A construction of bent functions from plateaued functions

Ayça Çeşmelioğlu, Wilfried Meidl

Sabancı University, MDBF, Orhanlı, 34956 Tuzla, İstanbul, Turkey.

Abstract

In this presentation, a technique for constructing bent functions from plateaued functions is introduced and analysed. This generalizes earlier techniques for constructing bent from near-bent functions. Using this construction, we obtain a big variety of inequivalent bent functions, some weakly regular and some non-weakly regular. Classes of bent function with some additional properties that enable the construction of strongly regular graphs are constructed, and explicit expressions for bent functions with maximal degree are presented.

1 Introduction

For a prime p, let f be a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. The *Fourier transform* of f is then defined to be the complex valued function $\widehat{f}$ on $\mathbb{F}_p^n$

$$\widehat{f}(b) = \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f(x)-b\cdot x}$$

where $\epsilon_p = e^{2\pi i/p}$ and $b \cdot x$ denotes the conventional dot product in $\mathbb{F}_p^n$. The Fourier spectrum $spec(f)$ of f is the set of all values of $\widehat{f}$. We remark that one can equivalently consider functions from an arbitrary n-dimensional vector space over $\mathbb{F}_p$ to $\mathbb{F}_p$, and substitute the dot product with any (non-degenerate) inner product. Frequently the finite field $\mathbb{F}_{p^n}$ with the inner product $\mathrm{Tr_n}(bx)$ is used, where $\mathrm{Tr_n}(z)$ denotes the absolute trace of $z \in \mathbb{F}_{p^n}$.

The function f is called a *bent function* if $|\widehat{f}(b)|^2 = p^n$ for all $b \in \mathbb{F}_p^n$. The *normalized Fourier coefficient* of f at $b \in \mathbb{F}_p^n$ is defined by $p^{-n/2}\widehat{f}(b)$. For a bent function the normalized Fourier coefficients are obviously ± 1 when $p = 2$, and for $p > 2$ we always have (cf. [7])

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

where f^* is a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$.

A bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called *regular* if for all $b \in \mathbb{F}_p^n$

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

When $p = 2$, a bent function is trivially regular, and as can be seen from (1), for $p > 2$ a regular bent function can only exist for even n and for odd n when $p \equiv 1 \bmod 4$.

A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called *weakly regular* if, for all $b \in \mathbb{F}_p^n$, we have

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

for some complex number ζ with $|\zeta| = 1$. By (1), ζ can only be ± 1 or $\pm i$. Note that regular implies weakly regular.

A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called plateaued if $|\widehat{f}(b)|^2 = A$ or 0 for all $b \in \mathbb{F}_p^n$. By *Parseval's identity*, we obtain that $A = p^{n+s}$ for an integer s with $0 \le s \le n$. Moreover, support of $\widehat{f}$ defined by $supp(\widehat{f}) = \{b \in \mathbb{F}_{p^n} \mid \widehat{f}(b) \neq 0\}$ has cardinality p^{n-s}. 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. For 1-plateaued functions the term *near-bent* function is common (see [3, 9]), binary 1-plateaued and 2-plateaued functions are referred to as *semi-bent* functions in [5].

We present a technique for constructing bent functions from plateaued functions which generalizes earlier constructions of bent functions from near-bent functions. Though the technique also works for $p = 2$, we assume in the following that p is odd, as we are mainly interested in this type of functions, which we also will call p-ary functions. In Section 2 we analyse the Fourier spectrum of quadratic functions and the effect of equivalence transformations to the Fourier spectrum. In particular, we show under which conditions the multiplication of a p-ary function with a constant changes the signs in the Fourier spectrum. The procedure for constructing bent functions from s-plateaued functions is presented in Section 3. In Section 4 we point out that the construction delivers a large variety of provable inequivalent bent functions, and we give some simple examples of weakly regular and non-weakly regular bent functions. Bent functions with some additional properties can be used to construct strongly regular graphs (see [6, 11, 12]). We will show how to obtain a large variety of such bent functions. Finally, we present simple explicit expressions for bent functions in odd dimension with maximal possible degree.

2 Fourier spectrum

Two functions f and g from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ are called *extended affine equivalent (EA-equivalent)* if

$$g(x) = cf(L(x) + u) + v \cdot x + e$$

for some $c \in \mathbb{F}_p^*, e \in \mathbb{F}_p$, $u, v \in \mathbb{F}_p^n$, and a linear permutation $L : \mathbb{F}_p^n \to \mathbb{F}_p^n$. As well known, EA-equivalence preserves the main characteristics of the Fourier spectrum, in particular if f is bent then also g is bent. More precisely we have the following properties which can be verified straightforward.

