Journal of Combinatorial Theory, Series A 119 (2012) 420–429

Contents lists available at SciVerse ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

A construction of weakly and non-weakly regular bent functions

Ayça Çeşmelioğlu [a], Gary McGuire [b,1], Wilfried Meidl [a]

[a] Sabancı University, MDBF, Orhanlı, 34956 Tuzla, İstanbul, Turkey
[b] School of Mathematical Sciences, University College Dublin, Ireland

ARTICLE INFO

Article history:
Received 13 October 2010
Available online 14 October 2011

Keywords:
Bent function
Near-bent function
Semi-bent function
Weakly regular
Non-weakly regular
Fourier transform

ABSTRACT

In this article a technique for constructing p-ary bent functions from near-bent functions is presented. This technique is then used to obtain both weakly regular and non-weakly regular bent functions. In particular we present the first known infinite class of non-weakly regular bent functions.

1. Introduction

Let p be a prime, and let V_n be any n-dimensional vector space over $\mathbb{F}_p$. For a function f from V_n to $\mathbb{F}_p$ the *Fourier transform* (*or Walsh transform*) of f is the complex-valued function $\widehat{f}$ on V_n given by

$$\widehat{f}(b) = \sum_{x \in V_n} \epsilon_p^{f(x) - \langle b, x \rangle} \tag{1.1}$$

where $\epsilon_p = e^{2\pi i/p}$ and $\langle , \rangle$ denotes any inner product on V_n. The *Fourier spectrum* of f is the multiset $\mathrm{spec}(f) = \{\widehat{f}(b) \mid b \in V_n\}$.

Definition 1.1. A function $f : V_n \to \mathbb{F}_p$ is called bent if $|\widehat{f}(b)|^2 = p^n$ for all $b \in V_n$.

E-mail address: cesmelioglu@sabanciuniv.edu (A. Çeşmelioğlu).

[1] Research supported by the Claude Shannon Institute, Science Foundation Ireland, Grant 06/MI/006.

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2011.10.002

Alternatively, a function f from V_n to $\mathbb{F}_p$ is bent if and only if for all nonzero $a \in V_n$, the derivative function $D_a f(x) = f(x+a) - f(x)$ is balanced. If $p = 2$ then $\epsilon_p = -1$ and $\widehat{f}(b)$ is an integer, so a necessary condition for the existence of a bent function is that n is even. This does not hold for odd p, where bent functions can exist for both odd and even n. When p is odd, bent functions are sometimes called p-ary bent functions.

As all vector spaces of dimension n over $\mathbb{F}_p$ are isomorphic, we may associate V_n with $\mathbb{F}_p^n$ or with the finite field $\mathbb{F}_{p^n}$. In the first case we use as inner product the conventional dot product, in the second 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 (1.1) is then adapted accordingly.

Often one considers the *normalized* Fourier coefficient $p^{-n/2}\widehat{f}(b)$ of a bent function. For any p, we can only say a priori that the normalized Fourier coefficients lie on the unit circle. For $p = 2$, a bent function must therefore have normalized Fourier coefficients ± 1, because the Fourier coefficients are integers. For odd p, there exists a function $f^* : V_n \to \mathbb{F}_p$ such that (cf. [4], [7, Property 8])

$$p^{-n/2}\widehat{f}(b) = \begin{cases} \pm\epsilon_p^{f^*(b)} & \text{if } n \text{ is even or } n \text{ is odd and } p \equiv 1 \bmod 4, \\ \pm i\epsilon_p^{f^*(b)} & \text{if } n \text{ is odd and } p \equiv 3 \bmod 4. \end{cases} \tag{1.2}$$

Definition 1.2. Let f be a bent function from V_n to $\mathbb{F}_p$. Then f is called regular if, for all $b \in V_n$, we have $p^{-n/2}\widehat{f}(b) = \epsilon_p^{f^*(b)}$ for a function $f^* : V_n \to \mathbb{F}_p$, i.e., the normalized Fourier coefficients of f form a subset, in fact the full set, of the p-th roots of unity. The bent function f is called weakly regular if every quotient of two Fourier coefficients is a p-th root of unity. Otherwise f is called non-weakly regular.

It is obvious from (1.2) that regular bent functions can only exist for even n and for odd n with $p \equiv 1 \bmod 4$. For example, when $p = 3$, regular bent functions can only exist in even dimensions. The normalized Fourier coefficients are then $\epsilon_3^{f^*(b)}$ for every $b \in V_n$ and a function $f^* : V_n \to \mathbb{F}_3$. A ternary weakly regular bent function (which is not regular) has normalized Fourier coefficients $-\epsilon_3^{f^*(b)}$ if n is even. If n is odd, then the normalized Fourier coefficients of a ternary weakly regular bent function are all of the form $i\epsilon_3^{f^*(b)}$, or all are of the form $-i\epsilon_3^{f^*(b)}$. In contrast, ternary non-weakly regular bent functions would have normalized Fourier coefficients $\epsilon_3^{f^*(b)}$ *and* $-\epsilon_3^{f^*(b)}$ when n is even, and $i\epsilon_3^{f^*(b)}$ *and* $-i\epsilon_3^{f^*(b)}$ if n is odd.

