A construction of bent functions from plateaued functions

Ayca Cesmelioglu, Wilfried Meidl

A construction of bent functions from plateaued functions

Ayça Çeşmelioğlu and Wilfried Meidl

Sabancı University, MDBF, Orhanlı, 34956 Tuzla, İstanbul, Turkey
cesmelioglu@sabanciuniv.edu, wmeidl@sabanciuniv.edu

Abstract. In this presentation a technique for constructing bent functions from plateaued functions is introduced. This generalizes earlier techniques for constructing bent from near-bent functions. Analysing the Fourier spectrum of quadratic functions we then can construct weakly regular as well as non-weakly regular bent functions both in even and odd dimension. This type of functions yield the first known infinite classes of non-weakly regular bent functions. Weakly regular bent functions with certain additional properties can be used to construct partial difference sets and strongly regular graphs. We show how to obtain appropriate bent functions using our construction.

Keywords: Bent functions, weakly regular bent, non-weakly regular bent, quadratic functions, plateaued functions.

1 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 $b \in V_n$.

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. [6])

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

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

A p-ary bent function f is called *regular* if for all $b \in V_n$

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

As easily seen from (1), a p-ary regular bent function can only exist for even n and for odd n when $p \equiv 1 \bmod 4$.

A p-ary 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. By (1), ζ can only be ± 1 or $\pm i$. Note that regular implies weakly regular.

A function f from V_n to $\mathbb{F}_p$ is called plateaued if $|\widehat{f}(b)|^2 = A$ or 0 for all $b \in V_n$. By *Parseval's identity* we obtain that $A = p^{n+s}$ for an integer s with $0 \leq s \leq n$. 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. For 1-plateaued functions the term *near-bent* function is common (see [3, 7]), binary 1-plateaued and 2-plateaued functions are referred to as *semi-bent* functions in [4].

We present a technique for constructing bent functions from plateaued functions which generalizes earlier constructions of bent functions from near-bent functions. Employing quadratic plateaued functions, families of bent functions with interesting properties are obtained. Using plateaued instead of only quadratic near-bent functions, we can obtain bent functions of various algebraic degree. With our construction, we obtain the first known infinite classes of non-weakly regular bent functions in odd dimension. Using direct sums of bent functions we also can construct non-weakly regular bent functions in even dimension.
Weakly regular bent functions with certain additional properties can be used to construct strongly regular graphs. With our construction, we can obtain various classes of bent functions in any characteristic that can be used to construct strongly regular graphs (of Latin square and of negative Latin square type). Until now, only a few such bent functions were known, though already yielding new strongly regular graphs, [9].

2 Quadratic functions

If we associate V_n with the finite field $\mathbb{F}_{p^n}$, we use the inner product $\langle x, y\rangle = \mathrm{Tr_n}(xy)$, where $\mathrm{Tr_n}(z)$ denotes the absolute trace of $z \in \mathbb{F}_{p^n}$. The Fourier transform of a function f from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is then the complex valued function on $\mathbb{F}_{p^n}$ given by

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

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

$$f(x) = \mathrm{Tr_n}\left(\sum_{i=0}^{l} a_i x^{p^i+1}\right) \tag{2}$$

is called *quadratic*, its algebraic degree is two, see [4, 6]. Every quadratic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is s-plateaued, where s is the dimension of the kernel of the linear transformation on $\mathbb{F}_{p^n}$ defined by

$$L(x) = \sum_{i=0}^{l} \left(a_i^{p^l} x^{p^{l+i}} + a_i^{p^{l-i}} x^{p^{l-i}} \right). \tag{3}$$

Choosing and fixing a basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, we correspond $x = \sum_{i=1}^{n} x_i \alpha_i$ to the vector $\mathbf{x} = (x_1, \ldots, x_n)$. Then we can associate a quadratic function $f(x) = \mathrm{Tr_n}(\sum_{i=0}^{l} a_i x^{p^i+1})$ with a quadratic form

$$f(\mathbf{x}) = \mathbf{x}^T A \mathbf{x},$$

where $\mathbf{x}^T$ denotes the transpose to the vector $\mathbf{x}$, and the matrix A has entries in $\mathbb{F}_p$. Any quadratic form is equivalent to a diagonal quadratic form, i.e. $D = C^T AC$ for a nonsingular matrix C over $\mathbb{F}_p$ and a diagonal matrix $D = diag(d_1, \ldots, d_n)$.

