Advances in Mathematics of Communications
Volume 7, No. 4, 2013, 425–440

doi:10.3934/amc.2013.7.425

# ON THE DUAL OF (NON)-WEAKLY REGULAR BENT FUNCTIONS AND SELF-DUAL BENT FUNCTIONS

Ayça Çeşmelioğlu

Faculty of Mathematics, Otto-von-Guericke University
Universitätsplatz 2, 39106, Magdeburg, Germany

Wilfried Meidl

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

Alexander Pott

Faculty of Mathematics, Otto-von-Guericke University
Universitätsplatz 2, 39106, Magdeburg, Germany

(Communicated by Cunsheng Ding)

Abstract. For weakly regular bent functions in odd characteristic the dual function is also bent. We analyse a recently introduced construction of non-weakly regular bent functions and show conditions under which their dual is bent as well. This leads to the definition of the class of dual-bent functions containing the class of weakly regular bent functions as a proper subclass. We analyse self-duality for bent functions in odd characteristic, and characterize quadratic self-dual bent functions. We construct non-weakly regular bent functions with and without a bent dual, and bent functions with a dual bent function of a different algebraic degree.

## 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 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 a bent function $f$ at $b \in \mathbb{F}_p^n$ is defined by $p^{-n/2}\widehat{f}(b)$. For $p = 2$ bent functions can only exist when $n$ is even, the normalized Fourier

2010 *Mathematics Subject Classification:* Primary: 11T71, 94A60, 06E30; Secondary: 11T24.

*Key words and phrases:* Duals of bent functions, self-dual bent functions, Fourier transform.

The first author is supported by Tübitak BİDEB 2219 Scholarship Programme. The second author is supported by Tübitak Project no.111T234.

coefficients are obviously ±1. For $p > 2$ bent functions exist for both, $n$ even and $n$ odd. For the normalized Fourier coefficients we always have (cf. [11])

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

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 $\zeta$ with $|\zeta| = 1$, otherwise it is called *non-weakly regular*. By (1), $\zeta$ can only be $\pm 1$ or $\pm i$. Note that regular implies weakly regular.

A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called *near-bent* if $|\widehat{f}(b)|^2 = p^{n+1}$ or 0 for all $b \in \mathbb{F}_p^n$. The support *supp*$(\widehat{f})$ of the Fourier transform of $f$ is defined by *supp*$(\widehat{f}) = \{b \in \mathbb{F}_p^n \mid \widehat{f}(b) \neq 0\}$. By *Parseval's identity* we then have $|supp(\widehat{f})| = p^{n-1}$. The normalized non-zero Fourier coefficients of a near-bent function resemble those of a bent function. Only the condition $n$ even (odd) has to be changed to $n + 1$ even (odd), and $f^*$ is now a function from *supp*$(\widehat{f})$ to $\mathbb{F}_p$. The notion of weak regularity is then also meaningful for near-bent functions.

Weakly regular bent functions always appear in pairs, since the weak regularity of $f$ guarantees that the function $f^*$ which is called the *dual* of $f$ is also (weakly regular) bent (see also [11]): For $y \in \mathbb{F}_p^n$ we get

$$\sum_{b\in\mathbb{F}_p^n} \epsilon_p^{b\cdot y}\widehat{f}(b) = \sum_{b\in\mathbb{F}_p^n} \epsilon_p^{b\cdot y} \sum_{x\in\mathbb{F}_p^n} \epsilon_p^{f(x)-b\cdot x} = \sum_{x\in\mathbb{F}_p^n} \epsilon_p^{f(x)} \sum_{b\in\mathbb{F}_p^n} \epsilon_p^{b\cdot(y-x)} = p^n\epsilon_p^{f(y)}, \tag{2}$$

a special case of *Poisson Summation Formula*. If $f$ is weakly regular, i.e. $\widehat{f}(b) = \zeta p^{n/2}\epsilon_p^{f^*(b)}$, with $\zeta$ independent from $b$, then

$$p^n\epsilon_p^{f(y)} = \zeta p^{n/2} \sum_{b\in\mathbb{F}_p^n} \epsilon_p^{f^*(b)+b\cdot y} = \zeta p^{n/2}\widehat{f^*}(-y).$$

Consequently

$$\widehat{f^*}(-y) = \zeta^{-1}p^{n/2}\epsilon_p^{f(y)} \tag{3}$$

and therefore $f^*$ is weakly regular bent. Furthermore we have $f^{**}(x) = f(-x)$ - if $p = 2$ forming the dual is an involution - and $f^{****}(x) = f(x)$. A weakly regular bent function $f$ is called self-dual if $f^* = f$. We observe that self-dual bent functions must satisfy $f(x) = f(-x)$. A weakly regular bent function $f$ is called anti-self-dual if $f^* = f + e$ for a constant $e \in \mathbb{F}_p^*$. As we will see in Remark 4 the latter term is only meaningful for $p = 2$ and then we have $e = 1$.

In Section 2 we analyze a construction of bent functions with respect to their duals. With this construction one can recursively obtain bent functions of a large degree in arbitrary dimension and their duals simultaneously. As we will see this construction also yields non-weakly regular bent functions for which the dual is bent as well. Until now the dual of a bent function has only been defined for weakly regular bent functions. This motivates the definition of a new class of bent functions, the class of bent functions for which the dual is also bent. In Section 3 we describe the duality properties of quadratic bent functions, and we completely characterize self-dual bent functions in odd characteristic. In Section 4 we give a general construction of self-dual non-quadratic bent functions in characteristic $p \equiv 1 \bmod 4$, and some results on self-dual bent functions for $p \equiv 3 \bmod 4$. In Section 5 we use our results and construct examples of bent functions and their duals with some interesting properties, amongst others non-weakly regular bent functions for which the dual is also bent, and self-dual bent functions.

## 2. Bent functions and their duals

In [5] the subsequent construction of bent functions has been utilized to construct the first infinite classes of non-weakly regular bent functions. We give a short proof of the correctness of the construction since the dual function $f^*$ which will be the object of our interest implicitly appears in this proof.

**Proposition 1** ([5])**.** *Let $f_0(x), f_1(x), \ldots, f_{p-1}(x)$ be near-bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ such that supp$(\widehat{f_i}) \cap$ supp$(\widehat{f_j}) = \emptyset$ for $0 \leq i \neq j \leq p-1$. Then the function $F(x,y)$ from $\mathbb{F}_p^{n+1}$ to $\mathbb{F}_p$ defined by*

$$F(x,y) = f_y(x)$$

*is bent. An explicit formula for $F(x,y)$ is obtained with the principle of Lagrange interpolation as*

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

*Proof.* For $a \in \mathbb{F}_p^n$ and $b \in \mathbb{F}_p$ we have

$$\widehat{F}(a,b) = \sum_{y\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_p^n} \epsilon_p^{f_y(x)-a\cdot x-by} = \sum_{y\in\mathbb{F}_p} \epsilon_p^{-by}\widehat{f_y}(a).$$

Since $a \in \mathbb{F}_p^n$ belongs to the support of exactly one $\widehat{f_y}$, $y \in \mathbb{F}_p$, for this $y$ we have

$$\widehat{F}(a,b) = \epsilon_p^{-by}\widehat{f_y}(a) = \zeta p^{\frac{n+1}{2}} \epsilon_p^{f_y^*(a)-by} \tag{4}$$

where $\zeta \in \{\pm1, \pm i\}$ depends on $y$ and $a$. □

**Theorem 1.** *Let $f_0(x), f_1(x), \ldots, f_{p-1}(x)$ be near-bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ with Fourier transforms with pairwise disjoint supports, and let $F(x,y) : \mathbb{F}_p^{n+1} \to \mathbb{F}_p$ be the bent function defined as in Proposition 1. Then the dual function $F^*(x,z) : \mathbb{F}_p^{n+1} \to \mathbb{F}_p$ of $F$ is given by*

$$F^*(x,z) = f_y^*(x) - yz, \quad \text{when } x \in supp(\widehat{f_y}),$$

*where the function $f_y^* : supp(\widehat{f_y}) \to \mathbb{F}_p$ is given by*

$$\widehat{f_y}(x) = \xi p^{\frac{n+1}{2}} \epsilon_p^{f_y^*(x)} \quad \text{for all } x \in supp(\widehat{f_y}).$$

