Constructions of Quadratic Bent Functions in Polynomial Forms

Nam Yul Yu and Guang Gong, *Member, IEEE*
Department of Electrical and Computer Engineering
University of Waterloo, CANADA

Abstract

In this correspondence, the constructions and enumerations of all bent functions represented by a polynomial form of $f(x) = \sum_{i=1}^{n/2-1} c_i Tr(x^{1+2^i}) + c_{n/2} Tr_1^{n/2}(x^{1+2^{n/2}}), c_i \in \mathbb{F}_2$, are presented for special cases of n. Using an iterative approach, the construction of bent functions of n variables with degree $\frac{n}{2}$ is also provided using the constructed quadratic bent functions.

Index Terms

Bent functions, Boolean functions, Maximum nonlinearity, Semi-bent functions.

I. Introduction

A bent function is a Boolean function with even number of variables whose Walsh transform has a constant magnitude [10]. In the coding context, it is a coset of the first order Reed-Muller code with the largest minimum weight [19]. In other words, a bent function has a maximum distance from a linear function, so it is *maximally nonlinear*. For the maximum nonlinearity, bent functions have been paid a lot of attention to by researchers for cryptographic applications [4] - [9]. Moreover, the maximum nonlinearity of bent functions corresponds to a minimized maximum correlation between the functions and a trace function. Thus, bent functions also have many applications in algebraic coding and sequence design [19] [22].

In [13] and [14], Khoo, Gong, and Stinson investigated the following sum of monomial trace terms with quadratic exponents where the exponent of variables has the Hamming weight 2. For

odd n,

$$f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{1+2^i}), \quad x \in \mathbb{F}_{2^n}, \quad c_i \in \mathbb{F}_2$$

where $Tr(x)$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. The spectrum of Hadamard transform of $f(x)$ (which will be formally defined in next section) belongs to the integer ring $\mathbb{Z}$. If the spectrum only takes three values of $\{0, \pm 2^{\frac{n+1}{2}}\}$, then $f(x)$ is called a *semi-bent function* for odd n [13]. Let $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$. Khoo, Gong, and Stinson derived a necessary and sufficient condition for a semi-bent function, i.e., $f(x)$ is semi-bent if and only if

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

Following this work, Charpin, Pasalic, and Tavernier [6] considered

$$f(x) = \begin{cases} \sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{1+2^i}), & n \text{ odd}, \ c_i \in \mathbb{F}_2, \\ \sum_{i=1}^{\frac{n-2}{2}} c_i Tr(x^{1+2^i}), & n \text{ even}, \ c_i \in \mathbb{F}_2. \end{cases} \tag{1}$$

For even n, $f(x)$ is called a semi-bent function in [6] if the spectrum of $f(x)$ belongs to $\{0, \pm 2^{\frac{n+2}{2}}\}$. They showed that for even n, $f(x)$ is semi-bent if and only if $\gcd(c(x), x^n + 1) = x^2 + 1$. For odd n, on the other hand, they derived some conditions that $f(x)$ with three or four trace terms is semi-bent. Then, they derived the construction of semi-bent functions of odd n with higher degree from semi-bent functions of even n in (1), and also derived the construction of bent functions with higher degree from semi-bent functions of odd n.

Applying the techniques developed in [13], Ma, Lee, and Zhang [18] showed that a necessary condition for the bent functions with such a representation is as follows.

$$f(x) = \sum_{i=1}^{n/2-1} c_i Tr(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}), \quad x \in \mathbb{F}_{2^n}, \ c_i \in \mathbb{F}_2 \tag{2}$$

where n is even and $Tr_1^{n/2}(x)$ is the trace function from $\mathbb{F}_{2^{n/2}}$ to $\mathbb{F}_2$. Or equivalently, the monomial trace term $Tr_1^{n/2}(x^{1+2^{n/2}})$ has to be presented in the representation. Furthermore, a necessary and sufficient condition for $f(x)$ given by (2) to be bent is $\gcd(c(x), x^n + 1) = 1$ [18] where

$$c(x) = \sum_{i=1}^{n/2-1} c_i(x^i + x^{n-i}) + x^{n/2}. \tag{3}$$

For the quadratic bent functions represented by a polynomial form (2), the known cases are: (a) all c_i's are zero corresponding to the Kasami (small) signal set [12], or all c_i's are one

giving the Udaya's construction [23], or ones of c_i's are distributed by equal distance of i giving the Kim and No's signal set [15], respectively; (b) all choices of c_i's for $n = 2^v$ [18]. For the polynomial construction of non-quadratic bent functions, on the other hand, the known cases are monomial trace functions with the Kasami [8] exponents and the Dillon exponents [7], and a sum of trace functions with the Niho exponents [9].

It is worthwhile to point out that all quadratic bent functions of Boolean forms are known, which can be obtained by applying the affine transform to $x_0, x_1, \cdots, x_{n-1}$ in $\sum_{i=0}^{n/2-1} x_{2i}x_{2i+1}$ [19]. The *Maiorana-McFarland's* construction [21] for quadratic bent functions also belongs to this class.

In this paper, we consider how to construct quadratic bent functions in polynomial forms. Precisely, we present the construction of all quadratic bent functions represented by a polynomial form (2) by giving a necessary and sufficient condition on c_i's for special cases of n. The paper is organized as follows. In Section II, we introduce some concepts and definitions which will be used throughout the paper. In Sections III and IV, we derive their respective constructions for $n = 2^v p$ and $n = 2^v p^r$ with $v \geq 1$ and $r \geq 2$, respectively, where p is odd prime and the order of 2 modulo p is $p-1$ or $\frac{p-1}{2} = s$ with odd s. An enumeration of such quadratic bent functions for the case $n = 2^v p$ is also given in Section III. For $n = 2^v p^2$, we list the result of the enumeration without proof in Section IV, since the proof is similar to that of $n = 2^v p$ but rather lengthy. In Section V, we demonstrate a way to apply the iterative method of Charpin, Pasalic, and Tavernier for constructing bent functions of n variables with degree $\frac{n}{2}$ using the quadratic bent functions constructed in this paper. Concluding remarks and discussion will be given in Section VI.

II. Preliminaries

The following notation will be used throughout the paper.

- p is odd prime with $p > 1$.
- $\mathrm{ord}_p(2)$ is the order of 2 modulo p, i.e., the smallest integer s such that $2^s \equiv 1 \pmod{p}$.
- $\mathbb{Z}$ represents the integer ring.
- $\mathbb{F}_q = GF(q)$ is the finite field with q elements and $\mathbb{F}_q^*$, the multiplicative group of $\mathbb{F}_q$.
- $\mathbb{F}_2^n$ is a vector space over $\mathbb{F}_2 = \{0, 1\}$ with a set of all binary n-tuples.

- Let n, m be positive integers and $m|n$, i.e., m is a divisor of n. The trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ is denoted by $Tr_m^n(x)$, i.e.,

$$Tr_m^n(x) = x + x^{2^m} + \cdots + x^{2^{m(\frac{n}{m}-1)}}, \ x \in \mathbb{F}_{2^n}.$$

  $Tr_1^n(x)$ is simply denoted as $Tr(x)$ if the context is clear.

A. Boolean and polynomial functions

Let $\mathbf{x} = (x_0, \cdots, x_{n-1})$ be a vector in $\mathbb{F}_2^n$ with $x_i \in \mathbb{F}_2$. A function $f(\mathbf{x})$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ which takes on values 0 or 1 is called a *Boolean function*. A Boolean function consists of a sum of all possible products of x_{i_j}'s with coefficients 0 or 1, i.e.,

$$f(\mathbf{x}) = f(x_0, \cdots, x_{n-1}) = \sum_{1 \le j \le n} c_{i_1 i_2 \cdots i_j} x_{i_1} x_{i_2} \cdots x_{i_j}, \quad c_{i_1 i_2 \cdots i_j} \in \mathbb{F}_2$$

where maximum value of j with nonzero $c_{i_1 i_2 \cdots i_j}$ is called the *degree* of the Boolean function $f(\mathbf{x})$.

A function $f(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ can be represented as

$$f(x) = \sum_i Tr_1^{n_i}(A_i x^{r_i}), \quad A_i \in \mathbb{F}_{2^{n_i}} \tag{4}$$

where r_i is a coset leader of a cyclotomic coset modulo $2^{n_i} - 1$, and $n_i|n$ is a size of the cyclotomic coset containing r_i. (4) is called a *polynomial representation* of $f(x)$. r_i is also referred to as an exponent of the monomial trace term $Tr_1^{n_i}(A_i x^{r_i})$. If the Hamming weight of r_i is equal to 2, then we also say r_i is a quadratic exponent because the degree of the Boolean form of $Tr_1^{n_i}(A_i x^{r_i})$ is equal to the Hamming weight of r_i.

