Constructions of Quadratic Bent Functions

Nam Yul Yu and Guang Gong, *Member, IEEE*

Department of Electrical and Computer Engineering

University of Waterloo, CANADA

Abstract

We show that a necessary condition for $f(x) = \sum_{i=1}^{n/2-1} c_i Tr(x^{1+2^i}) + c_{n/2} Tr_1^{n/2}(x^{1+2^{n/2}})$, $c_i \in \mathbb{F}_2$ being bent is $c_{n/2} = 1$. We then present several constructions and enumerations for such bent functions. Using an iterative approach, we give a method to construct bent functions with maximum degree $\frac{n}{2}$ by using quadratic bent functions constructed in this paper.

Index Terms

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

I. Introduction

A bent function is a Boolean function with even number of variables whose Walsh transform has a constant magnitude [1]. In coding context, it is a coset of the first order Reed-Muller code with the largest minimum weight [2]. 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, see [3] - [7]. Moreover, the maximum nonlinearity corresponds to the minimized maximum correlation with a trace function. Thus, bent functions also have many applications in algebraic coding and sequence design [2] [8].

In [9] and [10], Khoo, Gong and Stinson investigated the following sum of monomial trace terms with quadratic exponents, i.e., the exponent of variables has 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 case [10]. Let $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$. Khoo, Gong and Stinson derived the 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 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 [3] if the spectrum of $f(x)$ belongs to the set $\{0, \pm 2^{\frac{n+2}{2}}\}$. 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, they derived some conditions that $f(x)$ with three or four trace terms are semi-bent. Then, they derived several constructions of semi-bent functions with higher degree from semi-bent functions for even n in (1), and bent functions with higher degree from semi-bent functions for odd n in (1).

In this paper, we consider a case of even n. Note that $f(x)$ given by (1) for even n is not bent for any choices of $c_i \in \mathbb{F}_2$ [3]. Surprisingly, we found that a necessary condition for bent functions with such a construction is given by

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

where $Tr_1^{n/2}(x)$ 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 construction. (Note. The single term $Tr_1^{n/2}(x^{1+2^{n/2}})$ together with linear function $Tr(x)$ generates the Kasami (small) signal set [11] [12].) Using a similar approach as in [10], we show that a necessary and sufficient condition for $f(x)$, given by (2), being bent is $\gcd(c(x), x^n + 1) = 1$ where

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

Using this condition, we construct all bent functions of (2) for special cases of n. In addition, we show that the bent functions can be used for obtaining a bent function with high degree by applying a recursive construction.

This paper is organized as follows. In Section II, we will give some preliminaries on concepts and definitions which will be used throughout the paper. In Section III, we show a necessary and sufficient condition for $f(x)$, given by (2), being bent, and for $n = 2^v$, $f(x)$ is bent for any choices of c_i's. In Section IV and V, we give their respective constructions for $n = 2^v p$ and $n = 2^v p^r, r > 1$, where p is odd prime and the order of 2 modulo p is $p-1$ or $\frac{p-1}{2} = s$, where s is odd. An enumeration for the case $n = 2^v p$ is also given. In Section VI, we give an iterative construction of bent functions of n variables with degree $\frac{n}{2}$ by using quadratic bent functions constructed in this paper.

II. PRELIMINARIES

The following notations 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 multiplication 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 division 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 functions

Let $\mathbf{x} = (x_0, \cdots, x_{n-1})$ be a vector in $\mathbb{F}_2^n$ with $x_i \in \mathbb{F}_2$. $f(\mathbf{x})$ is a *Boolean function* from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ which takes on values 0 or 1. For the theory of Boolean functions and their polynomial representations, readers are referred to [1], [2] and [12]. A Boolean function consists of a sum of all possible products of x_{i_j}'s, i.e.,

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

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

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 $\mathbb{F}_2$ corresponds 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.

B. Bent functions

A Boolean function of n variables is called a *bent function* if its Walsh transform has a constant magnitude [1] [2], where the Walsh transform of a Boolean function $f(\mathbf{x})$ is defined by

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

In an 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. For example, the following polynomial function $f(x)$ corresponds to a quadratic bent function.

$$f(x) = \sum_{i=1}^{n/2-1} Tr(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}), \quad x \in \mathbb{F}_{2^n}. \tag{4}$$

C. Cyclotomic polynomials

A polynomial whose roots are the field elements of order d is called the *dth cyclotomic polynomial* [13], denoted by $Q_d(x)$. $Q_d(x)$ is a monic polynomial of order d and degree $\phi(d)$, where $\phi(\cdot)$ is the Euler-totient function. $Q_d(x)$ has the following basic properties [14] [15].