Almost all known p-ary bent functions are weakly regular. Until this paper, there are just a few sporadic examples of non-weakly regular bent functions known (see [4,5]).

Two functions f, g from V_n to $\mathbb{F}_p$ are called *extended affine equivalent* (EA-equivalent) if $g(x) = af(L(x) + u) + \langle v, x\rangle + c$ for some elements $a, c \in \mathbb{F}_p$, $u, v \in V_n$ and a linear permutation $L(x)$ of V_n (which corresponds to a coordinate transformation). It is well known that the absolute values in the Fourier spectrum are preserved by EA-equivalence. In particular if for $f : V_n \to \mathbb{F}_q$ we define $f_v(x) = f(x) + \langle v, x\rangle$ then $\widehat{(f_v + c)}(b) = \epsilon_p^c \widehat{f}(b - v)$. In the framework of the vector space $\mathbb{F}_p^n$ we have $L(x) = Ax$ for an invertible $n \times n$-matrix A over $\mathbb{F}_p$. Then $\widehat{f(Ax)}(b) = \widehat{f}((A^{-1})^T b)$, where A^T denotes the transpose of the matrix A.

For the binary case, where bent functions in odd dimension do not exist, the notion of *near-bent* functions was introduced in [8]. We generalize this now to characteristic p:

Definition 1.3. A function $f : V_n \to \mathbb{F}_p$ is called near-bent if $|\widehat{f}(b)|^2 = p^{n+1}$ or 0 for all $b \in V_n$.

We remark that the term *semi-bent* function in [3,6] and the term *three-valued almost-optimal* function in [1] are used for the same concept in characteristic 2.

In this article, we first generalize to characteristic p the technique presented in [8] (see also [3]) for constructing binary bent functions from near-bent functions. In Section 2, we illustrate the principle of the construction. In Section 3, we collect some classes of near-bent functions that can be used for the construction. The Fourier spectrum of quadratic functions is presented in detail in Section 4. With

these results, we construct infinite classes of weakly regular and non-weakly regular bent functions in Section 5.

2. Obtaining bent from near-bent functions

For a function $f : V_n \to \mathbb{F}_p$ let the support of $\widehat{f}$ be defined by $\operatorname{supp}(\widehat{f}) = \{b \in V_n \mid \widehat{f}(b) \neq 0\}$. For any p-ary function f we have

$$\sum_{b\in V_n} \left|\widehat{f}(b)\right|^2 = \sum_{b\in V_n} \sum_{x,y\in V_n} \epsilon_p^{f(x)-\langle b,x\rangle-(f(y)-\langle b,y\rangle)} = \sum_{x,y\in V_n} \epsilon_p^{f(x)-f(y)} \sum_{b\in V_n} \epsilon_p^{\langle b,y-x\rangle}.$$

Observing that $\sum_{b\in V_n} \epsilon_p^{\langle b,y-x\rangle} = 0$ if $x \neq y$, and $\sum_{b\in V_n} \epsilon_p^{\langle b,y-x\rangle} = p^n$ if $x = y$, we obtain the special case of *Parseval's relation*:

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

For a near-bent function f, clearly

$$\sum_{b\in V_n} \left|\widehat{f}(b)\right|^2 = \left|\operatorname{supp}(\widehat{f})\right| p^{n+1}$$

and combining this with Parseval's relation gives

$$\left|\operatorname{supp}(\widehat{f})\right| = p^{n-1}.$$

The following theorem presents how to obtain p-ary bent functions from a set of p near-bent functions $f_0(x), f_1(x), \ldots, f_{p-1}(x)$ from V_n to $\mathbb{F}_p$ with $\operatorname{supp}(\widehat{f_i}) \cap \operatorname{supp}(\widehat{f_j}) = \emptyset$ for $i \neq j$. We remark that then $\bigcup_{i=0}^{p-1} \operatorname{supp}(\widehat{f_i}) = \mathbb{F}_{p^n}$. The construction follows the principle of the classical Lagrange interpolation.

