Cryptography and Communications (2020) 12:899–912
https://doi.org/10.1007/s12095-020-00444-0

Vectorial bent functions in odd characteristic and their components

Ayça Çeşmelioğlu[1] · Wilfried Meidl[2] · Alexander Pott[3]

Received: 19 September 2019 / Accepted: 18 June 2020 / Published online: 15 July 2020

Abstract
Bent functions in odd characteristic can be either (weakly) regular or non-weakly regular. Furthermore one can distinguish between dual-bent functions, which are bent functions for which the dual is bent as well, and non-dual bent functions. Whereas a weakly regular bent function always has a bent dual, a non-weakly regular bent function can be either dual-bent or non-dual-bent. The classical constructions (like quadratic bent functions, Maiorana-McFarland or partial spread) yield weakly regular bent functions, but meanwhile one knows constructions of infinite classes of non-weakly regular bent functions of both types, dual-bent and non-dual-bent. In this article we focus on vectorial bent functions in odd characteristic. We first show that most p-ary bent monomials and binomials are actually vectorial constructions. In the second part we give a positive answer to the question if non-weakly regular bent functions can be components of a vectorial bent function. We present the first construction of vectorial bent functions of which the components are non-weakly regular but dual-bent, and the first construction of vectorial bent functions with non-dual-bent components.

Keywords Vectorial bent functions

Mathematics Subject Classification (2010) 94B25 · 11T71

This article belongs to the Topical Collection: *Boolean Functions and Their Applications IV*
Guest Editors: Lilya Budaghyan and Tor Helleseth

✉ Ayça Çeşmelioğlu
ayca.gul@bilgi.edu.tr

Wilfried Meidl
meidlwilfried@gmail.com

Alexander Pott
alexander.pott@ovgu.de

[1] İstanbul Bilgi University, Hacıahmet Mahallesi Pir Hüsamettin Sokak No:20, Beyoğlu, 34440 İstanbul, Turkey

[2] Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria

[3] Otto von Guericke University, Faculty of Mathematics, 39106 Magdeburg, Germany

1 Introduction

Let p be a prime, and $\mathbb{V}_n$ be an n-dimensional vector space over the prime field $\mathbb{F}_p$. A function $f : \mathbb{V}_n \to \mathbb{F}_p$ is called a *bent function* if its *Walsh transform*

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

has absolute value $p^{n/2}$ for all $b \in \mathbb{V}_n$, where $\langle b, x\rangle$ denotes a (nondegenerate) inner product of $\mathbb{V}_n$ (if $\mathbb{V}_n = \mathbb{F}_p^n$, one may take the conventional dot product, the standard inner product for $\mathbb{V}_n = \mathbb{F}_{p^n}$ is $\langle b, x\rangle = \mathrm{Tr_n}(bx)$, where $\mathrm{Tr_n}(z)$ denotes the absolute trace of $z \in \mathbb{F}_{p^n}$).

If $p = 2$, then $\widehat{f}(b)$ is an integer, hence Boolean bent functions only exist for even dimensions n. Note that then $\widehat{f}(b) = 2^{n/2}(-1)^{f^*(b)}$ for a Boolean function f^*, called the *dual* of f. Bent functions from $\mathbb{V}_n$ to $\mathbb{F}_p$, p odd, which we will call *p-ary bent functions*, exist for even and for odd n. For a p-ary bent function, the *Walsh coefficient* $\widehat{f}(b)$ at $b \in \mathbb{V}_n$ of f always satisfies (see [1])

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

where i is a complex primitive 4-th root of unity, and f^* is a function from $\mathbb{V}_n$ to $\mathbb{F}_p$, which again is called the dual of f.

A bent function $f : \mathbb{V}_n \to \mathbb{F}_p$ is called *weakly regular* if, for all $b \in \mathbb{V}_n$, we have $\widehat{f}(b) = \zeta\, \epsilon_p^{f^*(b)} p^{n/2}$ for some $\zeta \in \{\pm 1, \pm i\}$, cf. Equation (1). If $\zeta = 1$ we call f *regular*, which trivially applies if $p = 2$. If (the sign of) ζ changes with $b \in \mathbb{V}_n$, then f is called *non-weakly regular* bent. Weakly regular bent functions f belong to the class of *dual-bent functions*, for which the dual f^* is bent as well. A non-weakly regular bent function can be either dual-bent or *non-dual-bent*, see [2, 3].

Let $\mathbb{V}_n$ and $\mathbb{V}_m$ be vector spaces over $\mathbb{F}_p$. A function $F : \mathbb{V}_n \to \mathbb{V}_m$ is called *vectorial bent* if the *extended Walsh transform*

$$\widehat{F}(u, v) = \sum_{x \in \mathbb{V}_n} \epsilon_p^{\langle v, F(x)\rangle_m - \langle u,x\rangle_n}$$

has absolute value $p^{n/2}$ for all $u \in \mathbb{V}_n$ and nonzero $v \in \mathbb{V}_m$, where $\langle , \rangle_m$ and $\langle , \rangle_n$ denote an inner product of $\mathbb{V}_m$ and $\mathbb{V}_n$, respectively. Hence $F : \mathbb{V}_n \to \mathbb{V}_m$ is vectorial bent if and only if every *component function* $F_v = \langle v, F\rangle_m$, $v \neq 0$, from $\mathbb{V}_n$ to $\mathbb{F}_p$ is a bent function. The set of component functions together with the 0-function is then an m-dimensional vector space of bent functions from $\mathbb{V}_n$ to $\mathbb{F}_p$. As is well known, for a vectorial bent function $F : \mathbb{V}_n \to \mathbb{V}_m$ we always have $m \leq n/2$ if all component functions are regular (which in particular applies if $p = 2$), see [4]. Otherwise we have $m \leq n$, and if equality holds, then F is called a *planar function*.

