There are infinitely many bent functions for which the dual is not bent

Ayça Çeşmelioğlu[a], Wilfried Meidl[b], Alexander Pott[c]

[a] İstanbul Kemerburgaz University, School of Arts and Sciences, Bağcılar, 34217 İstanbul, Turkey. e-mail: ayca.cesmelioglu@kemerburgaz.edu.tr
[b] Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria. e-mail: meidlwilfried@gmail.com
[c] Otto-von-Guericke-University, Faculty of Mathematics, 39106 Magdeburg, Germany. e-mail: alexander.pott@ovgu.de

Abstract

Bent functions can be classified into regular bent functions, weakly regular but not regular bent functions, and non-weakly regular bent functions. Regular and weakly regular bent functions always appear in pairs since their duals are also bent functions. In general this does not apply to non-weaky regular bent functions. However, the first known construction of non-weakly regular bent functions by Ceşmelioğlu et *al.*, 2012, yields bent functions for which the dual is also bent. In this paper the first construction of non-weakly regular bent functions for which the dual is not bent is presented. We call such functions non-dual-bent functions. Until now, only sporadic examples found via computer search were known. We then show that with the direct sum of bent functions and with the construction by Ceşmelioğlu et *al.* one can obtain infinitely many non-dual-bent functions once one example of a non-dual-bent function is known.

1 Introduction

For a prime p, let f be a function from an n-dimensional vector space V_n over $\mathbb{F}_p$ to $\mathbb{F}_p$. The *Walsh transform* of f is the complex valued function

$$\widehat{f}(b) = \sum_{x \in V_n} \epsilon_p^{f(x)-\langle b,x\rangle}, \quad \epsilon_p = e^{2\pi i/p},$$

where $\langle b, x\rangle$ is a (nondegenerate) inner product in V_n. The function f is called a *bent function* if $|\widehat{f}(b)| = p^{n/2}$ for all $b \in V_n$. For Boolean bent functions we have $\widehat{f}(b) = (-1)^{f^*(b)}2^{n/2}$ for a Boolean function f^*, called the

dual of f. When p is odd, then a bent function f satisfies (cf. [8])

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

for a function f^* from V_n to $\mathbb{F}_p$. Accordingly f is called *regular* if $p^{-n/2}\widehat{f}(b) = \epsilon_p^{f^*(b)}$ for all $b \in V_n$, which for a Boolean bent function always holds. If $p^{-n/2}\widehat{f}(b) = \zeta\ \epsilon_p^{f^*(b)}$ for some $\zeta \in \{\pm 1, \pm i\}$, independent from b, we call f *weakly regular*, otherwise f is called *non-weakly regular*. Note that regular implies weakly regular.

Weakly regular bent functions f always appear in pairs, as also the dual f^* of f is bent. We restate here the argument in [8], see also [5]:
For $y \in V_n$ we get

$$\sum_{b\in V_n} \epsilon_p^{\langle b,y\rangle}\widehat{f}(b) = \sum_{b\in V_n} \epsilon_p^{\langle b,y\rangle} \sum_{x\in V_n} \epsilon_p^{f(x)-\langle b,x\rangle} = \sum_{x\in V_n} \epsilon_p^{f(x)} \sum_{b\in V_n} \epsilon_p^{\langle b,(y-x)\rangle} = p^n\epsilon_p^{f(y)}, \tag{2}$$

a special case of *Poisson Summation Formula*. We now use that f is weakly regular, hence $\widehat{f}(b) = \zeta p^{n/2}\epsilon_p^{f^*(b)}$, with ζ fixed, independent from b. Then

$$p^n\epsilon_p^{f(y)} = \zeta p^{n/2} \sum_{b\in V_n} \epsilon_p^{f^*(b)+\langle b,y\rangle} = \zeta p^{n/2}\widehat{f^*}(-y).$$

Consequently

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

and therefore f^* is weakly regular bent.

All classical constructions of bent functions yield weakly regular bent functions. The first sporadic examples of non-weakly regular bent functions, all in characteristic 3 and found by computer search, appeared in [8], [9] and [10]. In [11], it was observed that one can obtain more examples in dimension $m+n$ with the direct sum $F(x,y) = f(x) + g(y)$ if one chooses for f a (weakly) regular bent function in dimension m and for g a non-weakly regular bent function in dimension n. The first construction of infinite classes of non-weakly regular bent functions was given in [2], and further analysed in [3, 4, 5, 6]. The results indicate that though the "obvious" constructions yield (weakly) regular bent functions, being non-weakly regular is not at all an exceptional property for a bent function (in odd characteristic).