*If for all $j = 0, \ldots, p-1$ the near-bent functions $f_j : \mathbb{F}_p^n \to \mathbb{F}_p$ are weakly regular, then the dual $F^*$ is a bent function. Moreover $F^{**}(x,y) = F(-x,-y)$, $F^{****}(x,y) = F(x,y)$.*

*Proof.* From equation (4) we see that the dual function $F^*$ of $F$ is given by $F^*(x,z) = f_y^*(x) - yz$ when $x \in supp(\widehat{f_y})$. We suppose that all near-bent functions are weakly regular and show that $F^*$ is bent: With Poisson Summation Formula (2) we obtain the equality

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

For a weakly regular near-bent function $f$, i.e. for $a \in supp(\widehat{f})$ we have $\widehat{f}(a) = p^{(n+1)/2}\zeta\epsilon_p^{f^*(a)}$ where $\zeta$ is independent from $a$, this yields

$$\sum_{a \in supp(\widehat{f})} \epsilon_p^{f^*(a)+a\cdot x} = p^{(n-1)/2}\epsilon_p^{f(x)}\zeta^{-1}. \tag{5}$$

Let $a \in \mathbb{F}_p^n$ and $b \in \mathbb{F}_p$, then

$$\begin{aligned}\widehat{F^*}(a,b) &= \sum_{x\in\mathbb{F}_p^n, z\in\mathbb{F}_p} \epsilon_p^{F^*(x,z)-a\cdot x - bz} = \sum_{z\in\mathbb{F}_p} \epsilon_p^{-bz} \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{F^*(x,z)-a\cdot x} \\ &= \sum_{y\in\mathbb{F}_p} \sum_{x\in supp(\widehat{f}_y)} \epsilon_p^{f_y^*(x)-a\cdot x} \sum_{z\in\mathbb{F}_p} \epsilon_p^{-zy-bz} = p \sum_{x \in supp(\widehat{f}_{-b})} \epsilon_p^{f_{-b}^*(x)-a\cdot x} \\ &= p^{\frac{n+1}{2}} \epsilon_p^{f_{-b}(-a)} \zeta_b^{-1},\end{aligned}$$

where the last step follows from (5). We remark that $\zeta_b$ depends on $b$ but is independent from $a$. As can be seen from the last equality, the dual $F^{**}(x,y)$ of $F^*$ is $F(-x,-y)$. □

Let $f_j, j = 0,\dots,p-1$, be bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, then the functions $f_j + jx_{n+1}, j = 0,\dots,p-1$, form a set of near-bent functions from $\mathbb{F}_p^{n+1}$ to $\mathbb{F}_p$ with Fourier transforms with pairwise disjoint supports, see [6]. With this set of near-bent functions one obtains an interesting special case of Proposition 1. The resulting bent function $F$ is then a function from $\mathbb{F}_p^{n+2}$ to $\mathbb{F}_p$, and can be described by

$$F(x, x_{n+1}, y) = f_y(x) + x_{n+1}y. \tag{6}$$

**Theorem 2.** *For $j = 0,\dots,p-1$ let $f_j$ be bent functions in dimension $n$, and let $F : \mathbb{F}_p^{n+2} \to \mathbb{F}_p$ be the bent function defined as in equation (6). Then the dual function $F^*$ of $F$ is given by*

$$F^*(x, x_{n+1}, y) = f_{x_{n+1}}^*(x) - x_{n+1}y. \tag{7}$$

*If the dual functions $f_j^*$ of $f_j$, $j = 0,\dots,p-1$, are all bent, then also $F^*$ is a bent function. Furthermore, then $f_j(x)^{**} = f_j(-x)$ for $j = 0,\dots,p-1$, implies $F^{**}(x,x_{n+1},y) = F(-x,-x_{n+1},-y)$ and $F^{****}(x,x_{n+1},y) = F(x,x_{n+1},y)$.*

*Proof.* For $a \in \mathbb{F}_p^n$, $b,c \in \mathbb{F}_p$ we have

$$\begin{aligned}\widehat{F}(a,b,c) &= \sum_{\substack{x\in\mathbb{F}_p^n \\ x_{n+1},y\in\mathbb{F}_p}} \epsilon_p^{f_y(x)+x_{n+1}y-a\cdot x-bx_{n+1}-cy} \\ &= \sum_{\substack{x\in\mathbb{F}_p^n \\ y\in\mathbb{F}_p}} \epsilon_p^{f_y(x)-a\cdot x-cy} \sum_{x_{n+1}\in\mathbb{F}_p} \epsilon_p^{x_{n+1}(y-b)} = p\epsilon_p^{-bc} \sum_{x\in\mathbb{F}_p^n} \epsilon_p^{f_b(x)-a\cdot x} \\ &= p\epsilon_p^{-bc}\widehat{f}_b(a) = p^{\frac{n+2}{2}}\zeta\epsilon_p^{f_b^*(a)-bc}\end{aligned}$$

for some $\zeta \in \{\pm 1, \pm i\}$ which depends on $b$ and $a$. Consequently the dual function $F^*$ of $F$ is described by equation (7).

The function $F^*$ in (7) is obtained like the bent function $F$ in (6), only the dual functions $f_j^*$ are used as building blocks and the roles of $x_{n+1}$ and $y$ are interchanged. Hence if all $f_j^*$, $0 \le j \le p-1$, are bent, then $F^*$ is bent as well. Similarly as above we also get

$$\widehat{F^*}(a,b,c) = p^{\frac{n+2}{2}}\zeta\epsilon_p^{f_{-c}^{**}(a)+bc}$$

for some $\zeta \in \{\pm 1, \pm i\}$ which depends on $c$ and $a$. Hence $F^{**}(a,b,c) = f_{-c}^{**}(a)+bc = f_{-c}(-a)+bc = F(-a,-b,-c)$ for $(a,b,c) \in \mathbb{F}_p^n \times \mathbb{F}_p \times \mathbb{F}_p$. Immediately one then sees that $F^{****} = F$. □

**Remark 1.** By a recursive application of Theorems 1,2 a large variety of bent functions and their duals can be constructed simultaneously, see Section 5. For instance for the application of Theorem 2 one only needs a set of $p$ bent functions and their duals as a starting point.

As easily seen, a bent function obtained by the construction described in Proposition 1 is weakly regular if and only if all near-bent functions used as building blocks are weakly regular with the same sign in their normalized Fourier coefficients. This has been utilized in [5] to present the first construction of non-weakly regular bent functions. Until then only sporadic examples of non-weakly regular bent functions were known, namely

1. $g_1 : \mathbb{F}_{3^6} \to \mathbb{F}_3$ with $g_1(x) = \mathrm{Tr}_6(\xi^7 x^{98})$, where $\xi$ is a primitive element of $\mathbb{F}_{3^6}$, see [11],
2. $g_2 : \mathbb{F}_{3^4} \to \mathbb{F}_3$ with $g_2(x) = \mathrm{Tr}_4(a_0 x^{22} + x^4)$, where $a_0 \in \{\pm\xi^{10}, \pm\xi^{30}\}$ and $\xi$ is a primitive element of $\mathbb{F}_{3^4}$, see [12],
3. $g_3 : \mathbb{F}_{3^3} \to \mathbb{F}_3$ with $g_3(x) = \mathrm{Tr}_3(x^{22} + x^8)$, or alternatively $\tilde{g}_3 : \mathbb{F}_3^3 \to \mathbb{F}_3$ with $\tilde{g}_3(x_1,x_2,x_3) = x_2^2x_3^2 + 2x_3^2 + x_1x_3 + x_2^2$, see [19].
4. $g_4, g_5 : \mathbb{F}_{3^6} \to \mathbb{F}_3$ with $g_4(x) = \mathrm{Tr}_6(\xi x^{20} + \xi^{41}x^{92})$, $g_5(x) = \mathrm{Tr}_6(\xi^7 x^{14} + \xi^{35}x^{70})$, where $\xi$ is a primitive element of $\mathbb{F}_{3^6}$, see [13].

