Bent Functions of maximal degree

Ayça Çeşmelioğlu and Wilfried Meidl

Abstract—In this article a technique for constructing \(p\)-ary bent functions from plateaued functions is presented. This generalizes earlier techniques of constructing bent from near-bent functions. The Fourier spectrum of quadratic monomials is analysed, examples of quadratic functions with highest possible absolute values in their Fourier spectrum are given. Applying the construction of bent functions to the latter class of functions yields bent functions attaining upper bounds for the algebraic degree when \(p = 3, 5\). Until now no construction of bent functions attaining these bounds was known.

Index Terms—Bent functions, Fourier transform, algebraic degree, quadratic functions, plateaued functions

I. INTRODUCTION

Let \(p\) be a prime, and let \(V_n\) be any \(n\)-dimensional vector space over \(\mathbb{F}_p\) and \(f\) be a function from \(V_n\) to \(\mathbb{F}_p\). If \(p = 2\) we call \(f\) a binary or Boolean function, if \(p\) is an odd prime we call \(f\) a \(p\)-ary function. The Fourier transform of \(f\) is the complex valued function \(\hat{f}\) on \(V_n\) given by

\[
\hat{f}(b) = \sum_{x \in V_n} \epsilon_p^{f(x) - \langle b, x \rangle}
\]

where \(\epsilon_p = e^{2\pi i/p}\) and \(\langle , \rangle\) denotes any inner product on \(V_n\). The function \(f\) is called a bent function if \(|\hat{f}(b)|^2 = p^n\) for all \(b \in V_n\). Whereas for \(p = 2\), when \(\epsilon_p = -1\) thus \(\hat{f}(b)\) is an integer, bent functions can only exist for even \(n\), for odd \(p\) bent functions exist for both odd and even \(n\), see [7].

The normalized Fourier coefficient at \(b\) of a function from \(V_n\) to \(\mathbb{F}_p\) is defined by \(p^{-n/2} \hat{f}(b)\). A binary bent function clearly must have normalized Fourier coefficients \(\pm 1\), and for the \(p\)-ary case we always have (cf. [5], [7, Property 8])

\[
p^{-n/2} \hat{f}(b) = \begin{cases} 
\pm \epsilon_p^{f^*(b)} : & n \text{ even or } n \text{ odd, } p \equiv 1 \text{ mod } 4 \\
\pm i \epsilon_p^{f^*(b)} : & n \text{ odd and } p \equiv 3 \text{ mod } 4
\end{cases}
\]

where \(f^*\) is a function from \(V_n\) to \(\mathbb{F}_p\) that by definition gives the exponent of \(\epsilon_p\).

A bent function \(f\) is called regular if

\[
p^{-n/2} \hat{f}(b) = \epsilon_p^{f^*(b)}
\]

for all \(b \in V_n\), i.e., the coefficient of \(\epsilon_p^{f^*(b)}\) is always \(+1\). Observe that for a binary bent function this holds trivially. As easily seen from (1) a \(p\)-ary regular bent function can only exist for even \(n\) or for odd \(n\) when \(p \equiv 1 \text{ mod } 4\).

A bent function \(f\) is called weakly regular if, for all \(b \in V_n\), we have

\[
p^{-n/2} \hat{f}(b) = \zeta \epsilon_p^{f^*(b)}.
\]

for some complex number \(\zeta\) with absolute value 1 (see [7]). By (1), \(\zeta\) can only be \(\pm 1\) or \(\pm i\).

A function \(f\) from \(V_n\) to \(\mathbb{F}_p\) is called plateaued if \(|\hat{f}(b)|^2 = A\) or 0 for all \(b \in V_n\). Using (the special case of) Parseval’s identity

\[
\sum_{b \in V_n} |\hat{f}(b)|^2 = p^n
\]

we see that \(A = p^{n+s}\) for an integer \(s\) with \(0 \leq s \leq n\). We will call a plateaued function with \(|\hat{f}(b)|^2 = p^{n+s}\) or 0 an \(s\)-plateaued function. The case \(s = 0\) corresponds to bent functions by definition, and we have \(s = n\) if and only if \(f\) is an affine function or constant. We remark that for 1-plateaued functions the term near-bent function was used in [1], [8], binary 1-plateaued and 2-plateaued functions are referred to as semi-bent functions in [2].