In terms of a basis of $\mathbb{F}_{2^n}$, a polynomial function of a sum of trace functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is equivalent to a Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. For example, a sum of monomial trace terms with quadratic exponents corresponds to a quadratic Boolean function. For the theory of Boolean functions and their polynomial representations, readers are referred to [10], [11], and [19].

B. Bent functions

A Boolean function of n variables is called a *bent function* if its Walsh transform has a constant magnitude [10] [19], where the Walsh transform of a Boolean function $f(\mathbf{x})$ is defined

by

$$\widehat{f}(\mathbf{w}) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathbf{w}\cdot\mathbf{x}+f(\mathbf{x})}, \quad \mathbf{w} \in \mathbb{F}_2^m.$$

In the equivalent polynomial function $f(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, its Hadamard transform is defined by

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

Then, $f(x)$ is bent if $\widehat{f}(\lambda) \in \{\pm 2^{\frac{n}{2}}\}$ where n is even. For odd n, $f(x)$ is semi-bent if $\widehat{f}(\lambda) \in \{0, \pm 2^{\frac{n+1}{2}}\}$. For even n, on the other hand, $f(x)$ is semi-bent if $\widehat{f}(\lambda) \in \{0, \pm 2^{\frac{n+2}{2}}\}$. Bent functions exist only for even n.

C. Cyclotomic polynomials

A polynomial whose roots are the field elements of order d is called the *dth cyclotomic polynomial* [17], denoted by $Q_d(x)$. $Q_d(x)$ is a monic polynomial of order d and degree $\phi(d)$, where $\phi(d)$ is the Euler-totient function, defined as the number of integers k of $1 \leq k \leq d$ with $\gcd(k, d) = 1$ [17]. $Q_d(x)$ has the following basic properties [1] [20].

Property 1: Let $Q_d(x)$ be the dth cyclotomic polynomial.

(a) $x^m + 1 = \prod_{d|m} Q_d(x)$. In particular, $x^{p^r} + 1 = Q_1(x)Q_p(x)\cdots Q_{p^{r-1}}(x)Q_{p^r}(x)$ where p is prime.

(b) For $d \geq 2$, $x^{\phi(d)}Q_d(x^{-1}) = Q_d(x)$. In other words, $Q_d(x)$ is self-reciprocal (A polynomial $g(x)$ with degree m is called *self-reciprocal* if $x^m g(x^{-1}) = g(x)$).

(c) For prime p, $Q_p(x) = \sum_{i=1}^{p} x^{p-i} = x^{p-1} + x^{p-2} + \cdots + x + 1$.

(d) For prime p, $Q_{p^k}(x) = Q_p(x^{p^{k-1}})$.

A cyclotomic polynomial is irreducible over the integer ring $\mathbb{Z}$, but it may not be irreducible over $\mathbb{F}_2$. Throughout this paper, we consider cyclotomic polynomials over $\mathbb{F}_2$. We list several useful properties on the factorization of $Q_d(x)$ over $\mathbb{F}_2$ without proofs. For more details, see [1], [17], and [20].

Property 2: $Q_d(x)$ is irreducible over $\mathbb{F}_2$ if and only if $\mathrm{ord}_d(2)$ is $\phi(d)$.

Property 3: For prime p, let $Q_p(x) = g_1(x)g_2(x)\cdots g_t(x)$ where $g_i(x)$ for $1 \le i \le t$ is irreducible over $\mathbb{F}_2$. Then, the degree and the order of each $g_i(x)$ for $1 \le i \le t$ are given by $\frac{\phi(p)}{t} = \frac{p-1}{t}$ and p, respectively.

Property 4: For prime p, let $f_1(x), f_2(x), \cdots, f_t(x)$ be distinct monic irreducible polynomials over $\mathbb{F}_2$ of degree $\frac{\phi(p)}{t}$ and order p, and let $s = p^{k-1}$. Then, $f_1(x^s), f_2(x^s), \cdots, f_t(x^s)$ are distinct monic irreducible polynomials over $\mathbb{F}_2$ of degree $\frac{\phi(p)p^{k-1}}{t}$ and order p^k.

D. A criterion of bent functions with quadratic exponents

For odd n, Khoo, Gong, and Stinson showed a necessary and sufficient condition for a semi-bent function with quadratic exponents [13] [14]. Similarly, a necessary and sufficient condition for a bent function with quadratic exponents can be directly resulted from the techniques developed in [13] and [14]. The following fact appears in [18].

Fact 1: For even n, let

$$f(x) = \sum_{i=1}^{n/2-1} c_i Tr(x^{1+2^i}) + c_{n/2} Tr_1^{n/2}(x^{1+2^{n/2}}), \quad x \in \mathbb{F}_{2^n}, \quad c_i \in \mathbb{F}_2.$$

Then, $f(x)$ is bent if and only if $\gcd(c(x), x^n + 1) = 1$, where

$$c(x) = \sum_{i=1}^{n/2-1} c_i(x^i + x^{n-i}) + c_{n/2}x^{n/2}. \tag{5}$$

In addition, $c_{n/2} = 1$ if $f(x)$ is bent.

Corollary 1: For $n = 2^v m$ with $v \ge 1$ and odd m, $f(x)$ given by (2) is bent if and only if $\gcd(c(x), x^m + 1) = 1$.

Proof: From $x^n+1 = (x^m+1)^{2^v}$, $\gcd(c(x), x^n+1) = 1$ if and only if $\gcd(c(x), x^m+1) = 1$. Hence, Corollary 1 is true. ■

From Fact 1 and Corollary 1, it is immediate that for $n = 2^v$ with $v \ge 2$, $f(x)$ given by (2) is a bent function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ for any choices of c_i's [18]. Thus, the total number of such bent functions for $n = 2^v$ is equal to $2^{\frac{n}{2}-1}$.

III. Construction and enumeration for $n = 2^v p$

In this section, we construct and enumerate all bent functions given by

$$f(x) = \sum_{i=1}^{n/2-1} c_i Tr(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}), \quad x \in \mathbb{F}_{2^n},\ c_i \in \mathbb{F}_2 \tag{6}$$

for $n = 2^v p$ with $v \geq 1$, where p is odd prime with $\mathrm{ord}_p(2) = p-1$ or $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ with odd s.

Before we present the construction and enumeration, we need some preparations on the greatest common divisor of $c(x)$ given by (3), i.e., $c(x) = \sum_{i=1}^{n/2-1} c_i(x^i + x^{n-i}) + x^{n/2}$, and the pth cyclotomic polynomial $Q_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p+1}{x+1}$. In the following, when we talk about a root of a polynomial over $\mathbb{F}_2$, we always mean that the root belongs to some extension field of $\mathbb{F}_2$.

Lemma 1: Let $\bar{c}(x)$ be $c(x)$ reduced modulo $x^p + 1$, and z be a root of $x^p + 1$ with $z \neq 1$. Then,

(a)

$$\begin{aligned} \bar{c}(x) &\equiv c(x) \pmod{x^p+1} \\ &= \sum_{i=1}^{p-1} w_i(x^i + x^{p-i}) + 1 = \sum_{i=1}^{\frac{p-1}{2}} (w_i + w_{p-i})(x^i + x^{p-i}) + 1 \end{aligned} \tag{7}$$

where $w_i = c_i + c_{i+p} + \cdots + c_{i+\frac{n}{2}-p} = \sum_{l=0}^{\frac{n}{2p}-1} c_{i+lp}$.

(b) Let p be odd prime with $\mathrm{ord}_p(2) = p-1$ or $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ where s is odd. Then, $\gcd(c(x), x^p+1) \neq 1$ if and only if $\bar{c}(x) = Q_p(x)$, which is equivalent to

$$w_i \neq w_{p-i} \text{ for all } 1 \leq i \leq \frac{p-1}{2}. \tag{8}$$

Proof: (a) $c(x)$ can be rewritten as

$$\begin{aligned} c(x) = &\sum_{i=1}^{p-1} c_i(x^i + x^{n-i}) + c_p(x^p + x^{n-p}) + \sum_{i=p+1}^{2p-1} c_i(x^i + x^{n-i}) + c_{2p}(x^{2p} + x^{n-2p}) \\ &+ \cdots + \sum_{i=(\frac{n}{2p}-1)p+1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i}) + x^{\frac{n}{2}}. \end{aligned} \tag{9}$$

Hence, we obtain (7) from (9) modulo $x^p + 1$.