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

a) $x^m + 1 = \prod_{d|m} Q_d(x)$.

b) For $d \geq 2$, $x^{\phi(d)} Q_d(x^{-1}) = Q_d(x)$. In other words, $Q_d(x)$ is *self-reciprocal*.

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 integer ring $\mathbb{Z}$, but it may not be irreducible over $\mathbb{F}_2$. Throughout the whole paper, we will consider the cyclotomic polynomial over $\mathbb{F}_2$. We list several useful properties on factorizations of $Q_d(x)$ over $\mathbb{F}_2$ without proofs. For more details, see [13], [14] and [15].

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 $g_i(x), 1 \le i \le t$ is irreducible. Then, degree of each $g_i(x), 1 \le i \le t$ is given by $\frac{\phi(p)}{t} = \frac{p-1}{t}$, and the order of $g_i(x)$ is p.

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

III. 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 [9] [10]. Similarly, we can establish a necessary and sufficient condition for a bent function with quadratic exponents for even n.

Theorem 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

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

Proof: The result can be shown in a similar fashion of Theorem 3.2 in [10], so we only give an outline of the proof. Note that the rank of the symplectic form $B_f(x, z) = f(x) + f(z) + f(x + z)$ should be n if $f(x)$ is bent [2]. Then, the dimension of a cyclic code C, generated by the vector $(c_0, c_1, \cdots, c_{n-1})$, is also n. Finally, the degree of a generator polynomial $g(x)$ of C is equal to 0. This means that $f(x)$ is bent if and only if $g(x) = \gcd(c(x), x^n + 1) = 1$. ■

Theorem 2: With the notation in Theorem 1, $c_{n/2} = 1$ if $f(x)$ is bent.

Proof: If $c_{n/2} = 0$, we have $c(1) = 0$ which implies that $c(x)$ has a factor $x + 1$ and $\gcd(c(x), x^n + 1) \neq 1$. From Theorem 1, therefore, $f(x)$ with $c_{n/2} = 0$ cannot be bent. In other words, if $f(x)$ is bent, then $f(x)$ has the form of (2). ■

Corollary 1: For $n = 2^v m, v \geq 1$ with 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. ■

In the following, we present the bent case for $n = 2^v$.

Theorem 3: For $n = 2^v, v \geq 2$, $f(x)$ given by (2) is a bent function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ for any choices of c_i's. Thus, total number of bent functions for $n = 2^v$ is given by

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

Proof: For $n = 2^v$, $x^n + 1 = (x + 1)^{2^v}$. Since the number of x^i terms of $c(x)$ in (3) is always odd, $c(1) = 1$ and $\gcd(c(x), x + 1) = 1$ for any choices of c_i's. From Corollary 1, $f(x)$ is bent for all choices of c_i's. ■

Remark 1: For odd n, Khoo, Gong and Stinson showed that a sufficient condition that $f(x)$ given by (1) is semi-bent for any choices of c_i's is $n = p$ where p is prime with $\mathrm{ord}_p(2) = p-1$ or $\frac{p-1}{2} = s$ with odd s. For even n, in Theorem 3, we presented that a sufficient condition that $f(x)$ given by (2) is bent for any choices of c_i's is $n = 2^v, v \geq 2$, which is totally different from the case of odd n.

IV. Construction and Enumeration for $n = 2^v p$

In this section, we construct and enumerate all bent functions for $n = 2^v p$.

Theorem 4: Let $n = 2^v p, v \geq 1$ and p be odd prime with $\mathrm{ord}_p(2) = p - 1$ or $\frac{p-1}{2} = s$, where s is odd. Then, $f(x)$ given by (2) is bent if and only if there exists at least one i such that

$$w_i + w_{p-i} = 0, \quad 1 \leq i \leq \frac{p-1}{2} \tag{6}$$

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

Proof: From Theorem 1 and Corollary 1, $f(x)$ is non-bent if and only if $\gcd(c(x), x^p+1) \neq 1$ for the corresponding $c(x)$. From $x^p+1 = Q_1(x)Q_p(x)$ where $Q_1(x) = x+1$, non-bent functions exist for $c(x)$ with $\gcd(c(x), Q_p(x)) \neq 1$ due to $\gcd(c(x), Q_1(x)) = 1$. If $\gcd(c(x), Q_p(x)) \neq 1$, there exists a root z of $Q_p(x)$ such that $c(z) = 0$. Note that $c(x)$ can be rewritten as

$$\begin{aligned} c(x) = &\sum_{i=1}^{p-1} c_i(x^i + x^{n-i}) + c_p(x^p + x^{n-p}) + \sum_{i=p+1}^{2p-1} c_i(x^i + x^{n-i}) + c_{2p}(x^{2p} + x^{n-2p}) \\ &+ \cdots + \sum_{i=(\frac{n}{2p}-1)p+1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i}) + x^{\frac{n}{2}}. \end{aligned} \tag{7}$$