In [5] it was observed that the construction of non-weakly regular bent functions in [2], which uses previously known bent functions in dimension n to obtain one bent function in dimension $n+2$, yields bent functions for

which the dual is also a bent function. On the other hand, some of the found sporadic examples of non-weakly regular bent functions do not have a bent dual:

1. $g_1 : \mathbb{F}_{3^6} \to \mathbb{F}_3$ with $g_1(x) = \mathrm{Tr}_6(\xi^7 x^{98})$, where ξ is a primitive element of $\mathbb{F}_{3^6}$, see [8],

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 ξ is a primitive element of $\mathbb{F}_{3^4}$, see [9],

3. $g_3 : \mathbb{F}_{3^6} \to \mathbb{F}_3$ with $g_5(x) = \mathrm{Tr}_6(\xi^7 x^{14} + \xi^{35} x^{70})$, where ξ is a primitive element of $\mathbb{F}_{3^6}$, see [10].

Following this observation, in [5] a new concept of bent functions was introduced: A bent function f is called a *dual-bent function* if the dual function f^* defined as in (1) is also bent. Otherwise we call f a *non-dual-bent function*. Clearly every weakly regular bent function is a dual-bent function, but the converse does not hold.

For all types of dual-bent functions, regular, weakly regular but not regular, and non-weakly regular but dual-bent, we know constructions. What is missing, is a theoretical construction of non-dual-bent functions, i.e. a construction of bent functions for which the dual is not a bent function.

The objective of this paper is to close this gap, presenting the first construction of bent functions which yields non-dual-bent functions. In Section 2 we present a construction of bent functions which can be seen as an extension of the direct sum. In Section 3 we show that this construction in general yields non-dual-bent functions, and we give some examples of non-dual-bent functions. In Section 4 we show that with the direct sum of bent functions and with the construction in [2] one can obtain infinitely many non-dual-bent functions once one example of a non-dual-bent function is constructed.

2 A semi-direct sum of bent functions

A simple construction of a new bent function from two given bent functions is the *direct sum* of a bent function f from V_m to $\mathbb{F}_p$ and a bent function g from V_n to $\mathbb{F}_p$, which is the function $F : V_m \times V_n \to \mathbb{F}_p$ defined as $F(x, y) = f(x) + g(y)$. It is straightforward to determine that

$$\widehat{F}(a, b) = \widehat{f}(a)\widehat{g}(b).$$

In this section we present an extension of this secondary construction which we may call the *semi-direct sum* of two bent functions f and g. We will employ this semi-direct sum in the next section to provide the first construction of non-dual-bent functions.

Theorem 1. *Let $f : V_m \to \mathbb{F}_p$ and $g : V_n \to \mathbb{F}_p$ be bent, and let h be a function from V_m to V_n. The function $F : V_m \times V_n \to \mathbb{F}_p$ defined as*

$$F(x, y) = f(x) + g(y + h(x)) \tag{4}$$

is bent if and only if for all $b \in V_n$ the function $G_b : V_m \to \mathbb{F}_p$

$$G_b(x) = f(x) + \langle b, h(x)\rangle$$

is a bent function. The dual F^* of F is then

$$F^*(x, y) = G_y^*(x) + g^*(y).$$

Proof. For $a \in V_m$ and $b \in V_n$ we have

$$\begin{aligned}
\widehat{F}(a, b) &= \sum_{x\in V_m, y\in V_n} \epsilon_p^{f(x)+g(y+h(x))-\langle a,x\rangle-\langle b,y\rangle} \\
&= \sum_{x\in V_m} \epsilon_p^{f(x)-\langle a,x\rangle} \sum_{y\in V_n} \epsilon_p^{g(y)-\langle b,y-h(x)\rangle} \\
&= \sum_{x\in V_m} \epsilon_p^{f(x)+\langle b,h(x)\rangle-\langle a,x\rangle} \sum_{y\in V_n} \epsilon_p^{g(y)-\langle b,y\rangle} \\
&= \widehat{G_b}(a)\widehat{g}(b). \qquad (5)
\end{aligned}$$

