New Constructions of Quadratic Bent Functions in Polynomial Form

Nian Li, Xiaohu Tang, *Member, IEEE*, and Tor Helleseth, *Fellow, IEEE*

***Abstract*— New quadratic bent functions in polynomial form are constructed in this paper. The constructions give new Boolean bent, generalized Boolean bent and p-ary bent functions. Based on $\mathbb{Z}_4$-valued quadratic forms, a simple method provides several new constructions of generalized Boolean bent functions. From these generalized Boolean bent functions a method is presented to transform them into Boolean bent and semi-bent functions. Moreover, many new p-ary bent functions can also be obtained by applying similar methods.**

***Index Terms*— Boolean bent function, Galois ring, generalized Boolean function, p-ary bent function, quadratic form.**

I. Introduction

BOOLEAN bent functions were introduced by Rothaus in 1976 [18]. Let $\mathbb{Z}_l = \{0, 1, \ldots, l-1\}$ be the ring of integers modulo l. An m-variable Boolean function from $\mathbb{Z}_2^m$ to $\mathbb{Z}_2$ is bent if it has maximal Hamming distance to the set of affine Boolean functions. Boolean bent functions have attracted much attention due to their important applications in coding theory, cryptography and sequence design. As a logical extension of Rothaus' notion of a bent function, Kumar, Scholtz and Welch generalized it to p-ary bent functions from $\mathbb{Z}_p^m$ to $\mathbb{Z}_p$ [13], where p is an integer. In 2009, by adopting the viewpoint of cyclic codes over Galois rings [20], Schmidt introduced the generalized Boolean bent functions from $\mathbb{Z}_2^m$ to $\mathbb{Z}_p$. When $p = 4$, Solé and Tokareva have shown recently close connections between Boolean bent and generalized Boolean bent functions [21].

Let $\mathbb{F}_q$ be the finite field with $q = p^m$ elements, where p is a prime and m is a positive integer. Several classes of bent or semi-bent functions in polynomial form have been constructed using the theory of quadratic forms over $\mathbb{F}_q$. Let $f(x)$ be a quadratic function over the finite field $\mathbb{F}_q$ defined by

$$f(x)=\begin{cases}\sum_{i=1}^{(m-1)/2} tr_1^m(c_i x^{p^i+1}), & \text{odd } m,\\ \sum_{i=1}^{m/2-1} tr_1^m(c_i x^{p^i+1}) + tr_1^{m/2}(c_{m/2} x^{p^{m/2}+1}), & \text{even } m,\end{cases}$$

where $c_i \in \mathbb{F}_p$ and $tr_n^m(x) = \sum_{i=0}^{m/n-1} x^{p^{ni}}$ is the trace function from $\mathbb{F}_{p^m}$ to its subfield $\mathbb{F}_{p^n}$. The issue of choosing the coefficients c_i such that $f(x)$ is bent or semi-bent has been discussed in various papers. When $p = 2$ and m is even, a necessary and sufficient condition for $f(x)$ being bent was given in [16]. This line of work was further investigated in [23] by Yu and Gong who established the bentness of $f(x)$ for some special values of m, and Hu *et. al.* in [11] generalized it for general even m. Some similar results on semi-bent functions $f(x)$ were given in [12] when m is odd. Let k be a positive integer, a modified version of $f(x)$, say $g(x)$ was discussed in [2] for $p = 2$ and $k = 1$, where $g(x)$ is defined by

$$g(x) = \sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} tr_1^m(c_i x^{1+p^{ki}}). \tag{1}$$

For any odd prime p, similar conditions such that $f(x)$ is p-ary bent were given in [7], [12], and some results were obtained for special m [12], [15]. Helleseth and Kholosha proved that $g(x)$ with $c_i \in \mathbb{F}_q$ and $k = 1$ is bent if and only if a corresponding $m \times m$ symmetric matrix is nonsingular [7], and they also presented another necessary and sufficient condition such that $g(x)$ with $c_i \in \mathbb{F}_p$ and $k = 1$ is bent. For more p-ary bent functions, the reader is referred to [6] and [8]–[10].

In this paper, we first investigate a class of generalized Boolean bent functions of the form

$$Q(x) = Tr_1^m(x + 2\sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} c_i x^{1+2^{ki}}),\ c_i \in \mathbb{Z}_2,\ x \in \mathbb{L}, \tag{2}$$

where $Tr_1^m(\cdot)$ is the trace function from the Galois ring $\mathbb{R} = \mathbb{GR}(4, m)$ to $\mathbb{Z}_4$, and $\mathbb{L}$ is the Teichmüller set of $\mathbb{R}$. A necessary and sufficient condition concerning the bentness of $Q(x)$ is given based on the theory of $\mathbb{Z}_4$-valued quadratic forms [19]. By choosing the c_i's appropriately, new generalized Boolean bent functions of the form (2) can be obtained. In addition, a method to construct such generalized Boolean bent functions is also presented by means of some simple polynomials over finite fields.

Manuscript received January 14, 2012; revised June 19, 2013; accepted July 6, 2014. Date of publication July 17, 2014; date of current version August 14, 2014. X. Tang was supported in part by the Chinese Ministry of Education through the Key Grant Project under Grant 311031 and in part by the Innovative Research Team of Sichuan Province under Grant 2011JTD0007. T. Helleseth was supported in part by the Norwegian Research Council and in part by the High-End Foreign-Expert Program, through the State Administration of Foreign Experts Affairs, China. This paper was presented at the 2012 IEEE International Symposium on Information Theory.

N. Li and X. Tang are with the Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, Chengdu 610031, China (e-mail: nianli.2010@gmail.com; xhutang@swjtu.edu.cn).

T. Helleseth is with the Department of Informatics, University of Bergen, Bergen N-5020, Norway (e-mail: tor.helleseth@ii.uib.no).

Communicated by J.-P. Tillich, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2014.2339861

0018-9448 © 2014 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Further, by virtue of the links between generalized Boolean bent over $\mathbb{Z}_4$ and Boolean bent functions given by Solé and Tokareva in [21], new Boolean bent and semi-bent functions of the form

$$f_Q(x) = p(x) + \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} tr_1^m(c_i x^{1+2^{ki}}),\ c_i \in \mathbb{F}_2,\ x \in \mathbb{F}_{2^m} \quad (3)$$

are obtained in this paper, where $p(x)$ is defined as

$$p(x) = \begin{cases} \sum_{i=1}^{(m-1)/2} tr_1^m(x^{2^i+1}), & \text{odd } m, \\ \sum_{i=1}^{m/2-1} tr_1^m(x^{2^i+1}) + tr_1^{m/2}(x^{2^{m/2}+1}), & \text{even } m. \end{cases} \quad (4)$$

Solé and Tokareva's results together with our discussions show that the function $f_Q(x)$ is bent (resp. semi-bent) if $Q(x)$ is generalized Boolean bent with even (resp. odd) m.

The third contribution of this paper is that new p-ary quadratic bent functions of the form (1) can also be obtained by the same techniques used in the construction of generalized Boolean bent functions. As a result, several new p-ary quadratic bent functions are generated by choosing the c_i's appropriately, and a method to construct such bent functions is also given, which can produce many quadratic bent functions in a very simple way.