We emphasize that Theorems 1,2 show that the construction of bent functions $F$ described as in Proposition 1 yields bent functions which have a bent dual, also if $F$ is non-weakly regular. Whereas in the proof of Theorem 1 we use that the near-bent functions $f_j$, $j = 0,\dots,p-1$, are weakly regular, in Theorem 2 it suffices that for all bent functions $f_j$, $j = 0,\dots,p-1$, the dual bent function exists. However, having a dual which is bent is not a universal property of bent functions. Using MAGMA one sees that the duals of the bent functions $g_1, g_2, g_5$ are not bent, whereas the duals of $g_3, g_4$ are bent functions. This motivates the definition of a new class of bent functions. We call a bent function a *dual-bent function* if its dual function is also bent. The class of weakly regular bent functions is then a subclass of the class of dual-bent functions, non-weakly regular bent functions can be both, dual-bent functions or *non-dual-bent functions*.

**Remark 2.** By the properties P1-P4 below and Theorem 1 in [6], EA-equivalence transformations on a bent function $f$ imply EA-equivalence transformations on the dual $f^*$. Hence the class of dual-bent functions is invariant under EA-equivalence. For bent functions, CCZ-equivalence, see [2], is the same as EA-equivalence, see [8]. The existence of non-weakly regular dual-bent functions $f$ for which the dual $f^*$ is weakly regular is an open problem (in this case $f^{**}$ must be weakly regular as well, and $f^{*****} = f^*$).

## 3. Quadratic bent functions and their duals

In some sense the simplest bent functions are quadratic bent functions. In order to be able to use quadratic bent functions as a starting point to construct bent functions and their duals in higher algebraic degree, we describe the duals of quadratic bent functions in the following. First we collect the effect of EA-equivalence transformations to the Fourier coefficients of a function $f$ from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, which completely describes the effect of these transformations to the dual of a bent function: Let $b, u, v \in \mathbb{F}_p^n$ and $e \in \mathbb{F}_p$, then we have

P1: $\widehat{(f+e)}(b) = \epsilon_p^e \widehat{f}(b)$,
P2: if $f_v(x) = f(x) + v \cdot x$ then $\widehat{f_v}(b) = \widehat{f}(b - v)$,
P3: $\widehat{f(x+u)}(b) = \epsilon_p^{b \cdot u} \widehat{f}(b)$,
P4: if $A \in GL_n(\mathbb{F}_p)$ then $\widehat{f(Ax)}(b) = \widehat{f}((A^{-1})^T b)$, where $A^T$ denotes the transpose of the matrix $A$.

**Remark 3.** If $p$ is odd, a further EA-equivalence transformation is the multiplication of $f$ by a nonzero constant of $\mathbb{F}_p$. The effect of this transformation to the Fourier coefficients is somewhat more involved. For details we refer to [6, Theorem 1] and its proof.

**Remark 4.** If $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is bent, then with Property P1 we have $(f+e)^* = f^* + e$. If $f$ is a weakly regular anti-self-dual bent function then with $f^* = f + e$, $e \in \mathbb{F}_p^*$, we have $f = f^{****} = f + 4e$, which implies $p = 2$.

As it is well known, every quadratic bent function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is EA-equivalent to the function $Q(x) = x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$ which is a self-dual bent function, see [3, 14]. With Properties P1-P4 this describes the duals of all quadratic bent functions when $p = 2$.

We remark that Properties P1-P4 imply that self-duality of bent functions is not invariant under EA-equivalence transformations. As one can further see, self-duality is invariant under the transformation described in P4 if the matrix $A$ is orthogonal, see also [3, Theorem 4.6]. For a complete characterization of self-dual and anti-self-dual quadratic bent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ we again refer to [14].

We now consider the case of quadratic bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ for odd primes $p$. Using the Properties P1, P2, we can omit the affine part and restrict ourselves to the determination of the duals of quadratic bent functions of the form $f(x) = f(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$, $a_{ij} \in \mathbb{F}_p$.

We utilize the fact that every quadratic function $f$ of this form 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 $\mathbb{F}_p$. Every quadratic form can be transformed into a diagonal quadratic form by a coordinate transformation, i.e. there exists an invertible matrix $C$ over $\mathbb{F}_p$ and a diagonal matrix $D = diag(d_1, \ldots, d_n)$, such that $D = C^T A C$, see [17, Theorem 6.21]. Moreover, the corresponding function $f(x)$ is bent if and only if the quadratic form is nonsingular, i.e. $d_i \neq 0$, $i = 1, \ldots, n$ (cf. [5, Theorem 4.3]). Therefore it is sufficient to determine the dual of quadratic functions of the form

$$Q(x) = d_1 x_1^2 + d_2 x_2^2 + \cdots + d_n x_n^2 \tag{8}$$

for some $d_i \in \mathbb{F}_p^*$, $i = 1, \dots, n$. We follow the proof of [5, Theorem 4.3], where the expression of the dual is also implicitly given (see also the proof of Proposition 1 in [11]).

**Proposition 2.** *The dual of the quadratic bent function* $Q : \mathbb{F}_p^n \to \mathbb{F}_p$ *given by* $Q(x) = d_1x_1^2 + d_2x_2^2 + \cdots + d_nx_n^2$ *is*

$$Q^*(x) = -\frac{x_1^2}{4d_1} - \frac{x_2^2}{4d_2} - \cdots - \frac{x_n^2}{4d_n}.$$

*Proof.* For the function $Q(x) = dx^2$ on $\mathbb{F}_p$ we have by [17, Theorem 5.33]

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

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

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

and with [17, Theorem 5.15] we obtain

$$\widehat{Q}(b) = \begin{cases} \eta(d)p^{\frac{1}{2}}\epsilon_p^{-b^2/(4d)} & : \quad p \equiv 1 \bmod 4; \\ \eta(d)ip^{\frac{1}{2}}\epsilon_p^{-b^2/(4d)} & : \quad p \equiv 3 \bmod 4, \end{cases} \tag{9}$$

which shows the correctness of the assertion for $n = 1$.

For two functions $g_1 : \mathbb{F}_p^m \to \mathbb{F}_p$ and $g_2 : \mathbb{F}_p^n \to \mathbb{F}_p$, the direct sum $g_1 \oplus g_2$ from $\mathbb{F}_p^n \times \mathbb{F}_p^m = \mathbb{F}_p^{m+n}$ to $\mathbb{F}_p$ is defined by $(g_1 \oplus g_2)(x, y) = g_1(x) + g_2(y)$. Then (see also [4])

$$\widehat{(g_1 \oplus g_2)}(u, v) = \widehat{g_1}(u)\widehat{g_2}(v). \tag{10}$$

The assertion for arbitrary $n$ follows then from (9) applying (10) recursively. □

As a consequence of Proposition 2 we can also characterize self-dual quadratic bent functions in odd characteristic, which adds to the results of [3, 14] for the case that $p = 2$.

**Corollary 1.** *Let* $f : \mathbb{F}_p^n \to \mathbb{F}_p$ *be a bent function given by* $f(x) = x^TAx$ *for a symmetric matrix* $A$ *over* $\mathbb{F}_p$*. Then* $f$ *is self-dual if and only if* $A^2 = -4^{-1}I$*.*

*Proof.* We can write $A$ as $A = C^TDC$ for a nonsingular matrix $C$ and a (nonsingular) diagonal matrix $D = diag(d_1, \dots, d_n)$. Equivalently, $f(x) = x^TAx = x^TC^TDCx$ equals $f_1(Cx)$ with $f_1(x) = x^TDx$. From Proposition 2 we know that the dual of $f_1$ is given by $f_1^*(x) = x^T\tilde{D}x$ where $\tilde{D} = diag(-1/(4d_1), \dots, -1/(4d_n)) = -4^{-1}D^{-1}$.