Theorem 2.1. *Let $f_0(x), f_1(x), \ldots, f_{p-1}(x)$ be near-bent functions from V_n to $\mathbb{F}_p$ such that $\operatorname{supp}(\widehat{f_i}) \cap \operatorname{supp}(\widehat{f_j}) = \emptyset$ for $0 \leqslant i \neq j \leqslant p-1$. Then the function $F(x, y)$ from $V_n \times \mathbb{F}_p$ to $\mathbb{F}_p$ defined by*

$$F(x, y) = (p-1) \sum_{k=0}^{p-1} \frac{y(y-1)\cdots(y-(p-1))}{y-k} f_k(x)$$

is bent. Moreover the Fourier spectrum of $F(x, y)$ is

$$\operatorname{spec}(F) = \bigcup_{k=0}^{p-1} \bigcup_{b=0}^{p-1} \epsilon_p^{-bk} \operatorname{spec}(f_k) \setminus \{0\}.$$

Proof. For $(a, b), (x, y) \in V_n \times \mathbb{F}_p$ the inner product we use is $\langle a, x\rangle + by$. The Fourier transform $\widehat{F}$ of F at (a, b) is

$$\begin{aligned}
\widehat{F}(a, b) &= \sum_{x\in V_n,\ y\in\mathbb{F}_p} \epsilon_p^{F(x,y)-\langle a,x\rangle-by} = \sum_{y\in\mathbb{F}_p} \epsilon_p^{-by} \sum_{x\in V_n} \epsilon_p^{F(x,y)-\langle a,x\rangle} \\
&= \sum_{y\in\mathbb{F}_p} \epsilon_p^{-by} \sum_{x\in V_n} \epsilon_p^{(p-1)!(p-1)f_y(x)-\langle a,x\rangle} \\
&= \sum_{y\in\mathbb{F}_p} \epsilon_p^{-by} \sum_{x\in V_n} \epsilon_p^{f_y(x)-\langle a,x\rangle} = \sum_{y\in\mathbb{F}_p} \epsilon_p^{-by} \widehat{f}_y(a).
\end{aligned}$$

As each $a \in V_n$ belongs to the support of exactly one $\widehat{f}_y$, $y \in \mathbb{F}_p$, for this y we have $\widehat{F}(a, b) = \epsilon_p^{-by} \widehat{f}_y(a)$, and consequently $|\widehat{F}(a, b)| = |\epsilon_p^{-by} \widehat{f}_y(a)| = p^{\frac{n+1}{2}}$. □

3. Near-bent functions

The objective of this section is to collect near-bent functions for which the supports of their Fourier transforms are easy to describe. These functions can then be used in connection with Theorem 2.1 to construct new classes of bent functions. In Section 5 we will use some of them to construct infinite classes of non-weakly regular bent functions.

Quadratic functions. For a function f from V_n to $\mathbb{F}_p$, an element $a \in V_n$ for which $f(x+a) - f(x)$ is constant is called a *linear structure* of f. The set Λ of the linear structures of a function f from V_n to $\mathbb{F}_p$ is a subspace of V_n. Since adding a constant to a p-ary function preserves the absolute values in the Fourier spectrum we may assume w.l.o.g. that $f(0) = 0$. Then f is a linear transformation on Λ (otherwise the function $f(x) - f(0)$ is a linear transformation on Λ). A *quadratic* function f from V_n to $\mathbb{F}_p$ can be defined as a function for which $f(x+a) - f(x)$ is linear or constant for all $a \in V$. Note that then if a is not a linear structure of the quadratic function f, the function $f(x+a) - f(x)$ is balanced, i.e. every element in $\mathbb{F}_p$ is taken on precisely p^{n-1} times.

Partially bent functions. The set of quadratic functions is a subset of the set of *partially bent functions*, which can be defined as the set of functions f from V_n to $\mathbb{F}_p$ for which $f(x+a) - f(x)$ is either balanced or constant. Let f be a partially bent function from V_n to $\mathbb{F}_p$ with $f(0) = 0$, and let s be the dimension of Λ, then applying the standard Welch-squaring technique we obtain for $b \in V_n$

$$\begin{aligned}\left|\widehat{f}(b)\right|^2 &= \sum_{x,y \in V_n} \epsilon_p^{f(x)-f(y)-\langle b, x-y\rangle} = \sum_{y,z \in V_n} \epsilon_p^{f(y+z)-f(y)-\langle b,z\rangle} \\ &= \sum_{z \in V_n} \epsilon_p^{f(z)-\langle b,z\rangle} \sum_{y \in V_n} \epsilon_p^{f(y+z)-f(y)-f(z)}.\end{aligned}$$

Using that $f(y+z) - f(y) - f(z)$ is balanced as a function in variable y if $z \notin \Lambda$, we get

$$\left|\widehat{f}(b)\right|^2 = p^n \sum_{z \in \Lambda} \epsilon_p^{f(z)-\langle b,z\rangle} = \begin{cases} p^{n+s} & \text{if } f(z) - \langle b, z\rangle \equiv 0 \text{ on } \Lambda, \\ 0 & \text{otherwise} \end{cases} \tag{3.1}$$

where in the last step we used that $f(z) - \langle b, z\rangle$ is linear on Λ.