It is well known that the maximal (algebraic) degree of a binary bent function in dimension \(n\) is \(n/2\) (see [10]). For \(p\)-ary bent functions, \(p > 2\), Hou [6] showed the following bounds:

If \(f\) is a bent function from \(V_n\) to \(\mathbb{F}_p\), then the degree \(\text{deg}(f)\) of \(f\) satisfies

\[
\text{deg}(f) \leq \frac{(p - 1)n}{2} + 1.
\]

If \(f\) is weakly regular, then

\[
\text{deg}(f) \leq \frac{(p - 1)n}{2}.
\]

As remarked in [6] \(p\)-ary Maiorana-McFarland bent functions \(f\) from \(\mathbb{F}_p^n\) to \(\mathbb{F}_p\), which are always regular and for which \(n\) is always even (cf [7]), can be used to attain the bound (3). But in [6] it is left as an open problem if

I the bound (2) can be attained when \(n > 1\),

II the bound (3) can be attained when \(n \geq 3\) is odd.

Only very recently a bent function from \(\mathbb{F}_{27}\) to \(\mathbb{F}_3\) found by computer search attaining the bound (2) has been presented in [11]. To our best knowledge no general construction of bent functions attaining the bounds (2), (3) is known by now.

In [2], [8], [1] a method of constructing bent from near-bent functions has been presented. Applying this method, in [8] the first examples of non-weakly-normal bent functions (see [4]) in dimensions 10 and 12 have been presented, in [1] the first known infinite classes of non-weakly regular bent functions for arbitrary odd prime \(p\) have been introduced (until then only sporadic ternary examples were known), and a recursive method of obtaining an infinite family of non-weakly regular bent functions starting from one non-weakly regular bent function, see [11]).

In this article we further develop the method of [2], [8], [1], and obtain bent functions from \(s\)-plateaued functions. In Section II we give some results on quadratic \(s\)-plateaued
functions. In Section III we present the construction of bent functions from $s$-plateaued functions. In Section IV we utilize this construction to obtain bent functions of maximal degree. In particular we construct $p$-ary bent functions for $p = 3$ attaining the upper bound (2), and $p$-ary bent functions for $p = 3, 5$ in odd dimension that attain the upper bound (3), which partly solves open problems I and II.

II. PRELIMINARIES

As all vector spaces of dimension $n$ over $\mathbb{F}_p$ are isomorphic we may associate $V_n$ with the finite field $\mathbb{F}_{p^n}$. Then usually use the inner product $\langle x, y \rangle = \text{Tr}_n(xy)$ where $\text{Tr}_n(z)$ denotes the absolute trace of $z \in \mathbb{F}_{p^n}$. In this framework the Fourier transform of a function $f$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is the complex valued function on $\mathbb{F}_{p^n}$ given by

$$\hat{f}(b) = \sum_{x \in \mathbb{F}_{p^n}} f(x) - \text{Tr}_n(b(x-y)).$$

Recall that a function $f$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ of the form

$$f(x) = \text{Tr}_n \left( \sum_{i=0}^{l} a_i x^{p^i} + 1 \right)$$

is called quadratic, its algebraic degree is two (if $f$ is not constant), see [2], [5]. As well known, every quadratic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is plateaued. The value for $s$ can be obtained with the standard squaring technique (see [1, Theorem 2], [5]):

$$|\hat{f}(b)|^2 = \sum_{x,y \in \mathbb{F}_{p^n}} \epsilon_{f_p}^{x-y} (f(x) + \text{Tr}_n(b(x-y)))$$

$$= \sum_{z \in \mathbb{F}_{p^n}} \epsilon_{f_p}^{z} (f(x) + \text{Tr}_n(bz)) \sum_{y \in \mathbb{F}_{p^n}} \epsilon_{f_p}^{z} (f(y) - f(z)).$$

Straightforward one gets $f(x) = f(y) - f(z) = \text{Tr}_n \left( \sum_{i=0}^{l} a_i x^{p^i} + 1 \right)$.