(b) For the prime p, $x^p + 1 = Q_1(x)Q_p(x)$ where $Q_1(x) = x + 1$. We may write $Q_p(x) = \sum_{i=1}^{\frac{p-1}{2}}(x^i + x^{p-i}) + 1$. Then, $\gcd(c(x), Q_1(x)) = 1$.

If $\mathrm{ord}_p(2) = p-1$, $Q_p(x)$ is irreducible over $\mathbb{F}_2$. Hence,

$$\begin{aligned} \gcd(c(x), x^p+1) \neq 1 &\Longleftrightarrow \gcd(c(x), x^p+1) = Q_p(x) \\ &\Longleftrightarrow \bar{c}(x) = Q_p(x) \end{aligned} \tag{10}$$

The last equivalence is from the Euclidean algorithm. By comparing $\bar{c}(x)$ and $Q_p(x)$, we obtain (8).

If $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ where s is odd, on the other hand, $Q_p(x) = g_1(x)g_2(x)$ where $g_1(x)$ and $g_2(x)$ are irreducible over $\mathbb{F}_2$ with $g_2(x) = x^s g_1(x^{-1})$ [6]. Note that if z is a root of $g_1(x)$, then z^{-1} is a root of $g_2(x)$, and vice versa. (Note that if z is a root of $g_1(x)$, then z^{-1} cannot be its root [6].) Since z is a root of $Q_p(x)$, the order of z is p, i.e., $z^p = z^n = 1$. From (3), therefore,

$$c(z) = \sum_{i=1}^{n/2-1} c_i(z^i + z^{n-i}) + z^{n/2} = \sum_{i=1}^{n/2-1} c_i(z^i + z^{-i}) + z^{-n/2}$$

and thus z^{-1} is a root of $c(x)$ if z is its root. If $c(x)$ has the irreducible factor $g_1(x)$, therefore, it simultaneously has the other irreducible factor $g_2(x)$, and vice versa. Hence, (10) is also true in this case. Similar to the case of $\mathrm{ord}_p(2) = p-1$, we obtain (8). ■

Theorem 1: Let $n = 2^v p$ with $v \geq 1$ and p be odd prime with $\mathrm{ord}_p(2) = p-1$ or $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ where s is odd. Then, $f(x)$ given by (6) is bent if and only if there exists at least one i for $1 \leq i \leq \frac{p-1}{2}$ such that

$$w_i = w_{p-i} \tag{11}$$

where $w_i = \sum_{l=0}^{\frac{n}{2p}-1} c_{i+lp}$. The number of bent functions of $f(x)$, denoted by N_b, is given by

$$N_b = 2^{\frac{n}{2}-1} - 2^{\frac{n-1-p}{2}}.$$

Note that $N_{nb} = 2^{\frac{n-1-p}{2}}$ is the number of non-bent functions of $f(x)$.

Proof: From Fact 1 and Corollary 1, $f(x)$ is non-bent if and only if $\gcd(c(x), x^p+1) \neq 1$. Applying Lemma 1-(b), $f(x)$ is non-bent if and only if (8) is achieved. Therefore, $f(x)$ is bent if and only if there exists at least one i for $1 \leq i \leq \frac{p-1}{2}$ such that (11) is true, which completes the proof for the first part of the result.

Next, we consider the enumeration of vectors $\underline{\mathbf{c}} = (c_1, c_2, \cdots, c_{n/2-1})$ which satisfy (11). Note that we can arrange the elements of $\underline{\mathbf{c}}$ into an $\frac{n}{2p} \times p$ matrix as follows.

$$M = \begin{bmatrix} c_0 & c_1 & \cdots & c_{p-2} & c_{p-1} \\ c_p & c_{p+1} & \cdots & c_{2p-2} & c_{2p-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ c_{(\frac{n}{2p}-1)p} & c_{(\frac{n}{2p}-1)p+1} & \cdots & c_{\frac{n}{2}-2} & c_{\frac{n}{2}-1} \end{bmatrix}$$

where $c_0 = 0$. Then, w_i is equal to the sum of the entries in the ith column of M for $1 \leq i \leq p-1$. Thus, we see that all c_j's occurring in w_i and w_{p-i} in (11) are distinct. In the following, we will count the number of non-bent functions, i.e., the number of vectors $\underline{\mathbf{c}}$ satisfying (8). Note that the condition of (8) is equivalent to

$$w_i + w_{p-i} = 1 \text{ for all } 1 \leq i \leq \frac{p-1}{2},$$

i.e.,

$$c_i + c_{i+p} + \cdots + c_{i+(\frac{n}{2p}-1)p} + c_{p-i} + c_{p-i+p} + \cdots + c_{p-i+(\frac{n}{2p}-1)p} = 1 \text{ for all } 1 \leq i \leq \frac{p-1}{2}. \quad (12)$$

For each i, there are $\frac{n}{p} = 2^v$ c_j's in (12) where $j \in \{i, i+p, \cdots, i+(2^{v-1}-1)p, p-i, p-i+p, \cdots, p-i+(2^{v-1}-1)p\}$. For (12), the number of c_j's which take on the value 1 should be odd for each i. Therefore, there are $\binom{2^v}{1} + \binom{2^v}{3} + \cdots + \binom{2^v}{2^v-1} = \sum_{k=0}^{2^{v-1}-1} \binom{2^v}{2k+1}$ choices of such c_j's for each i. Since there are $\frac{p-1}{2}$ choices of i, the number of c_j's satisfying (12) is given by

$$A = \left[\sum_{k=0}^{2^{v-1}-1} \binom{2^v}{2k+1} \right]^{\frac{p-1}{2}} = 2^{(2^v-1)(\frac{p-1}{2})}.$$

Meanwhile, there are no conditions on c_j's for $j \in \{p, 2p, \cdots, (\frac{n}{2p}-1)p\}$ in M. Thus, the number of choices of such c_j's is given by

$$B = 2^{\frac{n}{2p}-1} = 2^{2^{v-1}-1}.$$

Consequently, the number of vectors $\underline{\mathbf{c}}$ which satisfy (8) is given by

$$N_{nb} = A \cdot B = 2^{\frac{n-1-p}{2}}$$

which is equal to the number vectors $\underline{\mathbf{c}}$ producing the non-bent functions. Therefore, the number of vectors $\underline{\mathbf{c}}$ producing the bent functions is given by N_b. ■

TABLE I

CONSTRUCTION OF BENT FUNCTIONS WITH QUADRATIC EXPONENTS FOR $n = 12$ (65 CORRESPONDS TO $Tr_1^6(x^{65})$)

$(c_1c_2c_3c_4c_5)$	Trace exponents	$(c_1c_2c_3c_4c_5)$	Trace exponents
(00000)	65	(01010)	5, 17, 65
(00100)	9, 65	(01110)	5, 9, 17, 65
(00011)	17, 33, 65	(10010)	3, 17, 65
(00111)	9, 17, 33, 65	(10110)	3, 9, 17, 65
(01001)	5, 33, 65	(11000)	3, 5, 65
(01101)	5, 9, 33, 65	(11100)	3, 5, 9, 65
(10001)	3, 33, 65	(11011)	3, 5, 17, 33, 65
(10101)	3, 9, 33, 65	(11111)	3, 5, 9, 17, 33, 65

Remark 1: The first few primes p of Theorem 1 are

$$3, 5, 7, 11, 13, 19, 23, 29, 37, 47, 53, 59, 61, 71, \cdots$$

Note that the matrix M is useful for understanding the construction in Theorem 1. In other words, in the proof of Theorem 1, let $M = [\mathbf{V}_0, \mathbf{V}_1, \cdots, \mathbf{V}_{p-1}]$ where $\mathbf{V}_i$ for $0 \leq i \leq p-1$ is the ith column vector of M. Then, $f(x)$ is bent if and only if there exists at least a pair of column vectors $\mathbf{V}_i$ and $\mathbf{V}_{p-i}$ for $1 \leq i \leq \frac{p-1}{2}$ such that the sum of elements in the pair is equal to 0.