Clearly a partially bent function is near-bent if the vector space Λ of its linear structures has dimension 1, i.e. $\Lambda = \{c\beta \mid c \in \mathbb{F}_p\}$ for some $\beta \in V_n$. By (3.1) the support of $\widehat{f}$ is a certain coset of the orthogonal complement of Λ, depending on $f(\beta)$.

Observation 3.1. Let f_i, f_j be near-bent functions with the same set of linear structures $\Lambda = \{c\beta \mid c \in \mathbb{F}_p\}$, then the supports of the Fourier transforms of $f_i(x) + \langle a_i, x\rangle$ and $f_j(x) + \langle a_j, x\rangle$ are disjoint if and only if $f_i(\beta) + \langle a_i, \beta\rangle \neq f_j(\beta) + \langle a_j, \beta\rangle$. Consequently there are many choices for separating the supports of the Fourier transforms for a set $\{f_k(x),\ 0 \leqslant k \leqslant p-1\}$ of near-bent functions with the same Λ by adding appropriate linear terms. However, since $\{\langle c\beta, \beta\rangle \mid c \in \mathbb{F}_p\} = \mathbb{F}_p$ it suffices to choose linear terms $\langle a, x\rangle$ with $a \in \Lambda$. In particular if $f_k(\beta) = d$ for all $k = 0, \ldots, p-1$, then $\{f_k(x) + \langle k\beta, x\rangle, 0 \leqslant k \leqslant p-1\}$ is a set of near-bent functions for which the Fourier transforms have pairwise disjoint support.

Example 1. For a bent function $f(x)$ from V_{n-1} to $\mathbb{F}_p$, we define a function $\tilde{f}(x, y)$ from $V_{n-1} \times \mathbb{F}_p$ to $\mathbb{F}_p$ by $\tilde{f}(x, y) = f(x)$. Then for $(u, v) \in V_{n-1} \times \mathbb{F}_p$ we have $\tilde{f}(x+u, y+v) - \tilde{f}(x, y) = f(x+u) - f(x)$, which vanishes if $u = 0$, and is balanced for $u \neq 0$ (as f is bent). Consequently $\tilde{f}$ is near-bent and the elements $(0, a)$, $a \in \mathbb{F}_p$ are the linear structures of $\tilde{f}$. As one easily sees from (3.1), the support of the Fourier transform of $\tilde{f}$ is the orthogonal complement of Λ (if w.l.o.g. we suppose $f(0) = 0$).

Example 2. The quadratic function $f(x_1,\dots,x_{n-1}) = d_1x_1^2 + \cdots + d_{n-1}x_{n-1}^2$ with $d_1,\dots,d_{n-1} \in \mathbb{F}_p^*$, is a bent function from $\mathbb{F}_p^{n-1}$ to $\mathbb{F}_p$ (see Section 4). Adding one variable x_n we obtain the near-bent function $\tilde{f}(x_1,\dots,x_{n-1},x_n) = d_1x_1^2+\cdots+d_{n-1}x_{n-1}^2$ from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. Obviously this example is a special case of the previous one, the linear structures of $\tilde{f}$ are the vectors $(0,\dots,0,a)$, $a \in \mathbb{F}_p$.

A topic of independent interest is finding polynomial representations of (quadratic) bent or near-bent functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Recall that a quadratic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, p odd, can be represented as (see [3,4])

$$f(x) = \mathrm{Tr}_n\left(\sum_{i=0}^{l} a_i x^{p^i+1}\right), \quad a_i \in \mathbb{F}_{p^n},\ 0 \leqslant i \leqslant l,$$

for an integer l, $0 \leqslant l \leqslant n/2$. Following the Welch-squaring technique we see that the linear structure Λ of f is the kernel of the linearized polynomial

$$L(z) = \sum_{i=0}^{l}\left(a_i^{p^l} z^{p^{l+i}} + a_i^{p^{l-i}} z^{p^{l-i}}\right). \tag{3.2}$$

We hereby can refer to [4, Proposition 2]. Accordingly, f is near-bent if the kernel of L given as in (3.2) is one dimensional.

We might hope for a monomial near-bent function, but unfortunately these do not exist as we now prove.

Theorem 3.2. *Quadratic monomial near-bent functions $f(x) = \mathrm{Tr}_n(ax^{p^r+1})$, $a \in \mathbb{F}_{p^n}$, in odd characteristic p do not exist.*

Proof. The linearized polynomial (3.2) that corresponds to $f(x) = \mathrm{Tr}_n(ax^{p^r+1})$ is given by $L(z) = az + a^{p^r} z^{p^{2r}}$.

