On Bent and Semi-Bent Quadratic Boolean Functions

Pascale Charpin, Enes Pasalic, and Cédric Tavernier

***Abstract*—The maximum-length sequences, also called m-sequences, have received a lot of attention since the late 1960s. In terms of linear-feedback shift register (LFSR) synthesis they are usually generated by certain power polynomials over a finite field and in addition are characterized by a low cross correlation and high nonlinearity. We say that such a sequence is generated by a *semi-bent* function. Some new families of such function, represented by $f(x)=\sum_{i=1}^{\frac{n-1}{2}} c_i Tr(x^{2^i+1})$, n odd and $c_i \in \mathbb{F}_2$, have recently (2002) been introduced by Khoo *et al.* We first generalize their results to even n. We further investigate the conditions on the choice of c_i for explicit definitions of new infinite families having three and four trace terms. Also, a class of nonpermutation polynomials whose composition with a quadratic function yields again a quadratic semi-bent function is specified. The treatment of semi-bent functions is then presented in a much wider framework. We show how bent and semi-bent functions are interlinked, that is, the concatenation of two suitably chosen semi-bent functions will yield a bent function and *vice versa*. Finally, this approach is generalized so that the construction of both bent and semi-bent functions of any degree in certain range for any $n \geq 7$ is presented, n being the number of input variables.**

***Index Terms*—Bent function, Boolean function, linear permutation, m-sequence, nonlinearity, quadratic mapping, semi-bent function.**

I. Introduction

In the late 1960s, the first family of m-sequences having low cross correlation has been introduced by Gold [7]. This is a family of 2^n+1 (n odd) cyclically distinct sequences, each of period 2^n-1, having a plateaued cross-correlation spectra. That is, for two such m-sequences $u(t)=\mathrm{Tr}(\alpha^t)$ and $v(t)=\mathrm{Tr}(\beta^t)$, where α and β have order 2^n-1 in $\mathbb{F}_{2^n}$

$$C_{u,v}(\tau)=\sum_{t=0}^{2^n-2}(-1)^{u(t+\tau)+v(t)}, \quad \text{with } C_{u,v}(\tau)\in\left\{-1,-1\pm 2^{(n+1)/2}\right\}. \quad (1)$$

This family has the trace representation $\mathrm{Tr}(x^{2^i+1})$, where $\gcd(i,n)=1$ and $\mathrm{Tr}(x)=x+x^2+\cdots+x^{2^{n-1}}$ (see [12, Sec. 5]). Such a family of maximum-length sequences, whose cross-correlation spectra attain exactly the values above, have a wide range of applications in cryptography and code-division multiple-access (CDMA) communication systems. Such a sequence is represented by a Boolean function which we call *a semi-bent* function, using the terminology of Khoo *et al.* [8].

After this pioneering work, a lot of research has been devoted to finding new families of semi-bent sequences. The main contributions in this direction are due to Niho [15], Helleseth [10], [11], Kumar and Helleseth [12], etc. However, almost all families of semi-bent functions have been derived from power polynomials, that is, $f(x)=\mathrm{Tr}(x^d)$ for a suitably chosen d. Thus, there is a strong interplay between the concepts of Gold sequences and certain power functions which are known as *almost-bent* mappings [4]. In other words, an *almost-bent* function x^d on $\mathbb{F}_{2^n}$ (n odd) means that the cross correlation between a binary m-sequence of length 2^n-1 and a decimation of that sequence by d takes on the values -1, $-1\pm 2^{(n+1)/2}$.

In a recent paper, Khoo *et al.* [8] have derived a new family of sequences represented by semi-bent functions of the form

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

n odd, where this sum has more than one term, n being the number of input variables. To such a function a cyclic code of length 2^n-1 was associated, spanned by

$$c(x), xc(x), \ldots x^{n-1}c(x) \text{ where } c(x)=\sum_{i=1}^{\frac{n-1}{2}} c_i\left(x^i+x^{n-i}\right).$$

Then it was proved that f is semi-bent if and only if $\gcd(c(x),x^n+1)=x+1$. This gives a very convenient tool for determining whether a function f having certain number of trace terms is semi-bent or not. For certain primes n, for instance the *Sophie–Germain primes*,[1] it was shown that f is semi-bent for any choice of coefficients c_i, $1\leq i\leq (n-1)/2$.

The main intention of this paper is to expand these results on quadratic functions in many directions. Concerning the class of quadratic semi-bent functions, we introduce some infinite classes of semi-bent functions having three and four trace terms. Thus, we extend the size of this class by giving some explicit criteria for the choice of the exponents in the trace sum

$$f(x)=\sum_{i=1}^{\frac{n-1}{2}} c_i \mathrm{Tr}(x^{2^i+1}).$$

It should be noted that the properties of semi-bent sequences are preserved when a linear permutation is applied to such a function. However, this is not the case when a composition with a nonpermutation is considered. We also specify certain classes

Manuscript received January 3, 2005; revised May 12, 2005.

P. Charpin is with the INRIA, Domaine de Voluceau, Rocquencourt, BP 105-78153, Le Chesnay Cedex, France (e-mail: Pascale.Charpin@inria.fr).

E. Pasalic is with the Technical University of Denmark, Matematiktorvet, Building 303, DK-2800 Kgs. Lyngby, Denmark (e-mail: E.Pasalic@mat.dtu.dk).

C. Tavernier is with Thales Communication, 92700 Colombes, France (e-mail: cedric.tavernier@fr.thalesgroup.com).

Communicated by K. G. Paterson, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2005.858929

[1] n is said to be a Sophie–Germain prime if both n and $2n+1$ are prime.

of nonpermutation polynomials from which we derive new families of quadratic semi-bent sequences.

In other direction, we derive an efficient criterion to determine whether two semi-bent functions defined by the trace representation have a nonintersecting spectra. Two functions f_1, f_2 are said to have a nonintersecting spectra when a nonzero value in the spectra of one function implies a zero value for the other function, and *vice versa*. Our criterion gives a very convenient method for generating bent functions through a simple concatenation of two semi-bent functions with nonintersecting spectra. The bent functions constructed in such a manner are cubic, and the concatenation of two suitably chosen such functions will yield a semi-bent function of degree 4. This technique is later further manipulated to provide a wider framework for the construction of bent and semi-bent functions of any degree in certain range.

We mention the fact that the construction of nonquadratic bent and semi-bent functions of varying degree is not unknown. Both these classes are constructible from the Maiorana–McFarland class. This class can be viewed as a concatenation of affine (linear) functions from a smaller variable space to generate a function with larger number of input variables. Different degrees are then attained by choosing suitable linear subfunctions in such a concatenation. Nevertheless, the technique we present here is basically based on the concatenation of quadratic functions and henceforth the classes are not equivalent. To the best of our knowledge, a similar approach has only been considered in [5] where the author mainly focused on the construction of resilient functions. Also, the necessary conditions for this method are quite hard to satisfy leading to a rather cumbersome geometric problems. The main difference, when comparing the two approaches, is that we can easily and in a deterministic way select quadratic functions with nonintersecting spectra which is not the case for the method in [5].

The class of Boolean functions generating the sequences (1) only exists for odd n. When n is even, then there are two important classes with plateaued spectra which are highly nonlinear. The spectra of the first class, namely, the class of bent functions, attains the value $\pm 2^{\frac{n}{2}}$, the second class has the spectra whose values belong to $\{0, \pm 2^{\frac{n+2}{2}}\}$. We call the letter class semi-bent functions, taking the same terminology as in the odd case. The similar criterion, as discussed above for odd n, is derived for semi-bent functions in the even case. This means that for even n we are able to select two semi-bent functions such that their concatenation gives a semi-bent function.

This paper is organized as follows. Section II serves as an introductory part providing some necessary definitions and notions. In Section III, the class of quadratic semi-bent functions represented by $f_c(x)$, with $c_i \in \mathbb{F}_2$, is discussed. This section provides some theoretical results regarding the possibilities and conditions of constructing the three classes of Boolean functions, namely: bent (n even) and semi-bent functions (n even and n odd). We generalize a result of Khoo *et al.* [8] to the case n even (Theorem 2). The necessary and sufficient conditions concerning the balancedness of the class of semi-bent functions are also derived here. Section IV gives some new infinite classes of quadratic semi-bent functions for odd n. This goal has been approached in two different ways. On the one hand we specify the conditions on the coefficients c_i in the expression of the form

$$f_c(x) = \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \mathrm{Tr}\left(c_i x^{2^i+1}\right), \qquad c_i \in \mathbb{F}_2$$

when there are three and four nonzero c_i. In other direction, we show that some infinite classes of quadratic semi-bent functions may be derived by composing a quadratic semi-bent function with certain nonpermutation linear polynomials.

Section V addresses the construction of nonquadratic semi-bent and bent functions. A strong relationship between the three classes mentioned above is exhibited. Using the concatenation of two suitably chosen quadratic bent or semi-bent functions in n variables we are able to generate a cubic semi-bent function in $n+1$ variables. The same technique can be then applied to two (suitably chosen) semi-bent functions to obtain a bent function of degree 4. In Section VI, we further take the advantage of the approach developed in Section V. It is shown that, based on the concatenation of quadratic functions, there exist bent functions of any degree in the range $d \in [2, n/2]$ and semi-bent functions of any degree $d \in [2, (n+1)/2]$.

Notation.

— $\mathbb{F}_{2^n}$ is the finite-field of order 2^n;
— $E^* = E \setminus \{0\}$, $\#E$ is the cardinality of the set E;
— Tr is the trace function on $\mathbb{F}_{2^n}$;
— $\mathcal{B}_n$ is the set of Boolean functions on $\mathbb{F}_{2^n}$;
— $\varphi_b : x \longmapsto \mathrm{Tr}(bx)$, the linear functions of $\mathcal{B}_n$;
— $\mathrm{wt}(c)$ is the Hamming weight of the binary vector c;
— $\mathcal{F}(f) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)}$ for any Boolean function f on $\mathbb{F}_{2^n}$;
— f_a: see (6) and (7);
— $\mathcal{K}(a)$ is the linear space of f_a (Definition 1).