Since g is bent, i.e. $\widehat{g}(b) = \zeta p^{n/2}\epsilon_p^{g^*(b)}$ for some $\zeta \in \{\pm 1, \pm i\}$ (which may depend on b), the function F is bent if and only if $|\widehat{G_b}(a)| = p^{m/2}$ for all $a \in V_m$ and $b \in V_n$, or equivalently G_b is bent for all $b \in V_n$. Then

$$\widehat{F}(a, b) = \zeta p^{(m+n)/2}\epsilon_p^{G_b^*(a)+g^*(b)}$$

for some $\zeta \in \{\pm 1, \pm i\}$ (which may depend on a and b), and the formula for the dual F^* follows. □

Remark 1. *If h is the zero function, then the condition in Theorem 1 trivially holds and the semi-direct sum reduces to the direct sum.*

Remark 2. *In [1], Carlet presented the special case of the construction in Theorem 1 where $p = 2$ and g is the quadratic Maiorana-McFarland bent function $g(x) = x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, n even. The function $F : V_m \times \mathbb{F}_2^n \to \mathbb{F}_2$ is then of the form*

$$F(x, y_1, \ldots, y_n) = f(x) + \sum_{i=1}^{n/2} (y_{2i-1} + h_{2i-1}(x))(y_{2i} + h_{2i}(x)) \qquad (6)$$

for some functions $h_1, \ldots, h_n$ from V_m to $\mathbb{F}_2$.

3 Bent functions for which the dual is not bent

We first present some examples of bent functions from $V_m \times \mathbb{F}_p^n$ to $\mathbb{F}_p$ obtained with the semi-direct sum. Note that to satisfy the conditions in Theorem 1 we need a bent function $f : V_m \to \mathbb{F}_p$ and a function $h(x) = (h_1(x), h_2(x), \ldots, h_n(x))$ from V_m to $\mathbb{F}_p^n$ such that for all $\Lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}_p^n$ the function

$$G_\Lambda(x) = f(x) + \Lambda \cdot h(x) = f(x) + \lambda_1 h_1(x) + \lambda_2 h_2(x) + \cdots + \lambda_n h_n(x)$$

is bent. To generate such functions $f, h_1, \ldots, h_n$ from V_m to $\mathbb{F}_p$ we will employ vectorial bent functions from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. Hence in this section V_m will be identified with the finite field $\mathbb{F}_{p^m}$. Examples for vectorial bent functions are quadratic PN-functions of which the simplest are quadratic monomials, or the Coulter-Matthews functions for $p = 3$.

Lemma 1 (Lemma 2 and Corollary 3 in [8])**.** *Let m and $0 \le k \le m$ be integers such that $m/\gcd(m, k)$ is odd. For a nonzero $\alpha \in \mathbb{F}_{p^m}$ let f_α be the function $f_\alpha(x) = \mathrm{Tr}_m(\alpha x^{p^k+1})$ from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. Then*

$$\widehat{f_\alpha}(u) = \begin{cases} \eta(\alpha)(-1)^{m-1} p^{m/2} \epsilon_p^{f_\alpha^*(u)} & : \quad p \equiv 1 (\mathrm{mod} 4) \\ \eta(\alpha)(-1)^{m-1} i^m p^{m/2} \epsilon_p^{f_\alpha^*(u)} & : \quad p \equiv 3 (\mathrm{mod} 4), \end{cases}$$

where $\eta(\alpha)$ denotes the quadratic character of α in $\mathbb{F}_{p^m}$.

Lemma 2 (see Lemma 2 in [7] and Proposition 2 in [6])**.** *Let m, k be positive integers such that $\gcd(2m, k) = 1$. For each $\alpha \in \mathbb{F}_{3^m}^*$, the Walsh transform $\widehat{f_\alpha}$ of the weakly regular bent function $f_\alpha(x) = \mathrm{Tr}_m(\alpha x^{\frac{3^k+1}{2}})$ satisfies*

$$\widehat{f_\alpha}(u) = \eta(\alpha)(-1)^{m-1} i^m 3^{m/2} \epsilon_3^{f_\alpha^*(u)},$$

where $\eta(\alpha)$ denotes the quadratic character of α in $\mathbb{F}_{3^m}$.