Example 1: For $n = 12 = 2^2 \times 3$, the matrix representation of each coefficients is given by

$$M = \begin{bmatrix} 0 & c_1 & c_2 \\ c_3 & c_4 & c_5 \end{bmatrix}$$

Thus, $f(x) = \sum_{i=1}^{5} c_i Tr_1^{12}(x^{1+2^i}) + Tr_1^6(x^{65})$ is bent if and only if

$$c_1 + c_4 + c_2 + c_5 = 0$$

and c_3 can be free to choose. Also, the number of bent functions is given by

$$N_b = 2^5 - 2^{\frac{12-1-3}{2}} = 32 - 16 = 16.$$

All possible 16 bent functions are listed in Table I.

Note. For $n = 2p$, we have $w_i = c_i$. Thus, $f(x)$ is bent if and only if there exists at least one i with $1 \leq i \leq \frac{p-1}{2}$ such that $c_i = c_{p-i}$. In Theorem 2 of [18], the authors attempted to state the sufficient condition of this result. However, the assertion appeared there is not in a clear way.

IV. CONSTRUCTION FOR $n = 2^v p^r$

In this section, we present a necessary and sufficient condition on c_i's that $f(x)$ given by (6) is bent for $n = 2^v p^r$ with $v \geq 1$ and $r \geq 2$, where p is odd prime with $\mathrm{ord}_p(2) = p-1$ or $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ with odd s. We start from the following definition and lemma.

Definition 1: Let $t(x) = \sum_{i=1}^{m} t_i x^i + 1$ where $t_i \in \mathbb{F}_2$ and m is even. Then, $t(x)$ is called *circular symmetric with* m if

$$t_{m+1-i} = t_i, \quad i = 1, 2, \cdots, m/2.$$

Lemma 2: Let $m = p^k - 1$ for odd prime p and an integer $k > 1$, and $t(x)$ be circular symmetric with m. Assume that there exists a polynomial $h(x) \in \mathbb{F}_2[x]$ such that $t(x) = Q_{p^k}(x)h(x)$, where $Q_{p^k}(x)$ is the p^kth cyclotomic polynomial. Then,

(a) $h(x)$ is circular symmetric with degree $\deg(h) \leq p^{k-1} - 1$.

(b) If we write $h(x) = \sum_{i=1}^{p^{k-1}-1} h_i x^i + 1,\ h_i \in \mathbb{F}_2$, then

$$t(x) = Q_{p^k}(x) + \sum_{j=0}^{p-1} \sum_{i=1}^{p^{k-1}-1} h_i x^{i+jp^{k-1}}.$$

In other words, $t(x)$ contains all monomial terms of $Q_{p^k}(x)$.

Proof: (a) The circular symmetric polynomial $t(x)$ with $m = p^k - 1$ has the following property.

$$x^{p^k} t(x^{-1}) = \sum_{i=1}^{p^k-1} t_i x^{p^k-i} + x^{p^k} = \sum_{i=1}^{p^k-1} t_{p^k-i} x^i + x^{p^k} = t(x) + x^{p^k} + 1. \tag{13}$$

From $t(x) = Q_{p^k}(x)h(x)$ and the self-reciprocity of $Q_{p^k}(x)$ (Property 1 in Section II),

$$\begin{aligned} x^{p^k} t(x^{-1}) &= x^{p^k} Q_{p^k}(x^{-1}) h(x^{-1}) = x^{\phi(p^k)} Q_{p^k}(x^{-1}) \cdot x^{p^k - \phi(p^k)} h(x^{-1}) \\ &= Q_{p^k}(x) \cdot x^{p^k - \phi(p^k)} h(x^{-1}). \end{aligned} \tag{14}$$

From (13) and (14), we have

$$Q_{p^k}(x)(x^{p^k-\phi(p^k)} h(x^{-1}) + h(x)) = x^{p^k} + 1 = \prod_{d|p^k} Q_d(x).$$

Therefore,

$$\begin{aligned} x^{p^k-\phi(p^k)} h(x^{-1}) + h(x) &= \prod_{d|p^k, d \neq p^k} Q_d(x) = Q_1(x) Q_p(x) \cdots Q_{p^{k-1}}(x) \\ &= x^{p^{k-1}} + 1. \end{aligned} \tag{15}$$

Since $\deg(t(x)) \le p^k - 1$, we have $\deg(h(x)) \le p^k - 1 - \phi(p^k) = p^{k-1} - 1$ where $\phi(p^k) = p^k\left(1 - \frac{1}{p}\right) = p^k - p^{k-1}$. Furthermore, $h(0) = 1$ from $t(0) = Q_{p^k}(0) = 1$. Thus, $h(x)$ can be written as $h(x) = 1 + \sum_{i=1}^{p^{k-1}-1} h_i x^i$ where $h_i \in \mathbb{F}_2$. Hence, we have

$$x^{p^k-\phi(p^k)}h(x^{-1}) = \sum_{i=1}^{p^{k-1}-1} h_i x^{p^{k-1}-i} + x^{p^{k-1}} = \sum_{i=1}^{p^{k-1}-1} h_{p^{k-1}-i}x^i + x^{p^{k-1}} \tag{16}$$

where the last equality is from the change of a variable from $p^{k-1} - i$ to i. Applying this to (15), we get the requirement of coefficient h_i, i.e.,

$$\sum_{i=1}^{\frac{p^{k-1}-1}{2}} (h_i + h_{p^{k-1}-i})(x^i + x^{p^{k-1}-i}) = 0$$

or equivalently,

$$h_i = h_{p^{k-1}-i}, \quad 1 \le i \le \frac{p^{k-1}-1}{2}.$$

From Definition 1, $h(x)$ is circular symmetric.

(b) We may write $t(x) = Q_{p^k}(x)h(x) = Q_{p^k}(x) + Q_{p^k}(x)\sum_{i=1}^{p^{k-1}-1} h_i x^i$. From $Q_{p^k}(x) = Q_p(x^{p^{k-1}}) = \sum_{j=0}^{p-1} x^{p^{k-1}j}$, we get

$$t(x) = Q_{p^k}(x) + \sum_{j=0}^{p-1}\sum_{i=1}^{p^{k-1}-1} h_i x^{i+p^{k-1}j} = Q_{p^k}(x) + A(x)$$

where $A(x)$ is the double summation of the second term. Note that an exponent of a monomial term in $A(x)$ has a form $i + p^{k-1}j$ where $1 \le i \le p^{k-1} - 1$ and $0 \le j \le p - 1$, and an exponent of a monomial term of $Q_{p^k}(x)$ has a form $p^{k-1}u$ where $0 \le u \le p - 1$. Thus, all monomial terms in $A(x)$ are distinct from the monomials in $Q_{p^k}(x)$. Therefore, all terms of $Q_{p^k}(x)$ remain in $t(x)$. ■

Similar to the case of $n = 2^v p$, we need to investigate $\bar{c_k}(x)$, $c(x)$ reduced modulo $x^{p^k} + 1$ for each k with $1 \le k \le r$ for the case of $n = 2^v p^r$ with $r \ge 2$. In order to do so, we need the following two lemmas on $\bar{c_k}(x)$.

Lemma 3: Let $\bar{c_k}(x)$ be $c(x)$ reduced modulo $x^{p^k} + 1$ for each k with $1 \le k \le r$, where $c(x)$ is given by (3) for $n = 2^v p^r$ with $v \ge 1$ and $r \ge 2$. Then,

$$\begin{aligned} \bar{c_k}(x) &\equiv c(x) \pmod{x^{p^k} + 1} \\ &= \sum_{i=1}^{p^k-1} w_{i,k}(x^i + x^{p^k-i}) + 1 = \sum_{i=1}^{\frac{p^k-1}{2}} (w_{i,k} + w_{p^k-i,k})(x^i + x^{p^k-i}) + 1 \end{aligned} \tag{17}$$

where $w_{i,k} = \sum_{l=0}^{\frac{n}{2p^k}-1} c_{i+lp^k}$. Furthermore, $\bar{c_k}(x)$ is circular symmetric.

Proof: Similar to (9), $c(x)$ can be rewritten as

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

With $w_{i,k} = \sum_{l=0}^{\frac{n}{2p^k}-1} c_{i+lp^k}$, $\bar{c_k}(x)$ is given by (17), which shows $\bar{c_k}(x)$ is circular symmetric. ■

Lemma 4: With the notation of Lemma 3,

(a) $\gcd(c(x), Q_{p^k}(x)) \neq 1$ if and only if $\gcd(\bar{c_k}(x), Q_{p^k}(x)) \neq 1$.

