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 $\widehat{f}$ on V_n given by

$$\widehat{f}(b) = \sum_{x \in V_n} \epsilon_p^{f(x)-\langle b,x\rangle}$$

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 $|\widehat{f}(b)|^2 = p^n$ for all $b \in V_n$. Whereas for $p = 2$, when $\epsilon_p = -1$ thus $\widehat{f}(b)$ 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 $b \in V_n$ of a function from V_n to $\mathbb{F}_p$ is defined by $p^{-n/2}\widehat{f}(b)$. A binary bent function clearly must have normalized Fourier coefficients ± 1, and for the p-ary case we always have (cf. [5], [7, Property 8])

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

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

A bent function f is called *regular* if

$$p^{-n/2}\widehat{f}(b) = \epsilon_p^{f^*(b)}$$

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 $p \equiv 1 \bmod 4$.

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

$$p^{-n/2}\widehat{f}(b) = \zeta\ \epsilon_p^{f^*(b)}.$$

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

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

$$\sum_{b \in V_n} \left|\widehat{f}(b)\right|^2 = p^{2n}$$

we see that $A = p^{n+s}$ for an integer s with $0 \le s \le n$. We will call a plateaued function with $|\widehat{f}(b)|^2 = p^{n+s}$ 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 $\deg(f)$ of f satisfies

$$\deg(f) \le \frac{(p-1)n}{2} + 1. \tag{2}$$

If f is weakly regular, then

$$\deg(f) \le \frac{(p-1)n}{2}. \tag{3}$$

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 $n \ge 3$ 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

The authors are with Sabancı University, MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey (email: cesmelioglu@sabanciuniv.edu, wmeidl@sabanciuniv.edu). The article was written when A. Çeşmelioğlu was working at INRIA Paris-Rocquencourt.

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 $\mathbb{F}_{p^n}$. We then usually use the inner product $\langle x, y\rangle = \mathrm{Tr_n}(xy)$ where $\mathrm{Tr_n}(z)$ 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

$$\widehat{f}(b) = \sum_{x\in\mathbb{F}_{p^n}} \epsilon_p^{f(x)-\mathrm{Tr_n}(bx)}.$$

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

$$f(x) = \mathrm{Tr_n}\left(\sum_{i=0}^{l} a_i x^{p^i+1}\right) \tag{4}$$

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]):

$$\begin{aligned} |\widehat{f}(-b)|^2 &= \sum_{x,y\in\mathbb{F}_{p^n}} \epsilon_p^{f(x)-f(y)+\mathrm{Tr_n}(b(x-y))} \\ &= \sum_{z\in\mathbb{F}_{p^n}} \epsilon_p^{f(z)+\mathrm{Tr_n}(bz)} \sum_{y\in\mathbb{F}_{p^n}} \epsilon_p^{f(y+z)-f(y)-f(z)}. \end{aligned}$$

Straightforward one gets $f(y+z) - f(y) - f(z) =$

$$\mathrm{Tr_n}\left(y^{p^l}\sum_{i=0}^{l}\left(a_i^{p^l} z^{p^{l+i}} + a_i^{p^{l-i}} z^{p^{l-i}}\right)\right) = \mathrm{Tr_n}(y^{p^l}L(z)).$$

Consequently

$$\begin{aligned} |\widehat{f}(-b)|^2 &= \sum_{z\in\mathbb{F}_{p^n}} \epsilon_p^{f(z)+\mathrm{Tr_n}(bz)} \sum_{y^{p^l}\in\mathbb{F}_{p^n}} \epsilon_p^{\mathrm{Tr_n}(yL(z))} \\ &= p^n \sum_{\substack{z\in\mathbb{F}_{p^n}\\ L(z)=0}} \epsilon_p^{f(z)+\mathrm{Tr_n}(bz)} \\ &= \begin{cases} p^{n+s} & \text{if } f(z)+\mathrm{Tr_n}(bz)\equiv 0 \text{ on } ker(L) \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

where in the last step we used that $f(z) + \mathrm{Tr_n}(bz)$ 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

$$L(x) = \sum_{i=0}^{l}\left(a_i^{p^l} x^{p^{l+i}} + a_i^{p^{l-i}} x^{p^{l-i}}\right). \tag{5}$$