II. Basic Properties of Quadratic Boolean Functions

Let $\mathcal{B}_n$ denote the set of Boolean functions on $\mathbb{F}_{2^n}$. In this paper, we mainly treat the functions in $\mathcal{B}_n$ of the form

$$f(x) = \sum_{i=1}^{k} \mathrm{Tr}\left(a_i x^i\right), \qquad a_i \in \mathbb{F}_{2^n} \tag{2}$$

where $k \leq 2^n - 2$ and $\mathrm{Tr}(\beta) = \beta + \cdots + \beta^{2^{n-1}}$. The linear Boolean functions on $\mathbb{F}_{2^n}$ are

$$\varphi_b : x \mapsto \mathrm{Tr}(bx), \qquad b \in \mathbb{F}_{2^n}. \tag{3}$$

The *Walsh transform* of f in point b is

$$\mathcal{F}(f + \varphi_b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\varphi_b(x)}.$$

We are interested in the Walsh spectrum of f, that is, the set of values

$$\mathcal{S}(f) = \{\pm \mathcal{F}(f + \varphi_b) \mid b \in \mathbb{F}_{2^n}\} \tag{4}$$

and the number of times these values occur. The *weight* of f is the number of x such that $f(x) = 1$ and is denoted by $\mathrm{wt}(f)$.

Recall that f is said to be *balanced* when $\mathrm{wt}(f) = 2^{n-1}$ or, equivalently, $\mathcal{F}(f) = 0$.

The *nonlinearity* N_f of f is related to its Walsh transform via the following expression:

$$N_f = 2^{n-1} - \frac{\mathcal{L}(f)}{2}, \text{ where } \mathcal{L}(f) = \max_{b \in \mathbb{F}_{2^n}} |\mathcal{F}(f + \varphi_b)|. \quad (5)$$

In this paper, we use some properties of derivatives of f.

Definition 1: Let $f \in \mathcal{B}_n$. The *derivative* of f, with respect to e, $e \in \mathbb{F}_{2^n}^*$, is the function $D_e f \in \mathcal{B}_n$ defined by

$$D_e f : x \mapsto f(x) + f(x+e).$$

When $D_e f$ is constant, e is said to be a *linear structure* of f. The set of those e plus 0 is called the *linear space* of f.

The quadratic Boolean functions on $\mathbb{F}_{2^n}$ are as follows:

$$f_a(x) = \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \mathrm{Tr}\left(a_i x^{2^i+1}\right), \qquad a_i \in \mathbb{F}_{2^n}. \quad (6)$$

Now, we present some basic properties on these functions which can be found in [14, Ch. 15] and [3] (see also [1]). The associated symplectic form of f_a is the mapping from $(\mathbb{F}_{2^n})^2$ to $\mathbb{F}_2$

$$\Psi(u,v) = f_a(0) + f_a(u) + f_a(v) + f_a(u+v).$$

The *kernel* of Ψ is defined as follows:

$$\mathcal{K}(a) = \{u \in \mathbb{F}_{2^n} \mid \forall v \in \mathbb{F}_{2^n} : \Psi(u,v) = 0\}.$$

The following properties are well known.

i) $\mathcal{K}(a)$ is the subspace of those e such that $D_e f_a$, the derivative of f_a with respect to $e \in \mathbb{F}_{2^n}$, is constant. According to Definition 1, $\mathcal{K}(a)$ is the linear space of f_a.

ii) f_a is balanced if and only if there is $e \in \mathcal{K}(a)$ such that $D_e f_a = 1$. This is equivalent to say that f_a is not constant on $\mathcal{K}(a)$. In this case, this holds for a half of elements $e \in \mathcal{K}(a)$.

iii) Set $\dim \mathcal{K}(a) = n - 2h$, $1 \le h \le \lfloor \frac{n}{2} \rfloor$; then the spectrum of f_a only depends on h (cf. [14, p. 441]). It is, since $f_a(0) = 0$

value	number it occurs
0	$2^n - 2^{2h}$
2^{n-h}	$2^{2h-1} + 2^{h-1}$
-2^{n-h}	$2^{2h-1} - 2^{h-1}$

Note that the dimension of $\mathcal{K}(a)$ is even when n is even and odd when n is odd. Now we define three kinds of functions which have *good* nonlinearity and recall their Walsh spectrum. Since nonquadratic functions with the same spectrum exist, we give a general definition. The reader can find a general proof for the computation of these kinds of spectrum in [2]. Note that for n odd, semi-bent functions have the best nonlinearity among quadratic functions. For functions of higher degree, the best nonlinearity is not known from $n = 9$. For even n, the bent functions are functions of best nonlinearity.

Definition 2: Let n be even. Any $f \in \mathcal{B}_n$, with $f(0) = 0$, is said to be *bent* if and only if its Walsh-spectrum is

value	number it occurs
$2^{n/2}$	$2^{n-1} + 2^{(n-2)/2}$
$-2^{n/2}$	$2^{n-1} - 2^{(n-2)/2}$

The quadratic function f_a, defined by (6), is said to be bent if and only if $\dim \mathcal{K}(a) = 0$ $(h = n/2)$.

Definition 3: Let n be odd. Any $f \in \mathcal{B}_n$, with $f(0) = 0$, is said to be *semi-bent* if and only if its Walsh-spectrum is

value	number it occurs
0	2^{n-1}
$2^{(n+1)/2}$	$2^{n-2} + 2^{(n-3)/2}$
$-2^{(n+1)/2}$	$2^{n-2} - 2^{(n-3)/2}$

The quadratic function f_a, defined by (6), is semi-bent if and only if $\dim \mathcal{K}(a) = 1$ $(h = (n-1)/2)$.

Definition 4: Let n be even. Any $f \in \mathcal{B}_n$, with $f(0) = 0$, is said to be *semi-bent* if and only its Walsh spectrum is

value	number it occurs
0	$2^{n-1} + 2^{n-2}$
$2^{(n+2)/2}$	$2^{n-3} + 2^{(n-4)/2}$
$-2^{(n+2)/2}$	$2^{n-3} - 2^{(n-4)/2}$

The quadratic function f_a, defined by (6), is semi-bent if and only if $\dim \mathcal{K}(a) = 2$ $(h = (n-2)/2)$.

III. Binary Case and Good Nonlinearity

From now on, we consider quadratic functions of $\mathcal{B}_n$ of the form

$$f_c(x) = \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} c_i \mathrm{Tr}\left(x^{2^i+1}\right), \qquad c_i \in \mathbb{F}_2 \quad (7)$$

with $c = (c_1, \ldots, c_\ell)$, $\ell = \lfloor (n-1)/2 \rfloor$. Note that ℓ is equal to $(n-1)/2$ for odd n and to $(n-2)/2$ for even n. For even n, we have $\mathrm{Tr}(x^{2^{n/2}+1}) = 0$, since $x^{2^{n/2}+1} \in \mathbb{F}_{2^{n/2}}$.

Since, for any $e \in \mathbb{F}_{2^n}^*$

$$D_e f_c = \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} c_i \mathrm{Tr}\left(\left(e^{2^i} + e^{2^{n-i}}\right)x + e^{2^i+1}\right). \quad (8)$$

Then

$$\mathcal{K}(c) = \left\{ e \mid \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} c_i \left(e^{2^i} + e^{2^{n-i}}\right) = 0 \right\}. \quad (9)$$

Clearly, the set $\{0, 1\}$ is included in $\mathcal{K}(c)$. Thus, the dimension $\boldsymbol{k}$ of $\mathcal{K}(c)$ is at least 1. For odd n, we can have $\boldsymbol{k} = 1$ providing the functions f_c of best nonlinearity, the so-called semi-bent functions (Definition 3).

This cannot hold for even n: f_c cannot be bent because $\boldsymbol{k}$ cannot be equal to 0. Hence, for even n, the best nonlinearity for the functions f_c is obtained when $\boldsymbol{k} = 2$. In fact, it is easy

to see that $\mathbb{F}_4$ is included in $\mathcal{K}(c)$. Indeed, for $e \in \mathbb{F}_4 \setminus \{0,1\}$, we have

$$e^{2^i} = \begin{cases} e, & \text{if } i \text{ is even} \\ e^2, & \text{if } i \text{ is odd.} \end{cases}$$

Thus, for any i, $e^{2^i} = e^{2^{n-i}}$ (n is even) which implies that e is in $\mathcal{K}(c)$. According to Definitions 3 and 4, we have the following characterizations. Recall that for any linear polynomial Q of $\mathbb{F}_{2^n}[x]$ one defines its *associated polynomial* $q(x)$ as follows:

$$Q(x) = \sum_{i=0}^{n-1} \lambda_i x^{2^i} \quad \text{and} \quad q(x) = \sum_{i=0}^{n-1} \lambda_i x^i. \tag{10}$$

Any linear polynomial H divides Q if and only if its associated polynomial h divides q [13, Theorem 3.62]. The function f_c is given by (7).

Lemma 1: Let n be odd. The function f_c given by (7) is semi-bent if and only if the roots of the polynomial

$$Q_c(x) = \sum_{i=1}^{(n-1)/2} c_i \left(x^{2^i} + x^{2^{n-i}} \right) \tag{11}$$

are 0 and 1 only. Equivalently, f_c is semi-bent if and only if the associated polynomial q_c of Q_c satisfies

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

In this case $\mathcal{K}(c) = \mathbb{F}_2$.

Proof: Note that $q_c(x) = \sum_{i=1}^{(n-1)/2} c_i (x^i + x^{n-i})$. We have seen that $\mathbb{F}_2$ is included in $\mathcal{K}(c)$ or, equivalently, that the polynomial $x^2 + x$ divides $Q_c(x)$. According to Definition 3, the function f_c is semi-bent if and only if $\mathcal{K}(c) = \mathbb{F}_2$. That is,

$$\gcd(Q_c(x), x^{2^n} + x) = x^2 + x.$$

This can be rewritten in terms of the associated polynomials of the linear polynomials $x^2 + x$ and $Q_c(x)$. We then obtain that f_c is semi-bent if and only if $\gcd(q_c(x), x^n + 1) = x + 1$. □

Lemma 2: Let n be even. The function f_c is semi-bent if and only if the polynomial

$$Q_c(x) = \sum_{i=1}^{(n-2)/2} c_i \left(x^{2^i} + x^{2^{n-i}} \right) \tag{12}$$

is such that $Q_c(x) = 0$ implies $x \in \mathbb{F}_4$. Equivalently, f_c is semi-bent if and only if the associated polynomial q_c of Q_c satisfies

$$\gcd(q_c(x),\ x^n + 1) = x^2 + 1.$$

In this case $\mathcal{K}(c) = \mathbb{F}_4$.