The remainder of this paper is organized as follows. Section II gives some preliminaries. In Section III, we derive a necessary and sufficient condition for the bentness of $Q(x)$, obtain some concrete generalized Boolean bent functions through choosing the c_i's appropriately, and propose a simple method to construct generalized Boolean bent functions of the form (2). In Section IV, as an application of Solé and Tokareva's result to $Q(x)$, several classes of new Boolean bent and semi-bent functions are obtained. By the same techniques used to construct generalized Boolean bent functions, new p-ary quadratic bent functions of the form (1) are obtained in Section V, and Section VI gives some concluding remarks.

II. Preliminaries

A. Galois Ring

Let $\mu : \mathbb{Z}_4 \to \mathbb{Z}_2$ be the modulus 2 reduction. A monic polynomial $h(x) = \sum_{i=0}^{m} h_i x^i$ of degree m in $\mathbb{Z}_4[x]$ is called primitive basic irreducible if $h(x)$ divides $x^{2^m-1} - 1 \pmod 4$ and its reduction $\sum_{i=0}^{m} \mu(h_i) x^i$ is primitive irreducible in $\mathbb{Z}_2[x]$, please refer to [4] and [22] for more details. The quiet ring $\mathbb{Z}_4[x]/(h(x))$, denoted by $\mathbb{R} = \mathbb{GR}(4, m)$, is called Galois ring of order 4^m with characteristic 4.

Let ξ be a root of $h(x)$, then $\xi^{2^m-1} = 1$ and the Galois ring can also be defined as $\mathbb{Z}_4[\xi]$. Then, it can be readily verified that every element $z \in \mathbb{R}$ can be uniquely expressed in the form

$$z = x + 2y, \quad x, y \in \mathbb{L},$$

where $\mathbb{L}$ is the Teichmüller set of $\mathbb{R}$ defined by $\mathbb{L} = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$. Notice that $\mathbb{R}$ is a local ring and $2\mathbb{R}$ is its unique maximal ideal. Thus, the mapping μ induces a homomorphism from the Galois ring $\mathbb{R}$ to the finite field $\mathbb{F}_{2^m}$ with 2^m elements if we identify $\mathbb{R}/2\mathbb{R}$ with $\mathbb{F}_{2^m}$ by taking the elements of $\mathbb{F}_{2^m}$ to be $\{\mu(x) : x \in \mathbb{L}\}$. For simplicity, $\mu(x)$ is sometimes denoted by $\overline{x}$.

The trace function $Tr_1^m(x) : \mathbb{R} \to \mathbb{Z}_4$ is defined as

$$Tr_1^m(x + 2y) = \sum_{j=0}^{m-1} (x^{2^j} + 2y^{2^j}), \quad x, y \in \mathbb{L}.$$

The relation between the trace function over $\mathbb{Z}_4$ and the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is well known:

1) $\overline{Tr_1^m(x)} = tr_1^m(\overline{x})$;
2) $2Tr_1^m(x) = 2tr_1^m(\overline{x})$.

It should be noted that $\mathbb{L}$ is not closed under addition. Specially, for any $x, y \in \mathbb{L}$, there exists a unique $z \in \mathbb{L}$ such that $z = x + y + 2\sqrt{xy}$. For convenience in this paper we define a new operation $\oplus$ on $\mathbb{L}$ by

$$x \oplus y = x + y + 2\sqrt{xy}.$$

Then $(\mathbb{L}, \oplus, \cdot)$ is isomorphic to the finite field $(\mathbb{F}_{2^m}, +, \cdot)$.

B. Three Kinds of Bent Functions

An m-variable Boolean function f is a mapping from $\mathbb{Z}_2^m$ to $\mathbb{Z}_2$, where $\mathbb{Z}_l = \{0, 1, \ldots, l-1\}$ is the ring of integers modulo l. The Walsh transform of f is defined by

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{Z}_2^m} (-1)^{f(x)+\lambda \cdot x}, \quad \lambda \in \mathbb{Z}_2^m,$$

where $\lambda \cdot x$ denotes the inner product of two vectors λ and x.

Definition 1: ([2], [18]) A Boolean function f is bent if $|\widehat{f}(\lambda)| = 2^{m/2}$ for all $\lambda \in \mathbb{Z}_2^m$. It is called semi-bent if $\widehat{f}(\lambda) \in \{0, \pm 2^{(m+1)/2}\}$ for all $\lambda \in \mathbb{Z}_2^m$.

As an extension of Boolean bent functions, Kumar, Scholtz and Welch generalized Boolean bent functions to p-ary bent functions from $\mathbb{Z}_p^m$ to $\mathbb{Z}_p$ [13], where p is an integer. Let $f : \mathbb{Z}_p^m \to \mathbb{Z}_p$ be a p-ary function in m variables, and w be a primitive p-th root of unity. The Walsh transform of f is

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{Z}_p^m} w^{f(x)-\lambda \cdot x}, \quad \lambda \in \mathbb{Z}_p^m.$$

Definition 2: ([13]) The p-ary function f is bent if $|\widehat{f}(\lambda)| = p^{m/2}$ for all $\lambda \in \mathbb{Z}_p^m$.

Another extension of a Boolean bent function was introduced by Schmidt in [20]. A generalized Boolean function f is a mapping from $\mathbb{Z}_2^m$ to $\mathbb{Z}_{2^s}$, and its Walsh transform is given by

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{Z}_2^m} w^{f(x)} (-1)^{\lambda \cdot x}, \quad \lambda \in \mathbb{Z}_2^m,$$

where s is a positive integer and w is a primitive 2^s-th root of unity.

Definition 3: ([20]) The generalized Boolean function f is bent if $|\widehat{f}(\lambda)| = 2^{m/2}$ for all $\lambda \in \mathbb{Z}_2^m$.

In this paper, we mainly focus on the constructions of Boolean bent functions, p-ary bent functions, where p is an odd prime, and generalized Boolean bent functions over $\mathbb{Z}_4$.

For any prime p, the Walsh transform of a function f from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ is defined by

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_{p^m}} w^{f(x) - tr_1^m(\lambda x)}, \quad \lambda \in \mathbb{F}_{p^m}.$$

It is well known that the finite field $\mathbb{F}_{p^m}$ is isomorphic to $\mathbb{F}_p^m$ through the choice of a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$. Hence, any p-ary function f in m variables can be represented by a function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ (2-ary function means Boolean function). Moreover, the Walsh transform of a function f from $\mathbb{F}_p^m$ to $\mathbb{F}_p$ is equivalent to that of its associated function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. For the same reason, let $i = \sqrt{-1}$, we can consider the Walsh transform of a generalized Boolean function f over $\mathbb{L}$ instead of $\mathbb{Z}_2^m$ as below

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{L}} i^{f(x) + 2Tr_1^m(\lambda x)}, \quad \lambda \in \mathbb{L}.$$

Solé and Tokareva recently studied the connections between Boolean bent and generalized Boolean bent functions over $\mathbb{Z}_4$, and obtained the following results.

Lemma 1: ([21]) Let $u(x)$ be a generalized Boolean function over $\mathbb{Z}_4$ and $u(x) = a(\overline{x}) + 2b(\overline{x})$ be its 2-adic expansion, where $x \in \mathbb{L}$, $a(\cdot)$ and $b(\cdot)$ are Boolean functions over $\mathbb{F}_{2^m}$. Then,

1) $2|\widehat{u}(\lambda)|^2 = \widehat{a}^2(\overline{\lambda}) + \widehat{a+b}^2(\overline{\lambda})$ for all $\lambda \in \mathbb{L}$;
2) If m is even, then $u(x)$ (with $x \in \mathbb{L}$) is bent if and only if both $b(x)$ and $a(x) + b(x)$ (with $x \in \mathbb{F}_{2^m}$) are bent.