Thus, $\bar{c}(x)$, $c(x)$ reduced modulo $x^p + 1$, is given by

$$\begin{aligned} \bar{c}(x) &\equiv c(x) \pmod{x^p + 1} \\ &= \sum_{i=1}^{p-1} w_i(x^i + x^{p-i}) + 1 = \sum_{i=1}^{\frac{p-1}{2}} (w_i + w_{p-i})(x^i + x^{p-i}) + 1 \end{aligned} \tag{8}$$

where $w_i = c_i + c_{i+p} + \cdots + c_{i+\frac{n}{2}-p} = \sum_{l=0}^{\frac{n}{2p}-1} c_{i+lp}$. From the definition of $\bar{c}(x)$, we have that $c(z) = 0$ if and only if $\bar{c}(z) = 0$.

If $\mathrm{ord}_p(2) = p-1$, $Q_p(x)$ is irreducible. Hence, $\bar{c}(z) = 0$ if and only if $\bar{c}(x) = Q_p(x) = \sum_{i=1}^{\frac{p-1}{2}} (x^i + x^{p-i}) + 1$. This is equivalent to

$$w_i + w_{p-i} = 1, \quad 1 \leq i \leq \frac{p-1}{2}. \tag{9}$$

If $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ and 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 and $g_2(x) = x^s g_1(x^{-1})$ [3]. From (8), we see that $\bar{c}(x)$ has a root of z^{-1} as well as z. If $\bar{c}(x)$ has an irreducible factor $g_1(x)$, therefore, it simultaneously has another irreducible factor $g_2(x)$, and vice versa. Hence, $\bar{c}(z) = 0$ if and only if $\bar{c}(x) = g_1(x)g_2(x) = Q_p(x)$. Finally, $f(x)$ is non-bent if and only if (9) is achieved regardless of $\mathrm{ord}_p(2)$. Conversely, $f(x)$ is bent if and only if there exists at least one i achieving (6).

Next, we consider the number of $c(x)$ corresponding to non-bent functions. From the definition of w_i, we have $w_{p-i} = \sum_{t=0}^{\frac{n}{2p}-1} c_{p-i+tp}$. We will show that the intersection of sets $\{i + lp | l = 0, \cdots, \frac{n}{2p} - 1\}$ and $\{p - i + tp | t = 0, \cdots, \frac{n}{2p} - 1\}$ is empty. If there is a pair (l, t) such that $i + lp = p - i + tp$, then $i = \frac{(t-l+1)p}{2}$. If $t < l$, then $i \leq 0$, and if $t \geq l$, then $i > \frac{p}{2}$. Therefore,

there exist no such i's for $1 \leq i \leq \frac{p-1}{2}$. Consequently, all indices k of c_k's in w_i and w_{p-i} are distinct. Since the number of distinct coefficients in w_i and w_{p-i} is $\frac{n}{p} = 2^v$, the number of c_i's satisfying (9) is given by

$$A = \left[\binom{2^v}{1} + \binom{2^v}{3} + \cdots + \binom{2^v}{2^v - 1} \right]^{\frac{p-1}{2}} = 2^{(2^v-1)(\frac{p-1}{2})}.$$

Besides, note that in (7), coefficients $c_p, c_{2p}, \cdots, c_{(\frac{n}{2p}-1)p}$ can take any values of 0 or 1, so the number of such cases is given by

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

Finally, the number of $c(x)$ corresponding to non-bent functions, denoted by N_{nb}, is given by

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

■

Remark 2: The first few primes p of Theorem 4 are

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

For easy visualizing the construction shown in Theorem 4, we consider a $\frac{n}{2p} \times p$ matrix of coefficients c_i, i.e.,

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

where $c_0 = 0$. Let $M = [\mathbf{V}_0, \mathbf{V}_1, \cdots, \mathbf{V}_{p-1}]$ where $\mathbf{V}_i, 0 \leq i \leq p-1$ is the ith column vector of M. Then, we see the sum of all elements of $\mathbf{V}_i, 1 \leq i \leq \frac{p-1}{2}$ is equal to w_i. From Theorem 4, therefore, $f(x)$ is bent if and only if there exists at least a pair of column vectors $\mathbf{V}_i$ and $\mathbf{V}_{p-i}$, $1 \leq i \leq \frac{p-1}{2}$ such that the sum of elements in the pair is equal to 0. We illustrates in Fig. 1 the construction of bent functions for $n = 2^v p$ with the matrix M.