Proof: As in the preceding proof, we know that the polynomial $x^4 + x$ divides $Q_c(x)$ and f_c is semi-bent if and only if $\mathbb{F}_4 = \mathcal{K}(c)$. This can be expressed with the associated polynomials: $\gcd(q_c(x), x^n + 1) = x^2 + 1$. □

Example 1: Let $f_c(x) = \mathrm{Tr}(x^{2^i+1})$ for some $i < n/2$. Thus,

$$Q_c(x) = x^{2^i} + x^{2^{n-i}} \quad \text{and} \quad q_c(x) = x^i + x^{n-i}.$$

It is well known that for odd n such a function f_c is semi-bent if and only if $\gcd(i, n) = 1$. When n is even, $n = 2p$, f_c is semi-bent if and only if $\mathcal{K}(c) = \mathbb{F}_4$ or equivalently

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

We have

$$x^i + x^{n-i} = x^i \left(1 + x^{n-2i}\right) = x^i \left(1 + x^{p-i}\right)^2.$$

Thus, f_c is semi-bent if and only if $\gcd(1 + x^{p-i}, 1 + x^p) = 1$, that is,

$$\gcd(p, p - i) = \gcd(p, i) = 1.$$

A. Generalization of a Result of [9]

We denote by $\mathrm{ord}_p(2)$ the order of 2 modulo p, that is, the smallest k such that p divides $2^k - 1$.

Khoo, Gong, and Stinson characterized the set of odd n such that f_c is semi-bent for all nonzero c [9, Sec. 4]. We summarize their results in the next theorem.

Theorem 1: Let us define the properties i) and ii) where p is any odd prime number:

i) $\mathrm{ord}_p(2) = p - 1$;
ii) $p = 2s + 1$, s is odd and $\mathrm{ord}_p(2) = s$.

Let n be odd. The functions f_c on $\mathbb{F}_{2^n}$ are defined by (7). Then, f_c is semi-bent, for any non zero c, if and only if n is an odd prime number satisfying i) or ii).

By using Lemma 2 we are able to prove a similar result when n is even. However, according to the next lemma, the situation is clearly different. We will prove that, unless $n = 4$, there is no n for which all f_c are semi-bent. Notation is as in Lemma 2.

Lemma 3: Let n be even, $n = 2p$ with $p > 2$. Let f_c be any function defined by (7). Then $x^p + 1$ divides $q_c(x)$ if and only if $c_i = c_{p-i}$ for all i, $1 \le i \le p - 1$.

Proof: Recall that $q_c(x) = \sum_{i=1}^{p-1} c_i (x^i + x^{2p-i})$. Thus,

$$q_c(x) \equiv \sum_{i=1}^{p-1} c_i \left(x^i + x^{p-i}\right) \bmod x^p + 1.$$

So $x^p + 1$ divides $q_c(x)$ if and only if for all x

$$\sum_{i=1}^{p-1} c_i \left(x^i + x^{p-i}\right) = 0.$$

This is possible if and only if $c_i = c_{p-i}$ for all i, $1 \le i \le p - 1$. □

Theorem 2: Let n be even. The functions f_c on $\mathbb{F}_{2^n}$, $c \neq 0$, are defined by (7). Then we have the following.

a) If $n = 4$ then f_c is semi-bent.
b) Assume that $n = 2p$, $p > 2$, and consider the functions f_c such that $c_i \neq c_{p-i}$ for some i. Then, f_c is semi-bent, for any such c, if and only if p is an odd prime satisfying part i) or part ii) of Theorem 1.

Proof: With notation of Lemma 2 and $n = 2p$, we have for any c

$$q_c(x) = \sum_{i=1}^{p-1} c_i \left(x^i + x^{2p-i}\right)$$

and we know that x^2+1 divides $q_c(x)$. If $n = 4$, there is only one function f_c. That is, $f_c(x) = \mathrm{Tr}(x^3)$ providing $q_c(x) = x + x^3$ and we have obviously $\gcd(x + x^3, x^4 + 1) = x^2 + 1$. Now we are going to prove part b) of the theorem. We consider functions f_c such that $c_i \neq c_{p-i}$ for some i. From Lemma 3, this means that $x^p + 1$ does not divide $q_c(x)$.

Let $n = 2p$, where p is an odd prime number. If p satisfies part i) of Theorem 1 then x^p+1 has only two irreducible factors. More precisely

$$x^n + 1 = x^{2p} + 1 = (x+1)^2(x^{p-1} + \cdots + x + 1)^2.$$

If $x^{p-1} + \cdots + x + 1$ divides $q_c(x)$, then $x^p + 1$ divides $q_c(x)$, which is impossible by hypothesis.

If p satisfies part ii) of Theorem 1, then $x^p + 1$ has only three irreducible factors

$$x^n + 1 = (x^p + 1)^2 = ((x+1)h_1(x)h_2(x))^2$$

where each h_i has degree $s = (p-1)/2$, s odd. Note that $h_2(x) = h_1(x^{-1})$. Indeed, if $\beta^p = 1$ for $\beta \in \mathbb{F}_{2^s}$, $\beta \neq 1$, then $(\beta^{-1})^p = 1$ since β belongs to the cyclic subgroup of $\mathbb{F}_{2^s}^*$ of order p. Assume that β is a root of h_1. If β^{-1} is a root of h_1 as well, then this property holds for any root β^{2^i} (for some i) of h_1. This is impossible since s is odd.

Suppose that there is β such that $h_1(\beta) = q_c(\beta) = 0$. Then

$$q_c(\beta) = \sum_{i=1}^{p-1} c_i(\beta^i + \beta^{-i}) = 0.$$

Clearly, both β and β^{-1} are roots of $q_c(\beta)$. Consequently, if h_1 divides q_c then h_2 divides q_c as well. But, in this case $x^p + 1$ divides $q_c(x)$. We have proved that when p satisfies part i) or ii) of Theorem 1, then $\gcd(q_c(x), x^n + 1) = x^2 + 1$ for any c such that $c_i \neq c_{p-i}$ for some i.

Conversely, suppose that any function f_c, for suitable c, is semi-bent. By *suitable* c, we mean that $c_i \neq c_{p-i}$ for some i. Then $n = 2p$ where p is an odd prime, since we know that otherwise there is i such that $x \mapsto \mathrm{Tr}(x^{2^i+1})$ is not semi-bent (see Example 1). Let $s = \mathrm{ord}_p(2)$ with $s \neq p-1$ and $s \neq (p-1)/2$. We have

$$x^n + 1 = (x^p + 1)^2 = ((x+1)h_1(x)\cdots h_k(x))^2$$

where the h_i are irreducible polynomials. By definition $\mathbb{F}_{2^s}$ is the splitting field of $x^p + 1$. Hence, each polynomial h_i has a degree dividing s. Assume that, for some i, h_i is of degree r with $1 < r < s$. So there is $\beta \in \mathbb{F}_{2^r} \setminus \{0, 1\}$ such that $h_i(\beta) = 0$ implying $\beta^p = 1$. Since p is prime, this is possible if p divides $2^r - 1$ only, which contradicts $s = \mathrm{ord}_p(2)$. Note that $r = 1$ is impossible since $x^2 + 1$ does not divide $x^p + 1$.

Thus, the h_i have the same degree s and $ks = p - 1$, $k > 2$. Set $g(x) = xh_1(x)h_\ell(x)$ where $h_\ell(x) = x^s h_1(x^{-1})$ and let d be the degree of g. Note that for s even, we can have $\ell = 1$. In this case, we take $g(x) = xh_1(x)$ and $d = s + 1$. In any case, $d \leq 2s + 1 < p - 1$. Set $g(x) = \sum_{i=1}^{d} c_i x^i$ and consider

$$f_c(x) = \sum_{i=1}^{d} c_i \mathrm{Tr}(x^{2^i+1}) \Rightarrow q_c(x) = \sum_{i=1}^{d} c_i x^i + \sum_{i=1}^{d} c_i x^{n-i}.$$

Note that c is suitable since $c_1 = 1$ while $c_{p-1} = 0$. Thus, f_c must be semi-bent. Let $\beta \in \mathbb{F}_{2^s}$, $\beta \neq 0$, such that $g(\beta) = 0$. Then $g(\beta^{-1}) = 0$ which implies

$$q_c(\beta) = g(\beta) + \beta^n g(\beta^{-1}) = 0.$$

We have proved that the polynomial $g(x)/x$, which divides $x^n + 1$ also divides $q_c(x)$. Then $\gcd(q_c(x), x^n + 1) \neq x^2 + 1$ which implies that f_c is not semi-bent, a contradiction. Thus, s cannot satisfy the hypothesis, completing the proof. □

B. Balanced Quadratic Functions

In this subsection, we study the balancedness of functions f_c of type (7) which are semi-bent. Our results will be used later for some constructions. Recall that $c = (c_1, \ldots, c_\ell)$, $\ell = \lfloor (n-1)/2 \rfloor$, and $c_i \in \mathbb{F}_2$. We denote by $\mathrm{wt}(c)$ the Hamming weight of c, that is the number of i such that $c_i = 1$.

For odd n, when f_c is semi-bent one can easily determine those a such that $f_c + \varphi_a$ is balanced.

Lemma 4: Let n be odd. Let us consider f_c defined by (7) which is semi-bent. Let $a \in \mathbb{F}_{2^n}$. Then the function $f_c + \varphi_a$ is balanced if and only if

- either $\mathrm{wt}(c)$ is odd and $\mathrm{Tr}(a) = 0$;
- or $\mathrm{wt}(c)$ is even and $\mathrm{Tr}(a) = 1$.

Proof: We know that $f_c + \varphi_a$ is balanced if and only if $f_c + \varphi_a$ is not constant on $\mathcal{K}(c)$ (see Section II). Since f_c is semi-bent, $\mathcal{K}(c) = \{0, 1\}$. Thus, $f_c + \varphi_a$ is balanced if and only if $(f_c + \varphi_a)(1) = 1$. We have

$$\begin{aligned}(f_c + \varphi_a)(1) = f_c(1) + \mathrm{Tr}(a) &= \sum_{i=1}^{(n-1)/2} c_i \mathrm{Tr}(1) + \mathrm{Tr}(a) \\ &\equiv \mathrm{wt}(c) + \mathrm{Tr}(a) \bmod 2.\end{aligned}$$

Then $f_c + \varphi_a$ is balanced if and only if $\mathrm{wt}(c) + \mathrm{Tr}(a)$ equals 1 modulo 2, completing the proof. □

The problem is a little more complicated for even n when $\mathcal{K}(c) = \mathbb{F}_4$. We denote by $\mathbb{F}_4^\perp$ the dual of $\mathbb{F}_4$, that is, the subspace of those $x \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}(xy) = 0$ for all $y \in \mathbb{F}_4$.

Lemma 5: Let n be even with $n = 2p$. Let us consider f_c defined by (7) which is semi-bent. Set

$$I_e = \{i \mid c_i \neq 0 \text{ and } i \text{ even}\}.$$

Consider the function $g_a = f_c + \varphi_a$. We have the following.