(i) $\widehat{(f+e)}(b) = \epsilon_p^e \widehat{f}(b)$,

(ii) if $f_v(x) = f(x) + v \cdot x$ then $\widehat{f_v}(b) = \widehat{f}(b - v)$,

(iii) $\widehat{f(x+u)}(b) = \epsilon_p^{b \cdot u} \widehat{f}(b)$,

(iv) if $L(x) = Ax$ for $A \in GL(\mathbb{F}_p)$ then $\widehat{f(L(x))}(b) = \widehat{f}((A^{-1})^T b)$, where A^T denotes the transpose of the matrix A.

We note that these transformations do not only preserve the absolute value of the Fourier coefficients but also their sign is not changed. This is different if f is multiplied by a constant $c \in \mathbb{F}_p^*$. Before we analyse the effect of this transformation, we give an analysis of the Fourier transform of quadratic functions. Using the properties (i),(ii), we omit the affine part and consider quadratic functions $f(x) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$ from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, where we put $x = (x_1, \ldots, x_n)$. Every such quadratic function f can be associated with a quadratic form

$$f(x) = x^T A x$$

where x^T denotes the transpose of the vector x, and A is a symmetric matrix with entries in $\mathbb{F}_p$. By [10, Theorem 6.21] any quadratic form can be transformed to a diagonal quadratic form by a coordinate transformation, i.e. $D = C^T AC$ for a nonsingular (even orthogonal) matrix C over $\mathbb{F}_p$ and a diagonal matrix $D = diag(d_1, \ldots, d_n)$, and it is sufficient to describe the Fourier spectrum of a quadratic form

$$f(x) = d_1 x_1^2 + \cdots + d_{n-s} x_{n-s}^2 := Q_{n,n-s}^d(x)$$

for some $0 \le s \le n-1$ and $d = (d_1, \ldots, d_{n-s})$. We may assume that the nonzero elements of the matrix D are $d_1, \ldots, d_{n-s}$. The following proposition

describing Fourier spectrum of $Q^d_{n,n-s}(x)$ was presented in [3], where bent functions have been constructed from near-bent functions. For convenience we will include the proof.

Proposition 1 *[3] For the quadratic function $Q^d_{n,n-s}(x) = d_1x_1^2 + \cdots + d_{n-s}x_{n-s}^2$ from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, let $\Delta = \prod_{i=1}^{n-s} d_i$, and let η denote the quadratic character of $\mathbb{F}_p$. The Fourier spectrum of $Q^d_{n,n-s}$ is given by*

$$spec(Q^d_{n,n-s}) = \begin{cases} \left\{0, \eta(\Delta)p^{\frac{n+s}{2}}\epsilon_p^{f^*(b)} \mid b \in supp(\widehat{Q^d_{n,n-s}})\right\} & : \quad p \equiv 1 \bmod 4, \\ \left\{0, \eta(\Delta)i^{n-s}p^{\frac{n+s}{2}}\epsilon_p^{f^*(b)} \mid b \in supp(\widehat{Q^d_{n,n-s}})\right\} & : \quad p \equiv 3 \bmod 4, \end{cases}$$

if $s > 0$, where $f^*(x)$ is a function from $supp(\widehat{Q^d_{n,n-s}})$ to $\mathbb{F}_p$, and

$$spec(Q^d_{n,n}) = \begin{cases} \left\{\eta(\Delta)p^{\frac{n}{2}}\epsilon_p^{f^*(b)} \mid b \in \mathbb{F}_p^n\right\} & : \quad p \equiv 1 \bmod 4, \\ \left\{\eta(\Delta)i^{n}p^{\frac{n}{2}}\epsilon_p^{f^*(b)} \mid b \in \mathbb{F}_p^n\right\} & : \quad p \equiv 3 \bmod 4, \end{cases}$$

where $f^*(x)$ is a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$.

Proof: We start with two facts which are simple to verify. For two functions $f : \mathbb{F}_p^n \to \mathbb{F}_p$ and $g : \mathbb{F}_p^m \to \mathbb{F}_p$, we define the function $f \oplus g$ from $\mathbb{F}_p^n \times \mathbb{F}_p^m$ by $(f \oplus g)(x, y) = f(x) + g(y)$. Then (see also [1])

$$\widehat{(f \oplus g)}(u, v) = \widehat{f}(u)\widehat{g}(v). \tag{2}$$

For a function $f : \mathbb{F}_p^m \to \mathbb{F}_p$ let $\tilde{f}$ be the function from $\mathbb{F}_p^{m+n} = \mathbb{F}_p^m \times \mathbb{F}_p^n$ to $\mathbb{F}_p$ defined by $\tilde{f}(x, y) = f(x)$. Then (see also [3, Lemma 2], and compare with Lemma 1 in Section 3)

$$\widehat{\tilde{f}}(b, c) = \begin{cases} p^n\widehat{f}(b) & : \quad c = 0, \\ 0 & : \quad \text{else.} \end{cases} \tag{3}$$