With Property P5 we get for the dual $f^*(x)$ of $f(x) = f_1(Cx)$,

$$\begin{aligned} f^*(x) &= f_1^*((C^{-1})^Tx) = ((C^{-1})^Tx)^T\tilde{D}(C^{-1})^Tx \\ &= x^TC^{-1}\frac{-1}{4}D^{-1}(C^{-1})^Tx = x^T(C^T(-4)DC)^{-1}x = x^T\frac{-1}{4}A^{-1}x. \end{aligned}$$

Consequently $f$ is self-dual if and only if for all $x \in \mathbb{F}_p^n$ we have

$$x^TAx = x^T\frac{-1}{4}A^{-1}x.$$

Since by assumption $A$ and hence also $\frac{-1}{4}A^{-1}$ is symmetric, and the representation of a $p$-ary quadratic function with a symmetric matrix is unique, $f$ is self-dual if and only if $A = \frac{-1}{4}A^{-1}$ or equivalently $A^2 = \frac{-1}{4}I$. □

**Remark 5.** A weakly regular self-dual bent function satisfies $f(x) = f(-x)$, hence (quadratic) self-dual bent functions do not have linear terms. Consequently Corollary 1 describes all $p$-ary self-dual quadratic bent functions.

**Remark 6.** As it follows immediately from Corollary 1, the quadratic function $Q(x) = d_1x_1^2 + d_2x_2^2 + \cdots + d_nx_n^2$ is self-dual if and only if $d_i^2 = -4^{-1} \in \mathbb{F}_p$ for $i = 1, 2, \ldots, n$. In particular, $Q(x)$ can only be self-dual if $p \equiv 1 \bmod 4$.

One example of a quadratic self-dual bent function in characteristic $p$ with $p \equiv 3 \bmod 4$, is the function $f : \mathbb{F}_3^2 \to \mathbb{F}_3$ given by $f(x) = x^TAx$ with $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$.

## 4. Self-dual bent functions in odd characteristic

As pointed out, for $p = 2$ quadratic self-dual (and anti-self-dual) bent functions have been completely characterized in [14]. Some results on self-duality for some primary and secondary constructions of bent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ are presented in [3]. In general it seems not to be easy to construct self-dual bent functions of degree other than 2. Some examples in [3] are self-dual partial spreads bent functions and bent functions arising from a secondary construction presented in [1] which is limited to the case $p = 2$ (see [3, Theorem 4.9]). In the following we present a construction of self-dual bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, $p \equiv 1 \bmod 4$.

The idea is to use self-dual bent functions in the construction (6), where we may use quadratic functions given as in Corollary 1. The resulting bent function is not yet self-dual, but one may try to use Property P4 to transform this function into a self-dual bent function with an appropriate coordinate transformation. We will use the following Lemma.

**Lemma 1.** *Let $\Theta : \mathbb{F}_p^2 \to \mathbb{F}_p$ be defined by $\Theta\left(\binom{x}{y}\right) = xy$. The matrix*

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

*satisfies*

$$\begin{pmatrix} 0 & 1 \end{pmatrix} B \begin{pmatrix} y \\ z \end{pmatrix} = \begin{pmatrix} k & 0 \end{pmatrix} (B^{-1})^T \begin{pmatrix} y \\ z \end{pmatrix} \tag{11}$$

*and*

$$\Theta\left(B\begin{pmatrix} y \\ z \end{pmatrix}\right) = -\Theta\left((B^{-1})^T\begin{pmatrix} y \\ z \end{pmatrix}\right) \tag{12}$$

*for all $y, z \in \mathbb{F}_p$ if and only if $k^2 = -1$, $d \in \mathbb{F}_p^*$, $b = k/(2d)$, and $a = \pm kb$, $c = \mp kd$, where different signs have to be chosen for $a$ and $c$.*

*Proof.* To satisfy condition (11) the transpose of the inverse of $B$ has to be of the form

$$(B^{-1})^T = \begin{pmatrix} k^{-1}c & k^{-1}d \\ u & v \end{pmatrix}$$

which yields the conditions

$$(i)\ ak^{-1}c + bk^{-1}d = 1, \quad (ii)\ cu + dv = 1,$$
$$(iii)\ au + bv = 0, \quad (iv)\ c^2 + d^2 = 0.$$

Furthermore, by condition (12) we require $(ay+bz)(cy+dz) = -(k^{-1}cy+k^{-1}dz)(uy+vz)$. Comparison of the coefficients yields

$$(v)\; a = -k^{-1}u \quad \text{and} \quad (vi)\; b = -k^{-1}v.$$

Using (v), (vi), from (i), (ii) we obtain $k^2 = -1$. We note that then $k^{-1} = -k$ and we arrive at the conditions

I $a^2+b^2 = 0$, i.e. $a = \pm kb$ (from (iii)),
II $c^2+d^2 = 0$, i.e. $c = \mp kd$ (from (iv)),
III $ac+bd = k$ (from (i)).

Observe that I and II also imply that $a,b,c,d \neq 0$. With I, II, equation III yields $b = k/(2d)$, where we remark that the signs for $a$ and $c$ in equations I and II have to be chosen different such that the left side of III does not vanish. For an arbitrary choice of $d \in \mathbb{F}_p^*$ (and a choice of $k$ with $k^2 = -1$) the value for $b$ is uniquely determined, which then also determines the pair $(a,c)$ ambiguously. □

**Theorem 3.** *For a prime $p \equiv 1 \bmod 4$ let $k$ be a square root of $-1$, and let $f_0, f_1, \dots, f_{p-1}$ be (quadratic) self-dual bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ such that $f_i = f_j$ when $i \equiv jk^l \bmod p$ for some $0 \le l \le 3$. Let $F(x,y,z)$ be the corresponding bent function (6) in dimension $n+2$, $A$ an orthogonal $n \times n$ matrix over $\mathbb{F}_p$ and $B$ a $2\times 2$ matrix as described in Lemma 1, and let $L(x,y,z)$, $x \in \mathbb{F}_p^n, y,z \in \mathbb{F}_p$, be the linear transformation given by the matrix*

$$\mathcal{A} = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

*Then $F(L(x,y,z))$ is a self-dual bent function in $n+2$ variables.*

*Proof.* Since $L(x,y,z) = (Ax, B\binom{y}{z})$, from (6) we obtain

$$F(L(x,y,z)) = F(Ax, B\begin{pmatrix} y \\ z \end{pmatrix}) = f_h(Ax) + \Theta\left(B\begin{pmatrix} y \\ z \end{pmatrix}\right)$$

where

$$h = \begin{pmatrix} 0 & 1 \end{pmatrix} B \begin{pmatrix} y \\ z \end{pmatrix}.$$

Using $(A^{-1})^T = A$, Property P4 and equation (7) we get

$$F(L(x,y,z))^* = F^*(Ax, (B^{-1})^T\begin{pmatrix} y \\ z \end{pmatrix}) = f_{\bar h}^*(Ax) - \Theta\left((B^{-1})^T\begin{pmatrix} y \\ z \end{pmatrix}\right)$$

where

$$\bar h = \begin{pmatrix} 1 & 0 \end{pmatrix} (B^{-1})^T \begin{pmatrix} y \\ z \end{pmatrix}.$$

As $B$ is chosen such that the conditions in Lemma 1 are satisfied we have $\bar h = kh$ by condition (11) and then by condition (12)

$$f_{\bar h}^*(Ax) - \Theta\left((B^{-1})^T\begin{pmatrix} y \\ z \end{pmatrix}\right) = f_{kh}^*(Ax) + \Theta\left(B\begin{pmatrix} y \\ z \end{pmatrix}\right).$$

By assumption we have $f_{kh}^* = f_{kh} = f_{\bar h}$ which completes the proof. □

**Remark 7.** Starting with quadratic self-dual bent functions, Theorem 3 can be applied recursively to obtain self-dual bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, $p \equiv 1 \bmod 4$, with high algebraic degree.