(b) Let p be odd prime with $\mathrm{ord}_p(2) = p-1$ or $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ where s is odd. Then, $\gcd(c(x), Q_{p^k}(x)) \neq 1$ if and only if $\gcd(\bar{c}(x), Q_{p^k}(x)) = Q_{p^k}(x)$.

Proof: (a) From the definition of $\bar{c_k}(x)$,

$$c(x) = b(x)(x^{p^k}+1) + \bar{c_k}(x) = b(x)Q_1(x)\prod_{i=1}^{k} Q_{p^i}(x) + \bar{c_k}(x)$$

where $b(x)$ is a quotient of $c(x)$ divided by $x^{p^k}+1$. Hence, if $Q_{p^k}(x)$ has a common factor with $\bar{c_k}(x)$, then it also has the common factor with $c(x)$, and vice versa.

(b) If $\mathrm{ord}_p(2) = p-1$, from Property 4 in Section II, $Q_{p^k}(x)$ is irreducible over $\mathbb{F}_2$ for a given k. From the irreducibility of $Q_{p^k}(x)$ and Lemma 4-(a), we have

$$\begin{aligned} \gcd(c(x), Q_{p^k}(x)) \neq 1 &\iff \gcd(\bar{c_k}(x), Q_{p^k}(x)) \neq 1 \\ &\iff \gcd(\bar{c_k}(x), Q_{p^k}(x)) = Q_{p^k}(x). \end{aligned} \tag{18}$$

If $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ where s is odd, on the other hand, we have

$$Q_{p^k}(x) = Q_p(x^{p^{k-1}}) = G_1(x)G_2(x), \quad G_i(x) = g_i(x^{p^{k-1}}),\ i = 1, 2.$$

where $g_1(x)$ and $g_2(x)$ are the irreducible factors of $Q_p(x)$ such that $Q_p(x) = g_1(x)g_2(x)$ and $g_2(x) = x^s g_1(x^{-1})$ [6]. From Property 4, $G_1(x)$ and $G_2(x)$ are irreducible over $\mathbb{F}_2$ and reciprocal to each other, i.e., $G_2(x) = x^{sp^{k-1}} G_1(x^{-1})$. Let z be a root of $Q_{p^k}(x)$. Then, $z \neq 1$. If z is a root of $G_1(x)$, then z^{-1} is a root of $G_2(x)$, and vice versa. (Note that if z is a root of $G_1(x)$, then z^{-1} cannot be its root. If it were true, then this holds for any other roots of $G_1(x)$ and thus the

number of valid roots of $G_1(x)$ should be even, which is impossible because sp^{k-1}, the degree of $G_1(x)$, is odd.) Since z is a root of $Q_{p^k}(x)$, we have $z^{p^k} = z^n = 1$. Thus, from (17), we have

$$\bar{c_k}(z) = \sum_{i=1}^{p^k-1} w_{i,k}(z^i + z^{p^k-i}) + 1 = \sum_{i=1}^{p^k-1} w_{i,k}(z^i + z^{-i}) + 1.$$

Hence, z^{-1} is a root of $\bar{c_k}(x)$ if z is its root. Therefore, if $\bar{c_k}(x)$ has the irreducible factor $G_1(x)$, then it simultaneously has the other irreducible factor $G_2(x)$, and vice versa. Similar to the case of $\mathrm{ord}_p(2) = p - 1$, we have (18) for a given k.

■

In (17), we denote

$$u_{i,k} = w_{i,k} + w_{p^k-i,k}, \quad 1 \le i \le p^k - 1 \tag{19}$$

for each k with $1 \le k \le r$. Let U_k be a $p \times p^{k-1}$ matrix whose entries are given by $u_{i,k}$, i.e.,

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

where we set $u_{0,k} = 1$. We write

$$U_k = \begin{bmatrix} \mathbf{A}_{0,k} & \mathbf{A}_{1,k} & \cdots & \mathbf{A}_{p^{k-1}-1,k} \end{bmatrix} \tag{20}$$

where $\mathbf{A}_{i,k}$ is the ith column vector of U_k. From (19), we have $u_{i,k} = u_{p^k-i,k}$. Using the matrix U_k, we give the construction of all bent functions represented by (6) for $n = 2^v p^r$ with $v \ge 1$ and $r \ge 2$.

Theorem 2: With the above notation, let p be odd prime with $\mathrm{ord}_p(2) = p - 1$ or $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ where s is odd, and $n = 2^v p^r$ with $v \ge 1$ and $r \ge 2$. Then, $f(x)$ given by (6) is bent if and only if for each k with $1 \le k \le r$, there exists at least one i for $0 \le i \le \frac{p^{k-1}-1}{2}$ such that $\mathbf{A}_{i,k}$, given by (20), is not a constant vector. In other words, $\mathbf{A}_{0,k} \ne (1, 1, \cdots, 1)$ or $\mathbf{A}_{i,k} \ne (c, c, \cdots, c)$ where $c \in \{0, 1\}$ for at least one i with $1 \le i \le \frac{p^{k-1}-1}{2}$.

Proof: Similar to the proof of Theorem 1, we will derive the conditions on $\bar{c_k}(x)$ for $f(x)$ given by (6) to be non-bent.

From Fact 1 and Corollary 1, $f(x)$ is bent if and only if $\gcd(c(x), x^n+1) = \gcd(c(x), x^{p^r}+1) = 1$. Since $Q_{p^k}(x)$'s for $1 \leq k \leq r$ are all factors of $(x^{p^r}+1)/(x+1)$, we have $\gcd(c(x), x^n+1) = 1$ if and only if $\gcd(c(x), Q_{p^k}(x)) = 1$ for every k. Therefore, $f(x)$ is non-bent if and only if there exists at least one k for $1 \leq k \leq r$ such that $\gcd(c(x), Q_{p^k}(x)) \neq 1$. From Lemma 4, we see that if $\mathrm{ord}_p(2) = p-1$ or $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ with odd s, then $\gcd(c(x), Q_{p^k}(x)) \neq 1$ if and only if $\gcd(\bar{c_k}(x), Q_{p^k}(x)) = Q_{p^k}(x)$. Thus, $\bar{c_k}(x)$ can be represented by

$$\bar{c_k}(x) = Q_{p^k}(x)h(x) \tag{21}$$

where $h(x) = 1 + \sum_{i=1}^{p^{k-1}-1} h_i x^i,\ h_i \in \mathbb{F}_2$.

From Lemma 3, $\bar{c_k}(x)$ is circular symmetric with $\deg(\bar{c_k}(x)) \leq p^k - 1$. Hence, $h(x)$ is also circular symmetric with $\deg(h(x)) \leq p^{k-1} - 1$ from Lemma 2. Thus, together with (21), and noticing that $\bar{c_k}(x)$ is circular symmetric, we can rewrite $\bar{c_k}(x)$ as follows.

$$\begin{aligned}\bar{c_k}(x) &= Q_{p^k}(x) + \sum_{j=0}^{p-1}\sum_{t=1}^{p^{k-1}-1} h_t x^{t+jp^{k-1}} \\ &= \sum_{j=1}^{\frac{p-1}{2}}(x^{jp^{k-1}} + x^{p^k-jp^{k-1}}) + 1 + \sum_{t=1}^{p^{k-1}-1} h_t \sum_{j=0}^{\frac{p-1}{2}}(x^{t+jp^{k-1}} + x^{p^k-t-jp^{k-1}}).\end{aligned} \tag{22}$$

From Lemma 3, on the other hand, we have

$$\begin{aligned}\bar{c_k}(x) &= \sum_{i=1}^{p^k-1} w_{i,k}(x^i + x^{p^k-i}) + 1 \\ &= \sum_{j=1}^{p-1} w_{jp^{k-1},k}(x^{jp^{k-1}} + x^{p^k-jp^{k-1}}) + 1 + \sum_{i=1, i\neq jp^{k-1}}^{p^k-1} w_{i,k}(x^i + x^{p^k-i}) \\ &= \sum_{j=1}^{\frac{p-1}{2}}(w_{jp^{k-1},k} + w_{p^k-jp^{k-1},k})(x^{jp^{k-1}} + x^{p^k-jp^{k-1}}) + 1 \\ &\quad + \sum_{t=1}^{p^{k-1}-1}\sum_{j=0}^{\frac{p-1}{2}}(w_{t+jp^{k-1},k} + w_{p^k-t-jp^{k-1},k})(x^{t+jp^{k-1}} + x^{p^k-t-jp^{k-1}}), \quad (i = t+jp^{k-1}) \\ &= \sum_{j=1}^{\frac{p-1}{2}} u_{jp^{k-1},k}(x^{jp^{k-1}} + x^{p^k-jp^{k-1}}) + 1 + \sum_{t=1}^{p^{k-1}-1}\sum_{j=0}^{\frac{p-1}{2}} u_{t+jp^{k-1},k}(x^{t+jp^{k-1}} + x^{p^k-t-jp^{k-1}}).\end{aligned} \tag{23}$$