We first consider $Q^d_{1,1}(\mathbf{x}) = dx^2$ and note that by [10, Theorem 5.33]

$$\widehat{Q^d_{1,1}}(0) = \sum_{x \in \mathbb{F}_p} \epsilon_p^{dx^2} = \eta(d)G(\eta, \chi_1)$$

where χ_1 is the canonical additive character of $\mathbb{F}_p$ and $G(\eta, \chi_1)$ is the associated Gaussian sum. Consequently

$$\widehat{Q^d_{1,1}}(b) = \sum_{x \in \mathbb{F}_p} \epsilon_p^{dx^2 - bx} = \sum_{x \in \mathbb{F}_p} \epsilon_p^{d(x - b/(2d))^2 - b^2/(4d)} = \epsilon_p^{-b^2/(4d)}\eta(d)G(\eta, \chi_1).$$

With [10, Theorem 5.15] we then obtain

$$\widehat{Q^d_{1,1}}(b) = \begin{cases} \eta(\Delta) p^{\frac{1}{2}} \epsilon_p^{-b^2/(4d)} & : \quad p \equiv 1 \bmod 4, \\ \eta(\Delta) i p^{\frac{1}{2}} \epsilon_p^{-b^2/(4d)} & : \quad p \equiv 3 \bmod 4. \end{cases}$$

With equation (3) we get the assertion for $Q^d_{n,1}$ for arbitrary n. The general assertion then follows with induction from equation (2). □

Remark 1 *Since the multiplication of a quadratic function f by a constant $c \in \mathbb{F}_p^*$ causes a multiplication by c of every element in the associated diagonal matrix, the Fourier spectra of the functions f and cf is identical if and only if $n-s$ is even or $n-s$ is odd and c is a square in $\mathbb{F}_p$. If $n-s$ is odd and c is a nonsquare, then the Fourier coefficients of f and cf have opposite sign.*

Remark 2 *Let $Q^d_{n,n-s}(x) = d_1 x_1^2 + \cdots + d_{n-s} x^2$ and $Q^{d'}_{n,n-s}(x) = d'_1 x_1^2 + \cdots + d'_{n-s} x^2$ be two quadratic s-plateaued functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, then one can be obtained from the other by a coordinate transformation if and only if $\eta(\Delta) = \eta(\Delta')$, where $\Delta = \prod_{i=1}^{n-s} d_i$ and $\Delta' = \prod_{i=1}^{n-s} d'_i$ (see e.g. [10, Exercise 6.24]). If $n-s$ is odd we can also change the character of Δ by multiplying the s-plateaued function by a nonsquare. Consequently every quadratic s-plateaued function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ is EA-equivalent to $x_1^2 + x_2^2 + \cdots + x_{n-s}^2$ if $n-s$ is odd. If $n-s$ is even then there are two EA-inequivalent classes of quadratic s-plateaued functions in dimension n.*

We will show next that Remark 1 is a special case of a much more general theorem.

For a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ and $b \in \mathbb{F}_p^n$, let $N_b(j) = |\{x \in \mathbb{F}_p^n : f(x) - b \cdot x = j\}|$ for each $j = 0, \ldots, p-1$. Then

$$\widehat{f}(b) = \sum_{j=0}^{p-1} N_b(j) \epsilon_p^j,$$

and for any $c \in \mathbb{F}_p^*$ we have

$$\widehat{cf}(cb) = \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{cf(x) - (cb)\cdot x} = \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{c(f(x) - b \cdot x)} = \sum_{j=0}^{p-1} N_b(j) \epsilon_p^{cj}. \qquad (4)$$

Suppose that $|\widehat{f}(b)| = p^{(n+s)/2}$, then we have [7, p.2019]

$$\sum_{j=0}^{p-1} N_b(j)\epsilon_p^j \mp p^{(n+s)/2}\epsilon_p^{f^*(b)} = 0 \tag{5}$$

when $n-s$ is even, and

$$\sum_{j=0}^{p-1} \left(N_b(j) \mp \left(\frac{j-f^*(b)}{p}\right) p^{(n+s-1)/2} \right) \epsilon_p^j = 0 \tag{6}$$

when $n-s$ is odd, where $0 \le f^*(b) \le p-1$ is an integer depending on b.

If $n-s$ is even, then using the automorphism σ_c of $\mathbb{Q}(\epsilon_p)$ that fixes $\mathbb{Q}$ and $\sigma_c(\epsilon_p) = \epsilon_p^c$, equation (5) implies

$$\sum_{j=0}^{p-1} N_b(j)\epsilon_p^{cj} = \pm p^{(n+s)/2}\epsilon_p^{cf^*(b)}.$$

Consequently using equation (4)

$$\widehat{cf}(cb) = \sum_{j=0}^{p-1} N_b(j)\epsilon_p^{cj} = \pm p^{(n+s)/2}\epsilon_p^{cf^*(b)}.$$

If $n-s$ is odd, with the automorphism σ_c and equation (6) we get

$$\sum_{j=0}^{p-1} N_b(j)\epsilon_p^{cj} \mp \left(\frac{j-f^*(b)}{p}\right) p^{(n+s-1)/2}\epsilon_p^{cj} = 0.$$