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

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

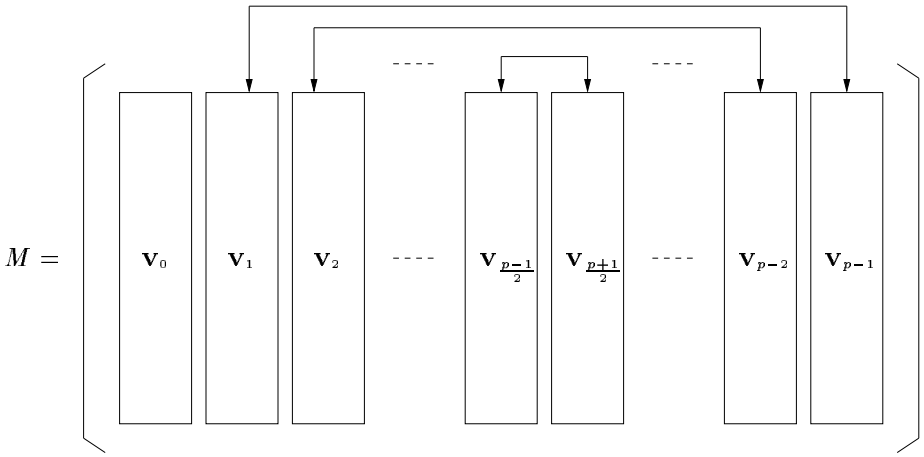

Fig. 1. Matrix illustration of construction of a bent function for $n = 2^v p$

TABLE I

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

$(c_1 c_2 c_3 c_4 c_5)$	Trace exponents	$(c_1 c_2 c_3 c_4 c_5)$	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

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.

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

In this section, we construct all bent functions for $n = 2^v p^r$ with $v \geq 1, r \geq 2$ which is a generalization of $n = 2^v p$ in Section IV. 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* if

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

Lemma 1: Let $t(x)$ be a circular symmetric polynomial of $m = p^k - 1$ for odd prime p and an integer $k > 1$. Assume that there exists $h(x)$ such that $t(x) = Q_{p^k}(x)h(x)$. Then,

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

(b)

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

where $h(x) = \sum_{i=1}^{p^{k-1}-1} h_i x^i + 1, h_i \in \mathbb{F}_2$. In other words, $t(x)$ contains all monomial terms in $Q_{p^k}(x)$.

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

$$x^{p^k} t(x^{-1}) = t(x) + x^{p^k} + 1. \tag{10}$$

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

$$\begin{aligned} x^{p^k} t(x^{-1}) &= x^{p^k} Q_{p^k}(x^{-1}) h(x^{-1}) = x^{\phi(p^k)} Q_{p^k}(x^{-1}) \cdot x^{p^k - \phi(p^k)} h(x^{-1}) \\ &= Q_{p^k}(x) \cdot x^{p^k - \phi(p^k)} h(x^{-1}). \end{aligned} \tag{11}$$

From (10) and (11),

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

Therefore,

$$\begin{aligned} x^{p^k - \phi(p^k)} h(x^{-1}) + h(x) &= \prod_{d | p^k, d \neq p^k} Q_d(x) = Q_1(x) Q_p(x) \cdots Q_{p^{k-1}}(x) \\ &= x^{p^{k-1}} + 1. \end{aligned} \tag{12}$$

From $\deg(t(x)) \leq p^k - 1$, $\deg(h(x)) \leq p^k - 1 - \phi(p^k) = p^{k-1} - 1$. Furthermore, $h(0) = 1$ from $t(0) = Q_{p^k}(0) = 1$. Thus, let $h(x) = 1 + \sum_{i=1}^{p^{k-1}-1} h_i x^i$, where $h_i \in \mathbb{F}_2$. Then,