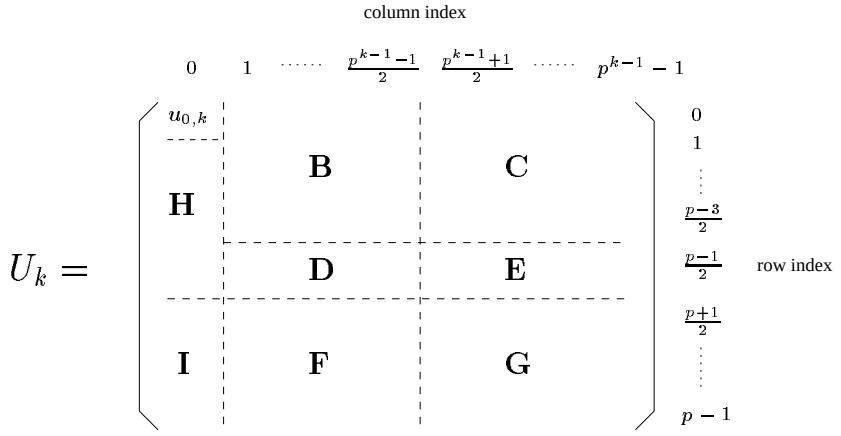

Fig. 1. Submatrix structure of U_k

By comparing (22) and (23), we have

$$u_{t+jp^{k-1},k} = \begin{cases} 1, & t = 0 \text{ and } 1 \le j \le \frac{p-1}{2}, \\ h_t, & 1 \le t \le p^{k-1}-1 \text{ and } 0 \le j \le \frac{p-1}{2}. \end{cases} \tag{24}$$

Thus, for the non-bent case, the entries of U_k, $u_{i,k}$ with $1 \le i \le \frac{p^k-1}{2}$, are determined by (24). This is equivalently saying that each column of U_k is a constant vector if and only if $f(x)$ is non-bent. This completes the proof for Theorem 2. ■

In the following, we write entries of U_k in detail in order to better understand Theorem 2. We see that U_k consists of several submatrices in Fig 1, which are defined as follows. Each of $\mathbf{B}, \mathbf{C}, \mathbf{F}, \mathbf{G}$ is an $l \times m$ matrix, where $l = \frac{p-1}{2}$ and $m = \frac{p^{k-1}-1}{2}$. Also, each of $\mathbf{D}$ and $\mathbf{E}$ is a $1 \times m$ matrix, and each of $\mathbf{H}$ and $\mathbf{I}$ is an $l \times 1$ matrix. From $u_{i,k} = u_{p^k-i,k}$ for $1 \le i \le \frac{p^k-1}{2}$, if $\mathbf{B} = [b_{i,j}]$, then $\mathbf{G} = [b_{l-i,m-j}]$. We denote this relation by $\mathbf{B} \sim \mathbf{G}$. Similarly, we have $\mathbf{C} \sim \mathbf{F}$. Also, if $\mathbf{D} = [d_{i,j}]$, then $\mathbf{E} = [d_{i,m-j}]$, denoted by $\mathbf{D} \sim \mathbf{E}$. Thus, each element in $\mathbf{E}, \mathbf{F}, \mathbf{G}$ is determined by each element in $\mathbf{B}, \mathbf{C}, \mathbf{D}$, respectively. In other words, column vectors $\mathbf{A}_{i,k}$ of U_k for $\frac{p^{k-1}+1}{2} \le i \le p^{k-1}-1$ are determined by column vectors $\mathbf{A}_{i,k}$ for $1 \le i \le \frac{p^{k-1}-1}{2}$.

Example 2: For $n = 18 = 2 \cdot 3^2$, $p = 3$ and $r = 2$. For $k = 1$, we consider U_1, i.e.,

$$U_1 = \begin{bmatrix} u_{0,1} \\ u_{1,1} \\ u_{2,1} \end{bmatrix} = \begin{bmatrix} 1 \\ w_{1,1} + w_{2,1} \\ w_{2,1} + w_{1,1} \end{bmatrix} = \begin{bmatrix} 1 \\ c_1 + c_4 + c_7 + c_2 + c_5 + c_8 \\ c_2 + c_5 + c_8 + c_1 + c_4 + c_7 \end{bmatrix}$$

From Theorem 2,

$$c_1 + c_4 + c_7 + c_2 + c_5 + c_8 = 0 \tag{25}$$

at $k = 1$ for $f(x)$ defined by (6) to be bent. If $k = 2$, on the other hand,

$$U_2 = \begin{bmatrix} u_{0,2} & u_{1,2} & u_{2,2} \\ u_{3,2} & u_{4,2} & u_{5,2} \\ u_{6,2} & u_{7,2} & u_{8,2} \end{bmatrix} = \begin{bmatrix} 1 & w_{1,2} + w_{8,2} & w_{2,2} + w_{7,2} \\ w_{3,2} + w_{6,2} & w_{4,2} + w_{5,2} & w_{5,2} + w_{4,2} \\ w_{6,2} + w_{3,2} & w_{7,2} + w_{2,2} & w_{8,2} + w_{1,2} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & c_1 + c_8 & c_2 + c_7 \\ c_3 + c_6 & c_4 + c_5 & c_5 + c_4 \\ c_6 + c_3 & c_7 + c_2 & c_8 + c_1 \end{bmatrix}.$$

Hence,

$$c_3 + c_6 = 0 \text{ or the vector } (c_1 + c_8, c_4 + c_5, c_7 + c_2) \text{ is not constant} \tag{26}$$

at $k = 2$ for $f(x)$ defined by (6) to be bent. Both (25) and (26) must be achieved so that $f(x)$ is bent. Hence, we see that $f(x)$ is bent at the following two exclusive cases.

(a) $c_1 + c_4 + c_7 + c_2 + c_5 + c_8 = 0$ and $c_3 + c_6 = 0 \Longrightarrow 64$ cases, or

(b) $(c_1 + c_8, c_4 + c_5, c_7 + c_2) = (0,1,1), (1,0,1), (1,1,0)$ and $c_3 + c_6 = 1 \Longrightarrow 48$ cases.

In (b), $c_3 + c_6 = 1$ is required to distinguish (b) from (a). For example, with $(c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8) = (01110100)$, $f(x) = Tr(x^5 + x^9 + x^{17} + x^{65}) + Tr_1^9(x^{513})$ is bent. Finally, we have in total of $64 + 48 = 112$ bent functions of $f(x)$ whose c_i's satisfy either (a) or (b). It is also verified by the results of computer experiments.

Remark 2: If $r = 2$, the number of the bent functions in Theorem 2 is given by

$$N_b = 2^{\frac{n}{2}-1} - N_{nb} = 2^{\frac{n}{2}-1} - \left[2^{\frac{n-p-1}{2}} + 2^{\frac{(n-p^2)(p^2-1)}{2p^2}} \cdot (2^{\frac{p-1}{2}} - 1)\right] \tag{27}$$

where the second term is the number of non-bent functions, denoted by N_{nb}. The proof of (27) is similar to those of the enumeration part of Theorem 1, but one needs to consider the condition for U_2. This makes the proof rather lengthy, so we omit it here.

If $r \geq 3$, in order to obtain the exact formula for the enumeration of the bent functions constructed in Theorem 2, one has to carefully distinguish a number of cases because the conditions imposed on c_i's in U_k for bent (or non-bent) functions are not independent for each k with $1 \leq k \leq r$.

V. Iterative construction of high degree bent functions using quadratic bent functions

In [6], Charpin, Pasalic, and Tavernier proposed a recursive construction of bent functions with high degree using bent functions with low degree. In this section, we apply this iterative method to construct bent functions with high degree using bent functions with quadratic exponents. As an example, we give the case of bent functions of n variables with degree $\frac{n}{2}$ using quadratic bent functions in polynomial forms.

In [6], Charpin, Pasalic, and Tavernier established the following fact to obtain bent functions with higher degree.