Corollary 1. *For integers m and n, $2 \leq n < m$, and let $\alpha_0, \alpha_1, \ldots, \alpha_n \in \mathbb{F}_{p^m}$ be linearly independent over $\mathbb{F}_p$, and let g be a weakly regular bent function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. Let*

- *$G(x) = x^{p^k+1}$ for some integer $0 \leq k \leq m$ such that $m/\gcd(m,k)$ is odd, and $f_{\alpha_j}(x) = \mathrm{Tr}_m(\alpha_j G(x))$, $0 \leq j \leq n$, or*

- *$p = 3$ and $G(x) = x^{\frac{3^k+1}{2}}$ for an integer k such that $\gcd(2m,k) = 1$ and $f_{\alpha_j}(x) = \mathrm{Tr}_m(\alpha_j G(x))$, $0 \leq j \leq n$.*

Then $F : \mathbb{F}_{p^m} \times \mathbb{F}_p^n \to \mathbb{F}_p$

$$F(x, y_1, \ldots, y_n) = f_{\alpha_0}(x) + g(y_1 + f_{\alpha_1}(x), y_2 + f_{\alpha_2}(x), \ldots, y_n + f_{\alpha_n}(x)).$$

is a bent function, which in general is non-weakly regular.

Proof. Clearly, F is the bent function (4) for $f = f_{\alpha_0}$ and $h_j = f_{\alpha_j}$, $1 \leq j \leq n$. Note that $G_{\lambda_1,\ldots,\lambda_n}(x) = \mathrm{Tr}_m((\alpha_0 + \sum_{j=1}^n \lambda_j \alpha_j) G(x))$ is bent since the elements α_j are chosen to be linearly independent, hence $\alpha_0 + \sum_{j=1}^n \lambda_j \alpha_j \neq 0$. To see that F is non-weakly regular, we choose $\lambda_1, \ldots, \lambda_n$ and $\bar{\lambda}_1, \ldots, \bar{\lambda}_n$ such that $\Lambda = \alpha_0 + \sum_{j=1}^n \lambda_j \alpha_j$ is a square and $\bar{\Lambda} = \alpha_0 + \sum_{j=1}^n \bar{\lambda}_j \alpha_j$ is a non-square in $\mathbb{F}_{p^m}$. Clearly in general such Λ, $\bar{\Lambda}$ exist. With Lemma 1 respectively Lemma 2, and the assumption that $\eta(\Lambda) \neq \eta(\bar{\Lambda})$, the non-weak regularity of F follows from (5) together with the weak regularity of g. □

In the remainder of this section we show that in general the construction in Theorem 1 yields bent functions for which the dual is not bent. Our functions are the first theoretically constructed non-dual-bent functions. We follow the approach of Corollary 1 where we employ vectorial bent functions for our construction. For simplicity we choose $n = 2$ and $G(x) = x^2$ and $g(y_1, y_2) = y_1 y_2$. Then

$$F(x, y_1, y_2) = f(x) + (y_1 + h_1(x))(y_2 + h_2(x))$$

where $f(x) = \mathrm{Tr}_m(x^2)$, $h_1(x) = \mathrm{Tr}_m(\alpha x^2)$, $h_2(x) = \mathrm{Tr}_m(\beta x^2)$ and $1, \alpha, \beta$ are linearly independent over $\mathbb{F}_p$ (we take $\alpha_0 = 1$, $\alpha_1 = \alpha$, $\alpha_2 = \beta$). As an application of Theorem 1 we obtain the subsequent corollary.

Corollary 2. *Let $1, \alpha, \beta \in \mathbb{F}_{p^m}$ be linearly independent over $\mathbb{F}_p$. If*

$$\Big| \sum_{y_1, y_2 \in \mathbb{F}_p} \eta(1 + y_1\alpha + y_2\beta) \epsilon_p^{-y_1 y_2} \Big| \neq p, \tag{7}$$

then the function $F : \mathbb{F}_{p^m} \times \mathbb{F}_p^2$

$$F(x, y_1, y_2) = \mathrm{Tr}_m(x^2) + (y_1 + \mathrm{Tr}_m(\alpha x^2))(y_2 + \mathrm{Tr}_m(\beta x^2)) \tag{8}$$

is a non-dual-bent function.