Hence equation (4) can be written as

$$\widehat{cf}(cb) = \pm p^{(n+s-1)/2} \left(\frac{j-f^*(b)}{p}\right) \epsilon_p^{cj}.$$

Replacing j first by $j+f^*(b)$ and then by $c^{-1}j$, we obtain

$$\begin{aligned}
\widehat{cf}(cb) &= \pm p^{(n+s-1)/2} \sum_{j=0}^{p-1} \epsilon_p^{cf^*(b)} \left(\frac{c^{-1}j}{p}\right) \epsilon_p^j \\
&= \pm \left(\frac{c^{-1}}{p}\right) \epsilon_p^{(c-1)f^*(b)} p^{(n+s-1)/2} \sum_{j=0}^{p-1} \epsilon_p^{f^*(b)} \left(\frac{j}{p}\right) \epsilon_p^j \\
&= \left(\frac{c}{p}\right) \epsilon_p^{(c-1)f^*(b)} \widehat{f}(b).
\end{aligned}$$

We have shown the following theorem.

Theorem 1 *For an element $b \in \mathbb{F}_p^n$ and a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ suppose that $|\widehat{f}(b)|^2 = p^{n+s}$ for some $s \geq 0$. If $n-s$ is even or $n-s$ is odd and c is a square in $\mathbb{F}_p$, then $\widehat{cf}(cb) = \epsilon^k \widehat{f}(b)$ for some integer k. If $n-s$ is odd and c is a nonsquare in $\mathbb{F}_p$, then $\widehat{cf}(cb) = -\epsilon_p^k \widehat{f}(b)$ for some integer k.*

3 The construction

In this section we describe the procedure to construct p-ary bent functions from $\mathbb{F}_p^{n+s}$ to $\mathbb{F}_p$ from s-plateaued functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. The construction seen in the framework of finite fields $\mathbb{F}_{p^n}$ has been used in [4] to show the existence of ternary bent functions attaining the upper bound on algebraic degree given by Hou [8]. The construction can be seen as a generalization of the constructions in [5, 3, 9] where $s = 1$.

Theorem 2 *For each $u = (u_1, u_2, \cdots, u_s) \in \mathbb{F}_p^s$, let $f_u(x) : \mathbb{F}_p^n \to \mathbb{F}_p$ be an s-plateaued function. If $supp(\widehat{f_u}) \cap supp(\widehat{f_v}) = \emptyset$ for $u, v \in \mathbb{F}_p^s, u \neq v$, then the function $F(x, y_1, y_2, \cdots, y_s)$ from $\mathbb{F}_p^{n+s}$ to $\mathbb{F}_p$ defined by*

$$F(x, y_1, y_2, \cdots, y_s) = \sum_{u \in \mathbb{F}_p^s} \frac{(-1)^s \prod_{i=1}^s y_i(y_i - 1) \cdots (y_i - (p-1))}{(y_1 - u_1) \cdots (y_s - u_s)} f_u(x)$$

is bent.

Proof: For $a \in \mathbb{F}_p^n$, $b \in \mathbb{F}_p^s$, and putting $y = (y_1, \ldots, y_s)$, the Fourier transform $\widehat{F}$ of F at (a, b) is

$$\begin{aligned} \widehat{F}(a,b) &= \sum_{x \in \mathbb{F}_p^n, y \in \mathbb{F}_p^s} \epsilon_p^{F(x,y) - a \cdot x - b \cdot y} = \sum_{y \in \mathbb{F}_p^s} \epsilon_p^{-b \cdot y} \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{F(x,y) - a \cdot x} \\ &= \sum_{y \in \mathbb{F}_p^s} \epsilon_p^{-b \cdot y} \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f_y(x) - a \cdot x} = \sum_{y \in \mathbb{F}_p^s} \epsilon_p^{-b \cdot y} \widehat{f}_y(a). \end{aligned}$$

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

Given s-plateaued functions, there are various possible approaches to produce a set of s-plateaued functions with Fourier transforms with pairwise disjoint support. We suggest a simple one using the following lemma.

Lemma 1 *For some integers n and $s < n$, let $f : \mathbb{F}_p^{n-s} \to \mathbb{F}_p$ be a bent function and $u = (u_{n-s+1}, \ldots, u_n) \in \mathbb{F}_p^s$. Then the function in dimension n*

$$f_u(x_1 \ldots, x_n) = f(x_1, \ldots, x_{n-s}) + \sum_{i=n-s+1}^{n} u_i x_i$$

is s-plateaued with

$$supp(\widehat{f_u}) = \{(b_1, \ldots, b_{n-s}, u_{n-s+1}, \ldots, u_n) \mid b_i \in \mathbb{F}_p, 1 \leq i \leq n-s\}.$$