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

Applying this to (12), we can 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) $t(x) = Q_{p^k}(x)h(x) = Q_{p^k}(x) + Q_{p^k}(x)\sum_{i=1}^{p^{k-1}-1} h_i x^i$. From $Q_{p^k}(x) = Q_p(x^{p^{k-1}}) = \sum_{j=0}^{p-1} x^{p^{k-1}j}$,

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

For $1 \le i \le p^{k-1} - 1$, it is clear that there are no i's such that an exponent of $x^{i+p^{k-1}j}$ in $A(x)$ is equal to $x^{p^{k-1}t}$ in $Q_{p^k}(x)$, i.e., $i + p^{k-1}j \ne p^{k-1}t$. Hence, 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 $k, 1 \le k \le r$. In order to do so, we need the following two lemmas on $\bar{c_k}(x)$.

Lemma 2: Let $\bar{c_k}(x)$ be $c(x)$ reduced modulo $x^{p^k} + 1$. Then,

$$\begin{aligned} \bar{c_k}(x) &\equiv c(x) \pmod{x^{p^k} + 1} \\ &= \sum_{i=1}^{p^k-1} w_{i,k}(x^i + x^{p^k-i}) + 1 = \sum_{i=1}^{\frac{p^k-1}{2}} (w_{i,k} + w_{p^k-i,k})(x^i + x^{p^k-i}) + 1 \end{aligned} \tag{13}$$

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

Proof: Similar to (7), $c(x)$ can be rewritten as

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

With $w_{i,k} = \sum_{l=0}^{\frac{n}{2p^k}-1} c_{i+lp^k}$, $\bar{c_k}(x)$ is given by (13). ■

Lemma 3: $Q_{p^k}(x)$ divides $c(x)$ if and only if $Q_{p^k}(x)$ divides $\bar{c_k}(x)$.

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

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

Hence, if $\bar{c_k}(x)$ has a factor of $Q_{p^k}(x)$, then $c(x)$ also has the factor, and vice versa. ■

In (13), we denote

$$u_{i,k} = w_{i,k} + w_{p^k-i,k}, \quad 1 \le i \le p^k - 1. \tag{14}$$

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

$$U_k = \begin{bmatrix} \mathbf{A}_{0,k} & \mathbf{A}_{1,k} & \cdots & \mathbf{A}_{p^{k-1}-1,k} \end{bmatrix} \tag{15}$$

where $\mathbf{A}_{i,k}$ is the ith column vector of U_k. From (14), $u_{i,k}$ is circular symmetric, i.e., $u_{i,k} = u_{p^k-i,k}$. Using the matrix U_k, we can construct bent functions for $n = 2^v p^r, r \ge 2$ in the following way.

Theorem 5: With the above notation, let p be odd prime with $\mathrm{ord}_p(2) = p-1$ or $\frac{p-1}{2} = s$, where s is odd, and $n = 2^v p^r, v \ge 1, r \ge 2$. Then, $f(x)$ given by (2) is bent if and only if for each $k, 1 \le k \le r$, there exist at least one $i, 0 \le i \le \frac{p^{k-1}-1}{2}$ such that $\mathbf{A}_{i,k}$ given by (15) is not a constant vector, i.e., $\mathbf{A}_{0,k} \ne (1,1,\cdots,1)$, or for $1 \le i \le \frac{p^{k-1}-1}{2}, \mathbf{A}_{i,k} \ne (c,c,\cdots,c)$ where $c \in \{0,1\}$.

Proof: From Theorem 1, $f(x)$ is bent if and only if $\gcd(c(x), x^n+1) = \gcd(c(x), x^{p^r}+1) = 1$. Since $Q_{p^k}(x), 1 \le k \le r$ 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 each k. Conversely, $f(x)$ is non-bent if and only if there exists at lease one $k, 1 \leq k \leq r$ such that $\gcd(c(x), Q_{p^k}(x)) \neq 1$.