The following proposition is obtained by generalizing the related result in [6], which corresponds to the case that $f(x)$ is nondegenerate, using [8, Theorem 6.27, Theorem 5.15] if $n - s$ odd and [8, Theorem 6.26] if $n - s$ is even.

Proposition 1. *Let f be an s-plateaued quadratic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ and $f(\mathbf{x}) = \mathbf{x}^T A \mathbf{x}$ be the associated quadratic form. Then a corresponding diagonal matrix D has $n - s$ (not necessarily distinct) nonzero entries $d_1, \ldots, d_{n-s}$, and the Fourier spectrum of f is given by*

$$\begin{aligned}
\left\{0, \eta(\Delta) p^{\frac{n+s}{2}} \epsilon_p^{J(b)}\right\} &: p \equiv 1 \bmod 4, \\
\left\{0, (-1)^{\frac{n-s-1}{2}} \eta(\Delta) i p^{\frac{n+s}{2}} \epsilon_p^{J(b)}\right\} &: p \equiv 3 \bmod 4 \text{ and } n-s \text{ odd}, \\
\left\{0, (-1)^{\frac{n-s}{2}} \eta(\Delta) p^{\frac{n+s}{2}} \epsilon_p^{J(b)}\right\} &: p \equiv 3 \bmod 4 \text{ and } n-s \text{ even},
\end{aligned}$$

where $J(x)$ is a function from the support $supp(\widehat{f}) := \{b \in \mathbb{F}_{p^n} \mid \widehat{f}(b) \neq 0\}$ of $\widehat{f}$ to $\mathbb{F}_p$, $\Delta = \prod_{i=1}^{n-s} d_i$, and η denotes the quadratic character in $\mathbb{F}_p$.

3 Construction of bent from plateaued functions

Theorem 1. *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.

Sketch of the proof
The Fourier transform $\widehat{F}$ of F at $(\alpha, \mathbf{a}) \in \mathbb{F}_{p^n} \times \mathbb{F}_p^s$ is

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

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 $\left|\widehat{F}(\alpha, \mathbf{a})\right| = |\epsilon_p^{-\mathbf{a} \cdot \mathbf{y}} \widehat{f_{\mathbf{y}}}(\alpha)| = p^{\frac{n+s}{2}}$. □

The following theorem shows how to construct a set of s-plateaued functions such that the supports of the Fourier transforms are pairwise disjoint.

Theorem 2. *For each $\mathbf{a} = (a_1, \cdots, a_s) \in \mathbb{F}_p^s$, let $g_{\mathbf{a}}$ be a quadratic s-plateaued function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ and $L_{\mathbf{a}}$ be the corresponding linearized polynomial. For all $\mathbf{a} \in \mathbb{F}_p^s$, if $L_{\mathbf{a}}$ has the same kernel in $\mathbb{F}_{p^n}$ with basis $\{\beta_1, \cdots, \beta_s\}$ and $\gamma_{\mathbf{a}} \in \mathbb{F}_{p^n}$ is such that*

$$g_{\mathbf{a}}(\beta_j) + \mathrm{Tr_n}(\gamma_{\mathbf{a}} \beta_j) = g_{\mathbf{0}}(\beta_j) + a_j, \tag{4}$$

for all $j = 1, \cdots, s$, then 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

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

□

Remark 1. By the linear independence of $\beta_1, \ldots, \beta_s$, the existence of $\gamma_{\mathbf{a}}$ satisfying equation (4) for all $j = 1, \ldots, s$, is guaranteed. In fact, if $\{\delta_1, \delta_2, \ldots, \delta_n\}$ and $\{\rho_1, \rho_2, \ldots, \rho_n\}$ are dual bases of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, and $\beta_j = b_{j1}\delta_1 + b_{j2}\delta_2 + \cdots + b_{jn}\delta_n$, then the coefficients x_i of $\gamma_{\mathbf{a}} = x_1\rho_1 + x_2\rho_2 + \cdots + x_n\rho_n$ satisfy

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

A value for $\gamma_{\mathbf{a}}$ is then obtained with 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 $c_j = g_{\mathbf{0}}(\beta_j) + a_j - g_{\mathbf{a}}(\beta_j)$, $j = 1, 2, \ldots, s$.