- If p is even then g_a is balanced if and only if $a \notin \mathbb{F}_4^\perp$.
- When p is odd there are two cases:
  - if $\#I_e$ is even then g_a is balanced if and only if $a \notin \mathbb{F}_4^\perp$;
  - if $\#I_e$ is odd; then g_a is balanced if and only if $\mathrm{Tr}(a) = 1$ or $a \in \mathbb{F}_4^\perp$.

Proof: Let us denote by u any nonzero element of $\mathcal{K}(c)$. Since f_c is semi-bent then $\mathcal{K}(c) = \mathbb{F}_4$. For any $a \in \mathbb{F}_{2^n}$, the function g_a is balanced if and only if $g_a(u) = 1$ for some such

$u \in \mathcal{K}(c)$. When $u = 1$, as in the previous proof (odd case), we get the condition

$$g_a(1) = \mathrm{wt}(c)\mathrm{Tr}(1) + \mathrm{Tr}(a) \equiv 1 \bmod 2.$$

But $\mathrm{Tr}(1) = 0$ since $n = 2p$. Thus, if $\mathrm{Tr}(a) = 1$ then g_a is balanced. We then get 2^{n-1} elements a such that g_a is balanced. Note that we know that there are $2^{n-1} + 2^{n-2}$ elements a such that g_a is balanced.

Now, suppose that $\mathrm{Tr}(a) = 0$ and take $u \neq 1$. We have

$$g_a(u) = \sum_{i=1}^{(n-2)/2} \left(c_i \mathrm{Tr}\left(u^{2^i+1}\right)\right) + \mathrm{Tr}(au).$$

Since $u^4 = u$, then

$$\mathrm{Tr}\left(u^{2^i+1}\right) = \begin{cases} \mathrm{Tr}(u^3) = \mathrm{Tr}(1) = 0, & \text{for odd } i \\ \mathrm{Tr}(u^2) = \mathrm{Tr}(u), & \text{for even } i. \end{cases}$$

Moreover, with $n = 2p$

$$\mathrm{Tr}(u) = \begin{cases} 0, & \text{when } p \text{ is even} \\ u^2 + u = 1, & \text{when } p \text{ is odd.} \end{cases}$$

Thus, if p is even we get the condition $g_a(u) = \mathrm{Tr}(au) = 1$. Finally, g_a is not balanced if and only if a belongs to the dual of $\mathbb{F}_4$. Note that we have proved that for even p, f_c is never balanced.

Now assume that p is odd. So we must have

$$g_a(u) = \sum_{i \in I_e} c_i + \mathrm{Tr}(au) = \#I_e + \mathrm{Tr}(au) \equiv 1 \bmod 2.$$

If $\#I_e$ is even then we get the previous condition. When $\#I_e$ is odd we get the condition $\mathrm{Tr}(au) = 0$. Finally, g_a is balanced if and only if either $\mathrm{Tr}(a) = 1$ or $\mathbb{F}_4$ is included in the kernel of φ_a, that is, $a \in \mathbb{F}_4^{\perp}$. □

Some properties that could be of interest in some context appeared in the previous proof. We summarize them in the next proposition.

Proposition 1: $n = 2p$; $f_c = \sum_{i=1}^{\frac{n-2}{2}} c_i \mathrm{Tr}(x^{2^i+1})$, $c_i \in \mathbb{F}_2$. Recall that $I_e = \{i \mid c_i \neq 0 \text{ and } i \text{ even}\}$.

i) If $\mathrm{Tr}(a) = 1$ then $f_c + \varphi_a$ is balanced.
ii) If p is even then f_c is not balanced, for any c.
iii) If p is odd then f_c is balanced if and only if the cardinality of I_e is odd.

Open Problem 1: Let f_c be defined by (7). What is the sign of each nonzero $\mathcal{F}(f_c + \varphi_u)$ when u runs through $\mathbb{F}_{2^n}$?

IV. New Families of Semi-Bent Sequences

In this section, n is odd. The main result in [8], [9] on the semi-bent functions of the form (7), having more than one trace term ($\mathrm{wt}(c) \geq 2$), was given in Theorem 1. Also, a class of functions containing exactly two trace terms has been specified.

Theorem 3 [8]: Let n be odd. Then the function

$$x \mapsto \mathrm{Tr}\left(x^{2^i+1} + x^{2^j+1}\right), \qquad x \in \mathbb{F}_{2^n}$$

is semi-bent for all (i, j), $1 \leq i < j \leq (n-1)/2$, if and only if n is prime.

In the subsection that follows we specify some infinite classes of semi-bent sequences having three and four trace terms. We later study some compositions with linear mappings.

A. Quadratic Semi-Bent Functions With Three and Four Trace Terms

Theorem 4: For odd n let $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$ be defined by

$$f(x) = \mathrm{Tr}\left(x^{2^i+1} + x^{2^j+1} + x^{2^t+1}\right), \quad 1 \leq i < j < t \leq \frac{n-1}{2},\ i + j = t. \tag{13}$$

Then f is semi-bent if and only if

$$\gcd(n, i) = \gcd(n, j) = \gcd(n, i + j) = 1.$$

Proof: Let $\ell(x) = x^i + x^j + x^t + x^{n-i} + x^{n-j} + x^{n-t}$. According to Lemma 1, we only need to express the condition $\gcd(\ell(x), x^n + 1) = x + 1$. Rearranging ℓ and setting $t = i + j$ we get

$$\begin{aligned} \ell(x) &= (x^i + 1)(x^j + 1) + 1 + x^n + x^n + x^{n-i} \\ &\quad + x^{n-j} + x^{n-i-j} \\ &= (x^i + 1)(x^j + 1) + (1 + x^n) \\ &\quad + x^n(x^{-i} + 1)(x^{-j} + 1) \\ &= (x^i + 1)(x^j + 1)(1 + x^{n-i-j}) + (1 + x^n). \end{aligned}$$

Thus,

$$\gcd(\ell(x), x^n + 1) = \gcd((x^i + 1)(x^j + 1)(1 + x^{n-t}), x^n + 1)$$

which is equal to $x + 1$ if and only if

$$\gcd(n, i) = \gcd(n, j) = \gcd(n, t) = 1.$$ □

A similar result may be derived for $i + j = 2t$.

Theorem 5: For odd n let

$$f(x) = \mathrm{Tr}\left(x^{2^i+1} + x^{2^j+1} + x^{2^t+1}\right), \quad 1 \leq i < j \leq \frac{n-1}{2},\ i + j = 2t. \tag{14}$$

Then f is semi-bent if and only if $\gcd(n, t) = 1$.

Proof: Like in the above, set

$$\ell(x) = x^i + x^j + x^t + x^{n-i} + x^{n-j} + x^{n-t}.$$

Then by setting $t = \frac{i+j}{2}$ and rearranging ℓ we get

$$\begin{aligned} \ell(x) &= x^i + x^j + x^{\frac{i+j}{2}} + x^n \left(x^{-i} + x^{-j} + x^{-\frac{(i+j)}{2}}\right) \\ &= x^i + x^j + x^{\frac{i+j}{2}} + x^{n-(i+j)} \left(x^i + x^j + x^{\frac{i+j}{2}}\right) \\ &= x^i \left(1 + x^{j-i} + x^{\frac{j-i}{2}}\right) \left(1 + x^{n-(i+j)}\right). \end{aligned}$$

Since n is odd then $\mathrm{Tr}(1) = 1$ and we have for any x

$$\mathrm{Tr}\left(1 + x^{j-i} + x^{\frac{j-i}{2}}\right) = \mathrm{Tr}(1) + 2\mathrm{Tr}(x^{j-i}) = \mathrm{Tr}(1) = 1.$$

So, $1+\beta^{j-i}+\beta^{\frac{j-i}{2}}=0$ is impossible for any $\beta\in\mathbb{F}_{2^n}$. Hence, β is a root of ℓ if and only if $\gcd(n,2t)\neq 1$. Moreover $\gcd(n,2t)=\gcd(n,t)$. □

Finally, for functions having three trace terms we consider the relationship of the exponents of the form $j-i=2t$.

Theorem 6: For odd n with $1\leq i,j,t\leq\frac{n-1}{2}$, let

$$f(x)=\mathrm{Tr}\left(x^{2^i+1}+x^{2^j+1}+x^{2^t+1}\right),\qquad i<j,\ j-i=2t,\ t\neq i. \quad (15)$$

Then f is semi-bent if and only if $\gcd(n,t)=1$.

Proof: The polynomial $\ell(x)$ is as in the previous proof. We set $h(x)$ as follows:

$$\begin{aligned}h(x)&=(x^{2t}+1)\left(x^{\frac{i+j}{2}}+x^{n-\frac{i+j}{2}}+1\right)+(x^n+1)\\&=x^{t+j}+x^{n-i+t}+x^{2t}+x^{\frac{i+j}{2}}+x^{n-\frac{i+j}{2}}+x^n\\&=x^{t+j}+x^{n-i+t}+x^{2t}+x^{t+i}+x^{n-(j-t)}+x^{n-t+t}\\&=x^t\left(x^j+x^i+x^t+x^{n-j}+x^{n-i}+x^{n-t}\right)\end{aligned}$$

since $t+(i+j)/2=j$ and $t-(i+j)/2=-i$. Thus, $h(x)=x^t\ell(x)$ with

$$x^t\ell(x)\equiv(x^{2t}+1)\left(x^{(i+j)/2}+x^{n-(i+j)/2}+1\right)\bmod x^n+1.$$

Now look at the condition $\gcd(\ell(x),x^n+1)=x+1$. Let β be a root of $h(x)$, with $\beta\notin\{0,1\}$ and $\beta^n=1$. If

$$\beta^{(i+j)/2}+\beta^{n-(i+j)/2}+1=0$$

then, multiplying by $\beta^{(i+j)/2}$

$$\beta^{i+j}+\beta^n+\beta^{(i+j)/2}=1+\beta^{(i+j)/2}+\beta^{i+j}=0$$

which is impossible since $1+x+x^2=0$ does not hold for $x\in\mathbb{F}_{2^n}$ with n odd. So the only possibility is $\beta^{2t}=1$, completing the proof. □

Regarding the functions having four trace terms we give the condition for the choice of the coefficients such that f is semi-bent. There might be some other relationships between the exponent values but we do not investigate this problem further.