Fact 2: For even n and $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$ with $x_i \in \mathbb{F}_2$, let $f_1(\mathbf{x})$ and $f_2(\mathbf{x})$ be distinct bent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then, $s_1(\mathbf{x}, x_n)$ and $s_2(\mathbf{x}, x_n)$ defined by

$$s_1(\mathbf{x}, x_n) = s_1(x_0, \cdots, x_n) = f_1||f_2 = x_n f_1(\mathbf{x}) + (1 + x_n) f_2(\mathbf{x}),$$

$$s_2(\mathbf{x}, x_n) = s_2(x_0, \cdots, x_n) = (1 + f_1)||f_2 = x_n(1 + f_1(\mathbf{x})) + (1 + x_n) f_2(\mathbf{x})$$

are semi-bent functions from $\mathbb{F}_2^{n+1}$ to $\mathbb{F}_2$. Also, $b(\mathbf{x}, x_n, x_{n+1})$ defined by

$$b(\mathbf{x}, x_n, x_{n+1}) = b(x_0, \cdots, x_n, x_{n+1}) = s_1||s_2 = x_{n+1} s_1(\mathbf{x}, x_n) + (1 + x_{n+1}) s_2(\mathbf{x}, x_n)$$

is a bent function from $\mathbb{F}_2^{n+2}$ to $\mathbb{F}_2$. The degree of $s_1(\mathbf{x}, x_n), s_2(\mathbf{x}, x_n)$ and $b(\mathbf{x}, x_n, x_{n+1})$ is given by

$$\deg(s_1(\mathbf{x}, x_n)) = \deg(s_2(\mathbf{x}, x_n)) = \deg(b(\mathbf{x}, x_n, x_{n+1})) = \max(\deg(f_1), \deg(f_2)) + 1.$$

Using Fact 2, Charpin, Pasalic, and Tavernier showed that a bent function with high degree can be recursively constructed by concatenating known bent functions with low degree. In Sections III and IV, we constructed a large number of quadratic polynomial bent functions. Using these bent functions and Fact 2, therefore, we can recursively construct bent functions with higher degree. In the following, we demonstrate a general procedure for applying the iterative method of Charpin, Pasalic, and Tavernier for the construction of bent functions of $n = 2k$ variables with degree k using the quadratic bent functions constructed in Sections III and IV.

Procedure: From $i = 0$ to $k - 3$,

Step 1) Initialization: Select b_0 as a quadratic bent function of 4 variables. In each iteration, b_i is a bent function of $2i + 4$ variables with degree $i + 2$ constructed from a previous iteration.

Step 2) Quadratic bent function: Select q_i as a quadratic bent function of $2i+4$ variables. Make sure that $q_0 \neq b_0$.

Step 3) Intermediate semi-bent functions: Compute semi-bent functions $s_{2i+1} = b_i||q_i$ and $s_{2i+2} = (1+b_i)||q_i$ of $2i+5$ variables with degree $i+3$.

Step 4) Higher degree bent function: Compute a bent function $b_{i+1} = s_{2i+1}||s_{2i+2}$ of $2i+6$ variables with degree $i+3$.

Step 5) Iteration: If $i = k-3$, stop iterations. Otherwise, increase i by 1, go back to Step 2) and iterate Step 2) $-$ 5).

In the above procedure, b_{k-2} is the bent function of $2k$ variables with degree k. The following is an example which illustrates the above iterative construction.

Example 3: Following the above iterative procedure, we obtain a bent function of 12 variables with degree $k = 6$.

1) $i = 0$: At Steps 1 and 2, we consider quadratic bent functions whose trace representations are given by

$$b_0(x) = Tr_1^4(x) + Tr_1^2(x^5), \quad q_0(x) = Tr_1^4(x^3) + Tr_1^2(x^5).$$

Using a basis $(1, \alpha, \alpha^2, \alpha^3)$ of $\mathbb{F}_{2^4}$ where α is a primitive element of $\mathbb{F}_{2^4}$ defined by $\alpha^4+\alpha+1=0$ and $x = \sum_{i=0}^{3} x_i\alpha^i$, we convert $b_0(x)$ and $q_0(x)$ into their Boolean representations which are given by

$$b_0(x) = b_0\left(\sum_{i=0}^{3} x_i\alpha^i\right) = x_1 + x_2 + x_3 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 = b_0(x_0, x_1, x_2, x_3),$$

$$q_0(x) = q_0\left(\sum_{i=0}^{3} x_i\alpha^i\right) = x_3 + x_0x_3 + x_1x_2 = q_0(x_0, x_1, x_2, x_3)$$

where the computation is performed in $\mathbb{F}_{2^4}$. At Step 3, concatenating b_0 and q_0, two semi-bent functions of 5 variables with degree 3 can be constructed, i.e.,

$$s_1(x_0, \cdots, x_4) = b_0||q_0 = x_4b_0(x_0, \cdots, x_3) + (1+x_4)q_0(x_0, \cdots, x_3),$$

$$s_2(x_0, \cdots, x_4) = (1+b_0)||q_0 = x_4(1+b_0(x_0, \cdots, x_3)) + (1+x_4)q_0(x_0, \cdots, x_3).$$

At Step 4, a new bent function of 6 variables with degree 3 can be constructed by concatenating s_1 and s_2, i.e.,

$$b_1(x_0, \cdots, x_5) = s_1||s_2 = x_5s_1(x_0, \cdots, x_4) + (1+x_5)s_2(x_0, \cdots, x_4).$$

2) $i = 1$: At Step 2, we select a quadratic bent function $q_1(x)$ from $\mathbb{F}_{2^6}$ to $\mathbb{F}_2$ given by $q_1(x) = Tr_1^6(x) + Tr_1^3(x^9)$ where $\mathbb{F}_{2^6}$ is defined by $\alpha^6 + \alpha + 1 = 0$ and $x = \sum_{i=0}^{5} x_i\alpha^i$. From the similar approach to 1), its Boolean representation $q_1(x_0, \cdots, x_5)$ is given by

$$q_1(x_0, \cdots, x_5) = x_0 + x_1 + x_2 + x_4 + x_5 + x_0x_5 + x_1x_2 + x_1x_3 + x_2x_4 + x_2x_5 + x_3x_5 + x_4x_5$$

where the computation is performed in $\mathbb{F}_{2^6}$. At Steps 3 and 4, we compute semi-bent functions $s_3(x_0, \cdots, x_6) = b_1||q_1$ and $s_4(x_0, \cdots, x_6) = (1 + b_1)||q_1$, and a bent function $b_2(x_0, \cdots, x_7) = s_3||s_4$ of 8 variables with degree 4, respectively.

3) $i = 2$: At Step 2, $q_2(x) = Tr_1^8(x^3)+Tr_1^4(x^{17})$ where $\mathbb{F}_{2^8}$ is defined by $\alpha^8+\alpha^4+\alpha^3+\alpha^2+1 = 0$ and $x = \sum_{i=0}^{7} x_i\alpha^i$. Then, the Boolean representation of $q_2(x)$ is given by

$$\begin{aligned} q_2(x_0, \cdots, x_7) =& x_5 + x_0x_5 + x_1x_3 + x_1x_6 + x_2x_5 + x_2x_6 + x_3x_6 + x_3x_7 + x_4x_5 \\ &+ x_4x_7 + x_5x_6 + x_5x_7 + x_6x_7 \end{aligned}$$

where the computation is performed in $\mathbb{F}_{2^8}$. At Steps 3 and 4, we obtain a new bent function of 10 variables with degree 5 defined by $b_3 = s_5||s_6$, where s_5 and s_6 are semi-bent functions defined by $s_5 = b_2||q_2$ and $s_6 = (1 + b_2)||q_2$, respectively.

4) $i = 3$: At Step 2, $q_3(x) = Tr_1^{10}(x^3) + Tr_1^5(x^{33})$ whose Boolean representation is given by

$$\begin{aligned} q_3(x_0, \cdots, x_9) =& x_0 + x_1 + x_2 + x_3 + x_4 + x_6 + x_8 + x_0x_7 + x_1x_2 + x_1x_8 + x_2x_4 + x_2x_7 \\ &+ x_2x_9 + x_3x_8 + x_4x_5 + x_4x_7 + x_4x_8 + x_5x_7 + x_5x_9 + x_6x_9 \end{aligned}$$

where $\mathbb{F}_{2^{10}}$ is defined by $\alpha^{10}+\alpha^3+1 = 0$, $x = \sum_{i=0}^{9} x_i\alpha^i$, and the computation is performed in $\mathbb{F}_{2^{10}}$. At Steps 3 and 4, $b_4 = s_7||s_8$, where s_7 and s_8 are semi-bent functions defined by $s_7 = b_3||q_3$ and $s_8 = (1 + b_3)||q_3$, respectively. Since $i = k - 3 = 3$, iterations stop. b_4 is a bent function with degree 6.