C. $\mathbb{Z}_4$-Valued Quadratic Form

A symmetric bilinear form on $\mathbb{L}$ is a mapping $B : \mathbb{L} \times \mathbb{L} \to \mathbb{Z}_2$ with two properties

1) $B(x, y) = B(y, x)$;
2) $B(x \oplus y, z) = B(x, z) \oplus B(y, z)$.

Specifically, B is called alternating if $B(x, x) = 0$ for all $x \in \mathbb{L}$.

The rank of B is defined as $\text{rank}(B) = m - \dim_{\mathbb{Z}_2}(\text{rad}(B))$, where

$$\text{rad}(B) = \{x \in \mathbb{L} : B(x, y) = 0, \quad \forall \ y \in \mathbb{L}\}. \tag{5}$$

Definition 4: ([1]) A $\mathbb{Z}_4$-valued quadratic form is a mapping $F : \mathbb{L} \to \mathbb{Z}_4$ that satisfies

1) $F(0) = 0$, and
2) $F(x \oplus y) = F(x) + F(y) + 2B(x, y)$,

where $B : \mathbb{L} \times \mathbb{L} \to \mathbb{Z}_2$ is a symmetric bilinear form. The quadratic form F is called alternating if B is alternating, and the rank of the $\mathbb{Z}_4$-valued quadratic form F is defined as $\text{rank}(F) = \text{rank}(B)$.

If F is alternating, it is well known that the Walsh distribution completely depends on its rank [5]. Schmidt developed the theory of $\mathbb{Z}_4$-valued quadratic form and established similar results when f is nonalternating, see [19] for more details, from which one can easily get the following result.

Lemma 2: ([19]) For a $\mathbb{Z}_4$-valued quadratic form $F(x)$, $F(x)$ is generalized Boolean bent if and only if $F(x)$ is of full rank.

III. New Generalized Boolean Bent Functions Over $\mathbb{Z}_4$

In this section, for any positive integer k, we discuss the generalized Boolean functions of the form

$$Q(x) = Tr_1^m(x + 2\sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} c_i x^{1+2^{ki}}), \quad c_i \in \mathbb{Z}_2, \quad x \in \mathbb{L}$$

based on the theory of $\mathbb{Z}_4$-valued quadratic forms.

Firstly, we need the following lemma.

Lemma 3: ([17, p.118]) Let $G(x) = \sum_{i=0}^{m-1} \lambda_i x^{p^i} \in \mathbb{F}_p[x]$. Then $G(x) = 0$ has only one root in $\mathbb{F}_{p^m}$ if and only if $\gcd(\sum_{i=0}^{m-1} \lambda_i x^i, x^m - 1) = 1$.

According to Definition 4, one can verify that $Q(x)$ is a $\mathbb{Z}_4$-valued quadratic form, and its corresponding symmetric bilinear form is given by

$$\begin{aligned} 2B(x, y) &= Q(x \oplus y) - Q(x) - Q(y) \\ &= 2Tr_1^m(xy + \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} (c_i x^{2^{ki}} y + c_i x y^{2^{ki}})). \end{aligned}$$

Recall that $2Tr_1^m(x) = 2tr_1^m(\overline{x})$ and $\mathbb{L}$ is isomorphic to the finite field $\mathbb{F}_{2^m}$ under the mapping μ, therefore we discuss the above equality over the finite field $\mathbb{F}_{2^m}$ instead of $\mathbb{L}$ in order to be consistent with Lemma 3. Then by (5), to determine the rank of $Q(x)$, we have to consider the roots of

$$x + \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} (c_i x^{2^{ki}} + c_i x^{2^{-ki}}) = 0, \ x \in \mathbb{F}_{2^m}. \tag{6}$$

Since $x^{2^{-ki}} = x^{2^{m-ki}} = x^{2^{(m-i)k}}$ if $x \in \mathbb{F}_{2^m}$, then (6) can be rewritten as

$$x + \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} (c_i x^{2^{ki}} + c_i x^{2^{(m-i)k}}) = 0, \ x \in \mathbb{F}_{2^m}. \tag{7}$$

According to Lemma 2, $Q(x)$ is bent if and only if it has full rank, i.e., (7) has only one root in $\mathbb{F}_{2^m}$. By Lemma 3, one has that (7) has only one root in $\mathbb{F}_{2^m}$ if and only if $\gcd(c(x^k), x^m - 1) = 1$, where

$$c(x) = 1 + \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} (c_i x^i + c_i x^{m-i}) \in \mathbb{F}_2[x]. \tag{8}$$

From this discussion we obtain the following result.

Theorem 1: Let m and k be positive integers. Then the generalized Boolean function $Q(x)$ is bent if and only if $\gcd(c(x^k), x^m - 1) = 1$, where $c(x)$ is defined by (8).

In what follows we give some specific values on $c_i, 1 \le i \le \lfloor \frac{m-1}{2} \rfloor$, and discuss the bentness of the function $Q(x)$ of the form (2). To do this, we need the following fact. Let p be a prime and m, k, r be positive integers, if $p \nmid r$, then for the polynomials over $\mathbb{F}_p[x]$, we have

$$\gcd(\frac{x^{rk} - 1}{x^k - 1}, x^m - 1) = \frac{x^{\gcd(m, rk)} - 1}{x^{\gcd(m,k)} - 1}. \tag{9}$$

Observe that $\frac{x^{rk}-1}{x^k-1} = 1 + x^k + x^{2k} + \cdots + x^{(r-1)k} \equiv r \pmod{x^k-1}$. Thus $\gcd(\frac{x^{rk}-1}{x^k-1}, x^k-1) = 1$ if $p \nmid r$. This leads to $\gcd(x^{rk}-1, x^m-1) = \gcd(\frac{x^{rk}-1}{x^k-1}, x^m-1) \cdot \gcd(x^k-1, x^m-1)$. Thus, (9) holds for $p \nmid r$ due to $\gcd(x^k-1, x^m-1) = x^{\gcd(m,k)} - 1$. According to (9), one has that $\gcd(\frac{x^{rk}-1}{x^k-1}, x^m-1) = 1$ if and only if $\gcd(m, rk) = \gcd(m, k)$. This will be frequently used to prove our results.

Corollary 1: Let m and k be positive integers, then

$$Q(x) = Tr_1^m(x + 2x^{1+2^{2k}} + 2x^{1+2^{3k}}), \quad x \in \mathbb{L},$$

is bent if and only if $\gcd(m, 3k) = \gcd(m, k)$.

Proof: The $c(x)$ associated to $Q(x)$ by (8) is given by $c(x) = 1 + x^2 + x^3 + x^{m-3} + x^{m-2}$ and then

$$\begin{aligned}\gcd(c(x^k), x^m - 1) &= \gcd(c(x^k) \cdot x^{3k}, x^m - 1)\\ &= \gcd(x^{6k} + x^{5k} + x^{3k} + x^k + 1, x^m - 1)\\ &= \gcd((\frac{x^{3k}-1}{x^k-1})^3, x^m - 1).\end{aligned}$$

This implies $\gcd(c(x^k), x^m - 1) = 1$ if and only if $\gcd(\frac{x^{3k}-1}{x^k-1}, x^m - 1) = 1$, i.e., $\gcd(m, 3k) = \gcd(m, k)$ according to (9). Then the result follows from Theorem 1. This completes the proof. ∎

Corollary 2: Let m, k and t be positive integers with even (resp. odd) m and $t < \frac{m-2}{4}$ (resp. $\frac{m-1}{2}$), then

$$Q(x) = Tr_1^m(x + 2\sum_{i=0}^{t} x^{1+2^{(2i+1)k}}), \quad x \in \mathbb{L},$$

is bent if and only if $\gcd(m, (2t+1)k) = \gcd(m, k)$ and $\gcd(m, (2t+3)k) = \gcd(m, k)$.