Proof. Observing that $g^*(y_1, y_2) = -y_1 y_2$, the dual of F is

$$F^*(x, y_1, y_2) = G^*_{y_1,y_2}(x) - y_1 y_2$$

where $G^*_{y_1,y_2}(x)$ is the dual of $G_{y_1,y_2}(x) = \mathrm{Tr}_m((1 + y_1\alpha + y_2\beta)x^2)$. By [8, Corollary 3],

$$G^*_{y_1,y_2}(x) = -\mathrm{Tr}_m(\frac{x^2}{4(1 + y_1\alpha + y_2\beta)}).$$

Furthermore,

$$G^{**}_{y_1,y_2}(x) = G_{y_1,y_2}(-x) = \mathrm{Tr}_m((1 + y_1\alpha + y_2\beta)x^2) = G_{y_1,y_2}(x).$$

We determine the Walsh coefficient of F^* at $(0, 0, 0)$:

$$\begin{aligned}
\widehat{F^*}(0,0,0) &= \sum_{\substack{x\in\mathbb{F}_{p^m}\\ y_1,y_2\in\mathbb{F}_p}} \epsilon_p^{G^*_{y_1,y_2}(x)-y_1y_2} = \sum_{y_1,y_2\in\mathbb{F}_p} \epsilon_p^{-y_1y_2} \sum_{x\in\mathbb{F}_{p^m}} \epsilon_p^{G^*_{y_1,y_2}(x)} \\
&= \sum_{y_1,y_2\in\mathbb{F}_p} \epsilon_p^{-y_1y_2} \widehat{G^*_{y_1,y_2}}(0) = \zeta p^{m/2} \sum_{y_1,y_2\in\mathbb{F}_p} \epsilon_p^{-y_1y_2} \eta(1 + y_1\alpha + y_2\beta) \epsilon_p^{G^{**}_{y_1,y_2}(0)} \\
&= \zeta p^{m/2} \sum_{y_1,y_2\in\mathbb{F}_p} \eta(1 + y_1\alpha + y_2\beta)\epsilon_p^{-y_1y_2},
\end{aligned}$$

where $\zeta \in \{\pm 1, \pm i\}$ only depends on p and m, see Lemma 1. As a consequence, if

$$|\sum_{y_1,y_2\in\mathbb{F}_p} \eta(1 + y_1\alpha + y_2\beta)\epsilon_p^{-y_1y_2}| \neq p,$$

then F^* is not bent. □

Condition (7) combines the additive and the multiplicative structure of the finite field and is therefore not easy to analyse. If all values for $1+\lambda_1\alpha+\lambda_2\beta$, $\lambda_1, \lambda_2 \in \mathbb{F}_p$, have the same quadratic character, then F is weakly regular, hence a dual-bent function. As obvious, in this case the character sum in (7) has in fact absolute value p. Clearly with a random choice of α, β this is quite unlikely, and one also would expect a chaotic behaviour of the character sum in (7). In particular it seems that its absolute value is rarely p. Below are some examples of non-dual-bent functions obtained with Corollary 2 for $p = 3$ and for $p = 5$.

Example 1. *Let $p = 3, m = 3$, and let w be a root of the irreducible polynomial $g(x) = x^3 + x^2 + 2 \in \mathbb{F}_3[x]$. For both choices*

(i) $\alpha = w$, $\beta = w^2 + 1$,

(ii) $\alpha = 2w + 1$, $\beta = w^2$

the character sum in (7) *has absolute value* $\sqrt{3}$. *Hence in both cases the dual of the bent function* $F(x, y_1, y_2) = \mathrm{Tr}_3(x^2) + (y_1 + \mathrm{Tr}_3(\alpha x^2))(y_2 + \mathrm{Tr}_3(\beta x^2))$ *from* $\mathbb{F}_{3^3} \times \mathbb{F}_3^2 \to \mathbb{F}_3$ *is not a bent function.*