We summarize the Boolean representations of b_1, b_2, b_3 and b_4 in Table II.

VI. Conclusion and discussion

We have constructed all bent functions represented by a polynomial form (2) by giving a necessary and sufficient condition on c_i's for $n = 2^v p^r$ with $v \geq 1$ and $r \geq 1$, where p is odd prime with $\mathrm{ord}_p(2) = p - 1$ or $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ with odd s. The enumeration for such bent functions has also been given for $n = 2^v p^r$ with $v \geq 1$ and $r = 1, 2$. Applying the

TABLE II

BENT FUNCTIONS OF n VARIABLES WITH DEGREE $\frac{n}{2}$, $n = 6, 8, 10, 12$.

n	Bent functions	Degree
6	$b_1 = x_3 + x_4 + x_0x_3 + x_1x_2 + x_1x_4 + x_2x_4 + x_4x_5 + x_1x_3x_4 + x_2x_3x_4$	3
8	$b_2 = x_0 + x_1 + x_2 + x_4 + x_5 + x_6 + x_0x_5 + x_0x_6 + x_1x_2 + x_1x_3 + x_1x_6 + x_2x_4 + x_2x_5 + x_2x_6$ $+x_3x_5 + x_3x_6 + x_4x_5 + x_5x_6 + x_6x_7 + x_0x_3x_6 + x_0x_5x_6 + x_1x_3x_6 + x_1x_4x_6 + x_2x_5x_6$ $+x_3x_5x_6 + x_1x_3x_4x_6 + x_2x_3x_4x_6$	4
10	$b_3 = x_5 + x_8 + x_0x_5 + x_0x_8 + x_1x_3 + x_1x_6 + x_1x_8 + x_2x_5 + x_2x_6 + x_2x_8 + x_3x_6 + x_3x_7 + x_4x_5$ $+x_4x_7 + x_4x_8 + x_5x_6 + x_5x_7 + x_6x_7 + x_4x_8 + x_6x_8 + x_8x_9 + x_0x_6x_8 + x_1x_2x_8 + x_3x_5x_8$ $+x_2x_4x_8 + x_3x_7x_8 + x_4x_7x_8 + x_5x_7x_8 + x_0x_3x_6x_8 + x_0x_5x_6x_8 + x_1x_3x_6x_8 + x_1x_4x_6x_8$ $+x_2x_5x_6x_8 + x_3x_5x_6x_8 + x_1x_3x_4x_6x_8 + x_2x_3x_4x_6x_8$	5
12	$b_4 = x_0 + x_1 + x_2 + x_3 + x_4 + x_6 + x_8 + x_{10} + x_0x_7 + x_0x_{10} + x_1x_2 + x_1x_8 + x_1x_{10} + x_2x_4 + x_2x_7$ $+x_2x_9 + x_2x_{10} + x_3x_8 + x_3x_{10} + x_4x_5 + x_4x_7 + x_4x_8 + x_4x_{10} + x_5x_7 + x_5x_9 + x_5x_{10} + x_6x_9$ $+x_6x_{10} + x_{10}x_{11} + x_0x_5x_{10} + x_0x_7x_{10} + x_0x_8x_{10} + x_1x_2x_{10} + x_1x_3x_{10} + x_1x_6x_{10} + x_2x_4x_{10}$ $+x_2x_5x_{10} + x_2x_6x_{10} + x_2x_7x_{10} + x_2x_8x_{10} + x_2x_9x_{10} + x_3x_6x_{10} + x_3x_7x_{10} + x_3x_8x_{10}$ $+x_5x_6x_{10} + x_5x_9x_{10} + x_6x_7x_{10} + x_6x_8x_{10} + x_6x_9x_{10} + x_8x_9x_{10} + x_0x_6x_8x_{10} + x_1x_2x_8x_{10}$ $+x_2x_4x_8x_{10} + x_3x_5x_8x_{10} + x_3x_7x_8x_{10} + x_4x_7x_8x_{10} + x_5x_7x_8x_{10} + x_0x_3x_6x_8x_{10} + x_0x_5x_6x_8x_{10}$ $+x_1x_3x_6x_8x_{10} + x_1x_4x_6x_8x_{10} + x_2x_5x_6x_8x_{10} + x_3x_5x_6x_8x_{10} + x_1x_3x_4x_6x_8x_{10} + x_2x_3x_4x_6x_8x_{10}$	6

recursive method of Charpin, Pasalic, and Tavernier, we have demonstrated an iterative procedure to construct bent functions with maximum degree using the polynomial quadratic bent functions constructed in this paper.

In this correspondence, however, we did not study the case for general n. In the light of the constructions for $n = 2^v p^r$, for general n, we need to know the complete factorization over $\mathbb{F}_2$ of the dth cyclotomic polynomials where d is a factor of n. Unfortunately, this is unknown in the literature even for the case $d = pq$ [16] where both p and q are primes.

ACKNOWLEDGMENT

The authors would like to thank Dr. Pascale Charpin for sending the preprint of [6].

REFERENCES

[1] E. R. Berlekamp, *Algebraic Coding Theory*. Aegean Park Press, CA, Revised ed. 1984.

[2] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "On cryptographic properties of the cosets of $R(1, m)$," *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1494-1513, 2001.

[3] A. Canteaut and P. Charpin, "Decomposing bent functions," *IEEE Trans. Inform. Theory*, vol. 49, no. 8, pp. 2004-2019, 2003.

[4] C. Carlet, "A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction," *Advances in Cryptology - CRYPTO 2002, no. 2442 in Lecture Notes in Computer Science*, pp. 549-564, 2002.

[5] C. Carlet, P. Charpin, and V. A. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystem," *Designs, Codes, and Cryptography*, vol. 15, pp. 125-156, 1998.

[6] P. Charpin, E. Pasalic, and C. Tavernier, "On bent and semi-bent quadratic Boolean functions," *IEEE Trans. Inform. Theory*, vol. 51, no. 12, pp. 4286-4298, Dec. 2005.

[7] J. F. Dillon, "Elementary Hadamard difference set," Ph. D. Thesis, University of Maryland, 1974.

[8] J. F. Dillon, "New cyclic difference sets with Singer parameters," *Finite Fields and Their Applications*, pp. 342-389, 2004.

[9] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, "Construction of bent functions via Niho power functions," *Journal of Combinatorial Theory, Series A*, to appear.

[10] S. W. Golomb and G. Gong, *Signal Design for Good Correlation - for Wireless Communication, Cryptography and Radar.* Cambridge University Press, 2005.

[11] T. Helleseth and P. V. Kumar, *Sequences with Low Correlation*. a chapter in *Handbook of Coding Theory*. Edited by V. Pless and C. Huffman, Elsevier Science Publishers, 1998.

[12] T. Kasami, "Weight enumerators for several classes of subcodes of the 2nd-order Reed-Muller codes," *Information and Control*, vol. 18, pp. 369-394, 1971.

[13] K. Khoo, G. Gong, and D. R. Stinson, "A new characterization of semi-bent and bent functions on finite fields," *Designs, Codes, and Cryptography*, to appear.

[14] K. Khoo, G. Gong, and D. R. Stinson, "A new family of Gold-like sequences," *in Proc. of IEEE International Symposium on Information Theory (ISIT)*, p. 181, Lausanne, Switzerland, 2002.

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

[16] T. Y. Lam and K. H. Leung, "On the cyclotomic polynomial $\Phi_{pq}(X)$," *Amer. Math. Monthly 10*, pp. 562-564, 1996.

[17] R. Lidl and H. Niederreiter, *Finite Fields*. Encyclopedia of Mathematics and Its Applications, vol. 20, Addison-Wesley, 1983.

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

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

[20] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, vol. 23, 1987.

[21] R. L. McFarland, "A new family of noncyclic difference sets," *Journal of Combinatorial Theory, Series A*, 15, pp. 1-10, 1973.

[22] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory*, vol. 28, pp. 858-864, 1982.

[23] P. Udaya, "Polyphase and frequency hopping sequences obtained from finite rings," Ph. D. dissertation, Dept. Elec. Eng., Indian Inst. Technol., Kanpur, 1992.