We can consequently construct bent functions starting with any quadratic function f. In a first step we determine the value of s for the function f. Then we can

choose p^s constants in $\mathbb{F}_p^*$ and the linearized polynomials have the same kernel in $\mathbb{F}_{p^n}$ for all of the form cf, $c \in \mathbb{F}_p^*$, hence we can apply Theorem 2 and Theorem 1. For some simple quadratic functions we know the value s in advance:

I: 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 $\nu(s) = \nu(r)+1$, where ν denotes the 2-adic valuation on integers. The appropriate elements $a \in \mathbb{F}_{p^n}^*$ can be determined and for the remaining a, $f(x)$ is bent.

II: Binomials. Let $c \in \mathbb{F}_p^*$, then the function $f(x) = \mathrm{Tr_n}\left(cx^{p^r+1} - cx^{p^t+1}\right)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is near-bent if and only if $\gcd(n, r+t) = \gcd(n, r-t) = \gcd(n, p) = 1$. The kernel of the corresponding linearized polynomial is $\mathbb{F}_p$. Moreover if n is odd, then Δ defined as in Proposition 1 is independent of the choice of r, t satisfying the above condition. Hence the Fourier spectrum is independent of the choice of r, t.

For $c \in \mathbb{F}_p^*$ the function $f = \mathrm{Tr_n}\left(cx^{p^r+1} + cx^{p^t+1}\right)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is near-bent if and only if $\gcd(n, 2(r+t)) = \gcd(n, 2(r-t)) = 2$, $r-t$ is odd, and $\gcd(n, p) = 1$. The kernel of the corresponding linearized polynomial consists of the solutions of $x^p + x$.

4 Non-weakly regular bent functions, weakly regular bent functions and strongly regular graphs

All classical examples of bent functions are weakly regular. However, in general, weak regularity is not easy to prove. With the subsequent corollaries of Proposition 1 and our construction presented in Section 3 we can design weakly regular and non-weakly regular bent functions. This also yields the first infinite classes of non-weakly regular bent functions.

In order to construct non-weakly regular bent functions, we need to change the signs of the Fourier coefficients of the s-plateaued functions. Proposition 1 suggests that if $n - s$ is odd, we can change signs by multiplying the functions with nonsquare elements of $\mathbb{F}_p$. If $n - s$ is even, we only obtain weakly regular bent functions for any choice of the coefficients. The following two corollaries can be seen as results of Proposition 1 and Theorem 1, 2. For the Corollaries 1,2 we fix the following notation: For integers n, s

- $\mathcal{G} = \{g_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{F}_p^s\}$ is a set of p^s quadratic s-plateaued functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ such that the corresponding linearized polynomials $L_{\mathbf{a}}$ have all the same kernel in $\mathbb{F}_{p^n}$;
- $\mathcal{C} = \{c_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{F}_p^s\}$ is a set of p^s nonzero elements of $\mathbb{F}_p$;
- $\{\gamma_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{F}_p^s\}$ is a set of elements of $\mathbb{F}_{p^n}$ such that the set $\mathcal{F} = \{f_{\mathbf{a}} \mid \mathbf{a} \in \mathbb{F}_p^s\}$ of p^s quadratic s-plateaued functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ defined by $f_{\mathbf{a}}(x) = c_{\mathbf{a}} g_{\mathbf{a}}(x) + \mathrm{Tr_n}(\gamma_{\mathbf{a}} x)$ satisfies $supp(\widehat{f_{\mathbf{a}}}) \cap supp(\widehat{f_{\mathbf{b}}}) = \emptyset$ for $\mathbf{a}, \mathbf{b} \in \mathbb{F}_p^s, \mathbf{a} \neq \mathbf{b}$.