Clearly this corresponds to

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

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

$$\deg(\gcd(A(x), x^n - 1)) = s, \tag{6}$$

where

$$A(x) = \sum_{i=0}^{l}\left(a_i^{p^l} x^{l+i} + a_i^{p^{l-i}} x^{l-i}\right) \tag{7}$$

is the *associate* of $L(x)$.

In some sense the simplest quadratic functions are quadratic monomials. It is well known that the monomial $f(x) = \mathrm{Tr_n}(ax^{p^r+1})$ 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 $f(x) = \mathrm{Tr_n}(ax^{p^r+1})$ is bent covering also the case when $n/\gcd(r, n)$ is even. In [1] it was shown that $f(x) = \mathrm{Tr_n}(ax^{p^r+1})$ 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 $p^s - 1|(p^n - 1)/2$ if and only if n/s is even, or equivalently $\nu(s) < \nu(n)$ where ν denotes the 2-adic valuation on integers.

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

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

$$L(x) = ax + a^{p^r} x^{p^{2r}}.$$

We want to find out under which conditions $ker(L)$ has dimension $s \geq 2$.

For a primitive element γ of $\mathbb{F}_{p^n}$, let $a = \gamma^c$ for some $c, 0 \leq c \leq p^n - 2$. Then $L(\gamma^t) = 0$ for an exponent $t, 0 \leq t \leq p^n - 2$, if and only if

$$\gamma^{\frac{p^n-1}{2}-c(p^r-1)} = \gamma^{(p^{2r}-1)t},$$

which is equivalent to

$$\frac{p^n-1}{2} - c(p^r-1) \equiv (p^{2r}-1)t \bmod (p^n-1).$$

The kernel has dimension s if and only if this congruence has $p^s - 1$ incongruent solutions, i.e.

(a) $\gcd(p^{2r} - 1, p^n - 1) = p^{\gcd(2r,n)} - 1 = p^s - 1$, or equivalently
$\gcd(2r, n) = s$,
(b) $p^s - 1|\frac{p^n-1}{2} - c(p^r - 1)$.

First, assume that n is odd. By (a) this implies that s is also odd and hence $\gcd(r, n) = s$. Consequently $p^s - 1$ divides $p^r - 1$, thus (b) holds if and only if $p^s-1|\frac{p^n-1}{2}$, which contradicts that n is odd. Therefore for the rest of the proof we may assume that n is even and hence by condition (a) also s is even. We consider two cases.

- Case I: $\frac{n}{s}$ is even.
  Condition (a) then implies that $\frac{2r}{s}$ is odd, hence $\nu(s) = \nu(r) + 1$. We remark that in this case and $p^s - 1$ does

not divide p^r-1. Due to condition (b) we then have to find solutions c, y for the equation

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

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

- Case II: $\frac{n}{s}$ is odd.
  We consider two subcases:
  (i) Suppose $\frac{2r}{s}$ is odd. Then we have $\nu(s)=\nu(r)+1$ and hence $p^s-1 \nmid p^r-1$. 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 $\frac{2r}{s}$ is even, i.e. $\nu(s)\leq\nu(r)$. Then $p^s-1 \mid p^r-1$ 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 $f(x)=\mathrm{Tr_n}(ax^{p^r+1})$ 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 $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, and $\widehat{f}$ denote its Fourier transform. The support of $\widehat{f}$ is then defined to be the set $supp(\widehat{f})=\{b\in\mathbb{F}_{p^n}\mid \widehat{f}(b)\neq 0\}$. In this section we describe a procedure to construct p-ary bent functions in dimension $n+s$ from s-plateaued functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. 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 $\mathbf{a}=(a_1,a_2,\cdots,a_s)\in\mathbb{F}_p^s$, let $f_{\mathbf{a}}(x)$ be an s-plateaued function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. If $supp(\widehat{f_{\mathbf{a}}})\cap supp(\widehat{f_{\mathbf{b}}})=\emptyset$ for $\mathbf{a},\mathbf{b}\in\mathbb{F}_p^s, \mathbf{a}\neq\mathbf{b}$, then the function $F(x,y_1,y_2,\cdots,y_s)$ from $\mathbb{F}_{p^n}\times\mathbb{F}_p^s$ to $\mathbb{F}_p$ defined by

