)2^{e(m/2-1)}$.*

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 $(x+1) \nmid c_f(x)$, i.e., $c_f(1) \ne 0$. Note that $c_f(1) = c_{m/2}$. From Theorm 4, $f(x)$ is bent if and only if $c_{m/2} \ne 0$. From the random choice of $c_i \in \mathrm{GF}(2^e)$ $(1 \le i \le m/2 - 1)$, the number of bent functions is $(2^e - 1)2^{e(m/2-1)}$. This theorem follows. □

Theorem 5 *Let $n = 2^{v_0} m_0$, where m_0 is odd. Let $\lambda \in \mathrm{GF}(2^{2e})^*$ satisfying $\lambda + \frac{1}{\lambda} \in \mathrm{GF}(2^e)^*$. Then the Boolean function $f(x) = \mathrm{Tr}_1^n(x^{1+2^{ei}}) + \mathrm{Tr}_1^{n/2}((\lambda + \frac{1}{\lambda}) x^{1+2^{n/2}})$ is bent if and only if $\lambda^{m_0/\gcd(i,m_0)} \ne 1$.*

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

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

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

Remark 2 Let $\beta \in \mathrm{GF}(2^e)^*$. Then $f(x)$ of the form (8) is bent if and only if $f_\beta(x) = \sum_{i=1}^{m/2-1} \mathrm{Tr}_1^n(\beta c_i x^{1+2^{ei}}) + \mathrm{Tr}_1^{n/2}(\beta c_{m/2} x^{1+2^{n/2}})$ is bent. Bent functions of the form (8) contain the functions studied in [10]. From the transformation $x \longmapsto \beta^{2^{e-1}} x$, $f(x)$ can be changed into $f_\beta(x)$, which explains the relationship between bent functions presented by Hu and Feng [10] and bent functions constructed by Ma et al. [18].

Theorem 6 *Let $c_i \in \mathrm{GF}(2^e)$ for $1 \leq i \leq m/2$ and $\beta \in \mathrm{GF}(2^e)$. Then $f(x)$ of the form (8) is bent if and only if $f_+(x) = f(x) + \sum_{i=1}^{m/2-1} \mathrm{Tr}_1^n(\beta x^{1+2^{ei}})$ is bent.*

Proof We have $c_{f_+}(x) = c_f(x) + \beta \sum_{i=1}^{m/2-1}(x^i + x^{m-i}) = c_f(x) + \beta(x^{m/2} + 1)\sum_{i=1}^{m/2-1} x^i$. 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 $\gcd(c_{f_+}(x), x^{m/2} + 1) = \gcd(c_f, x^{m/2} + 1)$. Hence, this theorem follows. □

From Theorem 6, we have a generalization of Theorem 5 in [10].

Corollary 5 *Let m_0 be the largest odd integer dividing m. Let $1 \leq k \leq m/2 - 1$, $d \geq 1$, $\beta_1 \in \mathrm{GF}(2^e)^*$ and $\beta_2 \in \mathrm{GF}(2^e)$. The Boolean function $f(x) = \sum_{i=1}^{m/2-1} \mathrm{Tr}_1^n(\beta_2 x^{1+2^{ei}}) + \mathrm{Tr}_1^{n/2}(\beta_1 x^{1+2^{n/2}}) + \sum_{i=1}^{k} \mathrm{Tr}_1^n(\beta_1 x^{1+2^{edi}})$ is bent if and only if $\gcd((2k+1)d, m_0) = \gcd(d, m_0)$.*