The construction in Theorem 3 requires that $p \equiv 1 \bmod 4$. The question arises naturally when self-dual bent functions exist for $p \equiv 3 \bmod 4$. A quadratic example in dimension 2 was given in Section 3. We start with a non-existence result.

**Corollary 2.** *Self-dual weakly regular bent functions $f : \mathbb{F}_p^n \to \mathbb{F}_p$ do not exist when $p \equiv 3 \bmod 4$ and $n$ is odd.*

*Proof.* If $f(x)$ is a weakly regular self-dual bent function we have $f^*(x) = f(x)$ and $f(x) = f^{**}(x) = f(-x)$. By equation (3), for any $b \in \mathbb{F}_p^n$, the Fourier coefficients of $f(x)$ and $f^*(x)$ can be written as

$$\widehat{f}(b) = \zeta p^{n/2}\epsilon_p^{f^*(b)},\ \widehat{f^*}(-b) = \zeta^{-1}p^{n/2}\epsilon_p^{f^*(b)}.$$

Using these two equations and $\widehat{f}(-b) = \widehat{f}(b)$, one sees that $\zeta^2 = 1$ and hence $\zeta \neq \pm i$, which by equation (1) contradicts $p \equiv 3 \bmod 4$ and $n$ odd. □

We remark that equation (3) was obtained under the assumption that $f$ is weakly regular. On the other hand, self-dual non-weakly regular bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, $p \equiv 3 \bmod 4$ and $n$ is odd exist: By MAGMA we see that the function $g_3(x) = \mathrm{Tr}_3(x^{22} + x^8)$ from $\mathbb{F}_{3^3}$ to $\mathbb{F}_3$ is self-dual. As a consequence, for any self-dual bent function $h$ on $\mathbb{F}_{3^n}$ with $n$ even, for which the existence is guaranteed by Proposition 3 below, also the function $f$ on $\mathbb{F}_{3^3} \times \mathbb{F}_{3^n}$ defined by

$$f(x, y) = g_3(x) + h(y)$$

is bent and by the fact that $f^* = g_3^* + h^*$ also self-dual. Finally we remark that using weakly regular bent functions as building blocks in our construction - which at least insures that the resulting function is dual-bent - we cannot find such self-dual functions since equation (3) holds then.

We finish this section with an example of a ternary bent function which shows that for $n$ even and $p \equiv 3 \bmod 4$ (weakly regular) nonquadratic self-dual bent functions exist. The example arises from bent functions from $\mathbb{F}_{3^n}$ to $\mathbb{F}_3$ presented in [11]. In the following proposition $K_k(a)$ denotes the Kloosterman sum (see [17, Definition 5.42])

$$K_k(a) = \sum_{x \in \mathbb{F}^*_{p^k}} \epsilon_p^{\mathrm{Tr_k}(x + ax^{-1})}.$$

**Proposition 3** ([11, Theorem 2])**.** *Let $n = 2k$ and $t$ be a positive integer satisfying $\gcd(t, p^k + 1) = 1$ and $p^k > 3$. Then the function $f(x) = \mathrm{Tr_n}(ax^{t(p^k - 1)})$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is bent if and only if $K_k(a^{p^k+1}) = -1$. If $K_k(a^{p^k+1}) = -1$ then $f(x)$ is regular bent and $\widehat{f}(b) = p^k\epsilon_p^{-\mathrm{Tr_n}(a^{p^k}b^{t(p^k-1)})}$.*

**Remark 8.** In [11] the existence of bent functions given as in Proposition 3 has been shown for $p = 3$. The existence of such bent functions in the general case was left as an open problem. It was shown in [15, Corollary 3] that bent functions of this form cannot exist for finite fields of characteristic $p > 3$.

**Remark 9.** In [16, Corollary 4], it was shown that the binary Dillon bent function $f(x) = \mathrm{Tr_n}(ax^{2^k-1})$ is self-dual bent if and only if $K_k(a) = -1$.

From Proposition 3 we see that if $f(x) = \mathrm{Tr_n}(ax^{t(3^k-1)})$ is bent, then its dual is the function $f^*(x) = -\mathrm{Tr_n}(a^{3^k}x^{t(3^k-1)})$. Consequently $f(x)$ is a self-dual bent function if and only if $a$ satisfies the conditions

$$\text{A.}\quad K_k(a^{3^k+1}) = -1, \qquad \text{B.}\quad a^{3^k} = -a.$$

Let $\alpha \in \mathbb{F}_{3^n}$ be a primitive element of $\mathbb{F}_{3^n}$. Then $a = \alpha^{\frac{3^k+1}{2}}$ satisfies condition B. We note that $a^{3^k+1} = \alpha^{\frac{3^k+1}{2}(3^k+1)} := w^{\frac{3^k+1}{2}}$, and observe that $w = \alpha^{3^k+1}$ is a primitive element of $\mathbb{F}_{3^k}$. We may hence write $K_k(a^{3^k+1}) = K_k(w^{\frac{3^k+1}{2}})$ and therefore, $f(x) = \mathrm{Tr_n}(\alpha^{\frac{3^k+1}{2}} x^{t(3^k-1)})$ from $\mathbb{F}_{3^n}$ to $\mathbb{F}_3$ is self-dual bent if and only if $K_k(w^{\frac{3^k+1}{2}}) = -1$. Using MAGMA one can confirm that for $k = 3, 5, 7$ and some choices of the primitive element $\alpha$ this condition is satisfied.

Consequently for $k = 3, 5, 7$ there exist self-dual bent functions $f$ with $f(x) = \mathrm{Tr_n}(\alpha^{\frac{3^k+1}{2}} x^{t(3^k-1)})$ from $\mathbb{F}_{3^n}$ to $\mathbb{F}_3$, $n = 2k$.

When $k$ is even then $f(x) = \mathrm{Tr_n}(\alpha^{\frac{3^k+1}{2}} x^{t(3^k-1)})$ is never bent. In this case $w^{\frac{3^k+1}{2}}$ cannot be a square in $\mathbb{F}_{3^k}$ since $w$ is a primitive element of $\mathbb{F}_{3^k}$, and then $K_k(w^{\frac{3^k+1}{2}}) \neq -1$ due to a divisibility result in Theorem 1.4 of [9] (see also [10, Corollary 1]).

## 5. Examples

In this section we highlight our main achievements with examples of bent functions obtained with the procedure described in Section 2.

5.1. Constructing bent functions and their duals simultaneously, $p = 2$. We apply construction (6) to the quadratic bent functions $f_0 = x_1x_2 + x_3x_4$ and $f_1 = x_1x_3 + x_2x_4$ from $\mathbb{F}_2^4$ to $\mathbb{F}_2$, which are both self-dual, to obtain $F_1 : \mathbb{F}_2^6 \to \mathbb{F}_2$, and its dual $F_1^*$ by equation (7). We may then recursively continue the procedure for instance using the obtained bent functions and their duals. With Lagrange interpolation principle we obtain the algebraic normal form of $F_1$ as

$$\begin{aligned} F_1(x_1,\dots,x_6) &= (x_6+1)(x_1x_2+x_3x_4) + x_6(x_1x_3+x_2x_4+x_5) \\ &= x_1x_2x_6 + x_1x_3x_6 + x_2x_4x_6 + x_3x_4x_6 + x_1x_2 + x_3x_4 + x_5x_6. \end{aligned}$$

With (7) we similarly obtain

$$F_1^*(x_1,\dots,x_6) = x_1x_2x_5 + x_1x_3x_5 + x_2x_4x_5 + x_3x_4x_5 + x_1x_2 + x_3x_4 + x_5x_6.$$

Using $F_1$ and $F_1^*$ as building blocks we then obtain

$$\begin{aligned} &F_2(x_1,\dots,x_8) = x_1x_2x_5x_8 + x_1x_2x_6x_8 + x_1x_3x_5x_8 + x_1x_3x_6x_8 + \\ &x_2x_4x_5x_8 + x_2x_4x_6x_8 + x_3x_4x_5x_8 + x_3x_4x_6x_8 + x_1x_2x_6 + x_1x_3x_6 + \\ &x_2x_4x_6 + x_3x_4x_6 + x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8 \end{aligned}$$

and the dual

$$\begin{aligned} &F_2^*(x_1,\dots,x_8) = x_1x_2x_5x_7 + x_1x_2x_6x_7 + x_1x_3x_5x_7 + x_1x_3x_6x_7 + \\ &x_2x_4x_5x_7 + x_2x_4x_6x_7 + x_3x_4x_5x_7 + x_3x_4x_6x_7 + x_1x_2x_5 + x_1x_3x_5 + \\ &x_2x_4x_5 + x_3x_4x_5 + x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8, \end{aligned}$$

both bent functions in dimension 8 with algebraic degree 4.