Proof: For $b = (b_1, \ldots, b_n)$

$$\begin{aligned}
\widehat{f_u}(b) &= \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f_u(x) - b \cdot x} \\
&= \sum_{x_{n-s+1}, \ldots, x_n \in \mathbb{F}_p} \epsilon_p^{\sum_{i=n-s+1}^{n} (u_i - b_i) x_i} \sum_{x_1, \ldots, x_{n-s} \in \mathbb{F}_p} \epsilon_p^{f(x_1, \ldots, x_{n-s}) - \sum_{i=1}^{n-s} b_i x_i}
\end{aligned}$$

Since f is a bent function in the variables $x_1, \ldots, x_{n-s}$, we have

$$\left| \sum_{x_1, \ldots, x_{n-s} \in \mathbb{F}_p} \epsilon_p^{f(x_1, \ldots, x_{n-s}) - \sum_{i=1}^{n-s} b_i x_i} \right| = p^{(n-s)/2}$$

and thus

$$|\widehat{f_u}(b)| = \begin{cases} p^{(n+s)/2} & \text{if } b_i = u_i,\ n-s+1 \leq i \leq n, \\ 0 & \text{else.} \end{cases}$$

□

As their Fourier spectrum is completely known we will apply Lemma 1 to quadratic functions $x_1^2 + \cdots + x_{n-s}^2$.

Corollary 1 *For $u \in \mathbb{F}_p^s$ let $d_u \in (\mathbb{F}_p^*)^{n-s}$. Then*

$$\left\{ d_u \cdot \begin{pmatrix} x_1^2 \\ \vdots \\ x_{n-s}^2 \end{pmatrix} + u \cdot \begin{pmatrix} x_{n-s+1} \\ \vdots \\ x_n \end{pmatrix}, u \in \mathbb{F}_p^s \right\}$$

is a set of s-plateaued functions with Fourier transforms having pairwise disjoint support.

We remark that this procedure of separating the supports of the Fourier transforms can be applied to any set of bent functions in $n-s$ variables which by Lemma 1 can be seen as a set of s-plateaued functions in n variables.

Example 1 For $p = 3$, $n = 2$, $s = 1$ we may choose $f_0(x) = x_1^2$, $f_1(x) = 2x_1^2 + x_2$, $f_2(x) = 2x_1^2 + 2x_2$. Writing x_3 for y, with Theorem 2 we obtain the bent function

$$F(\mathbf{x}) = x_1^2 x_3^2 + x_1^2 + x_2 x_3$$

in dimension 3 and algebraic degree 4.

4 Applications

Inequivalent bent functions

With the construction in Theorem 2, a large variety of inequivalent bent functions, weakly regular as well as non-weakly regular ones, can be obtained. As it is well known, EA-equivalent functions have always the same algebraic degree. By Theorem 1, EA-equivalence does not change the sign of the Fourier coefficients of bent functions in even dimension. If the dimension is odd, then an equivalence transformation either does not change the sign of any Fourier coefficient of a bent function, or the signs of all Fourier coefficients are altered. In particular a weakly regular bent function and a non-weakly regular bent function are never EA-equivalent. Using the construction in Theorem 2 we can design inequivalent bent functions of the same algebraic degree.

Example 2. Consider the 2-plateaued functions from $\mathbb{F}_3^4$ to $\mathbb{F}_3$

$$g_0(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2,\ g_1(x_1, x_2, x_3, x_4) = 2x_1^2 + x_2^2.$$

Choosing $f_{0j}(x_1, x_2, x_3, x_4) = g_0(x_1, x_2, x_3, x_4) + jx_4$ and $f_{ij}(x_1, x_2, x_3, x_4) = g_1(x_1, x_2, x_3, x_4) + ix_3 + jx_4$ for $i = 1, 2$ and $j = 0, 1, 2$, and applying the construction in Theorem 2, we get the bent function in dimension 6

$$F(x_1, x_2, x_3, x_4, y_1, y_2) = x_1^2 y_1^2 + x_1^2 + x_2^2 + x_3 y_1 + x_4 y_2.$$

Example 3. With the same 2-plateaued functions g_0 and g_1 from $\mathbb{F}_3^4$ to $\mathbb{F}_3$ as in Example 2, we choose $f_{00}(x_1, x_2, x_3, x_4) = g_0(x_1, x_2, x_3, x_4)$ and for $0 \leq i, j \leq 2$ and $(i, j) \neq (0, 0)$ we choose $f_{ij}(x_1, x_2, x_3, x_4) = g_1(x_1, x_2, x_3, x_4) + ix_3 + jx_4$. Then the construction in Theorem 2 yields the bent function

$$F(x_1, x_2, x_3, x_4, y_1, y_2) = 2x_1^2 y_1^2 y_2^2 + x_1^2 y_1^2 + x_1^2 y_2^2 + x_1^2 + x_2^2 + x_3 y_1 + x_4 y_2.$$