Proof: For this case, according to (8), one obtains that

$$c(x) = 1 + x + x^3 + \cdots + x^{2t+1} + x^{m-(2t+1)} + \cdots + x^{m-1}.$$

Observe that $\gcd(c(x), x^m - 1) = \gcd(c(x) \cdot x^{2t+1}, x^m - 1)$ and $c(x) \cdot x^{2t+1} \pmod{x^m-1} = x^{2t+1}(1 + x + x^3 + \cdots + x^{2t+1}) + (1 + x^2 + x^4 + \cdots + x^{2t})$. By the equality $1 + x + x^2 + \cdots + x^{2t+1} = \frac{x^{2t+2}-1}{x-1}$, one has

$$\begin{aligned}&c(x) \cdot x^{2t+1} \bmod (x^m - 1)\\ &\quad= (x^{2t+1} - 1)(1 + x + x^3 + \cdots + x^{2t+1}) + \frac{x^{2t+2} - x}{x - 1}\\ &\quad= \frac{x^{2t+1} - 1}{x - 1}(1 + x + x^2 + \cdots + x^{2t+2})\\ &\quad= \frac{x^{2t+1} - 1}{x - 1} \cdot \frac{x^{2t+3} - 1}{x - 1}\end{aligned}$$

which implies

$$\begin{aligned}\gcd(c(x^k), x^m - 1) &= \gcd(c(x^k) \cdot x^{(2t+1)k}, x^m - 1)\\ &= \gcd(\frac{x^{(2t+1)k}-1}{x^k - 1} \cdot \frac{x^{(2t+3)k}-1}{x^k-1}, x^m - 1).\end{aligned}$$

Then the result follows from (9) and Theorem 1. This completes the proof. ∎

Corollary 3: Let m, k and t be positive integers with even (resp. odd) m and $t < \frac{m}{4}$ (resp. $\frac{m-1}{2}$), then

$$Q(x) = Tr_1^m(x + 2x^{1+2^k} + 2\sum_{i=1}^{t} x^{1+2^{2ik}}), \quad x \in \mathbb{L},$$

is bent if and only if $\gcd(m, (2t-1)k) = \gcd(m, k)$ and $\gcd(m, (2t+3)k) = \gcd(m, k)$.

Proof: According to Theorem 1 and (8), to prove this result, it is sufficient to prove that $\gcd(c(x^k), x^m - 1) = 1$ if and only if $\gcd(m, (2t-1)k) = \gcd(m, k)$ and $\gcd(m, (2t+3)k) = \gcd(m, k)$, where

$$c(x) = 1 + x + x^2 + \cdots + x^{2t} + x^{m-2t} + \cdots + x^{m-2} + x^{m-1}.$$

To calculate $\gcd(c(x^k), x^m - 1)$, similar as in Corollary 2, we consider $c(x) \cdot x^{2t} \pmod{x^m-1}$ instead of $c(x)$. Through a detailed computation, we have $c(x) \cdot x^{2t} \pmod{x^m-1} = 1 + x^2 + x^4 + \cdots + x^{2t-2} + x^{2t-1} + x^{2t} + x^{2t+1} + x^{2t+2} + x^{2t+4} + \cdots + x^{4t}$ which can also be rewritten as $(1 + x + x^2 + \cdots + x^{2t+2}) + (x + x^3 + \cdots + x^{2t-3}) + x^{2t+4}(1 + x^2 + \cdots + x^{2t-4})$. Then by $1 + x + x^2 + \cdots + x^{2t+2} = \frac{x^{2t+3}-1}{x-1}$, one can derive

$$\begin{aligned}&c(x) \cdot x^{2t} \bmod (x^m - 1)\\ &\quad= \frac{x^{2t+3} - 1}{x - 1} + (x^{2t+4} - x)(1 + x^2 + \cdots + x^{2t-4})\\ &\quad= \frac{x^{2t+3} - 1}{x - 1}(1 + x(x-1)(1 + x^2 + \cdots + x^{2t-4}))\\ &\quad= \frac{x^{2t+3} - 1}{x - 1}(1 + x + x^2 + \cdots + x^{2t-2})\\ &\quad= \frac{x^{2t+3} - 1}{x - 1} \cdot \frac{x^{2t-1} - 1}{x - 1}.\end{aligned}$$

This leads to

$$\begin{aligned}\gcd(c(x^k), x^m - 1) &= \gcd(c(x^k) \cdot x^{2tk}, x^m - 1)\\ &= \gcd(\frac{x^{(2t+3)k} - 1}{x^k - 1} \cdot \frac{x^{(2t-1)k} - 1}{x^k - 1}, x^m - 1).\end{aligned}$$

Therefore, according to (9) and Theorem 1, the desired result is obtained. This completes the proof. ∎

Corollary 4: Let m and k be positive integers with $1 \le t < m/2$, then

$$Q(x) = Tr_1^m(x + 2\sum_{i=1}^{t} x^{1+2^{ik}}), \quad x \in \mathbb{L},$$

is bent if and only if $\gcd(m, (2t+1)k) = \gcd(m, k)$.

Proof: For the $Q(x)$ given in this case, by (8), one obtains that $c(x) = 1 + x + x^2 + \cdots + x^t + x^{m-t} + \cdots + x^{m-2} + x^{m-1}$ and $c(x) \cdot x^t \pmod{x^m-1} = (1 + x + x^2 + \cdots + x^t) \cdot x^t + (1 + x + x^2 + \cdots + x^{t-1}) = 1 + x + x^2 + \cdots + x^{2t} = \frac{x^{2t+1}-1}{x-1}$. This implies

$$\begin{aligned}\gcd(c(x^k), x^m - 1) &= \gcd(c(x^k) \cdot x^{tk}, x^m - 1)\\ &= \gcd(\frac{x^{(2t+1)k} - 1}{x^k - 1}, x^m - 1),\end{aligned}$$

and then the result follows from (9) and Theorem 1. This completes the proof. ∎

Note that by choosing different values for the c_i's, $1 \le i \le \lfloor \frac{m-1}{2} \rfloor$, different generalized Boolean bent functions can be obtained if $\gcd(c(x^k), x^m - 1) = 1$, where $c(x)$ is defined by (8). Thus, in order to construct generalized Boolean bent functions, in the following we present a simple method to produce the polynomial $c(x)$ of the form (8) such that the condition $\gcd(c(x^k), x^m - 1) = 1$ can be easily determined.

$$e^3(5,x) = x^6\big(1+(x^2+x^{-2})+(x^5+x^{-5})+(x^6+x^{-6})\big),$$
$$e^2(3,x)e(7,x) = x^5\big(1+(x+x^{-1})+(x^4+x^{-4})+(x^5+x^{-5})\big),$$
$$e(3,x)e(5,x)e(7,x) = x^6\big(1+(x^3+x^{-3})+(x^5+x^{-5})+(x^6+x^{-6})\big). \quad (10)$$

For any positive integer j, define $e(j,x) = \frac{x^j-1}{x-1} \in \mathbb{F}_2[x]$. Then, from these simple polynomials $e(j,x)$ over $\mathbb{F}_2$, many polynomials of the form (8) can be derived. For example, from $e(3,x)$, $e(5,x)$ and $e(7,x)$, we can easily have (10), as shown at the top of this page.