Corollary 1. *Let F be the bent function in dimension $n+s$ given as in Theorem 1 constructed with the set $\mathcal{F}$. If $n - s$ is odd, then F is weakly regular for ($p -$*

$1)^{p^s}/2^{p^s-1}$ *choices for* $\mathcal{C}$*, and non-weakly regular for the remaining* $(2^{p^s-1}-1)(p-1)^{p^s}/2^{p^s-1}$ *choices for* $\mathcal{C}$*.*

Corollary 2. *Let* $g_{\mathbf{a}} = g$ *for all* $\mathbf{a} \in \mathbb{F}_p^s$ *and let* F *be the bent function in dimension* $n+s$ *given as in Theorem 1 constructed with the set* $\mathcal{F}$*. If* $n-s$ *is even, then* F *is weakly regular. If* $n-s$ *is odd, then* F *is weakly regular if and only if all elements of* $\mathcal{C}$ *have the same quadratic character in* $\mathbb{F}_p$*.*

Remark 2. Versions of the above corollaries for the special case that $s = 1$ were used in our work [3] to present the first infinite classes of non-weakly regular bent functions. These bent functions are in odd dimension, their algebraic degree is $p+1$. With $s > 1$ non-weakly regular bent functions of higher degree can be constructed.

We now present the first construction of non-weakly regular bent functions in even dimension.
Let the vector space V_{m+n} of dimension $m+n$ over $\mathbb{F}_p$ be the direct sum of the vector spaces V_m and V_n of dimension m and n, respectively, and let f_1 be a p-ary function on V_m and f_2 be a p-ary function on V_n. Then the direct sum $f_1 \oplus f_2$ of f_1 and f_2 is defined as the p-ary function on $V_{m+n} = V_m \oplus V_n$ given by $(f_1 \oplus f_2)(x_1 + x_2) = f_1(x_1) + f_2(x_2)$.
As pointed out in [1], we have $\widehat{f_1 \oplus f_2} = \widehat{f_1}\widehat{f_2}$, thus $f_1 \oplus f_2$ is bent if f_1 and f_2 are bent. In particular if exactly one f_1 or f_2 is non-weakly regular, then $f_1 \oplus f_2$ is non-weakly regular. The latter argument was recently used in [10] to give a recursive approach to construct non-weakly regular bent functions - once a non-weakly regular bent function is obtained. Taking for f_1 a non-weakly regular bent function in odd dimension (Corollaries 1,2) and for f_2 a weakly regular bent function in odd dimension (e.g. quadratic bent function, Corollaries 1,2), then $f_1 \oplus f_2$ is non-weakly regular in even dimension.

Examples

Example 1. 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 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 ternary function

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

is a weakly regular bent function on $\mathbb{F}_{3^4}\times\mathbb{F}_3\times\mathbb{F}_3$ of algebraic degree 6.

Example 2. Let $p=3, n=8$. The quadratic binomials $g_0(x)=\mathrm{Tr}_8(x^{10}+x^4)$ and $g_1(x)=\mathrm{Tr}_8(x^{3^6+1}+x^{3^5+1})$ on $\mathbb{F}_{3^8}$ are near bent. The kernel of the corresponding linearized polynomial consists of the solutions of x^3+x. Let $\beta\in\mathbb{F}_{3^2}$ be a root of the polynomial $x^2+1\in\mathbb{F}_3[x]$. Then, the function

$$f_1(x,y) = 2y^2\mathrm{Tr}_8(x^{3^5+1}+2x^4+x)+y\mathrm{Tr}_8(x^{3^5+1}+2x^4+\beta x)+\mathrm{Tr}_8(x^{10}+x^4+x)$$

from $\mathbb{F}_{3^8}\times\mathbb{F}_3$ to $\mathbb{F}_3$ is a weakly regular bent function of algebraic degree 4.