5.2. Constructing bent functions and their duals simultaneously, weakly regular. By using the quadratic functions $f_0 = x_1^2, f_1 = 4x_1^2, f_2 = 4x_1^2, f_3 = x_1^2, f_4 = x_1^2$ from $\mathbb{F}_5$ to $\mathbb{F}_5$, we obtain $F_1$ by construction (6):

$$F_1(x_1,x_2,x_3) = 4x_1^2x_3^4 + x_1^2x_3^3 + x_1^2 + x_2x_3.$$

The functions $f_0, f_1, f_2, f_3, f_4$ are self-dual bent. Then with (7) we similarly obtain

$$F_1^*(x_1,x_2,x_3) = 3x_1^2x_2^4 + x_1^2 + 4x_2x_3.$$

As the coefficients of $x_1^2$ are squares in $\mathbb{F}_5$ for all $f_i$, $i = 0,\cdots,4$, the bent function $F_1$ (and also $F_1^*$) is weakly regular, see [5, Section 5].

By putting $f_0 = f_1 = f_2 = F_1$ and $f_3 = f_4 = 4F_1$, we may continue the construction of bent functions. Since we multiply $F_1$ by squares only, to obtain our functions $f_i$, $i = 0,\cdots,4$, we use for the construction, the resulting bent function and its dual will be weakly regular again. For details we again refer to [5]. We get

$$\begin{aligned}F_2(x_1,x_2,x_3,x_4,x_5) = {} & x_1^2x_3^4x_5^4 + x_1^2x_3^4x_5^4 + 3x_1^2x_3^4x_5 + 4x_1^2x_3^4 + 4x_1^2x_3^3x_5^4 \\ & + 4x_1^2x_3^3x_5^3 + 2x_1^2x_3^3x_5 + x_1^2x_3^3 + 2x_1^2x_3x_5^4 + 2x_1^2x_3x_5^3 \\ & + x_1^2x_3x_5 + 3x_1^2x_3 + 4x_1^2x_5^4 + 4x_1^2x_5^3 + 2x_1^2x_5 + x_1^2 \\ & + 4x_2x_3x_5^4 + 4x_2x_3x_5^3 + 2x_2x_3x_5 + x_2x_3 + x_4x_5,\end{aligned}$$

$$\begin{aligned}F_2^*(x_1,x_2,x_3,x_4,x_5) &= 4\sum_{j=0}^{4}\frac{x_4(x_4-1)(x_4-2)(x_4-3)(x_4-4)}{x_4-j}((f_j)^* - jx_5) \\ &= 4x_1^2x_2^4x_4^4 + 4x_1^2x_2^4x_4^3 + 2x_1^2x_2^4x_4 + 3x_1^2x_2^4 + 2x_1^2x_2^3x_4^4 \\ &+ 2x_1^2x_2^3x_4^3 + x_1^2x_2^3x_4 + x_1^2x_2x_4^4 + x_1^2x_2x_4^3 + 3x_1^2x_2x_4 \\ &+ 4x_1^2x_4^4 + 4x_1^2x_4^3 + 2x_1^2x_4 + x_1^2 + x_2x_3x_4^4 + x_2x_3x_4^3 \\ &+ 3x_2x_3x_4 + 4x_2x_3 + x_4x_5.\end{aligned}$$

Here the dual $(4F_1)^*$ is given by

$$(4F_1)^*(x_1,x_2,x_3) = 4\sum_{j=0}^{4}\frac{x_2(x_2-1)(x_2-2)(x_2-3)(x_2-4)}{x_2-j}((4f_j)^*(x_1) + jx_3).$$

As indicated in Remark 3, a direct way to obtain the dual of $cF$, $c \in \mathbb{F}_p^*$ from the dual $F^*$ of $F$ is shown in the proof of [6, Theorem 1].

### 5.3. Constructing bent functions and their duals simultaneously, non-weakly regular.

Consider the bent functions $f_0 = x_1^2, f_1 = 2x_1^2, f_2 = x_1^2$ from $\mathbb{F}_3$ to $\mathbb{F}_3$, then by Proposition 2 their duals are $f_0^* = 2x_1^2, f_1^* = x_1^2, f_2^* = 2x_1^2$. Using the principle of Lagrange interpolation, from construction (6) we get the bent function

$$\begin{aligned}F_1(x_1,x_2,x_3) \quad = \quad & 2\big((x_3-1)(x_3-2)x_1^2 + x_3(x_3-2)(2x_1^2+x_2) \\ & + x_3(x_3-1)(x_1^2+2x_2)\big) = 2x_1^2x_3^2 + 2x_1^2x_3 + x_2x_3 + x_1^2.\end{aligned}$$

With (7) we get its dual bent function

$$\begin{aligned}F_1^*(x_1,x_2,x_3) \quad = \quad & 2\big((x_2-1)(x_2-2)2x_1^2 + x_2(x_2-2)(x_1^2-x_3) \\ & + x_2(x_2-1)(2x_1^2-2x_3)\big) = x_1^2x_2^2 + x_1^2x_2 + 2x_2x_3 + 2x_1^2.\end{aligned}$$

As the coefficient of $x_1^2$ is the square 1 for $f_0$ and $f_2$, but the coefficient of $x_1^2$ in $f_1$ is the non-square 2, the bent function $F_1$ (and also $F_1^*$) is non-weakly regular, see [5, Section 5].

We may recursively continue for instance putting $f_0 = F_1, f_1 = 2F_1, f_2 = F_1$ and obtain the non-weakly regular bent function $F_2$ and its dual $F_2^*$ from $\mathbb{F}_3^5$ to $\mathbb{F}_3$

$$\begin{aligned}
F_2(x_1, \dots, x_5) &= 2\big((x_5-1)(x_5-2)f_0 + x_5(x_5-2)(f_1+x_4) \\
&+ x_5(x_5-1)(f_2+2x_4)\big) \\
&= x_1^2x_3^2x_5^2 + x_1^2x_3^2x_5 + 2x_1^2x_3^2 + x_1^2x_3x_5^2 + x_1^2x_3x_5 + 2x_1^2x_3 \\
&+ 2x_1^2x_5^2 + 2x_1^2x_5 + x_1^2 + 2x_2x_3x_5^2 + 2x_2x_3x_5 + x_2x_3 + x_4x_5, \\
F_2^*(x_1, \dots, x_5) &= 2\big((x_4-1)(x_4-2)f_0^* + x_4(x_4-2)(f_1^*-x_5) \\
&+ x_4(x_4-1)(f_2^*-2x_5)\big) \\
&= x_1^2x_2^2x_4^2 + x_1^2x_2^2x_4 + x_1^2x_2x_4^2 + x_1^2x_2x_4 + 2x_1^2x_3^2x_4^2 + 2x_1^2x_3^2x_4 \\
&+ 2x_1^2x_3^2 + 2x_1^2x_3x_4^2 + 2x_1^2x_3x_4 + 2x_1^2x_3 + x_1^2 + 2x_2x_3x_4^2 \\
&+ 2x_2x_3x_4 + x_2x_3 + 2x_4x_5.
\end{aligned}$$