Proof From Theorem 6 and Theorem 4 in [10], this theorem follows. □

Theorem 7 *Let $a_i, b_i \in \mathrm{GF}(2^e)$ for $1 \leq i \leq m/2$. Two Boolean functions $f_1(x)$ and $f_2(x)$ are defined by $f_1(x) = \sum_{i=1}^{m/2-1} \mathrm{Tr}_1^n(a_i x^{1+2^{ei}}) + \mathrm{Tr}_1^{n/2}(a_{m/2} x^{1+2^{n/2}})$ and $f_2(x) = \sum_{i=1}^{m/2-1} \mathrm{Tr}_1^n(b_i x^{1+2^{ei}}) + \mathrm{Tr}_1^{n/2}(b_{m/2} x^{1+2^{n/2}})$. Let $(\sum_{i=1}^{m/2-1} a_i(x + x^{m-i}) + a_{m/2}x^{m/2})(\sum_{i=1}^{m/2-1} b_i(x + x^{m-i}) + b_{m/2}x^{m/2})x^{m/2} \equiv \sum_{i=0}^{m-1} c_i x^i \mod x^m + 1$, where $c_i \in \mathrm{GF}(2^e)$. 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 $c_i = \sum_{\substack{j+k \equiv i+m/2 \bmod m \\ 0 \leq j,k \leq m-1}} a_j b_k$. Further,*

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

(2) $f_{1*2}(x) = \sum_{i=1}^{m/2-1} \mathrm{Tr}_1^n(c_i x^{1+2^{ei}}) + \mathrm{Tr}_1^{n/2}(c_{m/2} x^{1+2^{n/2}})$ *is bent if and only if both* $f_1(x)$ *and* $f_2(x)$ *are bent.*

Proof Note that $c_0 = \sum_{\substack{j+k \equiv m/2 \bmod m \\ 0 \le j,k \le m-1}} a_j b_k = 0$. For $1 \le i \le m-1$, we have $c_{m-i} = \sum_{\substack{j+k \equiv m/2-i \bmod m \\ 0 \le j,k \le m-1}} a_j b_k = c_i$ 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 4, Result (2) follows. □

Corollary 6 *Let* m_0 *be the maximum odd positive integer dividing* m*, then the Boolean function*

$$\begin{aligned} f(x) =& \mathrm{Tr}_1^n(x^{1+2^{ed_1}}) + \mathrm{Tr}_1^n(x^{1+2^{ed_2}}) + \mathrm{Tr}_1^n(x^{1+2^{e(d_1+d_2+m/2)}}) \\ &+ \mathrm{Tr}_1^n(x^{1+2^{e(d_1-d_2+m/2)}}) + \mathrm{Tr}_1^{n/2}(x^{1+2^{n/2}}) \end{aligned}$$

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 7 and Theorem 4 in [10], this corollary follows. □

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

In this section, we will determine the number of bent functions of the form (8). In [10, 27], 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 2 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 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 $0 < k < n_1 + n_2$, $c_{n_1+n_2-k} = \sum_{i+j=n_1+n_2-k} a_i b_j = \sum_{(n_1-i)+(n_2-j)=k} a_{n_1-i} b_{n_2-j} = c_k$. 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 $0 < k < n_2$, $b_k \ne b_{n_2-k}$ and $b_{k-1} = b_{n_2-(k-1)}, \ldots, b_0 = b_{n_2}$. Then $0 = c_k - c_{n_1+n_2-k} = b_k - b_{n_2-k}$. 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 2 *Let $A(x), g(x) \in \mathrm{GF}(2^e)[x]$ 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 7 *Let $A(x) \in \mathrm{GF}(2^e)[x]$ be a monic self-reciprocal polynomial. Then $A(x)$ has the following factorization.*

$$\begin{aligned} A(x) =& g_1(x)g_1^*(x)\cdots g_s(x)g_s^*(x)g_{s+1}(x)\cdots g_{s+t}(x) \\ =& \widetilde{g}_1(x)\cdots\widetilde{g}_s(x)\widetilde{g}_{s+1}(x)\cdots\widetilde{g}_{s+t}(x), \end{aligned} \tag{10}$$

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

Proof From Lemmas 1 and 2, this corollary follows. □

Let the monic self-reciprocal polynomial $A(x) \in \mathrm{GF}(2^e)[x]$ without duplicate factors have the following factorization of the form (10)

$$A(x) = \widetilde{g}_1(x)\cdots\widetilde{g}_s(x)\widetilde{g}_{s+1}(x)\cdots\widetilde{g}_{s+t}(x), \tag{11}$$

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

(i) $deg(C(x)) \le k$ 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

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

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

Lemma 3 *With the previously defined notation,*

$$\#(\mathfrak{R}_k) = 2^{\frac{ek}{2}}, \quad \#(\mathfrak{P}_h(A(x))) = 2^{\frac{eh}{2}} \prod_{i=1}^{s+t} \left(1 - \left(\frac{1}{2^e}\right)^{\frac{n_i}{2}}\right).$$