Example 3. With $g_0(x), g_1(x)$ in Example 2 and using different coefficients, we obtain the function

$$\begin{aligned} f_2(u,w) = 2w^2\mathrm{Tr}_8(v^{3^6+1}+2v^{3^5+1}+v)+w\mathrm{Tr}_8(v^{3^6+1}+v^{3^5+1}+v^{10}+v^4+\beta v)\\ +\mathrm{Tr}_8(v^{10}+v^4+v)\end{aligned}$$

from $\mathbb{F}_{3^8}\times\mathbb{F}_3$ to $\mathbb{F}_3$ which is a non-weakly regular bent function of algebraic degree 4 in odd dimension 9.

Example 4. The direct sum of f_1, f_2 is the ternary function

$$H(x,y,v,w) = f_1(x,y)+f_2(v,w)$$

on $(\mathbb{F}_{3^8}\times\mathbb{F}_3)\times(\mathbb{F}_{3^8}\times\mathbb{F}_3)$ which is a non-weakly regular bent function of algebraic degree 4 in even dimension 18.

Example 5. The direct sum of the weakly regular bent function $F(x,y,z)$ in Example 1 and the non-weakly regular bent function $f_2(v,w)$ of Example 3 is the ternary function

$$\begin{aligned} F(x,y,z)+f_2(v,w) = &\sum_{\mathbf{a}=(a_1,a_2)\in\mathbb{F}_3\times\mathbb{F}_3} \frac{yz(y-1)(z-1)(y-2)(z-2)}{(y-a_1)(z-a_2)} f_{\mathbf{a}}(x)\\ &+2w^2\mathrm{Tr}_8(v^{3^6+1}+2v^{3^5+1}+v)+w\mathrm{Tr}_8(v^{3^6+1}+v^{3^5+1}+v^{10}+v^4+\beta v)\\ &+\mathrm{Tr}_8(v^{10}+v^4+v)\end{aligned}$$

on $(\mathbb{F}_{3^4}\times\mathbb{F}_3\times\mathbb{F}_3)\times(\mathbb{F}_{3^8}\times\mathbb{F}_3)$ which is a non-weakly regular bent function of algebraic degree 6.

In [2, 5, 9] 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

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

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

Some of the classical bent functions (e.g. quadratic and Coulter-Matthews) satisfy condition (b). In fact, using Coulter-Matthews functions, some new strongly regular graphs have been discovered in [9]. But in general, condition (b) is not satisfied. With an appropriate choice of near bent functions, the construction of Theorem 1 yields bent functions satisfying (b):

Theorem 3. *Let g_0, g_1 be distinct quadratic near-bent functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ such that the corresponding linearized polynomials L_0, L_1 have the same (1-dimensional) kernel with basis $\{\beta\}$, and suppose that $g_0(\beta) = g_1(\beta) = 0$. Let $\gamma \in \mathbb{F}_{p^n}$ such that $\mathrm{Tr_n}(\gamma\beta) \neq 0$. Then the function*

$$F(x, y) = y^{p-1}(g_1(x) - g_0(x)) + y\mathrm{Tr_n}(\gamma x) + g_0(x)$$

is a bent function of degree $p+1$ that satisfies $F(tx, ty) = t^2 F(x, y)$ for all $t \in \mathbb{F}_p$.

Examples

In the following part, we construct examples of weakly regular bent functions in even dimension satisfying (b).

Example 6. $p = 3, n = 7$: Let $g_0(x) = \mathrm{Tr}_7(x^{10} - x^4), g_1(x) = \mathrm{Tr}_7(x^{82} - x^{28})$. Using Theorem 3, we construct the bent function

$$F(x, y) = y^2\mathrm{Tr}_7(x^{82} - 2x^{10} + x^4) + y\mathrm{Tr}_7(x) + \mathrm{Tr}_7(x^{10} - x^4)$$

in dimension 8 and of algebraic degree 4 on $\mathbb{F}_{3^7} \times \mathbb{F}_3$. The normalized Fourier spectrum of $F(x, y)$ with multiplicities is $(-1)^{2133}, (-\epsilon_3)^{2214}, (-\epsilon_3^2)^{2214}$ where ϵ_3 is a complex primitive third root of unity.