According to Theorem 1 and (10), new generalized Boolean bent functions can be obtained as follows.

Corollary 5: Let m and k be positive integers, then we have

1) $Q(x) = Tr_1^m(x + 2x^{1+2^{2k}} + 2x^{1+2^{5k}} + 2x^{1+2^{6k}})$ is bent if and only if $\gcd(m,5k) = \gcd(m,k)$;
2) $Q(x) = Tr_1^m(x + 2x^{1+2^k} + 2x^{1+2^{4k}} + 2x^{1+2^{5k}})$ is bent if and only if $\gcd(m,3k) = \gcd(m,k)$, and $\gcd(m,7k) = \gcd(m,k)$;
3) $Q(x) = Tr_1^m(x + 2x^{1+2^{3k}} + 2x^{1+2^{5k}} + 2x^{1+2^{6k}})$ is bent if and only if $\gcd(m,3k) = \gcd(m,k)$, $\gcd(m,5k) = \gcd(m,k)$, and $\gcd(m,7k) = \gcd(m,k)$.

Proof: We only give the proof for Case 1) since the other cases can be proven similarly. By Theorem 1 and (8), $Q(x) = Tr_1^m(x + 2x^{1+2^{2k}} + 2x^{1+2^{5k}} + 2x^{1+2^{6k}})$ is bent if and only if $\gcd(c(x^k), x^m - 1) = 1$, where $c(x) = 1 + x^2 + x^5 + x^6 + x^{m-6} + x^{m-5} + x^{m-2}$. Observe that $c(x) \bmod (x^m - 1) = \big(1 + (x^2 + x^{-2}) + (x^5 + x^{-5}) + (x^6 + x^{-6})\big)$. This together with the first equality in (10) implies

$$\begin{aligned}\gcd(c(x^k), x^m - 1) &= \gcd(c(x^k)x^{6k}, x^m - 1)\\ &= \gcd(e^3(5,x^k), x^m - 1)\\ &= \gcd((\frac{x^{5k}-1}{x^k-1})^3, x^m - 1).\end{aligned}$$

Thus, $\gcd(c(x^k), x^m - 1) = 1$ if and only if $\gcd(\frac{x^{5k}-1}{x^k-1}, x^m - 1) = 1$, i.e., $\gcd(m,5k) = \gcd(m,k)$ due to (9). This completes the proof. ∎

Remark 1: It should be noted that many equalities as the ones in (10) can be easily obtained by taking different combinations of $e(j,x)$, where j is a positive integer. Thus, many new generalized Boolean bent functions can be obtained in a very simple way based on this method.

To end this section, we point out the following facts. In [20], Schmidt derived the conditions for $a \in \mathbb{R}$ and $b \in \mathbb{L}$ such that $Tr_1^m(ax + 2bx^3)$ is generalized Boolean bent, and recently Solé and Tokareva proposed as an interesting open problem in [21] to characterize the functions of the form $f_{a,b}(x) = Tr_1^m(ax + 2bx^{1+2^k})$ which are bent. Actually, we have done this for odd $m/\gcd(m,k)$ in [14].

Theorem 2: ([14]) Let m and k be positive integers such that $m/\gcd(m,k)$ is odd. Let $a \in \mathbb{R}$, $b \in \mathbb{L}$. Then $f_{a,b}(x) = Tr_1^m(ax + 2bx^{1+2^k})$ is generalized Boolean bent if

1) $\overline{a} \neq 0$ and $\overline{b} = 0$;
2) $\overline{a}\overline{b} \neq 0$ and $\overline{b}^{2^k} x^{1+2^k} + \overline{c}^{2^{k+1}} x + \overline{b} = 0$ has either zero or two roots in $\mathbb{F}_{2^m}$.

Moreover, the number of (a,b) such that $f_{a,b}(x)$ is generalized Boolean bent has also been given in [14]. However, the case of $m/\gcd(m,k)$ being even still remains open.

IV. New Boolean Bent Functions Obtained From Generalized Boolean Bent Functions

In this section, by virtue of the connections between Boolean bent and generalized Boolean bent functions over $\mathbb{Z}_4$, new Boolean bent and semi-bent functions of the form

$$f_Q(x) = p(x) + \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} tr_1^m(c_i x^{1+2^{ki}}),\ c_i \in \mathbb{F}_2,\ x \in \mathbb{F}_{2^m}$$

can be obtained based on the generalized Boolean bent functions $Q(x)$ constructed in Section III.

First of all, we need the following representation of the trace function over Galois rings.

Lemma 4: ([4]) The trace function over $\mathbb{GR}(4,m)$ has 2-adic expansion given by

$$Tr_1^m(x) = tr_1^m(\overline{x}) + 2p(\overline{x}),\quad x \in \mathbb{L}$$

where $p(x)$ is defined by (4).

By Lemma 4, the function $Q(x)$ defined by (2) can be expressed as

$$Q(x) = a(\overline{x}) + 2b(\overline{x}), x \in \mathbb{L},$$

where $a(x) = tr_1^m(x)$, and $b(x) = p(x) + \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} tr_1^m(c_i x^{1+2^{ki}})$.

Note that $b(x)$ with $x \in \mathbb{F}_{2^m}$ is in fact the Boolean function $f_Q(x)$ defined by (3). For even m, by Lemma 1 one has that both $b(x)$ and $a(x) + b(x)$ are Boolean bent if $Q(x)$ is generalized Boolean bent. If m is odd and $Q(x)$ is generalized Boolean bent, again by Lemma 1, one can get

$$\widehat{b^2}(\overline{\lambda}) + \widehat{a+b}^2(\overline{\lambda}) = 2|\widehat{Q}(\lambda)|^2 = 2^{m+1},\quad \forall\ \lambda \in \mathbb{L},$$

which leads to $(|\widehat{b}(\overline{\lambda})|, |\widehat{a+b}(\overline{\lambda})|) = (0, 2^{(m+1)/2})$ or $(2^{(m+1)/2}, 0)$ for all $\lambda \in \mathbb{L}$ due to the well known results about the solution to the diophantine equation, i.e., the diophantine equation $x^2 + y^2 = 2^{2k}$ has exactly two nonnegative integer solutions as $(x,y) = (0, 2^k)$ and $(x,y) = (2^k, 0)$ for a nonnegative integer k [3]. This implies $b(x)$ is semi-bent.

Thus, we can obtain the following result from Theorem 1.

Theorem 3: Let m be even (resp. odd), k be a positive integer, and $p(x)$ be defined by (4). Then the Boolean function $f_Q(x)$ defined by (3) is bent (resp. semi-bent) if and only if $Q(x)$ defined by (2) is bent, i.e., $\gcd(c(x^k), x^m - 1) = 1$, where $c(x)$ is defined by (8).

In particular, let m, k be positive integers and t be defined as in Corollaries 1-4 of Section III, if $Q(x)$ is chosen as one of the functions obtained in Corollaries 1-4, then the following bent and semi-bent functions can be obtained.