Here the dual of $f_1^*(x_1, x_2, x_3) = (2F_1)^*(x_1, x_2, x_3)$ is given by the formula

$$\begin{aligned}
(2F_1)^*(x_1, x_2, x_3) &= 2\big((x_2-1)(x_2-2)x_1^2 + x_2(x_2-2)(2x_1^2-x_3) \\
&\quad + x_2(x_2-1)(x_1^2-2x_3)\big) = 2x_1^2x_2^2 + 2x_1^2x_2 + 2x_2x_3 + x_1^2.
\end{aligned}$$

### 5.4. Bent functions with duals of different algebraic degree.

We choose the bent functions $f_0 = x_1^2, f_1 = x_1^2, f_2 = 2x_1^2, f_3 = x_1^2, f_4 = 4x_1^2$ from $\mathbb{F}_5$ to $\mathbb{F}_5$, then by Proposition 2 their duals are $f_0^* = x_1^2, f_1^* = x_1^2, f_2^* = 3x_1^2, f_3^* = x_1^2, f_4^* = 4x_1^2$. With (6) and (7) we obtain the bent function $F$ and its dual $F^*$ as

$$\begin{aligned}
F(x_1, x_2, x_3) &= x_1^2x_3^4 + x_1^2x_3^3 + 3x_1^2x_3^2 + x_1^2 + x_2x_3, \\
F^*(x_1, x_2, x_3) &= 4x_1^2x_2^3 + 4x_1^2x_2^2 + 2x_1^2x_2 + x_1^2 + 4x_2x_3.
\end{aligned}$$

We observe that $F$ has algebraic degree 6 whereas $F^*$ has algebraic degree only 5, and thus $F$ and $F^*$ are inequivalent. We remark that in the construction of $F^*$ the term of degree 6 cancels, which results from the fact that the coefficients of the functions $f_i^*$ add to 0, i.e. $\sum_{i=0}^4 f_i^* = 0$. Moreover, as the coefficients for some $f_i$ $(f_i^*)$ are squares and some are non-squares in $\mathbb{F}_5$, the bent function $F$ $(F^*)$ is non-weakly regular.

The following example is a weakly regular bent function in characteristic 7 with a dual of different algebraic degree. Let $g_0 = x_1^2, g_1 = x_1^2, g_2 = x_1^2, g_3 = x_1^2, g_4 = 2x_1^2, g_5 = 4x_1^2, g_6 = 4x_1^2$ bent functions on $\mathbb{F}_7$, then their duals are $g_0^* = 5x_1^2, g_1^* = 5x_1^2, g_2^* = 5x_1^2, g_3^* = 5x_1^2, g_4^* = 6x_1^2, g_5^* = 3x_1^2, g_6^* = 3x_1^2$. Note that the functions $g_i$ are chosen so that $\sum_{i=0}^6 g_i = 0$. With (6) and (7) we obtain the weakly regular bent function $G$ of degree 7 and its dual $G^*$ of degree 8

$$\begin{aligned}
G(x_1, x_2, x_3) &= 6\big((x_3-1)(x_3-2)(x_3-3)(x_3-4)(x_3-5)(x_3-6)g_0 \\
&+ x_3(x_3-2)(x_3-3)(x_3-4)(x_3-5)(x_3-6)(g_1+x_2) \\
&+ x_3(x_3-1)(x_3-3)(x_3-4)(x_3-5)(x_3-6)(g_2+2x_2) \\
&+ x_3(x_3-1)(x_3-2)(x_3-4)(x_3-5)(x_3-6)(g_3+3x_2) \\
&+ x_3(x_3-1)(x_3-2)(x_3-3)(x_3-5)(x_3-6)(g_4+4x_2) \\
&+ x_3(x_3-1)(x_3-2)(x_3-3)(x_3-4)(x_3-6)(g_5+5x_2) \\
&+ x_3(x_3-1)(x_3-2)(x_3-3)(x_3-4)(x_3-5)(g_6+6x_2)\big) \\
&= 5x_1^2x_3^5 + 4x_1^2x_3^4 + 5x_1^2x_3^3 + x_1^2x_3^2 + 6x_1^2x_3 + x_1^2 + x_2x_3,
\end{aligned}$$

$$\begin{aligned}
G^*(x_1,x_2,x_3) &= 6\big((x_2-1)(x_2-2)(x_2-3)(x_2-4)(x_2-5)(x_2-6)g_0\\
&+ x_2(x_2-2)(x_2-3)(x_2-4)(x_2-5)(x_2-6)(g_1-x_3)\\
&+ x_2(x_2-1)(x_2-3)(x_2-4)(x_2-5)(x_2-6)(g_2-2x_3)\\
&+ x_2(x_2-1)(x_2-2)(x_2-4)(x_2-5)(x_2-6)(g_3-3x_3)\\
&+ x_2(x_2-1)(x_2-2)(x_2-3)(x_2-5)(x_2-6)(g_4-4x_3)\\
&+ x_2(x_2-1)(x_2-2)(x_2-3)(x_2-4)(x_2-6)(g_5-5x_3)\\
&+ x_2(x_2-1)(x_2-2)(x_2-3)(x_2-4)(x_2-5)(g_6-6x_3)\big)\\
&= 3x_1^2x_2^6+4x_1^2x_2^5+x_1^2x_2^4+2x_1^2x_2^3+2x_1^2x_2^2+2x_1^2x_2+5x_1^2+6x_2x_3.
\end{aligned}$$

5.5. NON-DUAL-BENT FUNCTIONS. To obtain more bent functions for which the dual is not bent, we have to employ one of the known non-dual-bent functions for our construction. An algebraic normal form for the non-weakly regular bent function $g_2(x)$ in Section 2 for $a_0=\xi^{10}\in\mathbb{F}_{3^4}$ is as follows:

$$\begin{aligned}
f_0 &= x_1^2x_2^2+x_1^2x_2x_3+2x_1^2x_2x_4+x_1^2x_3^2+x_1^2x_3x_4+x_1^2x_4^2+2x_1x_2^2x_4+2x_1x_2x_3^2\\
&\quad +x_1x_2x_3x_4+2x_1x_3+2x_1x_4+2x_2^2x_3x_4+x_2^2x_4^2+2x_2^2+x_2x_3+x_3^2x_4^2+x_3^2+2x_4^2.
\end{aligned}$$

Using the quadratic bent functions $f_1=x_1^2+x_2^2+x_3^2+x_4^2$, $f_2=2x_1^2+x_2^2+x_3^2+x_4^2$ together with $f_0$ we obtain the following bent function:

$$\begin{aligned}
F &= 2x_1^2x_2^2x_6^2+x_1^2x_2^2+2x_1^2x_2x_3x_6^2+x_1^2x_2x_3+x_1^2x_2x_4x_6^2+2x_1^2x_2x_4\\
&\quad +2x_1^2x_3^2x_6^2+x_1^2x_3^2+2x_1^2x_3x_4x_6^2+x_1^2x_3x_4+2x_1^2x_4^2x_6^2+x_1^2x_4^2\\
&\quad +x_1^2x_6+x_1x_2^2x_4x_6^2+2x_1x_2^2x_4+x_1x_2x_3^2x_6^2+2x_1x_2x_3^2+2x_1x_2x_3x_4x_6^2\\
&\quad +x_1x_2x_3x_4+x_1x_3x_6^2+2x_1x_3+x_1x_4x_6^2+2x_1x_4+x_2^2x_3x_4x_6^2+2x_2^2x_3x_4\\
&\quad +2x_2^2x_4^2x_6^2+x_2^2x_4^2+x_2^2+2x_2x_4x_6^2+x_2x_4+2x_3^2x_4^2x_6^2+x_3^2x_4^2\\
&\quad +2x_3^2x_6^2+2x_3^2+2x_3x_4x_6^2+x_3x_4+x_4^2x_6^2+x_5x_6.
\end{aligned}$$

Using MAGMA one can confirm that the dual of this function is in fact not bent.