$$F(x,y_1,y_2,\cdots,y_s)= \sum_{\mathbf{a}\in\mathbb{F}_p^s}\frac{(-1)^s\prod_{i=1}^s y_i(y_i-1)\cdots(y_i-(p-1))}{(y_1-a_1)\cdots(y_s-a_s)}f_{\mathbf{a}}(x)$$

is bent.

Proof: For $(\alpha,\mathbf{a}),(x,\mathbf{y})\in\mathbb{F}_{p^n}\times\mathbb{F}_p^s$ the inner product we use is $\mathrm{Tr_n}(\alpha x)+\mathbf{a}\cdot\mathbf{y}=\mathrm{Tr_n}(\alpha x)+a_1y_1+a_2y_2+\cdots+a_sy_s$, where $\mathbf{a}=(a_1,\cdots,a_s),\mathbf{y}=(y_1,\cdots,y_s)$. The Fourier transform $\widehat{F}$ of F at $(\alpha,\mathbf{a})$ is

$$\begin{aligned}\widehat{F}(\alpha,\mathbf{a}) &= \sum_{x\in\mathbb{F}_{p^n},y_1,\cdots,y_s\in\mathbb{F}_p}\epsilon_p^{F(x,y_1,\cdots,y_s)-\mathrm{Tr_n}(\alpha x)-\mathbf{a}\cdot\mathbf{y}}\\ &= \sum_{y_1,\cdots,y_s\in\mathbb{F}_p}\epsilon_p^{-\mathbf{a}\cdot\mathbf{y}}\sum_{x\in\mathbb{F}_{p^n}}\epsilon_p^{F(x,y_1,\cdots,y_s)-\mathrm{Tr_n}(\alpha x)}\\ &= \sum_{y_1,\cdots,y_s\in\mathbb{F}_p}\epsilon_p^{-\mathbf{a}\cdot\mathbf{y}}\sum_{x\in\mathbb{F}_p^n}\epsilon_p^{f_{\mathbf{y}}(x)-\mathrm{Tr_n}(\alpha x)}\\ &= \sum_{y_1,\cdots,y_s\in\mathbb{F}_p}\epsilon_p^{-\mathbf{a}\cdot\mathbf{y}}\widehat{f_{\mathbf{y}}}(\alpha).\end{aligned}$$

As each $\alpha\in\mathbb{F}_{p^n}$ belongs to the support of exactly one $\widehat{f_{\mathbf{y}}}$, $\mathbf{y}\in\mathbb{F}_p^s$, for this $\mathbf{y}$ we have $\left|\widehat{F}(\alpha,\mathbf{a})\right|=|\epsilon_p^{-\mathbf{a}\cdot\mathbf{y}}\widehat{f_{\mathbf{y}}}(\alpha)|=p^{\frac{n+s}{2}}$. □