Example 2. *Let* $w \in \mathbb{F}_{3^4}$ *be a root of the irreducible polynomial* $g(x) = x^4 + x^3 + 2 \in \mathbb{F}_3[x]$. *For* $\alpha = w$ *and* $\beta = w^2$ *we have* $|\sum_{y_1,y_2 \in \mathbb{F}_3} \eta(1 + y_1\alpha + y_2\beta)\epsilon_p^{-y_1y_2}| = |1 - 2\sqrt{3}i| = \sqrt{13} \neq 3$. *Hence the dual of the bent function* $F(x, y_1, y_2) = T_3(x^2) + (y_1 + \mathrm{Tr}_3(wx^2))(y_2 + \mathrm{Tr}_3(w^2x^2))$ *from* $\mathbb{F}_{3^4} \times \mathbb{F}_3^2$ *to* $\mathbb{F}_3$ *is not bent.*

Example 3. *Let* $w \in \mathbb{F}_{5^3}$ *be a root of the irreducible polynomial* $g(x) = x^3 + x + 1$, *let* $\alpha = \omega$, $\beta = \omega^2$, *and let* F *be the bent function from* $\mathbb{F}_{5^3} \times \mathbb{F}_5^2$ *to* $\mathbb{F}_5$ *given by* $F(x, y_1, y_2) = T_5(x^2) + (y_1 + \mathrm{Tr}_5(wx^2))(y_2 + \mathrm{Tr}_5(w^2x^2))$. *Since* $|\sum_{y_1,y_2 \in \mathbb{F}_5} \eta(1 + y_1\alpha + y_2\beta)\epsilon_p^{-y_1y_2}| = |4\epsilon_5^4 - 4\epsilon_5 + 1| \neq 5$, *the dual of* F *is not a bent function. We remark that all previously known sporadic examples of non-dual-bent functions are in characteristic* 3. *With our choice of* α *and* β, *checking the condition in Corollary 2 without difficulty we constructed a non-dual-bent function in characteristic* 5.

We add an example of a bent function of the form (8) for which the absolute value of the character sum in Corollary 2 equals p.

Example 4. *Let* $w \in \mathbb{F}_{3^3}$ *be as in Example 1, and choose* $\alpha = w$ *and* $\beta = w^2$. *In this case we have* $|\sum_{y_1,y_2 \in \mathbb{F}_3} \eta(1 + y_1\alpha + y_2\beta)\epsilon_p^{-y_1y_2}| = 3$. *Hence for the corresponding bent function* F *we have* $|\widehat{F}(0)| = 3^{5/2}$, *and* F *may or may not have a bent dual. Using Magma we confirmed that the dual of* F *is again not a bent function.*

4 Recursively constructing non-dual-bent functions

In this section we show that once a non-dual-bent function is constructed, one can recursively obtain infinitely many with the direct sum and the construction in [2]. We emphasize that these secondary constructions of bent functions cannot provide non-dual-bent functions if one does not use a bent function as building block which is already non-dual.

Recall that for two functions $f : V_m \to \mathbb{F}_p$ and $g : V_n \to \mathbb{F}_p$ the direct sum $F : V_m \times V_n \to \mathbb{F}_p$ is defined as $F(x, y) = f(x) + g(y)$. As easily seen

$$\widehat{F}(a, b) = \widehat{f}(a)\widehat{g}(b).$$

In particular if f and g are bent, then F is bent, and

$$\widehat{F}(a, b) = \zeta_{a,b} p^{\frac{m+n}{2}} \epsilon_p^{f^*(a)+g^*(b)}$$

for some $\zeta_{a,b} \in \{\pm 1, \pm i\}$. Hence the dual of F is $F^*(x, y) = f^*(x) + g^*(y)$.

Theorem 2. *The direct sum of a dual-bent function and a non-dual-bent function is a non-dual-bent function.*

Proof. Suppose that f^* is bent but g^* is not, hence $|\widehat{g^*}(b)| = A \neq p^{n/2}$ for some $b \in V_n$. Then

$$|\widehat{F^*}(a, b)| = p^{m/2} A \neq p^{(m+n)/2}$$

for all $a \in V_m$, which finishes the proof. □

Now we consider the construction introduced in [2] and further investigated in [3, 4, 5, 6], which combines p bent functions from V_n to $\mathbb{F}_p$ to one bent function in dimension $n + 2$. We follow the notation in [5] and use the multivariate representation, i.e. we represent V_n as $\mathbb{F}_p^n$.

Proposition 1. *For $j = 0, \ldots, p-1$ let f_j be functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. The function $F : \mathbb{F}_p^{n+2} \to \mathbb{F}_p$ defined as*

$$F(x, x_{n+1}, y) = f_y(x) + x_{n+1} y$$

is bent if and only if for all $0 \leq j \leq p-1$ the function f_j is bent.