Proof Note that the monic self-reciprocal polynomial $x^{2i}+a_{2i-1}x^{2i-1}+\cdots+a_ix^i+\cdots+a_1x^1+1$ 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 $0, 2, 4, 6, \ldots, k$ in $\mathfrak{R}_k$ are $1, (2^e-1), (2^e-1)(2^e)^1, (2^e-1)(2^e)^2, \ldots, (2^e-1)(2^e)^{k/2-1}$ respectively. Hence, $\#(\mathfrak{R}_k) = 1+\sum_{i=0}^{i=k/2-1}(2^e-1)(2^e)^i = 2^{\frac{ek}{2}}$.

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

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

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

From Lemma 1, for any $C(x) \in \mathfrak{M}_h(i_1, i_2, \ldots, i_k)$, $C(x)$ 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

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

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,

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

Hence, this lemma follows. □

Now we consider the number 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 $\mathrm{ord}_p(2) = p-1$ or $\mathrm{ord}_p(2) = (p-1)/2((p-1)/2 \text{ is odd})$. We first discuss the factorization of $x^{p^r}+1$ over $\mathrm{GF}(2^e)$, which is connected with cyclotomic polynomials [13]. 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. From [1,6], we have the following lemma.

Lemma 4 *With the previously defined notation, we have the following results.*

(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* $\mathrm{GF}(2^e)$. *If* $ord_p(2) = (p-1)/2$ *is odd, then* $Q_{p^i}(x) = g_i(x)g_i^*(x)$, *where* $g_i(x), g_i^*(x) \in \mathrm{GF}(2^e)$ *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* (10) *or* (11).

The following theorem presents the number of a special class of quadratic bent functions.

Theorem 8 *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* $ord_p(2) = (p-1)/2$ ($(p-1)/2$ *is odd*). *Let* $\gcd(e, p-1) = 1$. *The number of bent functions of the form* (8) *is*

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

Proof From Theorem 4, the Boolean function in (8) is bent if and only if the polynomial $c_f(x)$ in (9) 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, $\gcd(C(x), x^{p^r}+1) = 1$, i.e., $C(x) \in \mathfrak{P}_{m-2}(\frac{x^{p^r}+1}{x+1})$. Since $c_k \in \mathrm{GF}(2^e)^*$, the number of bent functions of the form (8) is

$$\#(\mathrm{GF}(2^e)^*)\#\left(\mathfrak{P}_{m-2}\left(\frac{x^{p^r}+1}{x+1}\right)\right). \tag{12}$$

From Result (6) in Lemma 4, $\frac{x^{p^r}+1}{x+1} = Q_p(x)\cdots Q_{p^r}(x)$ is the factorization of $\frac{x^{p^r}+1}{x+1}$ in the form (11) and $n_i = \phi(p^i) = p^i - p^{i-1}$ $(1 \le i \le r)$. From Lemma 3

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

From Identity (12), this theorem follows. □

Example 3 Let $m = 2p = 2\times 5$, and $e = 3$. Then $\mathrm{ord}_5(2) = 4$ and gcd(3, 4)=1. From Theorem 8, the Boolean function in (8) is bent. The number of such bent functions is 28224. This can be verified by a computer program.

Remark 3 From Remark 2, bent functions of the form (8) contain more functions than the functions defined in [10]. Under conditions in Theorem 8, the number of bent functions of the form (8) is greater than that of bent functions in Theorem 8 of [10].

5 Conclusion

In this paper, we present the relationship between quadratic Boolean functions and 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 derived from known quadratic bent functions. Finally, for special n, we present the construction and the number of quadratic bent functions. Our technique can be used in the study of semi-bent functions.

Acknowledgements The authors are very grateful to the anonymous reviewers and Prof. Teo Mora for their valuable comments and suggestions. This work is supported by the National Natural Science Foundation of China (Grant Nos. 11871058, 11531002, 11701129, 61672059). C. Tang also acknowledges support from 14E013, CXTD2014-4 and the Meritocracy Research Funds of China West Normal University. Y. Qi also acknowledges support from Zhejiang provincial Natural Science Foundation of China (LQ17A010008, LQ16A010005).