Theorem 3: For each $\mathbf{a}\in\mathbb{F}_p^s$, let $g_{\mathbf{a}}$ be a quadratic s-plateaued function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ with the corresponding linearized polynomial $L_{\mathbf{a}}$ such that for all $\mathbf{a}\in\mathbb{F}_p^s, L_{\mathbf{a}}$ has the same kernel $\{c_1\beta_1+\cdots+c_s\beta_s, 0\leq c_1,\cdots,c_s\leq p-1\}$ in $\mathbb{F}_{p^n}$. For each $\mathbf{a}=(a_1,\cdots,a_s)\in\mathbb{F}_p^s$, let $\gamma_{\mathbf{a}}\in\mathbb{F}_{p^n}$ be such that

$$g_{\mathbf{a}}(\beta_j)+\mathrm{Tr_n}(\gamma_{\mathbf{a}}\beta_j)=g_{\mathbf{0}}(\beta_j)+a_j, \qquad (9)$$

for all $j=1,\cdots,s$. Then for each $\mathbf{a}\in\mathbb{F}_p^s$, the s-plateaued function $f_{\mathbf{a}}$ defined by $f_{\mathbf{a}}(x)=g_{\mathbf{a}}(x)+\mathrm{Tr_n}(\gamma_{\mathbf{a}}x)$ satisfies $supp(\widehat{f_{\mathbf{a}}})\cap supp(\widehat{f_{\mathbf{b}}})=\emptyset$ for $\mathbf{b}\in\mathbb{F}_p^s, \mathbf{a}\neq\mathbf{b}$.

Proof: We have to show that $-\alpha\in supp(\widehat{f_{\mathbf{b}}})$ implies $-\alpha\notin supp(\widehat{f_{\mathbf{a}}})$ for $\mathbf{a}\neq\mathbf{b}$. Suppose $-\alpha\in supp(\widehat{f_{\mathbf{b}}})$, i.e.

$$g_{\mathbf{b}}(\beta_j)+\mathrm{Tr_n}(\gamma_{\mathbf{b}}\beta_j)+\mathrm{Tr_n}(\alpha\beta_j)=g_{\mathbf{0}}(\beta_j)+b_j+\mathrm{Tr_n}(\alpha\beta_j)=0,$$

for each $j=1,\cdots,s$.

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

$$\begin{aligned}&f_{\mathbf{a}}(\beta_j)+\mathrm{Tr_n}(\alpha\beta_j)=g_{\mathbf{a}}(\beta_j)+\mathrm{Tr_n}(\gamma_{\mathbf{a}}\beta_j)+\mathrm{Tr_n}(\alpha\beta_j)=\\ &g_{\mathbf{0}}(\beta_j)+a_j+\mathrm{Tr_n}(\alpha\beta_j)\neq 0.\end{aligned}$$

□

Observe that the existence of $\gamma_{\mathbf{a}}$ that satisfies equation (9) for all $j=1,\ldots,s$, is guaranteed by the linear independence of $\beta_1,\ldots,\beta_s$, the elements of the basis of the kernel for the linearized polynomial $L_{\mathbf{a}}$. To point to a deterministic way of obtaining $\gamma_{\mathbf{a}}$ we give a detailed argument for this observation: Let $\{\delta_1,\delta_2,\ldots,\delta_n\}$ and $\{\rho_1,\rho_2,\ldots,\rho_n\}$ be dual bases of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, and let $\beta_j=b_{j1}\delta_1+b_{j2}\delta_2+\cdots+b_{jn}\delta_n$. Put $\gamma_{\mathbf{a}}=x_1\rho_1+x_2\rho_2+\cdots+x_n\rho_n$, then

$$\mathrm{Tr_n}(\gamma_{\mathbf{a}}\beta_j)=b_{j1}x_1+b_{j2}x_2+\cdots+b_{jn}x_n.$$

A value for $\gamma_{\mathbf{a}}$ is then a solution of the linear system $B\mathbf{x}=\mathbf{c}$ over $\mathbb{F}_p$ for the $(s\times n)$-matrix $B=(b_{jk})$ and $\mathbf{c}=(c_1,\cdots,c_s)^T$ with $c_j=g_{\mathbf{0}}(\beta_j)+a_j-g_{\mathbf{a}}(\beta_j)$, $j=1,2,\ldots,s$.