Theorem 7: For odd n and $1\leq i,j,r,s\leq\frac{n-1}{2}$, let

$$f(x)=\mathrm{Tr}\left(x^{2^i+1}+x^{2^j+1}+x^{2^r+1}+x^{2^s+1}\right),\qquad i<j,\ r<s,\ i+j=r+s=k \quad (16)$$

(with $i\neq r$). Then f is semi-bent if and only if

$$\gcd(k,n)=\gcd(i-s,n)=\gcd(j-s,n)=1.$$

Proof: It is easily verified that

$$x^i+x^j+x^{n-i}+x^{n-j}=(x^i+x^j)(1+x^{n-k})$$

and we have a similar equality for (r,s) instead of (i,j). Thus, with ℓ as in the previous proofs

$$\begin{aligned}x^s\ell(x)&=x^s(1+x^{n-k})(x^i+x^j+x^s+x^r)\\&=(1+x^{n-k})(x^s+x^j)(x^s+x^i)\end{aligned}$$

since $i+j-s=r$. So

$$\gcd(\ell(x),x^n+1)=\gcd((x^i+x^s)(x^j+x^s)(1+x^{n-k}),x^n+1).$$

This is equal to $x+1$ (i.e., f is semi-bent) if and only if the conditions claimed in the statement are satisfied. □

As a consequence, we have the following corollary.

Corollary 1: For odd n, the functions defined by (13), (14), and (15) (resp., (16)) are semi-bent for any suitable choice of (i,j,t) (resp., of (i,j,r,s)) if and only if n is a prime integer.

B. Linear Polynomials and Semi-Bent Functions

We now try to derive new classes of semi-bent functions by considering the composition of nonpermutation linear polynomials on $\mathbb{F}_{2^n}$ with a semi-bent function of the same form as before. It is well known that the composition of any linear permutation polynomial P with a quadratic semi-bent function f will give again a semi-bent function $f\circ P$, that is, the function $x\mapsto f(P(x))$. We will now consider such P with coefficients in $\mathbb{F}_2$. We first recall a well-known result.

Lemma 6: Let $P(x)=\sum_{i=0}^{n-1}a_ix^{2^i}$ be any linear polynomial in $\mathbb{F}_2[x]$. Then P is a permutation polynomial of $\mathbb{F}_{2^n}$ if and only if

$$\gcd\left(\sum_{i=0}^{n-1}a_ix^i,\ x^n+1\right)=1$$

where $\sum_{i=0}^{n-1}a_ix^i$ is called the *associated* polynomial of P.

In general, this calculation can be done fast but for some special classes of prime numbers n, such as *Mersenne primes*,[2] we obtain a simple result as a consequence of a known factorization of x^n+1. Thus, for Mersenne primes of the form $n=2^m-1$ we may choose any P providing that its associated polynomial is irreducible of degree not equal to m.

Example 2: For instance $n=2^5-1=31$ is a Mersenne prime. Take any irreducible polynomial $h(x)$ of degree d such that $2\leq d\leq 30$ and $d\neq 5$. Set $h(x)=\sum_{i=0}^{d}a_ix^i$. Then we are sure that h has no root in $\mathbb{F}_{2^5}$, which implies

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

Now h can be seen as the associated polynomial of $P(x)=\sum_{i=0}^{d}a_ix^{2^i}$. According to Lemma 6, P is a linear permutation on $\mathbb{F}_{2^5}$. For any semi-bent function f, the function $f\circ P$ is again semi-bent. This is also true if h is chosen to be a product of irreducible polynomials of degree different from 5, with $\deg(h)<30$.

However, it is not necessary for P to be a permutation polynomial in order for $f\circ P$ to be semi-bent. One may choose a linear mapping $P:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ which is not a permutation of $\mathbb{F}_{2^n}$ but $f\circ P$ is still semi-bent.

[2]When $n=2^u-1$ is prime, for some integer u, n is said to be a Mersenne prime.

Example 3: Set $P(x) = x^{2^j} + x^{2^k}$, a linear polynomial on $\mathbb{F}_{2^n}$, where n is a prime. Then P is obviously not a permutation of $\mathbb{F}_{2^n}$, as $P(1) = 0$. Still, for a semi-bent function $f(x) = \mathrm{Tr}(x^{2^i+1})$, the function $f \circ P$ is semi-bent for suitably chosen j and k, $j < k$ and $k < i + j$. This is verified as follows:

$$\begin{aligned} f \circ P &= \mathrm{Tr}\left(\left(x^{2^j} + x^{2^k}\right)^{(2^i+1)}\right) \\ &= \mathrm{Tr}\left(\left(x^{2^{i+j}} + x^{2^{i+k}}\right)\left(x^{2^j} + x^{2^k}\right)\right) \\ &= \mathrm{Tr}\left(x^{2^i+1} + x^{2^s+1} + x^{2^r+1} + x^{2^i+1}\right) \\ &= \mathrm{Tr}\left(x^{2^s+1} + x^{2^r+1}\right) \end{aligned}$$

where $r = i + k - j$ and $s = i + j - k$. By Theorem 3, $f \circ P$ is semi-bent for any $1 \le r \ne s \le (n-1)/2$. Obviously, it is easy to choose j, k satisfying this condition. Recall that $f(x) = \mathrm{Tr}(x^{2^i+1})$ is semi-bent if and only if $\gcd(i, n) = 1$ (see Example 1).

Next we specify certain nonpermutation linear polynomials that preserve the semi-bent property when composed to a semi-bent function of type x^{2^i+1}.

Proposition 2: Let $f(x) = \mathrm{Tr}(x^{2^i+1})$ be a semi-bent function on $\mathbb{F}_{2^n}$, n odd, and $\gcd(i, n) = 1$. Let $P(x) = \sum_{k_j \in K} x^{2^{k_j}}$ be a linear polynomial on $\mathbb{F}_{2^n}$, where $K = \{k_1, k_2, \ldots, k_u\}$ is an ordered set of indices such that u is even and $1 \le k_1 < \cdots < k_u \le n-1$. Then

$$f(P(x)) = \sum_{k_l, k_m \in K,\ l<m} \mathrm{Tr}\left(x^{2^{a+b}+1} + x^{2^{a-b}+1}\right)$$

where for any $k_l, k_m \in K$, $l < m$, the exponent values a, b are computed as

$$(a, b) = (i, k_m - k_l) \Longleftrightarrow k_m - k_l \le i \tag{17}$$

$$(a, b) = (k_m - k_l, i) \Longleftrightarrow k_m - k_l > i. \tag{18}$$

Proof: A formal expansion of $f \circ P$ is as follows:

$$\begin{aligned} f(P(x)) &= \mathrm{Tr}\left(\left(\sum_{k_j \in K} x^{2^{k_j+i}}\right)\left(\sum_{k_j \in K} x^{2^{k_j}}\right)\right) \\ &= \mathrm{Tr}\Big(x^{2^{k_1}(2^i+1)} + x^{2^{k_2}(2^{i+k_1-k_2}+1)} + \cdots \\ &\quad + x^{2^{k_u}(2^{i+k_1-k_u}+1)} + \cdots + x^{2^{k_1}(2^{i+k_u-k_1}+1)} \\ &\quad + x^{2^{k_2}(2^{i+k_u-k_2}+1)} + \cdots + x^{2^{k_u}(2^i+1)}\Big). \end{aligned}$$

Note that $\mathrm{Tr}(x^{2^s w}) = \mathrm{Tr}(x^w)$ for any $s \ge 0$. Then the u terms $x^{2^{k_l}(2^i+1)}$ will vanish as u is even. Obviously, the terms above are symmetric meaning that whenever $x^{2^{k_l}(2^{i+k_m-k_l}+1)}$ is present so is $x^{2^{k_m}(2^{i+k_l-k_m}+1)}$. We will treat each such pair of terms, (k_m, k_l) with $l < m$.

Assuming that $k_l, k_m \in K$ are such that $k_m - k_l \le i$, we have

$$\mathrm{Tr}\left(x^{2^{k_m}(2^{i+k_l-k_m})+1}\right) = \mathrm{Tr}\left(x^{2^{i-(k_m-k_l)}+1}\right)$$

and

$$\mathrm{Tr}\left(x^{2^{k_l}(2^{i+k_m-k_l}+1)}\right) = \mathrm{Tr}\left(x^{2^{i+(k_m-k_l)}+1}\right). \tag{19}$$

This case corresponds to the selection of $(a, b) = (i, k_m - k_l)$. Now if $i < k_m - k_l$ then we rewrite

$$\begin{aligned} \mathrm{Tr}\left(x^{2^{k_m}(2^{i+k_l-k_m}+1)}\right) &= \mathrm{Tr}\left(x^{2^{i+k_l}+2^{k_m}}\right) \\ &= \mathrm{Tr}\left(x^{2^{i+k_l}(2^{k_m-k_l-i}+1)}\right) \\ &= \mathrm{Tr}\left(x^{2^{(k_m-k_l)-i}+1}\right). \end{aligned}$$

On the other hand, (19) holds in this case which corresponds to the selection of $(a, b) = (k_m - k_l, i)$. Summarizing the preceding equalities a compact expression for $f \circ P$ is as stated. □

Theorem 8: For odd n, let $P(x) = \sum_{k_j \in K} x^{2^{k_j}}$, where $K = \{k_1, k_2, \ldots, k_u\}$ and $1 \le k_1 < k_2 < \cdots < k_u \le (n-1)/2$, u even. Let $p(x)$ be the associated polynomial of P. Assume that p is of the form

$$p(x) = x^r(1 + x^s)m(x), \qquad \text{with } \gcd(m(x), x^n + 1) = 1$$

where $r \ge 0$, $s \ge 1$, and furthermore $\gcd(s, n) = 1$. Let $f(x) = x^{2^i+1}$ with $\gcd(i, n) = 1$. Assume that P and n are such that i can be chosen such that $k_m - k_l \le i$ for any $k_m, k_l \in K$. Then the function $f \circ P$ is a semi-bent function.