Example 7. $p = 3, n = 8$: $g_0(x) = \mathrm{Tr}_8(x^{3^6+1} + x^{3^5+1}), g_1(x) = \mathrm{Tr}_8(x^{10} + x^4)$. By using Theorem 3, we construct the ternary bent function

$$F(x, y) = y^2\mathrm{Tr}_8(x^{3^6+1} + x^{3^5+1} + 2x^{10} + 2x^4) + y\mathrm{Tr}_8(\gamma x) + \mathrm{Tr}_8(x^{10} + x^4)$$

of degree 4 in odd dimension 9. The quadratic monomial $f(x) = \mathrm{Tr}_5(x^{10})$ on $\mathbb{F}_{3^5}$ is weakly regular bent and if we form the direct sum of $F(x, y)$ with $f(x)$, the resulting ternary function on $\mathbb{F}_{3^8} \times \mathbb{F}_3 \times \mathbb{F}_{3^5}$ will be regular bent i.e. the normalized Fourier spectrum will be $\{1, \epsilon_3, \epsilon_3^2\}$. We remark that this direct sum preserves (b). We further remark that using $2g_0(x), 2g_1(x)$ instead of $g_0(x), g_1(x)$, changes the sign in the Fourier spectrum. The resulting strongly regular graph will then be of negative latin square type, see [9].

Example 8. $p = 5$ and $n = 7$: $g_0(x) = \mathrm{Tr}_7(x^{5^4+1}-x^2)$, $g_1(x) = \mathrm{Tr}_7(x^{5^3+1}-x^{5+1})$ be two functions from $\mathbb{F}_{5^7}$ to $\mathbb{F}_5$. Then we construct the following bent function of degree 6 on $\mathbb{F}_{5^7} \times \mathbb{F}_5$:

$$F(x,y) = y^4\mathrm{Tr}_7(x^{5^4+1} - x^{5^3+1} + x^{5+1} - x^2) + y\mathrm{Tr}_7(x) + \mathrm{Tr}_7(x^{5^4+1} - x^2).$$

Example 9. $p = 5, n = 4$: $g_0(x) = \mathrm{Tr}_4(x^{5^3+1} + x^{5^2+1})$, $g_1(x) = \mathrm{Tr}_4(4x^{5^3+1} + 4x^{5^2+1})$. We construct the following bent function on $\mathbb{F}_{5^4} \times \mathbb{F}_5$:

$$F(x,y) = y^4\mathrm{Tr}_4(3x^{5^3+1} + 3x^{5^2+1}) + y\mathrm{Tr}_4(\beta x) + \mathrm{Tr}_4(x^{5^3+1} + x^{5^2+1}).$$

The quadratic monomial $f(z) = \mathrm{Tr}_5(z^{26})$ is a bent function on $\mathbb{F}_{5^5}$ and by taking the direct sum, we obtain

$$\begin{aligned} G(x,y,z) &= F(x,y) + g(z) \\ &= y^4\mathrm{Tr}_4(3x^{5^3+1} + 3x^{5^2+1}) + y\mathrm{Tr}_4(\beta x) + \mathrm{Tr}_4(x^{5^3+1} + x^{5^2+1}) \\ &\quad + \mathrm{Tr}_5(z^{26}), \end{aligned}$$

which is a bent function of degree 6 defined on $(\mathbb{F}_{5^4} \times \mathbb{F}_5) \times \mathbb{F}_{5^5}$.

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. P. Charpin, E. Pasalic, C. Tavernier, On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inform. Theory 51 (2005), 4286–4298.
5. T. Feng, B. Wen, Q. Xiang, J. Yin, Partial difference sets from p-ary weakly regular bent functions and quadratic forms, preprint 2010.
6. T. Helleseth, A. Kholosha, Monomial and quadratic bent functions over the finite field of odd characteristic. IEEE Trans. Inform. Theory 52 (2006), 2018–2032.
7. G. Leander, G. McGuire, Construction of bent functions from near-bent functions. Journal of Combinatorial Theory, Series A 116 (2009), 960–970.
8. R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.
9. Y. Tan, A. Pott, T. Feng, Strongly regular graphs associated with ternary bent functions. Journal of Combinatorial Theory, Series A 117 (2010), 668–682.
10. 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.