Example 1: To obtain a 2-plateaued monomial function $\mathrm{Tr}_4(ax^{3^r+1})$ from $\mathbb{F}_{3^4}$ to $\mathbb{F}_3$, by Theorem 1 we can choose $r=1$ or $r=3$. In fact the monomials $g_0(x)=\mathrm{Tr}_4(x^4), g_1(x)=\mathrm{Tr}_4(x^{28})$ have the same corresponding linearized polynomial $L(x)=x+x^{3^2}$ with a kernel of dimension 2 in $\mathbb{F}_{3^4}$. A basis for this kernel is $\{\beta,\beta^3\}$ where β is a root of the polynomial x^4+x^2+2. Since we have $g_0(\beta)=g_0(\beta^3)=g_1(\beta)=g_1(\beta^3)=0$ for each $\mathbf{a}=(a_1,a_2)\in\mathbb{F}_3\times\mathbb{F}_3$, we choose $\gamma_{\mathbf{a}}\in\mathbb{F}_{3^4}$ such that $\mathrm{Tr}_4(\gamma_{\mathbf{a}}\beta)=a_1, \mathrm{Tr}_4(\gamma_{\mathbf{a}}\beta^3)=a_2$. For instance we can choose

$$\begin{array}{lll}\gamma_{(0,0)}=1, & \gamma_{(0,1)}=\beta^3+1, & \gamma_{(0,2)}=2\beta^3+2,\\ \gamma_{(1,0)}=\beta, & \gamma_{(1,1)}=\beta^3+\beta, & \gamma_{(1,2)}=2\beta^3+\beta+1,\\ \gamma_{(2,0)}=2\beta+1, & \gamma_{(2,1)}=\beta^3+2\beta, & \gamma_{(2,2)}=2\beta^3+2\beta,\end{array}$$

and for the nine required 2-plateaued functions with pairwise disjoint supports of their Fourier transforms we then can choose

$$\begin{aligned}
f_{(0,0)}(x) &= \mathrm{Tr}_4(x^4 + x),\\
f_{(0,1)}(x) &= \mathrm{Tr}_4(x^4 + (\beta^3 + 1)x),\\
f_{(0,2)}(x) &= \mathrm{Tr}_4(x^4 + (2\beta^3 + 2)x),\\
f_{(1,0)}(x) &= \mathrm{Tr}_4(x^4 + \beta x),\\
f_{(1,1)}(x) &= \mathrm{Tr}_4(x^4 + (\beta^3 + \beta)x),\\
f_{(1,2)}(x) &= \mathrm{Tr}_4(x^{28} + (2\beta^3 + \beta + 1)x),\\
f_{(2,0)}(x) &= \mathrm{Tr}_4(x^{28} + (2\beta + 1)x),\\
f_{(2,1)}(x) &= \mathrm{Tr}_4(x^{28} + (\beta^3 + 2\beta)x),\\
f_{(2,2)}(x) &= \mathrm{Tr}_4(x^{28} + (2\beta^3 + 2\beta)x).
\end{aligned}$$

The function

$$F(x,y,z) = \sum_{\substack{\mathbf{a}=(a_1,a_2)\\ \in\mathbb{F}_3\times\mathbb{F}_3}} \frac{yz(y-1)(z-1)(y-2)(z-2)}{(y-a_1)(z-a_2)} f_{\mathbf{a}}(x)$$

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-plateaued functions.