References

1. Berlekamp, E.R.: Algebraic Coding Theory, revised edn. Aegean Park, Laguna Hills (1984)
2. Boztas, S., Kumar, P.V.: Binary sequences with Gold-like correlation but larger linear span. IEEE Trans. Inf. Theory **40**, 532–537 (1994)
3. Canteaut, A., Charpin, P.: Decomposing bent functions. IEEE Trans. Inf. Theory **49**(8), 2004–2019 (2003)
4. Carlet, C.: A larger class of cryptographic Boolean functions via a study of the Maiorana–McFarland construction. In: Yung, M. (ed.) Advances in Cryptology-CRYPTO 2002. Lecture Notes in Computer Science, vol. 2442, pp. 549–564. Springer, Berlin (2002)
5. Carlet, C., Charpin, P., Zinoviev, V.A.: Codes, bent functions and permutations suitable for DES-like cryptosystem. Des. Codes. Cryptogr. **15**, 125–156 (1998)
6. Charpin, P., Pasalic, E., Tavernier, C.: On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inf. Theory **51**(12), 4286–4298 (2005)
7. Dobbertin, H., Leander, G., Canteaut, A., Carlet, C., Felke, P., Gaborit, P.: Construction of bent functions via Niho power functions. J. Comb. Theory, Ser. A **113**, 779–798 (2006)

8. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inf. Theory **14**(1), 154–156 (1968)
9. Golomb, S.W., Gong, G.: Signal Design for Good Correlation: for Wireless Communication, Cryptography and Radar. Cambridge University Press, Cambridge (2005)
10. Hu, H., Feng, D.: On quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory **53**(7), 2610–2615 (2007)
11. Helleseth, T., Kumar, P.V.: Sequences with low correlation. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, vol. 2, pp. 1765–1853. North-Holland, Amsterdam (1998)
12. Leander, G.: Monomial bent functions. IEEE Trans. Inf. Theory **52**(2), 738–743 (2006)
13. Lidl, R., Niederreiter, H.: Finite fields. In: Lidl, R., Niederreiter, H., Cohn, P.M. (eds.).). Encyclopedia of Mathematics and Its Applications, 20th edn. Addison-Wesley, Reading (1983)
14. Khoo, K., Gong, G., Stinson, D.R.: A new family of Gold-like sequences. In: Proceedings of IEEE International Symposium Information Theory, Lausanne, Switzerland, p. 181 (2002)
15. Khoo, K., Gong, G., Stinson, D.R.: A new characterization of semi-bent and bent functions on finite fields. Des. Codes. Cryptogr. **38**(2), 279–295 (2006)
16. Kim, S.H., No, J.S.: New families of binary sequences with low correlation. IEEE Trans. Inf. Theory **49**(11), 3059–3065 (2003)
17. Lempel, A., Cohn, M.: Maximal families of bent sequences. IEEE Trans. Inf. Theory **28**, 865–868 (1982)
18. Ma, W., Lee, M., Zhang, F.: A new class of bent functions. IEICE Trans. Fundam. **E88–A**(7), 2039–2040 (2005)
19. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
20. McEliece, R.J.: Finite Fields for Computer Scientists and Engineers. Kluwer, Dordrecht (1987)
21. Ore, O.: Theory of non-commutative polynomials. Ann. Math. **34**, 480–508 (1933)
22. Ore, O.: On a special class of polynomials. Trans. Am. Math. Soc. **35**, 559–584 (1933)
23. Olsen, J.D., Scholtz, R.A., Welch, L.R.: Bent-function sequences. IEEE Trans. Inf. Theory **28**(6), 858–864 (1982)
24. Rothaus, O.S.: On bent functions. J. Comb. Theory A **20**, 300–305 (1976)
25. Udaya, P.: Polyphase and frequency hopping sequences obtained from finite rings, Ph.D. Dissertation, Department of Electrical Engineering, Indian Institute of Technology, Kanpur, India (1992)
26. Wu, B., Liu, Z.: Linearized polynomials over finite fields revisited. Finite Fields Appl. **22**, 79–100 (2013)
27. Yu, N.Y., Gong, G.: Constructions of quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory **52**(7), 3291–3299 (2006)