Let Δ be defined as in Proposition 1, then for g_0 we have $\Delta = 1$, a square, and for g_1 we have $\Delta = 2$, a nonsquare in $\mathbb{F}_3$. Therefore the functions in Examples 2 and 3 are non-weakly regular. In the construction of Example 2 the function g_0 is used 3 times, g_1 is used 6 times. From the description of the Fourier spectrum of a quadratic function given in Proposition 1 we conclude that $3 \cdot 3^4$ Fourier coefficients have negative sign, and $6 \cdot 3^4$ Fourier coefficients have positive sign. In fact the Fourier spectrum of the bent function in Example 2 is $\{-27^{63}, 27^{162}, (27\epsilon_3^2)^{162}, -27\epsilon_3^{90}, 27\epsilon_3^{162}, (-27\epsilon_3^2)^{90}\}$, where the integer in the exponent denotes the multiplicity of the corresponding Fourier coefficient. For constructing Example 3, g_0 is used only once, 8 times g_1 is used. Consequently 3^4 Fourier coefficients have negative sign, $8 \cdot 3^4$ have positive sign. In fact the Fourier spectrum of the bent function in Example 3 is $\{-27^9, 27^{216}, (27\epsilon_3^2)^{216}, -27\epsilon_3^{36}, 27\epsilon_3^{216}, (-27\epsilon_3^2)^{36}\}$. By Theorem 1 the two bent functions of algebraic degree 6 are inequivalent.

Bent functions and strongly regular graphs

In [2, 6, 11] it is shown that *partial difference sets* and *strongly regular graphs* can be obtained from some classes of p-ary bent functions:
Let n be an even integer and $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a bent function with the additional properties that

(a) f is weakly regular

(b) for a constant k with $\gcd(k-1, p-1) = 1$ we have for all $t \in \mathbb{F}_p$

$$f(tx) = t^k f(x).$$

Then the sets D_0, D_R, D_N defined by

$$\begin{aligned} D_0 &= \{x \in \mathbb{F}_p^n \mid f(x) = 0\}, D_N = \{x \in \mathbb{F}_p^n \mid f(x) \text{ is a nonsquare of } \mathbb{F}_p\}, \\ D_R &= \{x \in \mathbb{F}_p^n \mid f(x) \text{ is a nonzero square of } \mathbb{F}_p\} \end{aligned}$$

are partial difference sets of $\mathbb{F}_p^n$. Their Cayley graphs are strongly regular.

There are a few examples of bent functions known that satisfy the above conditions, some of them yielding new strongly regular graphs, see [11]. Also note that every p-ary quadratic function f which does not have a linear term satisfies $f(tx) = t^2 f(x)$ for all $t \in \mathbb{F}_p$. But in general, a bent function does not satisfy those conditions.

In the following we relate our construction of bent functions to the construction of strongly regular graphs. We present a general formula for a class

of bent functions which enable the construction of strongly regular graphs. As we will see, this class of bent functions is interesting from different point of views.

For each $j \in \{1, \cdots, s\}$, let σ_j represent the *elementary symmetric function*

$$\sigma_j(y_1, \cdots, y_s) := \sum_{1 \le i_1 < \cdots < i_j \le s} y_{i_1} \cdots y_{i_j}$$

with s indeterminates over $\mathbb{F}_p$. We define a function $G(y_1, \cdots, y_s)$ from $\mathbb{F}_p^s$ to $\mathbb{F}_p$ by

$$G(y_1, \cdots, y_s) = \sum_{j=1}^{s} (-1)^j \sigma_j(y_1^{p-1}, \cdots, y_s^{p-1}).$$

Lemma 2

$$G(y_1, \cdots, y_s) = \begin{cases} 0 & \text{if } (y_1, \cdots, y_s) = (0, \cdots, 0) \\ -1 & \text{otherwise.} \end{cases}$$

Proof: If $y_1, y_2, \cdots, y_s \neq 0$ then

$$G(y_1, \cdots, y_s) = (-1)^s \binom{s}{s} + (-1)^{s-1} \binom{s}{s-1} + (-1)^{s-2} \binom{s}{s-2} + \cdots + (-1) \binom{s}{1} = -1.$$

If some $y_{i_1}, \cdots, y_{i_r} = 0$ then $G(y_1, \cdots, y_s)$ will be reduced to the sum of $(p-1)$st powers elementary symmetric functions in $s - r$ variables and we will have

$$G(y_1, \cdots, y_s) = (-1)^{s-r} \binom{s-r}{s-r} + (-1)^{s-r-1} \binom{s-r}{s-r-1} + \cdots + (-1) \binom{s-r}{1} = -1.$$

□

Theorem 3 *Let g_0, g_1 be two distinct bent functions from $\mathbb{F}_p^{n-s}$ to $\mathbb{F}_p$ satisfying $g_i(tx_1, \ldots, tx_{n-s}) = t^2 g_i(x_1, \ldots, x_{n-s})$ for all $t \in \mathbb{F}_p$. We interpret g_0, g_1 as s-plateaued functions in n variables, and define a function F from $\mathbb{F}_p^n \times \mathbb{F}_p^s = \mathbb{F}_p^{n+s}$ to $\mathbb{F}_p$ by*

$$F(\mathbf{x}, y_1, \cdots, y_s) = G(y_1, \cdots, y_s)(g_0(\mathbf{x}) - g_1(\mathbf{x})) + x_{n-s+1} y_1 + \cdots + x_n y_s + g_0(\mathbf{x})$$

Then F is a bent function of degree $s(p-1) + d$, where d is the degree of $g_0 - g_1$, that satisfies $F(t\mathbf{x}, ty_1, \cdots, ty_s) = t^2 F(\mathbf{x}, y_1, \cdots, y_s)$ for all $t \in \mathbb{F}_p$.