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

Proof: If the quadratic terms in $\sum_{\mathbf{a}\in\mathbb{F}_p^s} f_{\mathbf{a}}$ do not cancel, then in F given as in Theorem 2 the summand $(-1)^s y_1^{p-1} y_2^{p-1} \cdots y_s^{p-1} \sum_{\mathbf{a}\in\mathbb{F}_p^s} f_{\mathbf{a}}(x)$ having degree $(p-1)s+2$ does not vanish. Similarly, if $\sum_{\mathbf{a}\in\mathbb{F}_p^s} f_{\mathbf{a}} = \mathrm{Tr_n}(cx)$ for some $c \in \mathbb{F}_{p^n}$, then the bent function F in Theorem 2 has the summand $(-1)^s y_1^{p-1} y_2^{p-1} \cdots y_s^{p-1} \mathrm{Tr_n}(cx)$ 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 $s \le n$ and the set of n-plateaued functions precisely coincides with the set of affine and constant functions. Thus $s = n-1$ is the maximal value for s for s-plateaued quadratic functions. The following proposition shows that this maximal value can be obtained.

Proposition 2: For n even, the quadratic function $ch(x)$, $c \in \mathbb{F}_p^*$, from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ with

$$h(x) = \mathrm{Tr_n}\left(\frac{p+1}{2}x^{p^{n/2}+1} + \frac{p+1}{2}x^2 + \sum_{i=1}^{n/2-1} x^{p^i+1}\right) \tag{10}$$

is $(n-1)$-plateaued.

If n is odd, then the quadratic function $ch(x)$, $c \in \mathbb{F}_p^*$, from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ with

$$h(x) = \mathrm{Tr_n}\left(\frac{p+1}{2}x^2 + \sum_{i=1}^{(n-1)/2} x^{p^i+1}\right) \tag{11}$$

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 $A(x)$ (7) of the linearized polynomial (5) that corresponds to $ch(x)$ is given by

$$\begin{aligned}
A(x) &= c\Bigg(\frac{p+1}{2}x^n + \frac{p+1}{2} + 2\frac{p+1}{2}x^{n/2} + \\
&\qquad \sum_{i=1}^{n/2-1} x^{n/2+i} + x^{n/2-i}\Bigg)\\
&= c\left(\frac{p+1}{2}x^n - \frac{p+1}{2} + \sum_{i=0}^{n-1} x^i\right)\\
&= c\frac{p+1}{2}(x^n - 1) + c\sum_{i=0}^{n-1} x^i.
\end{aligned}$$

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 $\mathbf{a} = (a_1, a_2, \ldots, a_{n-1}) \in \mathbb{F}_p^{n-1}$ let
   - $c_{\mathbf{a}}$ be a nonzero element of $\mathbb{F}_p$,
   - $\gamma_{\mathbf{a}}$ be an element of $\mathbb{F}_{p^n}$, such that
     $$c_{\mathbf{a}}h(\beta_j) + \mathrm{Tr_n}(\gamma_{\mathbf{a}}\beta_j) = c_{\mathbf{0}}h(\beta_j) + a_j,\ j = 1, \ldots, n-1, \tag{12}$$
     for a fixed basis $\{\beta_1, \beta_2, \ldots, \beta_{n-1}\}$ for the kernel of the linearized polynomial L corresponding to h,
   - $h_{\mathbf{a}}(x) = c_{\mathbf{a}}h(x) + \mathrm{Tr_n}(\gamma_{\mathbf{a}}x)$.

Theorem 4: The function F defined by

$$F(x, y_1, y_2, \cdots, y_{n-1}) = \sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} \frac{(-1)^{n-1}\prod_{i=1}^{n-1} y_i(y_i-1)\cdots(y_i-(p-1))}{(y_1-a_1)\cdots(y_{n-1}-a_{n-1})} h_{\mathbf{a}}(x)$$

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 $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} c_{\mathbf{a}} \ne 0$, and degree $(p-1)(n-1)+1$ if $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} c_{\mathbf{a}} = 0$ and $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} \gamma_{\mathbf{a}} \ne 0$.