Proof: Since u is even, $P(0) = P(1) = 0$, implying that P is not a permutation polynomial. Then by Proposition 2 we may write

$$f(P(x)) = \sum_{k_l, k_m \in K,\ l<m} \mathrm{Tr}\left(x^{2^{a+b}+1} + x^{2^{a-b}+1}\right)$$

where $(a, b) = (i, k_m - k_l)$ due to the assumption that $k_m - k_l \le i$ for all $k_m, k_l \in K$. Hence,

$$f(P(x)) = \sum_{k_l, k_m \in K,\ l<m} \mathrm{Tr}\left(x^{2^{i+k_m-k_l}+1} + x^{2^{i-(k_m-k_l)}+1}\right). \tag{20}$$

Now we apply Lemma 1. We use notation Q instead of Q_c and q instead of q_c. Here we have

$$\begin{aligned} Q(x) = \sum_{k_l, k_m \in K,\ l<m} \Big(&x^{2^{i+k_m-k_l}} + x^{2^{n-i-k_m+k_l}} \\ &+ x^{2^{i-k_m+k_l}} + x^{2^{n-i+k_m-k_l}}\Big) \end{aligned}$$

and

$$\begin{aligned} q(x) &= \sum_{k_l, k_m \in K,\ l<m} x^{i+k_m-k_l} + x^{i-(k_m-k_l)} \\ &\quad + x^{n-(i+k_m-k_l)} + x^{n-(i-(k_m-k_l))} \\ &= (x^i + x^{n-i}) \sum_{k_l, k_m \in K,\ l<m} x^{k_m-k_l} + x^{-(k_m-k_l)}. \end{aligned}$$

Now $f(P)$ is semi-bent if and only if $\gcd(q(x), x^n + 1) = x + 1$. Since $\gcd(i, n) = 1$, setting

$$h(x) = \sum_{k_l, k_m \in K,\ l<m} (x^{k_m-k_l} + x^{-(k_m-k_l)});$$

this is equivalent to $\gcd(h(x), x^n + 1) = x + 1$. Note that the associated polynomial of P is given by $p(x) = x^{k_1} + x^{k_2} + \cdots + x^{k_u}$. Then the main trick is that

$$p(x)p(x^{-1}) = h(x)$$

which is easily verified by developing the product $p(x)p(x^{-1})$. On the other hand, by assumption, $p(x) = x^r(x^s+1)m(x)$, where $\gcd(m(x), x^n+1) = 1$. Hence, we get

$$\begin{aligned} h(x) &= x^r x^{-r}(1+x^s)(1+x^{-s})m(x)m(x^{-1}) \\ &= (1+x^s)(1+x^{-s})m(x)m(x^{-1}). \end{aligned}$$

Since $\gcd(s,n) = 1$, we obtain $\gcd(h(x), x^n+1) = x+1$ which concludes the proof. □

Example 4: Let $n = 19$ and let $f(x) = \mathrm{Tr}(x^{2^5+1})$ $(i = 5)$, which is semi-bent since $\gcd(5, 19) = 1$. Then, since

$$x^{19}+1 = (x+1)\left(\sum_{l=0}^{18} x^l\right)$$

we may, for instance, take

$$p(x) = x(x+1)(x^3+x+1) = x+x^3+x^4+x^5$$

which satisfies the conditions of Theorem 8. Then $p(x)$ is the associated polynomial of $P(x) = x^{2^1}+x^{2^3}+x^{2^4}+x^{2^5}$, which is not a permutation. Note that $k_m - k_l \le i$ for any $k_l, k_m \in K$, where $K = \{1,3,4,5\}$.

Hence, using (20), we compute (canceling out the terms appearing even number of times)

$$\begin{aligned} f(P(x)) &= \sum_{k_l,k_m\in K,\ l<m} \mathrm{Tr}\left(x^{2^{i+k_m-k_l}+1} + x^{2^{i-(k_m-k_l)}+1}\right) \\ &= \mathrm{Tr}\left(x^{2^{5+3}+1} + x^{2^{5-3}+1} + x^{2^{5+4}+1} + x^{2^{5-4}+1}\right) \\ &= \mathrm{Tr}\left(x^{2^8+1} + x^{2^2+1} + x^{2^9+1} + x^{2^1+1}\right) \end{aligned}$$

which is a semi-bent function with 4 trace terms.

It should be noticed that Theorem 8 always generates functions of even weight.

V. Construction of Nonquadratic Bent and Semi-Bent Functions

Now we utilize the results derived in Section III to prove the existence of nonquadratic bent and semi-bent functions. We simply concatenate suitably chosen quadratic semi-bent functions for this purpose. Even though we restrict ourselves here only to bent functions of degree 3 and semi-bent functions of degree 4, we will later use these functions recursively to obtain a much larger class with a broad degree range.

A. Bent Functions of Degree 3

The next proposition is a simpler form of [1, Theorem V.3]. Notation is defined in Section II.

Proposition 3: Let n be odd. Let g and h be two Boolean functions on $\mathbb{F}_{2^n}$. Let f be the Boolean function on $\mathbb{F}_{2^n} \times \mathbb{F}_2$

$$f : (x,y) \longmapsto g(x)y + h(x)(y+1).$$

Then f is bent if and only if the following two conditions are satisfied:

i) g and h are semi-bent;

ii) for any $a \in \mathbb{F}_{2^n}$: $\mathcal{F}(g+\varphi_a) = 0$ if and only if $\mathcal{F}(h+\varphi_a) = \pm 2^{(n+1)/2}$.

Thus, using our semi-bent quadratic functions, it is very easy to construct bent functions of degree 3 and of $n+1$ variables.

Theorem 9: Let n be odd such that there exist two semi-bent functions f_b and f_c, defined by (7), with $\mathrm{wt}(b)$ even and $\mathrm{wt}(c)$ odd. Let us define the Boolean function on $\mathbb{F}_{2^n} \times \mathbb{F}_2$

$$f : (x,y) \longmapsto f_b(x)y + f_c(x)(y+1).$$

Then f is a bent function of degree 3.

Proof: We apply Proposition 3. Condition i) of Proposition 3 is satisfied by hypothesis. Using Lemma 4 we have, for any $a \in \mathbb{F}_{2^n}$:

- if $\mathrm{Tr}(a) = 0$, then $f_b + \varphi_a$ is not balanced and $f_c + \varphi_a$ is balanced, since, respectively, $\mathrm{wt}(b)$ is even and $\mathrm{wt}(c)$ is odd;
- if $\mathrm{Tr}(a) = 1$ then $f_b + \varphi_a$ is balanced and $f_c + \varphi_a$ is not balanced.

Thus, $\mathcal{F}(f_b + \varphi_a) = 0$ if and only if $\mathcal{F}(f_c + \varphi_a) \neq 0$, for any a; so part ii) of Proposition 3 is satisfied. We conclude that f is bent.

Moreover $f(x) = y(f_b(x) + f_c(x)) + f_c(x)$. Since f_b and f_c do not have the same number of terms, $f_b + f_c \neq 0$; so f is of degree 3. □

Example 5: Let $n = 5$; thus, $(n-1)/2 = 2$. These functions

$$f_b(x) = \mathrm{Tr}(x^3+x^5) \text{ and } f_c(x) = \mathrm{Tr}(x^3)$$

are both semi-bent (see Theorem 3). Now set

$$\begin{aligned} f(x,y) &= \mathrm{Tr}(x^3+x^5)y + \mathrm{Tr}(x^3)(y+1) \\ &= \mathrm{Tr}(x^5)y + \mathrm{Tr}(x^3). \end{aligned}$$

The function f is bent, from Theorem 9. Moreover f is clearly of degree 3.

To generalize the construction of bent functions of degree 3 for any n we have to prove the existence of at least one semi-bent function of odd and one of even weight. To estimate the size of this class is a hard combinatorial problem. For larger n there will obviously be more choices to select the exponents such that the component functions are semi-bent. Note that the exponents in the trace terms must lie in the range $\left[1, \frac{n-1}{2}\right]$.

We first consider the existence of quadratic semi-bent functions of odd weight. This case is easy since we always can take one of the following two functions $f_c = \mathrm{Tr}(x^{2^1+1})$, $f_e = \mathrm{Tr}(x^{2^2+1})$, which are obviously semi-bent for any odd $n \ge 5$ due to the fact that $\gcd(1,n) = \gcd(2,n) = 1$. For the even weight we rely on the class of semi-bent functions having two trace terms given by Lemma 7.

Lemma 7 [9]: For odd n, let $f(x) = \mathrm{Tr}(x^{2^i+1} + x^{2^j+1})$. Then f is a semi-bent function for $1 \le i < j \le (n-1)/2$ if and only if $(n, j-i) = (n, i+j) = 1$.

For the existence of semi-bent functions with two terms we need the following results.

Lemma 8: Let r be coprime to n where n is odd. For any r, $2 < r < n-1$, we define

$$\begin{aligned} i &= \frac{r-1}{2}; \quad j = \frac{r+1}{2}; \qquad r \text{ odd} \\ i &= \frac{r}{2} - 1; \quad j = \frac{r}{2} + 1; \qquad r \text{ even}. \end{aligned}$$

Then $\gcd(i+j,n) = \gcd(j-i,n) = 1$.

Proof: We simply have $\gcd(i+j,n) = \gcd(r,n) = 1$ in both cases. Also, $\gcd(j-i,n) = \gcd(1,n) = 1$ for odd r, whereas $\gcd(j-i,n) = \gcd(2,n) = 1$ for even r. □

For the proof of the next lemma, we use the *Euler function* ϕ, defined as follows:

$$\phi(n) = \#\{a \in \mathbb{N} \mid 0 < a \le n,\ \gcd(a,n) = 1\}, \qquad n \in \mathbb{N}. \tag{21}$$

Recall that for $n = \prod_{i=1}^{k} p_i^{e_i}$, where p_i are distinct primes, and $e_i > 0$, $1 \le i \le k$, then

$$\phi(n) = \prod_{i=1}^{k} \left(p_i^{e_i} - p_i^{e_i - 1}\right). \tag{22}$$

Lemma 9: For any odd $n \ge 7$, there exist at least two distinct quadratic semi-bent functions of the form

$$f(x) = \mathrm{Tr}(x^{2^i+1}) + \mathrm{Tr}(x^{2^j+1}), \qquad 0 < i < j \le (n-1)/2.$$

Furthermore, for any odd $n \ge 5$ there exist at least one quadratic semi-bent function of even number of terms.

Proof: We use the result of Lemma 7 to prove the statement. Assume there exist two coprimes to n, say r_1, r_2, $3 \le r_1 \ne r_2 \le n-1$. Then we may define

$$f_b(x) = \mathrm{Tr}(x^{2^{i_1}+1} + x^{2^{j_1}+1})$$

and

$$f_d(x) = \mathrm{Tr}(x^{2^{i_2}+1} + x^{2^{j_2}+1})$$

where exponents i_1, j_1 and i_2, j_2 correspond, respectively, to r_1 and r_2 by means of Lemma 8. Then, both f_b and f_d are semi-bent functions from Lemma 8 and Lemma 7.

Now we utilize the Euler function ϕ (see (21) and (22)). Let

$$R = \{r \mid \gcd(r,n) = 1, 3 \le r \le n-2\}.$$

Then $\#R = \phi(n) - 3$. Thus, to assure that $\#R \ge 2$ for any n, we must have $\phi(n) \ge 5$. When n is prime, this condition is satisfied for $n \ge 7$ since $\phi(n) = n-1$. Now if n is composite we first consider the case $k \ge 2$ in (22). Since each $p_i > 2$ we have

$$\phi(n) \ge (p_1 - 1)(p_2 - 1) \ge 8.$$

It remains to consider the case $k = 1$ and $e_1 > 1$. In this case, $\phi(n) = p_1^{e_1} - p_1^{e_1 - 1}$, which implies $\phi(n) \ge 6$.