We have to show that for any odd prime p, integers $r, n \geqslant 1$ and $a \in \mathbb{F}_{p^n}$ the kernel Λ of the linear map on $\mathbb{F}_{p^n}$ induced by $L(z) = az + a^{p^r} z^{p^{2r}}$ does not have dimension 1. For a primitive element γ of $\mathbb{F}_{p^n}$ let $a = \gamma^c$ for some c, $0 \leqslant c \leqslant p^n - 2$. Then $L(\gamma^t) = 0$ for an exponent t, $0 \leqslant t \leqslant p^n - 2$, if and only if

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

which is equivalent to

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

Λ has dimension 1 if and only if this congruence has $p-1$ incongruent solutions. Solutions exist if and only if $p-1$ divides $\frac{p^n-1}{2} - c(p^r-1)$. And then, there are $p-1$ incongruent solutions if and only if $\gcd(p^{2r}-1, p^n-1) = p-1$. The second condition is satisfied if and only if $\gcd(2r,n) = 1$, in particular n is then odd, which contradicts the first condition. □

Remark 3.3. In [4] it is pointed out that f is bent, i.e. Λ has dimension 0, if and only if $p^{\gcd(2r,n)} - 1$ does not divide $\frac{p^n-1}{2} - c(p^r-1)$. By Theorem 3.2, Λ has at least dimension 2 in all remaining cases.

As a consequence of Theorem 3.2 we must consider non-monomial quadratic functions in order to be able to apply Theorem 2.1. A class of binomial near-bent functions is presented in the following theorem.

Theorem 3.4. *Let $c \neq 0$ be an element of $\mathbb{F}_p$. The function f from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$*

$$f(x) = \mathrm{Tr}_n\left(cx^{p^r+1} - cx^{p^t+1}\right) \tag{3.3}$$

is near-bent if and only if $\gcd(n, r+t) = \gcd(n, r-t) = \gcd(n, p) = 1$.

Proof. We show that the kernel Λ of the linearized polynomial $L(x)$ given as in (3.2) corresponding to $f(x)$ has dimension 1 as a subspace of $\mathbb{F}_{p^n}$, i.e. $\gcd(L(x), x^{p^n} - x)$ has degree p. Equivalently Λ is one dimensional if and only if the associates $A(x)$ and $x^n - 1$ of $L(x)$ and $x^{p^n} - x$, respectively, satisfy $\deg(\gcd(A(x), x^n - 1)) = 1$, see [9, p. 118].

For the binomial (3.3) we have $L(x) = c(x + x^{p^{2r}} - x^{p^{r-t}} - x^{p^{r+t}})$, consequently $A(x) = c(1 + x^{2r} - x^{r-t} - x^{r+t}) = c(x^{r+t} - 1)(x^{r-t} - 1)$. Using $\gcd(x^m - 1, x^n - 1) = x^{\gcd(m,n)} - 1$ we easily see that $\deg(\gcd(A(x), x^n - 1)) = 1$ if and only if $\gcd(n, r+t) = \gcd(n, r-t) = \gcd(n, p) = 1$. The last condition prevents 1 from being a multiple root of $x^n - 1$. □

Remark 3.5. The kernel Λ of $L(x)$ in $\mathbb{F}_{p^n}$ for the function (3.3) is the set of the solutions of $x^p - x$, which is $\mathbb{F}_p$.

Remark 3.6. With similar arguments one can show that the function $f(x) = \mathrm{Tr}_n(cx^{p^r+1} + cx^{p^t+1})$ 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 $\gcd(n, p) = 1$. For this function Λ is the set of the solutions of $x^p + x$. We note that the conditions for this function to be near-bent imply that n is even.

A further construction of near-bent functions which can be seen as a generalization of the Maiorana–McFarland construction is described in Zheng and Zhang [10]. Let P be any injective function from $\mathbb{F}_p^{k-1}$ to $\mathbb{F}_p^k$, then the function $f(x, y) = P(x) \cdot y$ from $\mathbb{F}_p^{2k-1} = \mathbb{F}_p^{k-1} \times \mathbb{F}_p^k$ to $\mathbb{F}_p$ is near-bent. Let $(u, v) \in \mathbb{F}_p^{k-1} \times \mathbb{F}_p^k$, then

$$\begin{aligned}
\widehat{f}(u, v) &= \sum_{\substack{x \in \mathbb{F}_p^{k-1} \\ y \in \mathbb{F}_p^k}} \epsilon_p^{P(x)\cdot y - u\cdot x - v\cdot y} \\
&= \sum_{x \in \mathbb{F}_p^{k-1}} \epsilon_p^{u\cdot x} \sum_{y \in \mathbb{F}_p^k} \epsilon_p^{(P(x)-v)\cdot y} = p^k \sum_{P(x)=v} \epsilon_p^{u\cdot x} \\
&= \begin{cases} p^k \epsilon_p^{uP^{-1}(v)} & \text{if } P^{-1}(v) \text{ exists,} \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}$$