Proof: For all $\mathbf{a} \in \mathbb{F}_p^{n-1}$ the linearized polynomials $L_{\mathbf{a}}$ corresponding to $c_{\mathbf{a}}h$ have the same kernel, and the definition (12) for $\gamma_{\mathbf{a}}$ guarantees that the Fourier transforms of the $(n-1)$-plateaued functions $h_{\mathbf{a}}$, $\mathbf{a} \in \mathbb{F}_p^{n-1}$, have pairwise disjoint support. By Theorem 2 the function F is bent. Since $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} h_{\mathbf{a}} = (\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} c_{\mathbf{a}})h + \mathrm{Tr_n}(\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} \gamma_{\mathbf{a}}x)$ has degree 2 if $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} c_{\mathbf{a}} \ne 0$ and degree 1 if $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} c_{\mathbf{a}} = 0$ and $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} \gamma_{\mathbf{a}} \ne 0$, 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 $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} c_{\mathbf{a}} \ne 0$. We emphasize that for any choice of the set $\{c_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{F}_p^{n-1}\}$ we can choose $\{\gamma_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{F}_p^{n-1}\}$ such that $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} \gamma_{\mathbf{a}} \ne 0$, since for every $\mathbf{a} \in \mathbb{F}_p^{n-1}$ the linear system from which we obtain $\gamma_{\mathbf{a}}$ 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 $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} c_{\mathbf{a}} \neq 0$, and the second bound for arbitrary odd dimensions when $p=3$, $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} c_{\mathbf{a}} = 0$, $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} \gamma_{\mathbf{a}} \neq 0$, and when $p=5$, $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} c_{\mathbf{a}} \neq 0$. 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 $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} c_{\mathbf{a}} \neq 0$. 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 $c_{\mathbf{a}}$ with the same quadratic character under the condition $p=3$ and $\sum_{\mathbf{a}\in\mathbb{F}_p^{n-1}} c_{\mathbf{a}} \neq 0$. 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

[1] A. Çeşmelioğlu, G. McGuire, W. Meidl, A construction of weakly and non-weakly regular bent functions, preprint 2010.

[2] P. Charpin, E. Pasalic, C. Tavernier, On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inform. Theory 51 (2005), 4286–4298.

[3] P. Dembowski, T. Ostrom, Planes of order n with collineation groups of order n^2. Math. Z. 103 (1968), 239–258.

[4] H. Dobbertin, Construction of bent functions and balanced boolean functions with high nonlinearity, in: Fast Software Encryption (B. Preneel, Eds.), Second International Workshop, Proceedings, Lecture Notes in Computer Science 1008, Springer-Verlag, Berlin, 1995, pp. 61–74.

[5] T. Helleseth, A. Kholosha, Monomial and quadratic bent functions over the finite field of odd characteristic. IEEE Trans. Inform. Theory 52 (2006), 2018–2032.

[6] X.D. Hou, p-ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields Appl. 10 (2004), 566–582.

[7] P.V. Kumar, R.A. Scholtz, L.R. Welch, Generalized bent functions and their properties. Journal of Combinatorial Theory, Series A 40 (1985), 90–107.

[8] G. Leander, G. McGuire, Construction of bent functions from near-bent functions. Journal of Combinatorial Theory, Series A 116 (2009), 960–970.

[9] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.

[10] O.S. Rothaus, On "bent" functions. Journal of Combinatorial Theory, Series A 20 (1976), 300–305.

[11] Y. Tan, J. Yang, X. Zhang, A recursive approach to construct p-ary bent functions which are not weakly regular. In: Proceedings of IEEE International Conference on Information Theory and Information Security, Beijing, 2010, to appear.

Ayça Çeşmelioğlu received the Ph.D. degree in mathematics from Sabancı University, İstanbul, Turkey, in June 2008.

Currently, she is a postdoc researcher at Sabanci University. Her research interests include 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, ha was with the Institute of Discrete Mathematics, OEAW, Vienna, Austria. From 2002 to 2004, ha was with Temasek Labs, National University of Singapore and from 2004 to 2005 with RICAM, Linz, Austria. He is now with Sabancı University, MDBF, İstanbul, Turkey. His research interests include sequences, permutation polynomials, pseudorandom number generation, finite fields and their applications, APN-functions, bent-functions.