If $\mathrm{ord}_p(2) = p-1$, $Q_{p^k}(x)$ is irreducible for each $k, 1 \leq k \leq r$ and $\gcd(c(x), Q_{p^k}(x)) \neq 1$ if and only if $\gcd(\bar{c_k}(x), Q_{p^k}(x)) \neq 1$ from Lemma 3. Furthermore, $\gcd(\bar{c_k}(x), Q_{p^k}(x)) \neq 1$ if and only if $\gcd(\bar{c_k}(x), Q_{p^k}(x)) = Q_{p^k}(x)$. If $\mathrm{ord}_p(2) = \frac{p-1}{2} = s$ where s is odd, on the other hand, $Q_{p^k}(x) = Q_p(x^{p^{k-1}}) = G_1(x)G_2(x)$, where $G_i(x) = g_i(x^{p^{k-1}}), i = 1, 2$ and $g_1(x)$ and $g_2(x)$ are irreducible factors of $Q_p(x)$ with $g_2(x) = x^s g_1(x^{-1})$ [3]. From Property 4, $G_1(x)$ and $G_2(x)$ are irreducible, and reciprocal with each other, i.e., $G_2(x) = x^{sp^{k-1}} G_1(x^{-1})$. From (5) and (13), $c(x)$ and $\bar{c_k}(x)$ have a solution of a form of x^{-1} as well as x, respectively. If $\bar{c_k}(x)$ (or $c(x)$) has an irreducible factor $G_1(x)$, therefore, it simultaneously has another irreducible factor $G_2(x)$, and vice versa. Hence, for each $k, 1 \leq k \leq r$, $\gcd(c(x), Q_{p^k}(x)) \neq 1$ if and only if $\gcd(\bar{c_k}(x), Q_{p^k}(x)) \neq 1$, and furthermore $\gcd(\bar{c_k}(x), Q_{p^k}(x)) \neq 1$ if and only if $\gcd(\bar{c_k}(x), Q_{p^k}(x)) = Q_{p^k}(x)$. In both cases, we have

$$\bar{c_k}(x) = Q_{p^k}(x)h(x) \tag{16}$$

where $h(x) = 1 + \sum_{i=1}^{p^{k-1}-1} h_i x^i, h_i \in \mathbb{F}_2$. From Lemma 2, $\bar{c_k}(x)$ is circular symmetric of $\deg(\bar{c_k}(x)) \leq p^k - 1$. Hence, if (16) is true in a non-bent function $f(x)$, $h(x)$ is also circular symmetric with $\deg(h(x)) \leq p^{k-1} - 1$ from Lemma 1. Thus, from (16), and notice that $\bar{c_k}(x)$ is circular symmetric, we can write $\bar{c_k}(x)$ as follows.

$$\begin{aligned} \bar{c_k}(x) &= Q_{p^k}(x) + \sum_{j=0}^{p-1} \sum_{t=1}^{p^{k-1}-1} h_t x^{t+jp^{k-1}} \\ &= \sum_{j=1}^{\frac{p-1}{2}} (x^{jp^{k-1}} + x^{p^k - jp^{k-1}}) + 1 + \sum_{t=1}^{p^{k-1}-1} h_t \sum_{j=0}^{\frac{p-1}{2}} (x^{t+jp^{k-1}} + x^{p^k - t - jp^{k-1}}). \end{aligned} \tag{17}$$

From Lemma 2, on the other hand, we have

$$\begin{aligned}
\bar{c}_k(x) &= \sum_{i=1}^{p^k-1} w_{i,k}(x^i + x^{p^k-i}) + 1 \\
&= \sum_{j=1}^{p-1} w_{jp^{k-1},k}(x^{jp^{k-1}} + x^{p^k-jp^{k-1}}) + 1 + \sum_{i=1, i\neq jp^{k-1}}^{p^k-1} w_{i,k}(x^i + x^{p^k-i}) \\
&= \sum_{j=1}^{\frac{p-1}{2}} (w_{jp^{k-1},k} + w_{p^k-jp^{k-1},k})(x^{jp^{k-1}} + x^{p^k-jp^{k-1}}) + 1 \\
&\quad + \sum_{t=1}^{p^{k-1}-1} \sum_{j=0}^{\frac{p-1}{2}} (w_{t+jp^{k-1},k} + w_{p^k-t-jp^{k-1},k})(x^{t+jp^{k-1}} + x^{p^k-t-jp^{k-1}}), \quad (i = t + jp^{k-1}) \\
&= \sum_{j=1}^{\frac{p-1}{2}} u_{jp^{k-1},k}(x^{jp^{k-1}} + x^{p^k-jp^{k-1}}) + 1 + \sum_{t=1}^{p^{k-1}-1} \sum_{j=0}^{\frac{p-1}{2}} u_{t+jp^{k-1},k}(x^{t+jp^{k-1}} + x^{p^k-t-jp^{k-1}}).
\end{aligned} \tag{18}$$