Consequently

$$|\hat{f}(b)|^2 = \sum_{z \in \mathbb{F}_{p^n}} \epsilon_{f_p}^{z} \sum_{y \in \mathbb{F}_{p^n}} \epsilon_{f_p}^{z} \text{Tr}_n(y L(z)).$$

$$= \sum_{z \in \mathbb{F}_{p^n}} \epsilon_{f_p}^{z} (f(z) + \text{Tr}_n(bz))$$

where in the last step we used that $f(x) + \text{Tr}_n(bz)$ is linear on the kernel $\ker(L)$ of $L$. Summarizing, the square of the Fourier transform of the quadratic function $f$ in (4) takes absolute values 0 and $p^n + s$, where $s$ is the dimension of the kernel of the linear transformation on $\mathbb{F}_{p^n}$ defined by

$$L(x) = \sum_{i=0}^{l} (a_i x^{p^i} + a_i^{p^i-1} x^{p^i-1}).$$

Clearly this corresponds to

$$\deg(\gcd(L(x), x^{p^n} - x)) = s,$$

or equivalently (see [9, p.118])

$$\deg(\gcd(A(x), x^n - 1)) = s,$$

where

$$A(x) = \sum_{i=0}^{l} (a_i x^{p^i} + a_i^{p^i-1} x^{p^i-1})$$

is the associate of $L(x)$.

In some sense the simplest quadratic functions are quadratic monomials. It is well known that the monomial $f(x) = \text{Tr}_n(ax^{p^r+1})$ is bent for every $a \in \mathbb{F}_{p^n}$ if and only if $n/\gcd(r, n)$ is odd ([3]). In [5] it was examined for which $a \in \mathbb{F}_{p^n}$ the function $f = \text{Tr}_n(ax^{p^r+1})$ is bent covering also the case when $n/\gcd(r, n)$ is even. In [1] it was shown that $f(x) = \text{Tr}_n(ax^{p^r+1})$ is never 1-plateaued. A full treatment of quadratic monomials is given in the following theorem. In particular we will see that quadratic monomials are never $s$-plateaued for any odd $s$. At some positions in the proof we will use that for a divisor $s$ of $n$ we have $p^n - 1/(p^{n-1}/2)$ if and only if $n/s$ is even, or equivalently $\nu(s) < \nu(n)$ where $\nu$ denotes the 2-adic valuation on integers.

**Theorem 1:** The quadratic monomial $f(x) = \text{Tr}_n(ax^{p^r+1}) \in \mathbb{F}_{p^n}[x]$ is $s$-plateaued for some $a \in \mathbb{F}_{p^n}$ if and only if $n/s$ is even, $s$ is an even divisor of $n$ and $\nu(s) = \nu(r) + 1$.

**Proof:** The linearized polynomial $L(x)$ corresponding to $f(x) = \text{Tr}_n(ax^{p^r+1}) \in \mathbb{F}_{p^n}[x]$ is given by

$$L(x) = ax + a^{p^r} x^{p^r}.$$
not divide $p^r - 1$. Due to condition (b) we then have to find solutions $c, y$ for the equation

$$y(p^s - 1) + c(p^r - 1) = \frac{p^n - 1}{2}. \quad (8)$$

Equation (8) has solutions if and only if $\gcd(p^s - 1, p^r - 1) = p^{\gcd(r,s)} - 1 | \frac{p^n - 1}{2}$, which is guaranteed since $n/s$ is even.

* Case II: $p$ is odd.

We consider two subcases:

(i) Suppose $\frac{2s}{p}$ is odd. Then we have $\nu(s) = \nu(r) + 1$ and hence $p^s - 1 | p^r - 1$. Condition (b) is satisfied for some integer $c$ if and only if equation (8) has solutions. This is guaranteed by $\nu(n) = \nu(s) = \nu(r) + 1$.

(ii) Suppose $\frac{2s}{p}$ is even, i.e. $\nu(s) \leq \nu(r)$. Then $p^s - 1 | p^r - 1$ and for condition (b), we need $p^s - 1 | \frac{p^n - 1}{2}$ which contradicts that $n/s$ is odd.

We remark that for $n, r, s$ satisfying the conditions of the theorem, the elements $a = \gamma^c$ for which $f(x) = Tr_n(\alpha x^{p^r + 1})$ is $s$-plateaued are obtained from the congruence (8). For the remaining elements $a \in \mathbb{F}_{p^n}^*$, the corresponding monomial is bent.