Finally, the second part of the statement follows from the first part and the fact that for $n = 5$, the function $f(x) = \mathrm{Tr}(x^3 + x^5)$ is a semi-bent function. This concludes the proof. □

As a consequence, we may state the following result without proof.

Theorem 10: For any even $n \ge 6$, one can construct bent functions of degree 3 by means of Theorem 9.

Remark 1: The bent functions, defined by Theorem 9, are interesting since they are simply defined. Moreover, for large n, a lot of constructions are possible. Note that they are *normal* (i.e., constant on some flat of dimension $(n+1)/2$) since any quadratic semi-bent function is normal when it is not balanced; more precisely, they are of the form $f = (g,h)$ where g or h is not balanced and both are semi-bent (see [6, Theorem 4 and Proposition 7]).

B. Semi-Bent Functions of Degree 4

Similarly as above, we are going to prove the existence of semi-bent functions of degree 4 of n variables for any odd $n \ge 9$.

Proposition 4: Let n be odd such that there exist four semi-bent functions defined by (7)

$$f_b, f_c, f_d, f_e, \text{ with } \mathrm{wt}(b),\ \mathrm{wt}(d) \text{ even, and } \mathrm{wt}(c),\ \mathrm{wt}(e) \text{ odd}$$

such that $f_b + f_c + f_d + f_e \ne 0$. Let us define the Boolean function on $\mathbb{F}_{2^n} \times \mathbb{F}_2^2$

$$\begin{aligned} f(x,y) = f_b(x)(y_1+1)(y_2+1) + f_c(x)(y_1+1)y_2 \\ + f_d(x)y_1(y_2+1) + f_e(x)y_1y_2. \end{aligned}$$

Then f is a semi-bent function of degree 4.

Proof: This is simply because f is the concatenation of two bent functions

$$f = f_b(x)(y_2+1) + f_c(x)y_2 \| f_d(x)(y_2+1) + f_e(x)y_2$$

where $f_b(x)(y_2+1) + f_c(x)y_2$ and $f_d(x)(y_2+1) + f_e(x)y_2$ are bent, by Theorem 9. Clearly, such a function is semi-bent (see [1]). □

Notation. The function f defined above is actually the concatenation of the functions f_b, f_c, f_d, f_e. We sometimes, instead of the algebraic expression given above, use a shorter notation $f = f_b \| f_c \| f_d \| f_e$.

Now we prove that this construction is always possible. Notation is as in the previous proposition.

Theorem 11: Let n be odd with $n \ge 7$. Set $f_c = \mathrm{Tr}(x^3)$ and $f_e = \mathrm{Tr}(x^5)$. Then there exist at least two distinct quadratic semi-bent functions of even number of terms, say f_b and f_d, satisfying $f_b + f_c + f_d + f_e \ne 0$. Furthermore, for any odd $n \ge 7$ one can construct semi-bent functions of degree 4 and of $n+2$ variables by means of Proposition 4.

Proof: By Lemma 9, for any odd $n \ge 7$ there exist two distinct quadratic semi-bent functions $f_b, f_d : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ with two trace terms. By construction, these functions are such that $f_b + f_c + f_d + f_e \ne 0$.

Then by Proposition 4, the function $f = f_b \| f_c \| f_d \| f_e$ is a semi-bent function on $\mathbb{F}_2^{n+2}$ of degree 4. □

C. Bent and Semi-Bent Functions Through Semi-Bent Functions

When n is even, $\mathbb{F}_4$ is a subspace of $\mathbb{F}_{2^n}$ as well as its dual $\mathbb{F}_4^\perp$. Precisely

$$\mathbb{F}_4^\perp = \{u \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(uv) = 0 \text{ for all } v \in \mathbb{F}_4\}. \tag{23}$$

Throughout this subsection, $\mathbb{F}_4$ and $\mathbb{F}_4^\perp$ are subspaces of $\mathbb{F}_{2^n}$. On the other hand, the functions we construct here are defined on a space of dimension greater than n. A coset of $\mathbb{F}_4^\perp$ is any subset of $\mathbb{F}_{2^n}$ of the form $u + \mathbb{F}_4^\perp$, $u \in \mathbb{F}_{2^n}$.

It is easy to state an equivalent of Proposition 3 for constructing semi-bent functions from two semi-bent functions.

Proposition 5: Let n be even. Let g and h be two semi-bent functions on $\mathbb{F}_{2^n}$. Let f be the Boolean function on $\mathbb{F}_{2^n} \times \mathbb{F}_2$

$$f : (x, y) \longmapsto g(x)y + h(x)(y + 1).$$

Then f is semi-bent if and only if for any $a \in \mathbb{F}_{2^n}$

$$\mathcal{F}(g + \varphi_a) = \pm 2^{(n+2)/2} \Longrightarrow \mathcal{F}(h + \varphi_a) = 0. \tag{24}$$

Proof: For any $a \in \mathbb{F}_{2^n}$ and $\epsilon \in \mathbb{F}_2$

$$\begin{aligned}\mathcal{F}(f + \varphi_a + \epsilon y) = &\sum_{x \in \mathbb{F}_{2^n}, y=0} (-1)^{h(x)+\varphi_a} \\ &+ \sum_{x \in \mathbb{F}_{2^n}, y=1} (-1)^{g(x)+\varphi_a+\epsilon} \\ &= \mathcal{F}(h + \varphi_a) + \mathcal{F}(g + \varphi_a + \epsilon).\end{aligned}$$

If (24) is satisfied, then the spectrum of f is clearly $\{0, \pm 2^{(n+2)/2}\}$. Hence, f is semi-bent. If (24) is not satisfied, then the value $\pm 2^{(n+4)/2}$ appears in the spectrum of f. □

Theorem 12: Let $n = 2p$. Let f_b and f_c, defined by (7), be two semi-bent functions on $\mathbb{F}_{2^n}$. Let $u \in \mathbb{F}_{2^n}$. Let us define the Boolean function on $\mathbb{F}_{2^n} \times \mathbb{F}_2$

$$f : (x, y) \longmapsto (f_b + \varphi_u)(x)y + f_c(x)(y + 1).$$

Set

$$I_e(b) = \{i | b_i \neq 0 \text{ and } i \text{ even}\}$$

and

$$I_e(c) = \{i | c_i \neq 0 \text{ and } i \text{ even}\}.$$

Then we have the following.

i) Assume that p *is even* or $\{\#I_e(b)$ and $\#I_e(c)$ are even$\}$. Then, for any $u \notin \mathbb{F}_4^\perp$, the function f is semi-bent. Moreover, $f + \varphi_a + \epsilon y$ is balanced if and only if $u + a \notin \mathbb{F}_4^\perp$.

ii) Assume that p *is odd*, $\#I_e(b)$ *is odd*, $\#I_e(c)$ *is even*, and $u = 0$. Then f, which is equal to $f_b || f_c$, is semi-bent.

Moreover, f is of degree 3 if and only if $f_b + f_c \neq 0$.

Proof: We apply the previous proposition together with Lemma 5.

i) The function $f_b + \varphi_{u+a}$ is not balanced, for some a, if and only if $a + u \in \mathbb{F}_4^\perp$. Note that $u \notin \mathbb{F}_4^\perp$ implies that $a \notin \mathbb{F}_4^\perp$. Thus, $f_c + \varphi_a$ is balanced. Such f satisfies (24), thus, it is semi-bent.

Moreover, $f_b + \varphi_{u+a}$ is balanced when $a + u \notin \mathbb{F}_4^\perp$, that is, a and u are not in the same coset of $\mathbb{F}_4^\perp$. Taking $u \notin \mathbb{F}_4^\perp$ we get 2^{n-1} element a which are neither in $\mathbb{F}_4^\perp$ nor in its coset containing u. Thus, for such a, $f_b + \varphi_{u+a}$ and $f_c + \varphi_a$ are both balanced. These are the cases where $f + \varphi_a + \epsilon y$ is balanced.

ii) Set $u = 0$. Since $\#I_e(b)$ is odd, the function $f_b + \varphi_a$ is not balanced if and only if $\mathrm{Tr}(a) = 0$ and $a \notin \mathbb{F}_4^\perp$. Hence, $f_c + \varphi_a$ is balanced, since $\#I_e(c)$ is even. Then f, which satisfies (24), is semi-bent. □

Remark 2: For odd n, we gave some constructions which are suitable only if some semi-bent functions exist. When n is even, we have this situation for ii) only. However, for p odd there exist functions f_b with $\#I_e(b)$ odd and which are semi-bent (see Example 1).

Note that the functions obtained by the previous construction are not really interesting, because they have a linear structure. Indeed, $f = (g, h)$ where g and h have both $\mathbb{F}_4$ as kernel in their symplectic form. Thus, there is a nonzero element u of $\mathbb{F}_4$ such that $D_u g = D_u h = \xi$, with $\xi \in \{0, 1\}$. Recall that the best nonlinearity for cubic functions of n variables, n odd, is an important open problem. It was proved that it is $2^{n-1} - 2^{(n-1)/2}$ for $n \leq 13$.

Next we are going to use an argument which we used in Theorem 12, that is to consider $f_b + \varphi_u$ instead of f_b.

Theorem 13: Let $n = 2p$, p even. Let four semi-bent functions defined by (7)

$$f_b,\ f_c,\ f_d,\ f_e, \qquad \text{with } f_b + f_c + f_d + f_e \neq 0.$$

Let V denotes the dual of $\mathbb{F}_4^\perp$ in $\mathbb{F}_{2^n}$ (see (23)). Let $u, v, w \notin V$, defining three distinct cosets of V in $\mathbb{F}_{2^n}$. Let us define the Boolean function $f : (x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_2^2 \mapsto \mathbb{F}_2$ as

$$\begin{aligned}f(x, y) = &(f_b(x) + \varphi_u)(y_1 + 1)(y_2 + 1) \\ &+ (f_c(x) + \varphi_v)(y_1 + 1)y_2 \\ &+ (f_d + \varphi_w)(x)y_1(y_2 + 1) + f_e(x)y_1y_2.\end{aligned}$$

Then f is a bent function of degree 4.

Proof: Note that the functions φ_a are in $\mathcal{B}_n$. From hypothesis, and applying Lemma 5, we have for $a \in \mathbb{F}_{2^n}$:

- $f_e + \varphi_a$ is not balanced if and only if $a \in V$;
- $f_b + \varphi_{u+a}$ is not balanced if and only if $a \in u + V$;
- $f_c + \varphi_{v+a}$ is not balanced if and only if $a \in v + V$;
- $f_d + \varphi_{w+a}$ is not balanced if and only if $a \in w + V$.