From the comparison of (17) and (18), we have

$$u_{t+jp^{k-1},k} = \begin{cases} 1, & t = 0, \quad 1 \le j \le \frac{p-1}{2} \\ h_t, & 1 \le t \le p^{k-1} - 1, \quad 0 \le j \le \frac{p-1}{2} \end{cases} \tag{19}$$

Thus, for the non-bent case, the entries of U_k: $u_{i,k}, 1 \le i \le \frac{p^k-1}{2}$, are determined by (19). Since entries of U_k are circular symmetric, i.e., $u_{i,k} = u_{p^k-i,k}$, this is equivalently saying that the columns of U_k are constant vectors if $f(x)$ is non-bent. This completes the proof for Theorem 5. ■

In the following, we write entries in U_k in detail in order to better visualize the construction in Theorem 5. We see that U_k consists of several submatrices in Fig 2, which are defined as follows. Each of $\mathbf{B}, \mathbf{C}, \mathbf{F}, \mathbf{G}$ is a $l \times m$ matrix, where $l = \frac{p-1}{2}$ and $m = \frac{p^{k-1}-1}{2}$. Also, each of $\mathbf{D}$ and $\mathbf{E}$ is $1 \times m$ matrix, and each of $\mathbf{H}$ and $\mathbf{I}$ is $l \times 1$ matrix. From $u_{i,k} = u_{p^k-i,k}, 1 \le i \le \frac{p^k-1}{2}$, 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, $\frac{p^{k-1}+1}{2} \le i \le p^{k-1} - 1$ are determined by column vectors $\mathbf{A}_{i,k}, 1 \le i \le \frac{p^{k-1}-1}{2}$.

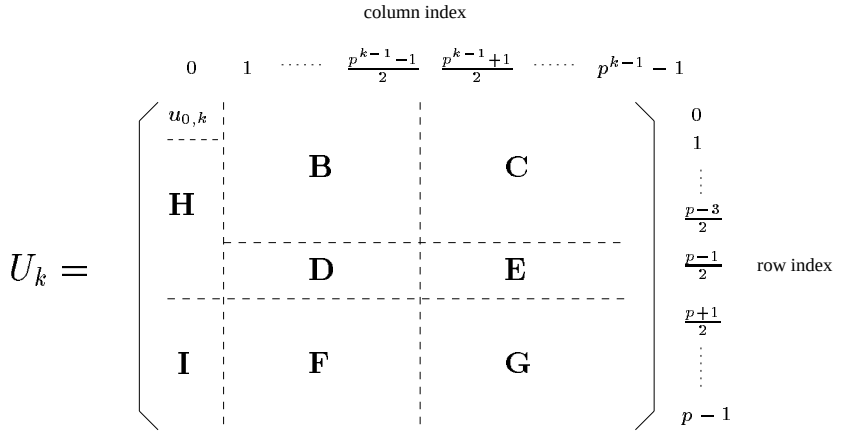

Fig. 2. Submatrix structure of U_k

Example 2: For $n = 18$, $p = 3$ and $r = 2$. For $k = 1$, we can 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 5,

$$c_1 + c_4 + c_7 + c_2 + c_5 + c_8 = 0$$

at $k = 1$ for $f(x)$ defined by (2) 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,

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

at $k = 2$ for $f(x)$ defined by (2) to be bent. Finally, $f(x)$ is bent at two distinct cases.

a) $c_1 + c_4 + c_7 + c_2 + c_5 + c_8 = 0$ and $c_3 + c_6 = 0 \Rightarrow 64$ cases.

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

In b), $c_3 + c_6 = 1$ is required to distinguish b) from a). For example, with $(c_1c_2c_3c_4c_5c_6c_7c_8) = (01110100)$, $f(x) = Tr(x^5+x^9+x^{17}+x^{65})+Tr_1^9(x^{513})$ is bent. Finally, we have total $64+48 = 112$ bent functions of $f(x)$ whose c_i's satisfies 1) and 2). It is identical to the results from computer experiments.

VI. Iterative construction of high degree bent functions by using quadratic bent functions

In [3], Pascal, Pasalic and Tavernier proposed a recursive construction of bent functions with high degree by using bent functions with low degree. In this section, we show bent functions with quadratic exponents can be used for obtaining a bent function with high degree by applying the recursive construction. As an example, we give an iterative construction of bent functions of n variables with degree $\frac{n}{2}$ by using quadratic bent functions.