III. obtaining bent functions from s-plateaued functions

Let $f$ be a function from $\mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$, and $\hat{f}$ denote its Fourier transform. The support of $\hat{f}$ is then defined to be the set $\text{supp}(\hat{f}) = \{ b \in \mathbb{F}_{p^n} \mid \hat{f}(b) \neq 0 \}$. In this section we describe a procedure to construct $p$-ary bent functions in dimension $n + s$ from $s$-plateaued functions from $\mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$. The $s$-plateaued functions must be chosen so that the supports of their Fourier transforms are pairwise disjoint. Our construction can be seen as a generalization of the constructions in [2], [1], [8] where $s = 1$.

**Theorem 2:** For each $a = (a_1, a_2, \ldots, a_s) \in \mathbb{F}_{p^n}^*$, let $f_a(x)$ be an s-plateaued function from $\mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$. If $\text{supp}(f_a) \cap \text{supp}(f_b) = \emptyset$ for $a, b \in \mathbb{F}_{p^n}^*, a \neq b$, then the function $F(x, y_1, y_2, \ldots, y_s) = \sum_{a \in \mathbb{F}_{p^n}^*} (-1)^{a} F(x, y_1, y_2, \ldots, y_s)(y_1 - (a_1 + \cdots + a_s))$ is bent.

**Proof:** For $(a, a), (x, y) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}$ the inner product we use is $\text{Tr}_n(\alpha x y) + a y = \text{Tr}_n(\alpha x) + a y_1 + a y_2 + \cdots + a y_s$, where $a = (a_1, a_2, \ldots, a_s), y = (y_1, \ldots, y_s)$. The Fourier transform $\hat{F}$ of $F$ at $(a, \alpha)$ is

$$\hat{F}(\alpha, a) = \sum_{x \in \mathbb{F}_{p^n}^*} e_{p}(x, y_1, y_2, \ldots, y_s) - \text{Tr}_n(\alpha x) - a y = \sum_{a \in \mathbb{F}_{p^n}^*} e_{p}(x, y_1, y_2, \ldots, y_s) = \sum_{y_1, \ldots, y_s \in \mathbb{F}_p} e_{p}^{-a y} = \sum_{y_1, \ldots, y_s \in \mathbb{F}_p} e_{p}^{-a y} f_{x}(y) = \sum_{y_1, \ldots, y_s \in \mathbb{F}_p} e_{p}^{-a y} \text{Tr}_n(\alpha y)$$

As each $\alpha \in \mathbb{F}_{p^n}^*$ belongs to the support of exactly one $\text{Tr}_n(y), y \in \mathbb{F}_{p^n}$, for this $y$ we have $|\hat{F}(\alpha, a)| = |e_{p}^{-a y} \text{Tr}_n(y)| = p^{\frac{s-1}{2}}$.

**Theorem 3:** For each $a \in \mathbb{F}_{p^n}^*$, let $g_a$ be a quadratic $s$-plateaued function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, with the corresponding linearized polynomial $L_a$ such that for all $a \in \mathbb{F}_{p^n}, L_a$ has the same kernel $\{c_1, c_2, \ldots, c_s, 0 \leq c_1, \ldots, c_s \leq p - 1\}$ in $\mathbb{F}_{p^n}$. For each $a = (a_1, \ldots, a_s) \in \mathbb{F}_{p^n}^*$, let $\gamma_a \in \mathbb{F}_{p^n}$ be such that

$$g_a(\beta_j) + Tr_n(\gamma_a \beta_j) = g_0(\beta_j) + a_j,$$  \quad (9)

for all $j = 1, \ldots, s$. Then for each $a \in \mathbb{F}_{p^n}^*$, the $s$-plateaued function $f_a$ defined by $f_a(x) = g_a(x) + Tr_n(\gamma_a x)$ satisfies $\text{supp}(f_a) \cap \text{supp}(f_b) = \emptyset$ for $b \in \mathbb{F}_{p^n}^*, a \neq b$.