5.6. SELF-DUAL BENT FUNCTIONS. In order to satisfy the conditions of Theorem 3 we choose the quadratic functions $f_0=x_1^2$, $f_1=f_2=f_3=f_4=4x_1^2$, from $\mathbb{F}_5$ to $\mathbb{F}_5$, which are self-dual bent functions. With the construction (6) we obtain the bent function

$$F(x_1,x_2,x_3)=3x_1^2x_3^4+x_1^2+x_2x_3.$$

According to Lemma 1 we may choose $B=\begin{pmatrix}2&1\\3&1\end{pmatrix}$, and we obtain the matrix

$$\mathcal{A}=\begin{pmatrix}1&0&0\\0&2&1\\0&3&1\end{pmatrix}$$

as described in Theorem 3. Applying the coordinate transform defined by this matrix to the bent function $F$ we then obtain the following self-dual bent function:

$$\begin{aligned}
F(\mathcal{A}\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}) &= F(x_1,2x_2+x_3,3x_2+x_3)\\
&= 3x_1^2x_2^4+4x_1^2x_2^3x_3+2x_1^2x_2^2x_3^2+x_1^2x_2x_3^2+3x_1^2x_3^4+x_1^2+x_2^2+x_3^2.
\end{aligned}$$

Note that the dual of $F(\mathcal{A}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix})$ is

$$F^*(x_1, (B^{-1})^T \begin{pmatrix} x_2 \\ x_3 \end{pmatrix}) = F^*(x_1, 4x_2 + 3x_3, x_2 + 3x_3)$$

and $F^*(x_1, x_2, x_3) = 3x_1^2x_2^4 + x_1^2 + 4x_2x_3$.

We finish the article with a remark on bent functions and strongly regular graphs. In [7, 18] it is shown that for weakly regular bent functions $f : \mathbb{F}_p^{2n} \to \mathbb{F}_p$ satisfying

$$f(tx) = t^k f(x) \text{ for all } t \in \mathbb{F}_p \tag{13}$$

for a constant $k$ with $\gcd(k-1, p-1) = 1$, the sets

$$\begin{aligned} D_S &= \{x \in \mathbb{F}_p^{2n} : f(x) \text{ is a nonzero square in } \mathbb{F}_p\}, \\ D_N &= \{x \in \mathbb{F}_p^{2n} : f(x) \text{ is a nonsquare in } \mathbb{F}_p\}, \\ D_0 &= \{x \in \mathbb{F}_p^{2n} \setminus \{0\} : f(x) = 0\}, \end{aligned}$$

are partial difference sets of $\mathbb{F}_p^{2n}$. Their Cayley graphs are strongly regular. In [7] it is pointed out that the sets $D_0, D_N, D_S$ for the non-weakly regular bent function $g_1(x) = \mathrm{Tr}_6(\xi^7 x^{98})$ defined in Section 2, which satisfies (13) for $k = 2$, are not partial difference sets. As this counterexample is a non-weakly regular bent function which is not dual-bent, one may ask the question if the condition of being dual-bent is already sufficient for obtaining partial difference sets. We looked at the following non-weakly regular but dual-bent functions obtained as described in Theorem 2, starting with some quadratic functions. All are in even dimension and satisfy (13) for $k = 2$:

$$\begin{aligned} &F_1(x_1, x_2, x_3, y) = x_1^2y^2 + x_1^2 + x_2^2 + x_3y \in \mathbb{F}_3[x_1, x_2, x_3, y], \\ &F_2(x_1, x_2x_3, y) = 2x_1^2 + 2x_2^2y^2 + 2x_2^2 + x_3y \in \mathbb{F}_3[x_1, x_2, x_3, y] \text{ and} \\ &F_1(x_1, x_2, x_3, y) = 3x_1^2y^4 + x_1^2 + 4x_2^2y^4 + 2x_2^2 + x_3y \in \mathbb{F}_5[x_1, x_2, x_3, y], \\ &F_2(x_1, x_2, x_3, y) = 2x_1^2y^4 + x_1^2 + x_2^2 + x_3y \in \mathbb{F}_5[x_1, x_2, x_3, y]. \end{aligned}$$

With MAGMA we obtained that for all four functions none of the sets $D_0, D_N, D_S$ are partial difference sets, and conclude that in general the weakly regular condition is needed to obtain strongly regular graphs.

## Acknowledgments

We would like to thank the referees very much for their valuable comments and suggestions, in particular for pointing to the existence of non-weakly regular self-dual bent functions in characteristic $p \equiv 3 \bmod 4$ and odd dimension.

## References

[1] C. Carlet, On the secondary constructions of resilient and bent functions, in *Coding, Cryptography and Combinatorics*, Birkhäuser Basel, 2004, 3–28.

[2] C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.*, **15** (1998), 125–156.

[3] C. Carlet, L. E. Danielsen, M. G. Parker and P. Solé, Self-dual bent functions, *Int. J. Inform. Coding Theory*, **1** (2010), 384–399.

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

[5] A. Çeşmelioğlu, G. McGuire and W. Meidl, A construction of weakly and non-weakly regular bent functions, *J. Comb. Theory Ser. A*, **119** (2012), 420–429.

[6] A. Çeşmelioğlu and W. Meidl, A construction of bent functions from plateaued functions, *Des. Codes Cryptogr.*, **66** (2013), 231–242.

[7] Y. M. Chee, Y. Tan and X. D. Zhang, Strongly regular graphs constructed from $p$-ary bent functions, *J. Algebr. Comb.*, **34** (2011), 251–266.

[8] Y. Edel and A. Pott, On the equivalence of nonlinear functions, in *NATO Advanced Research Workshop on Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, Amsterdam, 2009, 87–103.

[9] K. Garaschuk and P. Lisoněk, On ternary Kloosterman sums modulo 12, *Finite Fields Appl.*, **14** (2008), 1083–1090.

[10] F. Göloğlu, G. McGuire and R. Moloney, Ternary Kloosterman sums modulo 18 using Stickelberger's theorem, in *Proceedings of SETA 2010* (eds. C. Carlet and A. Pott), Springer-Verlag, Berlin, 2010, 196–203.

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

[12] T. Helleseth and A. Kholosha, New binomial bent functions over the finite fields of odd characteristic, *IEEE Trans. Inform. Theory*, **56** (2010), 4646–4652.

[13] T. Helleseth and A. Kholosha, Crosscorrelation of m-sequences, exponential sums, bent functions and Jacobsthal sums, *Cryptogr. Commun.*, **3** (2011), 281–291.

[14] X. D. Hou, Classification of self dual quadratic bent functions, *Des. Codes Cryptogr.*, **63** (2012), 183–198.

[15] K. P. Kononen, M. J. Rinta-aho and K. O. Väänänen, On integer values of Kloosterman sums, *IEEE Trans. Inform. Theory*, **56** (2010), 4011–4013.

[16] N. G. Leander, Monomial bent functions, *IEEE Trans. Inform. Theory*, **52** (2006), 738–743.

[17] R. Lidl and H. Niederreiter, *Finite Fields*, Second edition, Cambridge Univ. Press, Cambridge, 1997.

[18] Y. Tan, A. Pott and T. Feng, Strongly regular graphs associated with ternary bent functions, *J. Comb. Theory Ser. A*, **117** (2010), 668–682.

[19] Y. Tan, J. Yang and 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, 156–159.

Received July 2012; revised March 2013.

*E-mail address:* cesmelio@ovgu.de
*E-mail address:* wmeidl@sabanciuniv.edu
*E-mail address:* alexander.pott@ovgu.de