As can be seen immediately, $\mathrm{supp}(\widehat{f}) = \{(u, v) \mid v \in im(P), u \in \mathbb{F}_p^{k-1}\}$. Hence it is easy to construct sets of near-bent functions of this class with pairwise disjoint support. We remark that differently to the previous examples of near-bent functions, linear structures can be avoided with an appropriate choice of the mapping P, see [10]. Finally we point out that this class of near-bent functions is always regular, in the sense that $\widehat{f}(b) = p^{(n+1)/2}\epsilon_p^{J(b)}$ for all $b \in \mathrm{supp}(\widehat{f})$, where $J(b)$ is a function from $\mathrm{supp}(\widehat{f})$ to $\mathbb{F}_p$.

4. Fourier spectrum of quadratic functions

In this section we explicitly determine the Fourier spectrum of quadratic functions. We will use this result in Section 5 to construct weakly regular and non-weakly regular bent functions. Thereby we obtain the first known construction of infinite classes of non-weakly regular bent functions.

Fixing a basis of V_n we associate V_n with $\mathbb{F}_p^n$ and consider quadratic functions $f(x) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j$ from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, where we put $x = (x_1, \ldots, x_n)$. We note that we may omit the affine

part of the function as it does essentially not affect the Fourier spectrum. Then we can associate f with a quadratic form

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

where x^T denotes the transpose of the vector x, and A is a symmetric matrix with entries in $\mathbb{F}_p$. By [9, 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 $D = \operatorname{diag}(d_1, \ldots, d_n)$. Hence it is sufficient to describe the Fourier spectrum of a quadratic form $f(x) = d_1x_1^2 + \cdots + d_{n-s}x_{n-s}^2 := Q^d_{n,n-s}(x)$ for some $0 \leqslant s \leqslant n-1$ and $d = (d_1, \ldots, d_{n-s})$. Here we assume w.l.o.g. that the nonzero elements of the matrix D are $d_1, \ldots, d_{n-s}$. We will use the following simple lemmas, for the first see also [2].

Lemma 4.1. *For two functions f and g from V_n to $\mathbb{F}_p$ and from V_m to $\mathbb{F}_p$ respectively, we define the direct sum $f \oplus g$ from $V_{n+m} = V_n \times V_m$ to $\mathbb{F}_p$ by $(f \oplus g)(x, y) = f(x) + g(y)$. Then $\widehat{(f \oplus g)}(u, v) = \widehat{f}(u)\widehat{g}(v)$.*

Lemma 4.2. *Let f be a function from V_m to $\mathbb{F}_p$ and let $\tilde{f}$ be the function from $V_{m+n} = V_m \times V_n$ to $\mathbb{F}_p$ defined by $\tilde{f}(x, y) = f(x)$. Then $\widehat{\tilde{f}}(b, c) = p^n \widehat{f}(b)$ if $c = 0$ and $\widehat{\tilde{f}}(b, c) = 0$ if $c \neq 0$.*

Proof. We have

$$\begin{aligned}\widehat{\tilde{f}}(b, c) &= \sum_{\substack{x \in V_m \\ y \in V_n}} \epsilon_p^{\tilde{f}(x,y) - \langle b,x\rangle - \langle c,y\rangle} = \sum_{y \in V_n} \epsilon_p^{-\langle c,y\rangle} \sum_{x \in V_m} \epsilon_p^{f(x) - \langle b,x\rangle} \\ &= \begin{cases} p^n \widehat{f}(b) & \text{if } c = 0, \\ 0 & \text{else.} \end{cases} \qquad \square\end{aligned}$$

Theorem 4.3. *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*

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

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

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

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

Proof. We first consider $Q^d_{1,1}(x) = dx^2$ and note that by [9, Theorem 5.33]

$$\widehat{Q^d_{1,1}}(0) = \sum_{x \in \mathbb{F}_p} \epsilon_p^{dx^2} = \eta(d) G(\eta, \chi_1) \tag{4.1}$$

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 [9, Theorem 5.15] we then obtain

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

With Lemma 4.2 we get the assertion for $Q^d_{n,1}$ for arbitrary n. The general assertion then follows with induction from Lemma 4.1. □

Remark 4.4. The multiplication of a quadratic function f by c, $c \in \mathbb{F}_p^*$, causes a multiplication by c of the elements in the associated diagonal matrix. Consequently, Theorem 4.3 implies that f and cf have the same Fourier spectrum if and only if $n-s$ is even or $n-s$ is odd and c is a square in $\mathbb{F}_p$.