Proof: For each nonzero vector $(y_1, \cdots, y_s) \in \mathbb{F}_p^s$, we define the function $f_{y_1,\cdots,y_s}(\mathbf{x}) = g_1(\mathbf{x}) + x_{n-s+1}y_1 + \cdots + x_n y_s$ from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. By Corollary 1 and the remarks thereafter $\{g_0, f_{y_1,\cdots,y_s} \mid (y_1, \cdots, y_s) \in \mathbb{F}_p^s \setminus \{(0, \ldots, 0)\}\}$ is a set of s-plateaued functions with Fourier transforms with pairwise disjoint support. Then

$$\widehat{F}(\mathbf{a}, b_1, \cdots, b_s) = \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{F(\mathbf{x}, y_1, \cdots, y_s) - \mathbf{a}.\mathbf{x} - b_1 y_1 - \cdots - b_s y_s}$$

$$= \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{g_0(x) - \mathbf{a}.\mathbf{x}} \sum_{(y_1,\cdots,y_s) \in \mathbb{F}_p^s} \epsilon_p^{(g_0(x) - g_1(x))G(y_1,\cdots,y_s) + (x_{n-s+1} - b_1)y_1 + \cdots + (x_n - b_s)y_s}$$

$$= \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{g_0(x) - \mathbf{a}.\mathbf{x}} \left(1 + \sum_{(y_1,\cdots,y_s) \in \mathbb{F}_p^s \setminus \{(0,\cdots,0)\}} \epsilon_p^{(g_1(x) - g_0(x)) + (x_{n-s+1} - b_1)y_1 + \cdots + (x_n - b_s)y_s} \right)$$

$$= \widehat{g_0}(\mathbf{a}) + \sum_{(y_1,\cdots,y_s) \in \mathbb{F}_p^s \setminus \{(0,\cdots,0)\}} \epsilon_p^{-b_1 y_1 - \cdots - b_s y_s} \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{g_1(x) + x_{n-s+1}y_1 + \cdots + x_n y_s - \mathbf{a}.\mathbf{x}}$$

$$= \widehat{g_0}(\mathbf{a}) + \sum_{(y_1,\cdots,y_s) \in \mathbb{F}_p^s \setminus \{(0,\cdots,0)\}} \epsilon_p^{-b_1 y_1 - \cdots - b_s y_s} \widehat{f_{y_1, y_2, \cdots, y_s}}(\mathbf{a})$$

□

Remark 3 *The bent function of Theorem 3 is obtained with the construction in Theorem 2 taking $f_{\mathbf{0}} = g_0$ and $f_{\mathbf{u}} = g_1$, $\mathbf{u} \neq \mathbf{0}$, and by separating the supports of the Fourier transforms similarly as in Corollary 1 for quadratic functions.*

Example 4. For the 1-plateaued quadratic functions $g_0, g_1 : \mathbb{F}_3^3 \to \mathbb{F}_3$ given by $g_0(x_1, x_2, x_3) = 2x_1^2 + x_2^2$ and $g_1(x_1, x_2, x_3) = x_1^2 + 2x_2^2$ with Theorem 3 (and putting $y = x_4$) we obtain the bent function of algebraic degree 4

$$F_1(x_1, x_2, x_3, x_4) = 2x_1 x_4^2 + x_2^2 x_4^2 + x_3 x_4 + 2x_1^2 + x_2^2.$$

Example 5. Applying Theorem 3 to the 2-plateaued quadratic functions $g_0(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2$, $g_1(x_1, x_2, x_3, x_4) = 4x_1^2 + x_2^2$ from $\mathbb{F}_5^4$ to $\mathbb{F}_5$, yields the bent function of algebraic degree 6

$$F_2(x_1, x_2, x_3, x_4, x_5, x_6) = 2x_1^2 x_5^4 x_6^4 + 3x_1^2 x_5^4 + 3x_1^2 x_6^4 + x_3 x_5 + x_4 x_6 + x_1^2 + x_2^2.$$

The functions in Examples 2 and 3 are all in even dimension and satisfy the conditions (a),(b), therefore correspond to strongly regular graphs. According to the signs of the Fourier coefficients, the graph corresponding to F_1 is of negative Latin square type, and the graph corresponding to F_2 is of Latin square type (see [11]).