Now, we compute the Walsh spectrum of f. Let λ and μ in $\mathbb{F}_2$ and $a \in \mathbb{F}_{2^n}$. Set $g(x, y) = f(x, y) + \varphi_a(x) + \lambda y_1 + \mu y_2$; g is the concatenation

$$f_b + \varphi_{u+a} || f_c + \varphi_{v+a} + \mu || f_d + \varphi_{w+a} + \lambda || f_e + \varphi_a + \mu + \lambda$$

where (y_1, y_2) equals respectively $(0, 0), (0, 1), (1, 0)$, and $(1, 1)$. Thus,

$$\sum_{x,y} (-1)^{g(x,y)} = \sum_{y_1, y_2} \sum_{x} (-1)^{g(x,y)}$$

leads to

$$\begin{aligned}\mathcal{F}(g) = &\mathcal{F}(f_b + \varphi_{u+a}) + \mathcal{F}(f_c + \varphi_{v+a} + \mu) \\ &+ \mathcal{F}(f_d + \varphi_{w+a} + \lambda) + \mathcal{F}(f_e + \varphi_a + \mu + \lambda).\end{aligned}$$

Any element a is in one and only one coset of V. Suppose that $a \in V$; then among the four terms above, only $\mathcal{F}(f_e+\varphi_a+\mu+\lambda)$ is not zero, equal to $\pm 2^{(n+2)/2}$ for any value of the pair (λ, μ). And we have the same result for $a \in u + V$, for instance: here only $f_b + \varphi_{u+a}$ is not balanced. So we can conclude that for any a, λ, and μ

$$\mathcal{F}(f + \varphi_a + \lambda y_1 + \mu y_2) = \pm 2^{(n+2)/2}.$$

That is, f is bent. Moreover, the function f is of degree 4 since $f_b + f_c + f_d + f_e \neq 0$. □

Remark 3: The previous construction is of interest (not trivial or known) since we can describe a large set of functions f_c semi-bent. We proved this by Theorem 2.

Note that, from Lemma 5, one can do the same construction for p odd and functions such that $\#I_e$ is even. Another construction is possible when p is odd and functions such that $\#I_e$ is odd are involved.

VI. A Recursive Construction of Nonquadratic Bent and Semi-Bent Functions

A natural question we may pose now is whether we can generalize this approach to obtain bent and semi-bent functions of higher degree. We first note that a straightforward approach of choosing two semi-bent functions, constructed by means of Proposition 5 will not yield a bent function in general.

However, this problem has been investigated in [2] and the derived result that we utilize here is as follows. Let g_1, g_2 be two bent functions on $\mathbb{F}_2^{n+1}$, for odd n. Then the function $h = g_1||g_2||1+g_1||g_2$ is a bent function on $\mathbb{F}_2^{n+3}$. It is easily verified that $\deg(h) = \deg(g_1+g_2)+1$. In particular, if g_1 and g_2 are of different degree then $\deg(h) = \max\{\deg(g_1), \deg(g_2)\}+1$.

Note that requiring $g_1 \neq g_2$ is not necessary. For a bent function g on $\mathbb{F}_2^{n+1}$, the function $g' = g||g||1 + g||g$ is also bent on $\mathbb{F}_2^{n+3}$. Obviously, g and g' are of the same degree.

We now utilize the construction method described above in order to deduce similar results as in the preceding section but with further increase of the degree. For this purpose, we consider quadratic semi-bent functions on $\mathbb{F}_2^5$ to obtain a semi-bent function on $\mathbb{F}_2^7$ and bent function on $\mathbb{F}_2^8$, where both functions are of degree 4.

However, there are only three quadratic semi-bent functions with the trace representation considered here when $n = 5$ (note that the power exponents of trace terms must lie in the range $[1, (n-1)/2]$). These are

$$f_1(x) = \mathrm{Tr}(x^3), \quad f_2(x) = \mathrm{Tr}(x^5), \quad f_3(x) = \mathrm{Tr}(x^3 + x^5).$$

Then, according to Theorem 9, $h = f_1||f_3$, and $h' = f_2||f_3$ are two distinct bent functions of degree 3 on $\mathbb{F}_2^6$. Furthermore, $h||h'$ is a semi-bent function on $\mathbb{F}_2^7$ of degree 4 as

$$f_1 + f_3 + f_2 + f_3 = f_1 + f_2 \neq 0.$$

Also, the function $B = h||h'||1 + h||h'$ is a bent function on $\mathbb{F}_2^8$ of degree 4 as $\deg(h + h') = 3$. We now generalize this as follows.

Theorem 14: For any $k \geq 0$, it is always possible to construct

$$B : \mathbb{F}_2^{8+2k} \mapsto \mathbb{F}_2 \quad \text{and} \quad G : \mathbb{F}_2^{7+2k} \mapsto \mathbb{F}_2$$

where B is a bent function of degree $4+k$ and G is a semi-bent function of degree $4 + k$.

Proof: The statement is obviously true for $k = 0$ from the preceding discussion. Hence, we simply use functions h, h' of different degree in the concatenation of the form $h||h'||1+h||h'$.

Let us consider the case $k = 1$. Clearly, we can construct bent functions on $\mathbb{F}_2^8$ of degrees 3 and 4, denoted by h and h', respectively. Then using the concatenation of such two bent functions we get a semi-bent function $G = h||h'$ of degree 5 on $\mathbb{F}_2^9$. Also, the function $B = h||h'||1 + h||h'$ is bent of degree $\deg(h') + 1 = 5$ on $\mathbb{F}_2^{10}$.

To further clarify this technique we consider the case $k = 2$. From the above, B is a bent function on $\mathbb{F}_2^{10}$ of degree 5. Let B' be another bent function on $\mathbb{F}_2^{10}$ but of degree 3. Then the function $G = B||B'$ is a semi-bent function on $\mathbb{F}_2^{11}$ of degree 6. Similarly, $b = B||B'||1 + B||B'$ is a bent function on $\mathbb{F}_2^{12}$ of degree 6.

Then the iterative procedure is continued by using two bent functions of different degree on $\mathbb{F}_2^{8+2k}$ to construct a semi-bent function on $\mathbb{F}_2^{7+2(k+1)}$ of degree $4+k+1$ and the bent function of degree $4 + k + 1$ on $\mathbb{F}_2^{8+2(k+1)}$. □

Hence, we easily deduce the following important result. Once again we point out that the significance of the result below lies in the fact that we concatenate quadratic functions which differs from the Maiorana-McFarland method.

Theorem 15: For any even $n \geq 6$, there exist bent functions in $\mathcal{B}_n$ of arbitrary degree d in the range $d \in \left[3, \frac{n}{2}\right]$.

Furthermore, for odd $n \geq 7$, there exists semi-bent functions in $\mathcal{B}_n$ of arbitrary degree d in the range $d \in \left[2, \frac{n+1}{2}\right]$

Proof: Concerning the bent functions the case $d = 3$ follows directly from Theorem 10. This also covers the case $n = 6$. Then for any $d \in \left[4, \frac{n}{2}\right]$ we proceed as follows.

Let n be even, $n \geq 8$, and $d \in \left[4, \frac{n}{2}\right]$. Thus, $n = 8 + 2\ell$ for some ℓ. If $d = n/2$ then we are done: applying Theorem 14, we get a bent function h on $\mathbb{F}_2^{8+2\ell}$ of degree $d = 4 + \ell$.

On the other hand, when $4 \leq d < n/2$, $d = 4 + k$ with $k \geq 0$, Theorem 14 provides the construction of bent functions $h : \mathbb{F}_2^{8+2k} \to \mathbb{F}_2$ of degree $4 + k$. Repeatedly use ($\ell - k$ times) the concatenation of the type $h||h||1+h||h$ to get a bent function g on $\mathbb{F}_2^n$. By noticing that $\deg(g) = \deg(h) = d$ we complete the proof regarding bent functions.

Quite similarly, the assertion on semi-bent functions is proved. Here Theorem 12 is used instead of Theorem 10. Note that for a semi-bent function g on $\mathbb{F}_2^n$ the function $g||g||1 + g||g$ is a semi-bent function on $\mathbb{F}_2^{n+2}$. □

To conclude, we want to explain our purpose in this section. Our aim is to show that one can construct bent and semi-bent functions of any degree by concatenating quadratic functions (bent or semi-bent). We have proved that for small degrees (3 and 4) we have a lot of possibilities (increasing with n). By the two previous theorems, we expand our results to any degree but using classical tools of concatenation. We claim that more interesting constructions can be done by combining different functions at each stage, since we dispose of a large corpus of functions of small degree.

REFERENCES

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

[2] A. Canteaut and P. Charpin, "Decomposing bent functions," *IEEE Trans. Inf. Theory*, vol. 49, no. 8, pp. 2004–2019, Aug. 2003.

[3] C. Carlet, "Codes de Reed-Muller, Codes de Kerdock et de Preparata," Ph.D. dissertation, Université Paris 6, Paris, France, 1990.

[4] C. Carlet, P. Charpin, and V. A. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Des., Codes Cryptogr.*, vol. 15, pp. 125–156, 1998.

[5] C. Carlet, "A larger class of cryptographic boolean functions via a study of the Maiorana-Mcfarland construction," in *Advances in Cryptology—CRYPT0 2002 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2002, vol. 2442, pp. 549–564.

[6] P. Charpin, "Normal boolean functions," *J. Complexity*, vol. 20, pp. 245–265, 2004.

[7] R. Gold, "Maximale recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, vol. IT-14, no. 1, pp. 154–156, Jan. 1968.

[8] K. Khoo, G. Gong, and D. R. Stinson, "A new family of Gold-like sequences," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, Jun./Jul. 2002, p. 181.

[9] ——, "A new characterization of semi-bent and bent functions on finite fields," *Des., Codes, Cryptogr.*, to be published.

[10] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discr. Math.*, vol. 16, pp. 209–232, 1976.

[11] ——, "Correlation of m-sequences and related topics," in *Proc. SETA'98, Discrete Mathematics and Theoretical Computer Science*, C. Ding, T. Helleseth, and H. Niederreiter, Eds. London, U.K.: Springer, 1999, pp. 49–66.

[12] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory, Part 3: Applications*, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, 1998, ch. 21.

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

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1986.

[15] Y. Niho, "Multi-valued cross-correlation functions between two maximal linear recursive sequences," Ph.D. dissertation, Univ. Sothern Calif., Los Angeles, 1972.