Corollary 6: Let m be an even (resp. odd) positive integer, and $p(x)$ be defined by (4). Then

1) $f_Q(x) = p(x) + tr_1^m(x^{1+2^{2k}}) + tr_1^m(x^{1+2^{3k}})$ is bent (resp. semi-bent) if and only if $\gcd(m, 3k) = \gcd(m, k)$;
2) $f_Q(x) = p(x) + \sum_{i=0}^{t} tr_1^m(x^{1+2^{(2i+1)k}})$ is bent (resp. semi-bent) if and only if $\gcd(m, (2t+1)k) = \gcd(m, k)$, and $\gcd(m, (2t+3)k) = \gcd(m, k)$;
3) $f_Q(x) = p(x) + tr_1^m(x^{1+2^k}) + \sum_{i=1}^{t} tr_1^m(x^{1+2^{2ik}})$ is bent (resp. semi-bent) if and only if $\gcd(m, (2t-1)k) = \gcd(m, k)$, and $\gcd(m, (2t+3)k) = \gcd(m, k)$;
4) $f_Q(x) = p(x) + \sum_{i=1}^{t} tr_1^m(x^{1+2^{ik}})$ is bent (resp. semi-bent) if and only if $\gcd(m, (2t+1)k) = \gcd(m, k)$.

Notice that $f_Q(x) = p(x) + \sum_{i=1}^{t} tr(x^{1+2^{ik}})$ is bent in $\mathbb{F}_{2^m}$ for even m if and only if $\gcd(m, (2t+1)k) = \gcd(m, k)$. This result in fact has been obtained in [11] and we apply a different approach to obtain it in this paper.

Corollary 7: Let m be even (resp. odd), $Q(x)$ be any of the functions obtained in Corollary 5 and let $p(x)$ be defined by (4). Then

1) $f_Q(x) = p(x) + tr_1^m(x^{1+2^{2k}}) + tr_1^m(x^{1+2^{5k}}) + tr_1^m(x^{1+2^{6k}})$ is bent (resp. semi-bent) if and only if $\gcd(m, 5k) = \gcd(m, k)$;
2) $f_Q(x) = p(x) + tr_1^m(x^{1+2^k}) + tr_1^m(x^{1+2^{4k}}) + tr_1^m(x^{1+2^{5k}})$ is bent (resp. semi-bent) if and only if $\gcd(m, 3k) = \gcd(m, k)$, and $\gcd(m, 7k) = \gcd(m, k)$;
3) $f_Q(x) = p(x) + tr_1^m(x^{1+2^{3k}}) + tr_1^m(x^{1+2^{5k}}) + tr_1^m(x^{1+2^{6k}})$ is bent (resp. semi-bent) if and only if $\gcd(m, 3k) = \gcd(m, k)$, $\gcd(m, 5k) = \gcd(m, k)$, and $\gcd(m, 7k) = \gcd(m, k)$.

Remark 2: According to Theorem 3, a new Boolean bent or semi-bent function $f_Q(x)$ can be obtained once a generalized Boolean bent function $Q(x)$ over $\mathbb{Z}_4$ is constructed. It can be shown from Remark 1 that many generalized Boolean bent functions $Q(x)$ can be constructed in a simple way. Thus, many new Boolean bent and semi-bent functions can also be obtained accordingly.

By Theorem 2 and Lemma 4, we can also obtain the following result.

Theorem 4: Let $f_{a,b}(x)$ be defined as in Theorem 2, and a, b be chosen in $\mathbb{L}$ such that $f_{a,b}(x)$ (with $x \in \mathbb{L}$) is generalized Boolean bent. Then, the Boolean function

$$p(\overline{a}x) + tr_1^m(\overline{b}x^{1+2^k}), \quad x \in \mathbb{F}_{2^m},$$

is bent (resp. semi-bent) for even (resp. odd) m.

Notice that it is not clear how to obtain the new Boolean bent and semi-bent functions $f_Q(x)$ of the form (3) from the theory of quadratic forms over finite fields. However, we can easily obtain them from $\mathbb{Z}_4$-valued quadratic forms and relationships between Boolean bent and generalized Boolean bent functions over $\mathbb{Z}_4$.

V. New p-ary Quadratic Bent Functions

In this section, we derive new p-ary quadratic bent functions $g(x)$ of the form (1), i.e.,

$$g(x) = \sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} tr_1^m(c_i x^{1+p^{ki}}), \quad c_i \in \mathbb{F}_p$$

for odd prime p by the same techniques used in Section III.

Helleseth and Kholosha in [7] proved that the p-ary function $g(x)$ with $k = 1$ is bent if and only if $\gcd(c_p(x), x^m - 1) = 1$, where $c_p(x)$ is defined by

$$c_p(x) = \sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} (c_i x^i + c_i x^{m-i}) \in \mathbb{F}_p[x]. \tag{11}$$

By the squaring technique used in [7] and Lemma 3, one can easily improve the result in [7] by deriving a sufficient and necessary condition for arbitrary k rather than k=1.

Theorem 5: Let m, k be positive integers, and p be an odd prime. Then the p-ary function $g(x)$ is bent if and only if $\gcd(c_p(x^k), x^m - 1) = 1$, where $c_p(x)$ is defined by (11).

Similar as in Section III, new p-ary bent functions can be obtained from specific values on $c_i, 0 \le i \le \lfloor \frac{m-1}{2} \rfloor$. To begin with, for the polynomials $x^r + 1, x^m - 1 \in \mathbb{F}_p[x]$, we calculate the $\gcd(x^r + 1, x^m - 1)$ for a positive integer r and an odd prime p. Note that $\gcd(x^r + 1, x^r - 1) = 1$ which implies $x^{\gcd(2r,m)} - 1 = \gcd(x^{2r} - 1, x^m - 1) = \gcd(x^r + 1, x^m - 1) \cdot \gcd(x^r - 1, x^m - 1) = \gcd(x^r + 1, x^m - 1) \cdot (x^{\gcd(r,m)} - 1)$. This leads to

$$\gcd(x^r + 1, x^m - 1) = \frac{x^{\gcd(2r,m)} - 1}{x^{\gcd(r,m)} - 1}, \tag{12}$$

and then $\gcd(x^r + 1, x^m - 1) = 1$ if and only if $\gcd(2r, m) = \gcd(r, m)$, i.e., $m/\gcd(r, m)$ is odd.

Corollary 8: Let m, s, t and k be integers that satisfy $0 \le t \le s \le \lfloor \frac{m-1}{2} \rfloor$, then

$$g(x) = tr_1^m(x^{p^{tk}+1} + x^{p^{sk}+1})$$

is bent if and only if both $m/\gcd(m, (s-t)k)$ and $m/\gcd(m, (s+t)k)$ are odd.

Proof: According to Theorem 5 and (11), to prove this result, it is sufficient to derive the conditions such that $\gcd(c_p(x^k), x^m - 1) = 1$, where $c_p(x) = x^t + x^s + x^{m-s} + x^{m-t}$. Note that

$$\begin{aligned}\gcd(c_p(x^k), x^m - 1) &= \gcd(c_p(x^k) \cdot x^{sk}, x^m - 1) \\ &= \gcd((x^{(s+t)k} + 1)(x^{(s-t)k} + 1), x^m - 1).\end{aligned}$$

Thus, according to (12), $\gcd(c_p(x^k), x^m - 1) = 1$ if and only if both $m/\gcd(m, (s-t)k)$ and $m/\gcd(m, (s+t)k)$ are odd. This completes the proof. ∎

Remark 3: This corollary implies

1) If $s = t > 0$, then $g(x) = tr_1^m(2x^{p^{sk}+1})$ is bent if and only if $m/\gcd(m, 2sk)$ is odd;
2) If $s > t = 0$, then $g(x) = tr_1^m(x^2 + x^{p^{sk}+1})$ is bent if and only if $m/\gcd(m, sk)$ is odd.

$$
\begin{aligned}
e_p(1,x)^2 e_p(2,x) &= x^2\big(2+2(x+x^{-1})+(x^2+x^{-2})\big),\\
e_p(2,x)e_p(5,x)^2 &= x^6\big(2(x+x^{-1})+(x^4+x^{-4})+(x^6+x^{-6})\big),\\
e_p(1,x)e_p(2,x)e_p(3,x) &= x^3\big(2+(x+x^{-1})+(x^2+x^{-2})+(x^3+x^{-3})\big),\\
e_p(2,x)(x^5-1)/(x-1) &= x^3\big(2+2(x+x^{-1})+(x^2+x^{-2})+(x^3+x^{-3})\big),\ p\neq 5. \qquad (13)
\end{aligned}
$$

Corollary 9: Let p be an odd prime, m, k and t be positive integers such that $t < m$ and $p \nmid t$, then

$$g(x) = \sum_{i=1}^{t} tr_1^m(x^{1+p^{ik}})$$

is bent if and only if $m/\gcd(m,(t+1)k)$ is odd and $\gcd(m,tk) = \gcd(m,k)$.