Proof. By definition, F is bent if for all $a \in \mathbb{F}_p^n$, $b, c \in \mathbb{F}_p$ the Walsh transform $\widehat{F}(a, b, c)$ has absolute value $p^{(n+2)/2}$. For $a \in \mathbb{F}_p^n$, $b, c \in \mathbb{F}_p$ we have

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

Consequently $|\widehat{F}(a,b,c)| = p^{(n+2)/2}$ for all $a \in \mathbb{F}_p^n$, $b,c \in \mathbb{F}_p$ if and only if $|\widehat{f_b}(a)| = p^{n/2}$ for all $a \in \mathbb{F}_p^n$, $b \in \mathbb{F}_p$, which applies if and only if f_b is bent for all $0 \leq b \leq p-1$. □

We observe that if f_b, $0 \leq b \leq p-1$, is bent, then $\widehat{F}(a,b,c) = p^{\frac{n+2}{2}} \zeta \epsilon_p^{f_b^*(a)-bc}$. Consequently, as also observed in [5], the dual of the bent function F

$$F^*(x, x_{n+1}, y) = f^*_{x_{n+1}}(x) - x_{n+1}y, \tag{9}$$

is obtained with the same construction method from f_j^*, $0 \leq j \leq p-1$, (the roles of the variables x_{n+1} and y are interchanged). With those observations and Proposition 1 we get the following theorem.

Theorem 3. *For $j = 0, \ldots, p-1$ let f_j be bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. The bent function $F : \mathbb{F}_p^{n+2} \to \mathbb{F}_p$ defined as*

$$F(x, x_{n+1}, y) = f_y(x) + x_{n+1}y$$

is dual-bent if and only if for all $0 \leq j \leq p-1$ the function f_j is dual-bent.

5 Concluding remarks

In the literature many constructions and explicit representations of bent functions, also in odd characteristic, can be found. Almost all of them describe (weakly) regular bent functions. In [2] the first construction of infinite classes of non-weakly regular bent functions has been presented. This construction combines regular and weakly regular (but not regular) bent functions in dimension n, of which many infinite classes are known, to one non-weakly regular bent function in $n+2$ variables. As observed in [5], the resulting bent functions are dual-bent, a property which non-weakly regular bent functions do not necessarily have. In this article the first theoretical construction of non-dual-bent functions is presented. Moreover we show that with the direct sum of bent functions and with the construction in [2], recursively one can obtain infinitely many non-dual-bent functions once one example of a non-dual-bent function is known. Our results indicate that being non-dual-bent is not an exceptional property for a bent function.

Acknowledgement. The second author is supported by the Austrian Science Fund (FWF) Project no. M 1767-N26.

References

[1] C. Carlet, A transformation on Boolean functions, its consequences on some problems related to Reed-Muller codes. Eurocode '90 (Udine, 1990), 42–50, Lecture Notes in Comput. Sci., 514, Springer, Berlin, 1991

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

[3] A. Çeşmelioğlu and W. Meidl, Bent functions of maximal degree. IEEE Trans. Inform. Theory 58 (2012), 1186–1190.

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

[5] A. Çeşmelioğlu, W. Meidl, A. Pott On the dual of (non)-weakly regular bent functions and self-dual bent functions, Advances in Mathematics of Communications **7** (2013), no.4, 425–440.

[6] A. Çeşmelioğlu, W. Meidl, A. Pott, Generalized Maiorana-McFarland class and normality of p-ary bent functions, Finite Fields Appl. 24 (2013), 105–117.

[7] K. Feng, J. Luo, Value distributions of exponential sums from perfect nonlinear functions and their applications, IEEE Trans. Inform. Theory 53 (2007), no. 9, 3035–3041.

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

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

[10] T. Helleseth, A. Kholosha, Crosscorrelation of m-sequences, exponential sums, bent functions and Jacobsthal sums, Cryptogr. Commun., **3** (2011), no. 4, 281–291.

[11] Y. Tan, J. Yang, X. Zhang, A recursive approach to construct p-ary bent functions which are not weakly regular, In: Proceedings of IEEE

International Conference on Information Theory and Information Security, Beijing, 2010, 156–159.