**Proof:** We have to show that $-\alpha \in \text{supp}(\hat{f}_b)$ implies $-\alpha \not\in \text{supp}(\hat{f}_a)$ for $a \neq b$. Suppose $-\alpha \in \text{supp}(\hat{f}_b)$, i.e. $g_b(\beta_j) + Tr_n(\gamma_b \beta_j) + Tr_n(\alpha \beta_j) = g_0(\beta_j) + b_j + Tr_n(\alpha \beta_j) = 0$, for each $j = 1, \ldots, s$.

Let $a \neq b$ and suppose that $a_j \neq b_j$ for some $1 \leq j \leq s$. Then

$$f_a(\beta_j) + Tr_n(\alpha \beta_j) = g_a(\beta_j) + Tr_n(\gamma_a \beta_j) + Tr_n(\alpha \beta_j) = g_0(\beta_j) + a_j + Tr_n(\alpha \beta_j) \neq 0.$$
choose
\[ f_{(0,0)}(x) = Tr_4(x^4 + x), \]
\[ f_{(0,1)}(x) = Tr_4(x^4 + (3β + 1)x), \]
\[ f_{(0,2)}(x) = Tr_4(x^4 + (2β^3 + 2)x), \]
\[ f_{(1,0)}(x) = Tr_4(x^4 + βx), \]
\[ f_{(1,1)}(x) = Tr_4(x^4 + (β^3 + β)x), \]
\[ f_{(1,2)}(x) = Tr_4(x^{28} + (2β^3 + β + 1)x), \]
\[ f_{(2,0)}(x) = Tr_4(x^{28} + (2β^3 + β + 1)x), \]
\[ f_{(2,1)}(x) = Tr_4(x^{28} + (β^3 + 2β)x), \]
\[ f_{(2,2)}(x) = Tr_4(x^{28} + (2β^3 + 2β)x). \]
The function
\[ F(x, y, z) = \sum_{a=(a_1, a_2) \in \mathbb{F}_p^2} \sum_{c \in \mathbb{F}_p} yz(y-1)(z-1)(y-2)(z-2) f_a(x) \]
is then bent.

IV. BENT FUNCTIONS WITH HIGH ALGEBRAIC DEGREE

In this section we construct 3-ary bent functions attaining the bound (2), and 3-ary and 5-ary bent functions attaining the bound (3) also for odd dimension. This can be seen as the main result of this paper. We start with a proposition on the degree of the bent functions constructed in Theorem 2 with quadratic s-planeaued functions.

**Proposition 1:** Let \( \{f_a \mid a \in \mathbb{F}_p^s\} \) be a set of quadratic s-planeaued functions satisfying the conditions of Theorem 2. If \( \sum_{a \in \mathbb{F}_p^s} f_a \) is affine then the bent function \( F \) in Theorem 2 has degree \( \deg(F) = (p-1)s + 1 \).

**Proof:** If the quadratic terms in \( \sum_{a \in \mathbb{F}_p^s} f_a \) do not cancel, then in \( F \) given as in Theorem 2 the summand \( (-1)^s y_1 y_2 \cdots y_p \sum_{a \in \mathbb{F}_p^s} f_a(x) \) having degree \( (p-1)s + 2 \) does not vanish. Similarly, if \( \sum_{a \in \mathbb{F}_p^s} f_a = Tr_n(cz) \) for some \( c \in \mathbb{F}_p^n \), then the bent function \( F \) in Theorem 2 has the summand \( (-1)^s y_1 y_2 \cdots y_p \sum_{a \in \mathbb{F}_p^s} Tr_n(cz) \) of degree \( \deg(F) = (p-1)s + 1 \) as term of largest degree.

In order to obtain bent functions of highest possible degree we have to choose \( s \) as large as possible. Naturally we have \( s \leq n \) and the set of \( n \)-planeaued functions precisely coincides with the set of affine and constant functions. Thus \( s = n-1 \) is the maximal value for \( s \) for \( s \)-planeaued quadratic functions. The following proposition shows that this maximal value can be obtained.

**Proposition 2:** For \( n \) even, the quadratic function \( ch(x) \),
\[ h(x) = Tr_n \left( \frac{p+1}{2} x^{n/2} + \frac{p+1}{2} x^2 + \sum_{i=1}^{n/2-1} x^{p^i+1} \right) \]
is \( (n-1) \)-plateaued.