Remark 4.5. Two quadratic functions $Q^d_{n,n-s}(x) = d_1x_1^2 + \cdots + d_{n-s}x^2$ and $Q^{d'}_{n,n-s}(x) = d'_1x_1^2 + \cdots + d'_{n-s}x^2$ from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ are equivalent, i.e. 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. [9, Exercise 6.24]).

5. (Non)-weakly regular bent functions, examples

In this section we employ quadratic near-bent functions to construct both weakly regular and non-weakly regular bent functions. We will present examples using both commonly used representations of p-ary functions, functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ and functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. In the latter case, the obtained bent functions will be functions from $\mathbb{F}_{p^n} \times \mathbb{F}_p$ to $\mathbb{F}_p$.

Let $c_0, \ldots, c_{p-1}$ be nonzero elements of $\mathbb{F}_p$, then by Theorem 4.3 the functions

$$f_k(x) = c_k x_1^2 + x_2^2 + \cdots + x_{n-1}^2, \quad 0 \leqslant k \leqslant p-1, \tag{5.1}$$

are near-bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, all with the set of linear structures $\Lambda = \{(0, \ldots, 0, a) \mid a \in \mathbb{F}_p\}$. By Observation 3.1 the set

$$\left\{ f_k(x) + kx_n \;\middle|\; 0 \leqslant k \leqslant p-1 \right\} \tag{5.2}$$

is a set of near-bent functions for which the supports of the Fourier transforms are pairwise disjoint. The function given as in Theorem 2.1 is then bent. By Theorem 4.3, the signs of the Fourier coefficients of the functions f_k given by (5.1) are the same if and only if all c_k, $0 \leqslant k \leqslant p-1$, have the same quadratic character. By the description of the Fourier spectrum in Theorem 2.1, the constructed bent function is then weakly regular if and only if $\eta(c_0) = \eta(c_1) = \cdots = \eta(c_{p-1})$. We emphasize that the vast majority of these bent functions are non-weakly regular.

Example 3. By the above arguments, the functions $f_0(x_1, x_2, x_3, x_4, x_5) = x_1^2 + x_2^2 + x_3^2 + x_4^2$, $f_1(x_1, x_2, x_3, x_4, x_5) = 2x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5$, $f_2(x_1, x_2, x_3, x_4, x_5) = 2x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2x_5$ are near-bent functions from $\mathbb{F}_3^5$ to $\mathbb{F}_3$, for which $\operatorname{supp}(\widehat{f_i}) \cap \operatorname{supp}(\widehat{f_j}) = \emptyset$ for $0 \leqslant i \neq j \leqslant 3$. With the construction of Theorem 2.1 we obtain the bent function F from $\mathbb{F}_3^6$ to $\mathbb{F}_3$ of algebraic degree 4:

$$\begin{aligned} F(x_1, x_2, x_3, x_4, x_5, y) &= 2(y-1)(y-2)f_0 + 2y(y-2)f_1 + 2y(y-1)f_2 \\ &= 2y^2(f_0 + f_1 + f_2) + 2y(f_1 + 2f_2) + f_0 \\ &= x_1^2y^2 + x_5y + x_1^2 + x_2^2 + x_3^2 + x_4^2. \end{aligned}$$

As $\eta(1) \neq \eta(2)$ in $\mathbb{F}_3$, the bent function F is non-weakly regular.

Example 4. Since in $\mathbb{F}_5$ we have $\eta(2) = \eta(3)$, with the near-bent functions $f_0(x_1, x_2, x_3) = 2x_1^2 + x_2^2$, $f_1(x_1, x_2, x_3) = 2x_1^2 + x_2^2 + x_3$, $f_2(x_1, x_2, x_3) = 2x_1^2 + x_2^2 + 2x_3$, $f_3(x_1, x_2, x_3) = 3x_1^2 + x_2^2 + 3x_3$,

$f_4(x_1, x_2, x_3) = 3x_1^2 + x_2^2 + 4x_3$ from $\mathbb{F}_5^3$ to $\mathbb{F}_5$ we obtain with Theorem 2.1 the weakly regular bent function F from $\mathbb{F}_5^4$ to $\mathbb{F}_5$ and algebraic degree 6,

$$F(x_1, x_2, x_3, y) = 3x_1^2y^4 + 3x_1^2y^3 + 4x_1^2y + x_3y + 2x_1^2 + x_2^2.$$

Finally we point to constructing bent functions using near-bent functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. We will apply our construction method to near-bent functions $f(x)$ of the form (3.3). We recall that the space of the linear structures of $f(x)$ is $\Lambda = \mathbb{F}_p$ and observe that $f(a) = 0$ for $a \in \Lambda$. With Observation 3.1 we can construct appropriate near-bent functions to apply Theorem 2.1. We will use that by Remark 4.4, if f is a quadratic near-bent function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ and $c \in \mathbb{F}_p^*$, then f and cf have the same Fourier spectrum if and only if n is odd or n is even and c is a square in $\mathbb{F}_p$.