Proof: For the given function $g(x)$, by (11), one obtains that

$$c_p(x) = x + x^2 + x^3 + \cdots + x^t + x^{m-t} + \cdots + x^{m-1}.$$

Notice that

$$
\begin{aligned}
&c_p(x)\cdot x^t \bmod (x^m-1)\\
&\quad = (x+x^2+\cdots+x^t)x^t + (1+x+\cdots+x^{t-1})\\
&\quad = (1+x+\cdots+x^{t-1})(x^{t+1}+1)\\
&\quad = \frac{x^t-1}{x-1}\cdot(x^{t+1}+1)
\end{aligned}
$$

which implies

$$
\begin{aligned}
\gcd(c_p(x^k), x^m-1) &= \gcd(c_p(x^k)\cdot x^{tk}, x^m-1)\\
&= \gcd\Big(\frac{x^{tk}-1}{x^k-1}\cdot(x^{(t+1)k}+1), x^m-1\Big).
\end{aligned}
$$

Since $p \nmid t$, then by (9), one has $\gcd(\frac{x^{tk}-1}{x^k-1}, x^m-1) = 1$ if and only if $\gcd(m,tk) = \gcd(m,k)$. On the other hand, by (12), one has $\gcd((x^{(t+1)k}+1), x^m-1) = 1$ if and only if $m/\gcd(m,(t+1)k)$ is odd. Thus, the result follows from Theorem 5. This completes the proof. ∎

Corollary 10: Let p be an odd prime, m, k and t be positive integers such that $1 \le t < \frac{m-1}{2}$ and $p \nmid (t+1)$, then

$$g(x) = \sum_{i=0}^{t} tr_1^m(x^{1+p^{(2i+1)k}})$$

is bent if and only if $\gcd(m,(2t+2)k) = \gcd(m,2k)$.

Proof: To complete the proof, according to Theorem 5 and (11), it suffices to show that $\gcd(c_p(x^k), x^m-1) = 1$ if and only if $\gcd(m,(2t+2)k) = \gcd(m,2k)$, where $p \nmid (t+1)$ and

$$c_p(x) = x + x^3 + \cdots + x^{2t+1} + x^{m-(2t+1)} + \cdots + x^{m-1}.$$

By a simple computation, one obtains that

$$
\begin{aligned}
&c_p(x)\cdot x^{2t+1} \bmod (x^m-1)\\
&\quad = (x+x^3+\cdots+x^{2t+1})x^{2t+1} + (1+x^2+\cdots+x^{2t})\\
&\quad = (1+x^2+\cdots+x^{2t})(x^{2t+2}+1)\\
&\quad = \frac{x^{2t+2}-1}{x^2-1}\cdot(x^{2t+2}+1)\\
&\quad = \frac{x^{4t+4}-1}{x^2-1}.
\end{aligned}
$$

This leads to

$$
\begin{aligned}
\gcd(c_p(x^k), x^m-1) &= \gcd(c_p(x^k)\cdot x^{(2t+1)k}, x^m-1)\\
&= \gcd\Big(\frac{x^{(2t+2)\cdot 2k}-1}{x^{2k}-1}, x^m-1\Big).
\end{aligned}
$$

Then by (9), for $p \nmid (t+1)$, one has that $\gcd(c_p(x^k), x^m-1) = 1$ if and only if $\gcd(m,(2t+2)k) = \gcd(m,2k)$. This completes the proof. ∎

Through the construction of the polynomials $c_p(x)$, new p-ary bent functions $g(x)$ of the form (1) can also be constructed from some simple polynomials over the finite field $\mathbb{F}_p$ as below. For an odd prime p and a positive integer j, define $e_p(j,x) = x^j + 1 \in \mathbb{F}_p[x]$. Then many polynomials $c_p(x)$ of the form (11) can be obtained from $e_p(j,x) = x^j + 1$. For example, by a direct computation, we can have (13), as shown at the top of this page.

Then, according to Theorem 5 and (13), we can derive the following results.

Corollary 11: Let m and k be positive integers, then

1) $g(x) = tr_1^m(x^2+2x^{1+p^k}+x^{1+p^{2k}})$ is bent in $\mathbb{F}_{p^m}$ if and only if $m/\gcd(m,k)$ is odd;
2) $g(x) = tr_1^m(2x^{1+p^k} + x^{1+p^{4k}} + x^{1+p^{6k}})$ is bent in $\mathbb{F}_{p^m} (p \neq 5)$ if and only if both $m/\gcd(m,2k)$ and $m/\gcd(m,5k)$ are odd; and it is bent in $\mathbb{F}_{5^m}$ if and only if $m/\gcd(m,k)$ is odd;
3) $g(x) = tr_1^m(x^2 + x^{1+p^k} + x^{1+p^{2k}} + x^{1+p^{3k}})$ is bent in $\mathbb{F}_{p^m}$ if and only if $m/\gcd(m,k)$ is odd;
4) $g(x) = tr_1^m(x^2 + 2x^{1+p^k} + x^{1+p^{2k}} + x^{1+p^{3k}})$ is bent in $\mathbb{F}_{p^m} (p \neq 5)$ if and only if $m/\gcd(m,2k)$ is odd, and $\gcd(m,5k) = \gcd(m,k)$.

Proof: We only prove Case 1) since the other cases can be proven in the same manner. According to Theorem 5, $g(x) = tr_1^m(x^2 + 2x^{1+p^k} + x^{1+p^{2k}})$ is bent in $\mathbb{F}_{p^m}$ if and only if $\gcd(c_p(x^k), x^m-1) = 1$, where $c_p(x) = 2 + 2x + x^2 + x^{m-2} + 2x^{m-1}$. By the fact

$$c_p(x) \bmod (x^m-1) = 2 + 2(x+x^{-1}) + (x^2+x^{-2})$$

and the first equality in (13), one has

$$
\begin{aligned}
\gcd(c_p(x^k), x^m-1) &= \gcd(c_p(x^k)x^{2k}, x^m-1)\\
&= \gcd(e_p(1,x^k)^2 e_p(2,x^k), x^m-1)\\
&= \gcd((x^k+1)^2(x^{2k}+1), x^m-1).
\end{aligned}
$$

Thus, $\gcd(c_p(x^k), x^m-1) = 1$ if and only if both $\gcd(x^k+1, x^m-1) = 1$ and $\gcd(x^{2k}+1, x^m-1) = 1$, i.e., both $m/\gcd(m,k)$ and $m/\gcd(m,2k)$ are odd due to (12). Then, the result follows from Theorem 5 and the fact that $m/\gcd(m,2k)$ is a factor of $m/\gcd(m,k)$. This completes the proof. ∎

It should be noted that many equalities as the ones in (13) can be obtained by taking different combinations of $e_p(j,x)$ and $\frac{x^j-1}{x-1}$ over $\mathbb{F}_p$, where p is an odd prime and j is a positive integer. Thus, many new p-ary bent functions can be obtained accordingly as the ones in Corollary 11.