If \( n \) is odd, then the quadratic function \( ch(x) \), \( c \in \mathbb{F}_p^s \), from \( \mathbb{F}_p^{s+p} \) to \( \mathbb{F}_p^p \) with
\[ h(x) = Tr_n \left( \frac{p+1}{2} x^2 + \sum_{i=1}^{(n-1)/2} x^{p^i+1} \right) \]
is \( (n-1) \)-plateaued.

Proof: We only show the statement for \( n \) even, the case where \( n \) is odd is shown in the same way. Straightforward one sees that the associate \( A(x) \) of the linearized polynomial (5) that corresponds to \( ch(x) \) is given by
\[ A(x) = c \left( \frac{p+1}{2} x^n + \frac{p+1}{2} + \sum_{i=1}^{n/2-1} x^{n/2+i} + x^{n/2-i} \right) + \frac{p+1}{2} x^{n/2} + \sum_{i=1}^{n/2-1} x^{n/2+i} + x^{n/2-i} \]

Evidently we have \( \gcd(A(x), x^n-1) = \sum_{i=0}^{n-1} x^i \), thus \( h(x) \) is \( (n-1) \)-plateaued by equation (6).

For the subsequent theorem we fix the following notation:

1) \( h \) is the function (10) and (11) when \( n \) is even and odd, respectively.

2) for each \( a = (a_1, a_2, \ldots, a_{n-1}) \in \mathbb{F}_p^{n-1} \) let
- \( c_a \) be a nonzero element of \( \mathbb{F}_p^p \),
- \( \gamma_a \) be an element of \( \mathbb{F}_p^{n-1} \), such that
\[ c_a h(β_j) + Tr_n(γ_a β_j) = c_a h(β_j) + a_j, \quad j = 1, \ldots, n-1, \]
for a fixed basis \( \{β_1, β_2, \ldots, β_{n-1}\} \) for the kernel of the linearized polynomial \( L_a \) corresponding to \( h \),
- \( h_a(x) = c_a h(x) + Tr_n(γ_a x) \).

**Theorem 4:** The function \( F \) defined by
\[ F(x, y_1, y_2, \ldots, y_{n-1}) = \sum_{a \in \mathbb{F}_p^{n-1}} \left( \frac{(-1)^n}{(y_1 - a_1) \cdots (y_{n-1} - a_{n-1})} h_a(x) \right) \]
from \( \mathbb{F}_p^n \times \mathbb{F}_p^{n-1} \) to \( \mathbb{F}_p \) is bent, and has degree \( (p-1)(n-1) + 2 \) if \( \sum_{a \in \mathbb{F}_p^{n-1}} c_a \neq 0 \), and degree \( (p-1)(n-1) + 1 \) if \( \sum_{a \in \mathbb{F}_p^{n-1}} c_a = 0 \) and \( \sum_{a \in \mathbb{F}_p^{n-1}} γ_a \neq 0 \).

**Proof:** For all \( a \in \mathbb{F}_p^{n-1} \) the linearized polynomials \( L_a \) corresponding to \( c_a h \) have the same kernel, and the definition (12) for \( γ_a \) guarantees that the Fourier transforms of the \( (n-1) \)-plateaued functions \( h_a \), \( a \in \mathbb{F}_p^{n-1} \), have pairwise disjoint support. By Theorem 2 the function \( F \) is bent. Since \( \sum_{a \in \mathbb{F}_p^{n-1}} h_a = (\sum_{a \in \mathbb{F}_p^{n-1}} c_a) h + Tr_n(\sum_{a \in \mathbb{F}_p^{n-1}} γ_a x) \) has degree 2 if \( \sum_{a \in \mathbb{F}_p^{n-1}} c_a = 0 \) and degree 1 if \( \sum_{a \in \mathbb{F}_p^{n-1}} c_a = 0 \) and \( \sum_{a \in \mathbb{F}_p^{n-1}} γ_a \neq 0 \), the bent function \( F \) has degree \( (p-1)(n-1) + 2 \) and \( (p-1)(n-1) + 1 \), respectively, by Proposition 1.