Fact 1: [3] For even n and $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1}), x_i \in \mathbb{F}_2$, let $f_1(\mathbf{x})$ and $f_2(\mathbf{x})$ be two 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 1, Pascal, Pasalic and Tavernier showed that a bent function with high degree can be recursively constructed by concatenating known bent functions with low degree. In Section III - V, we constructed a large number of quadratic bent functions. Using these bent functions and Fact 1, we can recursively construct bent functions with higher degree. In the following, we give a general procedure of an iterative construction of bent functions of $n = 2k$ variables with degree k by using the quadratic bent functions constructed in Section III - V.

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

In the above procedure, b_{k-2} is a final bent function of $2k$ variables with degree k. The following example illustrates the 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 $\mathbb{F}_{2^4}$, we convert $b_0(x)$ and $q_0(x)$ into their Boolean representations. In other words, from $x = \sum_{i=0}^{3} x_i\alpha^i, x_i \in \mathbb{F}_2$, we have

$$Tr_1^4(x) = \sum_{i=0}^{3} x_i Tr_1^4(\alpha^i), \quad Tr_1^4(x^3) = \sum_{i=0}^{3}\sum_{j=0}^{3} x_i x_j Tr_1^4(\alpha^{2i+j}),$$

$$Tr_1^2(x^5) = \sum_{i=0}^{3}\sum_{j=0}^{3} x_i x_j Tr_1^2(\alpha^{4i+j}) = \sum_{i=0}^{3} x_i Tr_1^2(\alpha^{5i}) + \sum_{i=0}^{3}\sum_{j>i}^{3} x_i x_j Tr_1^4(\alpha^{4i+j}).$$

Evaluating each trace function, Boolean representations of $b_0(x)$ and $q_0(x)$ are given by

$$b_0(x_0, x_1, x_2, x_3) = x_1 + x_2 + x_3 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3,$$

$$q_0(x_0, x_1, x_2, x_3) = x_3 + x_0x_3 + x_1x_2.$$

At Step 3, concatenating b_0 and q_0, two semi-bent functions of 5 variables with degree 3 can be constructed, i.e.,

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

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

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.,

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

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 $q_1(x) = Tr_1^6(x) + Tr_1^3(x^9)$. From a similar approach to 1), its Boolean representation $q_1(x_0, \cdots, x_5)$ is given by

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

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, $q_2(x) = Tr_1^8(x^3) + Tr_1^4(x^{17})$ whose Boolean representation is given by

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

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

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

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 final bent function with degree 6.

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

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

VII. CONCLUSIONS

We discovered that a necessary condition for $f(x) = \sum_{i=1}^{n/2-1} c_i Tr(x^{1+2^i}) + c_{n/2} Tr_1^{n/2}(x^{1+2^{n/2}}), c_i \in \mathbb{F}_2$ being bent is $c_{n/2} = 1$. In other words, a necessary condition for a linear combination over $\mathbb{F}_2$ of monomial trace terms $Tr(x^{1+2^i}), 1 \leq i \leq \frac{n}{2} - 1$ and $Tr_1^{n/2}(x^{1+2^{n/2}})$ is that the term $Tr_1^{n/2}(x^{1+2^{n/2}})$ must be presented, i.e.,

$$f(x) = \sum_{i=1}^{n/2-1} c_i Tr(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}), \quad c_i \in \mathbb{F}_2. \tag{20}$$

We have solved constructions and enumerations for the following cases ($c_{n/2} = 1$).

i) If $n = 2^v$, then $f(x)$ given by (20) is bent for all choices of c_i's.

ii) If $n = 2^v p^r, r \geq 1$ where p is odd prime with $\mathrm{ord}_p(2) = p - 1$ or $\frac{p-1}{2} = s$, where s is odd, then a condition on c_i's for $f(x)$ being bent is given, in which the enumeration is solved for the case $n = 2^v p$.

Applying Pascal, Pasalic and Tavernier's recursive process, we present an iterative procedure to construct a bent function with maximum degree by using quadratic bent functions constructed here.

REFERENCES

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

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

[3] P. Charpin, E. Pasalic, and C. Tavernier. Around bent and semi-bent quadratic Boolean functions. *IEEE Trans. Inform. Theory*, to appear.

[4] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. On cryptographic properties of the cosets of $R(1, m)$. *IEEE Trans. Inform. Theory*, 47(4), pp. 1494-1513, 2001.

[5] A. Canteaut and P. Charpin. Decomposing bent functions. *IEEE Trans. Inform. Theory*, 49(8), pp. 2004-2019, 2003.

[6] 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.

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

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

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

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