VI. Conclusion

The quadratic bent functions, including Boolean bent functions, generalized Boolean bent functions and p-ary bent functions, in polynomial forms are investigated in this paper. New generalized Boolean bent functions $Q(x)$ of the form (2) are obtained based on the theory of $\mathbb{Z}_4$-valued quadratic forms, and a method to construct such functions is also proposed. From these constructions together with the links between generalized Boolean bent and Boolean bent functions [21], new classes of Boolean bent and semi-bent functions $f_Q(x)$ of the form (3) are presented. Moreover, by the same techniques, many new p-ary bent functions $g(x)$ of the form (1) are obtained, and a simple method to construct such functions is also given.

Acknowledgements

The authors would like to express their deep gratitude to the Associate Editor Professor Jean-Pierre Tillich and the anonymous reviewers for their comments that improved the presentation and quality of this paper.

References

[1] E. H. Brown, "Generalizations of the Kervaire invariant," *Ann. Math.*, vol. 95, no. 2, pp. 368–383, Mar. 1972.

[2] 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.

[3] E. Grosswald, *Representation of Integers as Sum of Squares*. New York, NY, USA: Springer-Verlag, 1985.

[4] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, Mar. 1994.

[5] T. Helleseth and P. V. Kumar, *Sequences With Low Correlation* (Handbook of Coding Theory), V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998.

[6] T. Helleseth, H. D. L. Hollmann, A. Kholosha, Z. Wang, and Q. Xiang, "Proofs of two conjectures on ternary weakly regular bent functions," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 5272–5283, Nov. 2009.

[7] T. Helleseth and A. Kholosha, "Monomial and quadratic bent functions over the finite field of odd characteristic," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2018–2032, May 2006.

[8] T. Helleseth and A. Kholosha, "New binomial bent functions over the finite fields of odd characteristic," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4646–4652, Sep. 2010.

[9] T. Helleseth and A. Kholosha, "On generalized bent functions," in *Proc. IEEE Inf. Theory Appl. Workshop (ITA)*, Jan./Feb. 2010, pp. 1–6.

[10] T. Helleseth and A. Kholosha, "Sequences, bent functions and Jacobsthal sums," in *Sequences and Their Applications—SETA* (Lecture Notes in Computer Science), vol. 6338, C. Carlet and A. Pott, Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 416–429.

[11] H. Hu and D. Feng, "On quadratic bent functions in polynomial forms," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2610–2615, Jul. 2007.

[12] K. Khoo, G. Gong, and D. R. Stinson, "A new characterization of semi-bent and bent functions on finite fields," *Designs, Codes Cryptograph.*, vol. 38, no. 2, pp. 279–295, Feb. 2006.

[13] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *J. Combinat. Theory Ser. A*, vol. 40, no. 1, pp. 90–107, Sep. 1985.

[14] N. Li, X. Tang, and T. Helleseth, "Several classes of codes and sequences derived from a $\mathbb{Z}_4$-valued quadratic form," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7618–7628, Nov. 2011.

[15] S. Li, L. Hu, and X. Zeng, "Constructions of p-ary quadratic bent functions," *Acta Appl. Math.*, vol. 100, no. 3, pp. 227–245, Feb. 2008.

[16] W. Ma, M. Lee, and F. Zhang, "A new class of bent functions," *IEICE Trans. Fundam.*, vol. E88-A, no. 7, pp. 2039–2040, Jul. 2005.

[17] R. Lidl and H. Niederreiter, *Finite Fields*, in *Encyclopedia of Mathematics and its Applications*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 1997.

[18] O. S. Rothaus, "On 'bent' functions," *J. Combinat. Theory Ser. A*, vol. 20, no. 3, pp. 300–305, May 1976.

[19] K.-U. Schmidt, "$\mathbb{Z}_4$-valued quadratic forms and quaternary sequence families," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5803–5810, Dec. 2009.

[20] K.-U. Schmidt, "Quaternary constant-amplitude codes for multicode CDMA," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1824–1832, Apr. 2009.

[21] P. Solé and N. Tokareva. (2009, Nov. 5). *Connections Between Quaternary and Binary Bent Functions*. [Online]. Available: http://www.eprint.iacr.org/2009/544

[22] M. Yamada, "Distance-regular digraphs of girth 4 over an extension ring of $\mathbb{Z}/4\mathbb{Z}$," *Graphs Combinat.*, vol. 6, no. 4, pp. 381–394, 1990.

[23] 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.

Nian Li received the B.S. and M.S. degrees in mathematics from Hubei University, Wuhan, China, in 2006 and 2009, respectively, and he received the Ph.D. degree at the Southwest Jiaotong University, Chengdu, China, in 2013. From Sept. 2011 to Aug. 2013, he was a visiting Ph.D. student in the Department of Informatics, University of Bergen, Norway. Currently, he is working as a postdoc in the Department of Mathematics, the Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong. His research interests include sequence design and coding theory.

Xiaohu Tang (M'04) received the B.S. degree in applied mathematics from the Northwest Polytechnic University, Xi'an, China, the M.S. degree in applied mathematics from the Sichuan University, Chengdu, China, and the Ph.D. degree in electronic engineering from the Southwest Jiaotong University, Chengdu, China, in 1992, 1995, and 2001 respectively.

From 2003 to 2004, he was a postdoctoral member in the Department of Electrical and Electronic Engineering, Hong Kong University of Science and Technology. From 2007 to 2008, he was a visiting professor at University of Ulm, Germany. Since 2001, he has been in the Institute of Mobile Communications, Southwest Jiaotong University, where he is currently a professor. His research interests include sequence design, coding theory and cryptography.

Dr. Tang was the recipient of the National excellent Doctoral Dissertation award in 2003 (China), the Humboldt Research Fellowship in 2007 (Germany).

Tor Helleseth (M'89–SM'96–F'97) received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively.

From 1973 to 1980, he was a Research Assistant at the Department of Mathematics, University of Bergen. From 1981 to 1984, he was at the Chief Headquarters of Defense in Norway. Since 1984, he has been a Professor in the Department of Informatics at the University of Bergen. During the academic years 1977-1978 and 1992-1993, he was on sabbatical leave at the University of Southern California, Los Angeles, and during 1979-1980, he was a Research Fellow at the Eindhoven University of Technology, Eindhoven, The Netherlands. His research interests include coding theory and cryptology.

Prof. Helleseth served as an Associate Editor for Coding Theory for IEEE Transactions on Information Theory from 1991 to 1993 and for Sequences from 2012 to 2014. He was Program Chairman for Eurocrypt'93 and for the Information Theory Workshop in 1997 in Longyearbyen, Norway. He was a Program Co-Chairman for SETA04 in Seoul, Korea, and SETA06 in Beijing, China. He was also a Program Co-Chairman for the IEEE Information Theory Workshop in Solstrand, Norway in 2007. During 2007-2009 he served on the Board of Governors for the IEEE Information Theory Society. In 2004 he was elected a member of Det Norske Videnskaps-Akademi.