Of course it is always possible to choose \( \sum_{a \in \mathbb{F}_p^{n-1}} c_a \neq 0 \). We emphasize that for any choice of the set \( \{c_a \mid a \in \mathbb{F}_p^{n-1}\} \) we can choose \( \{γ_a \mid a \in \mathbb{F}_p^{n-1}\} \) such that \( \sum_{a \in \mathbb{F}_p^{n-1}} γ_a \neq 0 \), since for every \( a \in \mathbb{F}_p^{n-1} \) the linear system from which we obtain \( γ_a \) does not have a unique solution.
Considering that the bent function $F$ in Theorem 4 is in dimension $n + s = 2n - 1$ the bounds (2) and (3) become $\deg(f) \leq (p - 1)(n - 1) + (p - 1)/2 + 1$ and $\deg(f) \leq (p - 1)(n - 1) + (p - 1)/2$, respectively. As we can see the function $F$ in Theorem 4 attains the first bound when $p = 3$ and $\sum_{a \in \mathbb{F}_p^{n-1}} c_a \neq 0$, and the second bound for arbitrary odd dimensions when $p = 3$, $\sum_{a \in \mathbb{F}_p^{n-1}} c_a = 0$, $\sum_{a \in \mathbb{F}_p^{n-1}} \gamma_a \neq 0$, and when $p = 5$, $\sum_{a \in \mathbb{F}_p^{n-1}} c_a \neq 0$. We obtained the following corollaries partially solving open problems I and II.

**Corollary 1:** The bounds (2) and (3) can be attained for $p = 3$ in arbitrary odd dimension.

**Corollary 2:** The bound (3) can be attained for $p = 5$ in arbitrary odd dimension.

**Remark 1:** As the bound (2) can only be attained by non-weakly regular bent functions, the function $F$ in Theorem 4 must be non-weakly regular for $p = 3$ and $\sum_{a \in \mathbb{F}_p^{n-1}} c_a \neq 0$. In fact this can be seen by a generalization of the arguments in [1] where infinite classes of non-weakly regular bent functions have been constructed. The reason behind $F$ being non-weakly regular is that we cannot choose all $c_a$ with the same quadratic character under the condition $p = 3$ and $\sum_{a \in \mathbb{F}_p^{n-1}} c_a \neq 0$. This is not a problem for $p = 5$ where non-weakly regular as well as weakly regular $F$ attaining the bound (3) can be found. We recall that for weakly regular bent functions the bound (3) is best possible.

**V. Conclusions**

In [1], [2], [8] a construction of bent functions from near-bent functions has been presented. In this article we generalize the this construction and present a technique to construct bent functions from plateaued functions. As quadratic functions are always plateaued we investigate some classes of quadratic functions. We completely describe the Fourier spectrum of quadratic monomials, and present classes of quadratic functions with maximal possible absolute values in their Fourier spectrum. We apply our construction to the latter classes of quadratic functions and thereby obtain the first construction of bent functions in characteristic 3 and 5 attaining upper bounds on the algebraic degree of bent functions presented by Hou in [6]. This partly solves open problems on the degree of bent functions and we can reformulate the open problems as follows:

(i) Can the bound (2) be attained for $p \geq 5$;
(ii) Can the bound (2) be attained in even dimension;
(iii) Can the bound (3) be attained for $p \geq 7$ and odd dimension.

**Acknowledgments**

The first author would like to thank the hospitality of INRIA Paris-Rocquencourt and she also wishes to thank Prof. Pascale Charpin who made the research visit possible.

Parts of the article were written during a short visit of the second author at INRIA Paris-Rocquencourt. He would like to thank the institute for the hospitality.

**References**


Ayça Çeşmeliolu received the Ph.D. degree in mathematics from Sabanci University, Istanbul, Turkey, in June 2008.

Currently, she is a postdoc researcher at Sabanci University. Her research interests include sequences, permutation polynomials, cryptographically significant functions and pseudorandom sequences.

Meidl Wilfried received the M.Sc and Ph.D degrees from Klagenfurt University, Austria, in 1994 and 1998, respectively.

From 2000 to 2002, he was with the Institute of Discrete Mathematics, OEAW, Vienna, Austria. From 2002 to 2004, he was with Ternasek Labs, National University of Singapore and from 2004 to 2005 with RICAM, Linz, Austria. He is now with Sabanci University, MDBF, Istanbul, Turkey. His research interests include sequences, permutation polynomials, pseudorandom number generation, finite fields and their applications, APN-functions, bent-functions.