Example 5. Let $p = 3$, $n = 5$, $f(x) = \mathrm{Tr}_n(x^{3^2+1} - x^{3+1})$. For any c_0, c_1, c_2 in $\mathbb{F}_3^*$ the Fourier transforms of the near-bent functions $f_0(x) = c_0 f(x)$, $f_1(x) = c_1 f(x) + x$, $f_2 = c_2 f(x) + 2x$ have pairwise disjoint support, hence we can apply Theorem 2.1. Since n is odd every choice of c_0, c_1, c_2 in $\mathbb{F}_3^*$ yields a weakly regular bent function from $\mathbb{F}_{3^5} \times \mathbb{F}_3$ to $\mathbb{F}_3$.

Example 6. Choose $p = 3$, $n = 8$, $f(x) = \mathrm{Tr}_n(x^{3^2+1} - x^{3+1})$. Applying Theorem 2.1 to $f_0(x) = c_0 f(x)$, $f_1(x) = c_1 f(x) + x$, $f_2 = c_2 f(x) + 2x$ for some c_0, c_1, c_2 in $\mathbb{F}_3^*$ yields a non-weakly regular bent function whenever $\eta(c_0) = \eta(c_1) = \eta(c_2)$ does not hold (i.e. as $p = 3$, c_0, c_1, c_2 are not all the same).

Remark 5.1. With the presented procedure of constructing bent from near-bent functions a broad variety of (weakly regular and non-weakly regular) bent functions can be obtained.

1. The concept of equivalence can be utilized to generate a large diversity of near-bent functions serving as building blocks for the construction. For example, one may compose the binomial $f(x)$ given as in (3.3) with a linearized permutation polynomial $\pi(x)$. If π fixes $\mathbb{F}_p$, e.g. if π has coefficients in $\mathbb{F}_p$, then the near-bent function $f(\pi(x))$ has again $\mathbb{F}_p$ as set of linear structures.
2. In the construction, for some of the near-bent functions Maiorana–McFarland near-bent functions can be taken. Recall that the support of their Fourier transform can be chosen with an appropriate choice of the involved mapping P (see Section 3). By this, one can expect new inequivalent bent functions as some of the employed near-bent functions can be chosen without linear structure.
3. Finally the procedure can be applied recursively. After producing a bent function in dimension n, in a first step, one can add one variable and obtain again a near-bent function in dimension $n + 1$ as described in Example 1. This function can then serve as a building block for a next step generating bent functions in dimension $n + 2$ and after l steps in dimension $n + 2l$.

Acknowledgments

The authors would like to thank the anonymous referees whose accurate remarks helped to greatly improve our manuscript. In particular we thank for sketching a simple proof for Theorem 4.3.

References

[1] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, On cryptographic properties of the cosets of $R(1, m)$, IEEE Trans. Inform. Theory 47 (2001) 1494–1513.
[2] C. Carlet, H. Dobbertin, G. Leander, Normal extensions of bent functions, IEEE Trans. Inform. Theory 50 (2004) 2880–2885.
[3] P. Charpin, E. Pasalic, C. Tavernier, On bent and semi-bent quadratic Boolean functions, IEEE Trans. Inform. Theory 51 (2005) 4286–4298.
[4] T. Helleseth, A. Kholosha, Monomial and quadratic bent functions over the finite field of odd characteristic, IEEE Trans. Inform. Theory 52 (2006) 2018–2032.
[5] T. Helleseth, A. Kholosha, New binomial bent functions over the finite fields of odd characteristic, IEEE Trans. Inform. Theory 56 (2010) 4646–4652.
[6] K. Khoo, G. Gong, D. Stinson, A new characterization of semi-bent and bent functions on finite fields, Des. Codes Cryptogr. 38 (2006) 279–295.

[7] P.V. Kumar, R.A. Scholtz, L.R. Welch, Generalized bent functions and their properties, J. Combin. Theory Ser. A 40 (1985) 90–107.
[8] G. Leander, G. McGuire, Construction of bent functions from near-bent functions, J. Combin. Theory Ser. 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] Y. Zheng, X.-M. Zhang, On plateaued functions, IEEE Trans. Inform. Theory 47 (2001) 1215–1223.