Examples of bent functions with maximal degree

A p-ary bent function f in dimension n can have algebraic degree at most $(p-1)n/2+1$, see Hou [8]. The bent function f must then be non-weakly regular. In a first approach, in [4] the construction described in Theorem 2 is used with maximal possible $s = n-1$ to show the existence of ternary bent functions in odd dimension attaining the Hou's upper bound on the algebraic degree. Constructions of such functions from $\mathbb{F}_{3^n} \times \mathbb{F}_3^s$ to $\mathbb{F}_3$ are described. We here present some simple explicit expressions for such bent functions.

We first use Theorem 3 to obtain a closed formula for arbitrary odd dimension. The functions $g_0(\mathbf{x}) = x_1^2$, $g_1(\mathbf{x}) = 2x_1^2$ from $\mathbb{F}_3^n$ to $\mathbb{F}_3$ are $(n-1)$-plateaued. Applying Theorem 3 to these functions yields a ternary bent function in dimension $n+s$ and algebraic degree $2n$. As obvious this function attains Hou's bound on the algebraic degree, and we have the following corollary.

Corollary 2 *For an arbitrary integer n let $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_{n-1})$. The function F from $\mathbb{F}_3^n \times \mathbb{F}_3^s = \mathbb{F}_3^{n+s}$ to $\mathbb{F}_3$*

$$F(\mathbf{x}, \mathbf{y}) = 2x_1^2 G(y_1, \ldots, y_{n-1}) + x_1^2 + x_2 y_1 + \cdots + x_n y_{n-1} \tag{7}$$

is a bent function with maximal possible algebraic degree.

Example 6. For $n = 2$ the ternary function (7) of maximal possible algebraic degree 4 is the function in Example 1

$$F(\mathbf{x}) = x_1^2 x_3^2 + x_1^2 + x_2 x_3,$$

for $n = 3$, function (7) is the ternary function

$$F(x_1, x_2, x_3, y_1, y_2) = 2x_1^2 y_1^2 y_2^2 + x_1^2 y_1^2 + x_1^2 y_2^2 + x_2 y_1 + x_3 y_2 + x_1^2$$

of algebraic degree 6.

Corollary 2 gives one explicit formula for a ternary bent function with maximal algebraic degree in arbitrary odd dimension. A large number of ternary bent functions with maximal degree can be obtained using sets of s-plateaued functions described as in Corollary 1 with $s = n-1$.

Example 7. Using the notation of Corollary 1 for $n = 3$ thus $s = 2$ we may choose $d_{00} = d_{02} = d_{20} = d_{11} = d_{22} = 1$ and $d_{01} = d_{10} = d_{12} = d_{21} = 2$. Applying the construction of Theorem 2, yields the ternary bent function

$$\begin{aligned} F(x_1, x_2, x_3, y_1, y_2) \;=\; & x_1^2 y_1^2 y_2^2 + x_1^2 y_1^2 y_2 + 2x_1^2 y_1^2 + x_1^2 y_1 y_2^2 + x_1^2 y_1 y_2 + \\ & 2x_1^2 y_1 + 2x_1^2 y_2^2 + 2x_1^2 y_2 + x_1^2 + x_2 y_1 + x_3 y_2 \end{aligned}$$

of degree 6.

By Remark 3 the bent function in dimension 5 in Example 6 is obtained by choosing $d_{00} = 1$ and $d_{\mathbf{u}} = 2$ for $\mathbf{u} \neq 00$. By Proposition 1 the proportion of Fourier coefficients with positive sign is smaller than for the function in Example 7. Consequently these two functions of maximal algebraic degree are inequivalent.

Remark 4 *One may hope that this construction of ternary bent functions of maximal degree can be generalized to the case $p > 3$. One may start with bent functions from $\mathbb{F}_p$ to $\mathbb{F}_p$, i.e. in dimension 1, with algebraic degree $(p+1)/2$, interpret this functions as $(n-1)$-plateaued functions in dimension n and proceed as above for the case $p = 3$ to construct a bent function of maximal degree $(p-1)(2n-1)/2+1$ in dimension $2n-1$. But by [8, Theorem 4.6] bent functions from $\mathbb{F}_p$ to $\mathbb{F}_p$ are always quadratic. Consequently this procedure is only applicable for $p = 3$.*

References

[1] C. Carlet, H. Dobbertin, G. Leander, Normal extensions of bent functions. IEEE Trans. Inform. Theory 50 (2004), 2880–2885.

[2] Y.M. Chee, Y. Tan, X.D. Zhang, Strongly regular graphs constructed from p-ary bent functions, preprint 2010.

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

[4] A. Çeşmelioğlu, W. Meidl, Bent functions of maximal degree, preprint 2010.

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

[6] T. Feng, B. Wen, Q. Xiang, J. Yin, Partial difference sets from p-ary weakly regular bent functions and quadratic forms, preprint 2010.

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

[8] 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.

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

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

[11] Y. Tan, A. Pott, T. Feng, Strongly regular graphs associated with ternary bent functions. Journal of Combinatorial Theory, Series A 117 (2010), 668–682.

[12] 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.