The goal of this paper is to investigate the structure of component functions of vectorial bent functions. At first view it seems that bent functions which are components of vectorial bent functions should be rare. However, not for a single bent function it is known that it is not a component of a vectorial bent function with $m \geq 2$. One could expect that functions with "nice" properties like regularity or being dual-bent tend to be component functions

of vectorial bent functions, and that "strange" looking bent functions are perhaps "lonely" in the sense they are not components of vectorial bent functions. In this paper we show that "being strange" is not a criteria that prevents a function from being a component of a vectorial bent function.

Recall that two functions from $\mathbb{V}_n$ to $\mathbb{V}_m$ are called *extended affine equivalent (EA-equivalent)* if one is obtained from the other by affine coordinate transformations and the addition of an affine function. As is well known, (vectorial) bentness is invariant under EA-equivalence.

Famous classes of bent functions (see [5]), are the Maiorana-McFarland class (MMF) and the partial spread class (PS) for arbitrary primes p, and for $p = 2$, Dillon's H class (and its generalization for arbitrary spreads, [6, 7]), which all give regular bent functions. These constructions are essentially vectorial constructions from $\mathbb{V}_n$ to $\mathbb{V}_{n/2}$ (assumingly that for PS a complete spread is used). Every MMF bent function, PS bent function (on a complete spread), and every function in Dillon's H class is a component function of some vectorial bent function. Almost all planar functions, i.e., vectorial bent functions from $\mathbb{V}_n$ to $\mathbb{V}_n$, are quadratic, hence they have quadratic and therefore (weakly) regular component functions. The only known example with non-quadratic components is the Coulter-Matthews function, but, again, its component functions are (weakly) regular, see [8].

By now, one knows many further (not vectorial) constructions of infinite classes of weakly regular bent functions. For some recent results on vectorial bent functions in characteristic 2 we refer to [9]. The first construction of non-weakly regular bent functions, but dual-bent functions, appeared in [10]. The first construction of non-dual-bent functions is in [3].

The question which bent functions can be component functions of a vectorial bent function (of dimension at least 2) has a relation to the hypothesis of Tokareva in [11, 12], that every Boolean function of degree at most $n/2$ can be written as the sum of two Boolean bent functions from $\mathbb{V}_n$ to $\mathbb{F}_2$. Applied to Boolean bent functions, this hypothesis implies that every Boolean bent function is a component function of a vectorial bent function of dimension at least 2. The according statement for odd primes p, i.e., that for every bent function f there exists a bent function g such that every nontrivial linear combination $af(x) + bg(x)$, $a, b \in \mathbb{F}_p$, is bent, is certainly a stronger condition.

Weakly regular bent functions have nice properties, for instance their dual is always a (weakly regular) bent function as well, hence one may expect that they are also good candidates to form vector spaces of bent functions of dimension 2 or larger. In fact, all known planar functions have weakly regular components. The classical examples of vectorial bent functions from $\mathbb{V}_n$ to $\mathbb{V}_m$, $m = n/2$, i.e., p-ary Maiorana-McFarland and p-ary vectorial spread, all have regular bent component functions.

This article is organised as follows. In Section 2 we analyse some classes of (weakly) regular bent functions, like bent monomials and binomials. The objective is to show that those classes are actually vectorial bent functions, i.e., every function in the class is a component function of a vectorial bent function (of dimension at least 2). In Section 3 we show that non-weakly regular dual-bent functions can be components of a vectorial bent function. In Section 4 we present the first construction of vectorial bent functions which have non-dual-bent component functions.

2 Weakly regular vectorial bent functions

The known classes of p-ary vectorial bent functions comprise all planar functions, all of which are quadratic except from the Coulter-Matthews planar function $F(x) = x^{(3^k+1)/2}$

with $\gcd(2n, k) = 1$ on $\mathbb{F}_{3^n}$, the Maiorana-McFarland class, i.e., the class of functions $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ of the form $F(x, y) = x\pi(y) + \rho(y)$ for a permutation π of $\mathbb{F}_{p^m}$ and an arbitrary function ρ on $\mathbb{F}_{p^m}$, and the class of vectorial spread bent functions. All their component functions are by definition a component of a vectorial bent function. In particular, every function $\mathbb{V}_n \to \mathbb{F}_p$ in the (completed) Maiorana-McFarland class (functions that are EA-equivalent to an MMF bent function) and every p-ary partial spread bent function defined on a (complete) spread are components of a suitable vectorial bent function.

In this section we first recall the situation for the somewhat less known (vectorial) spread bent functions. We then give a short argument, showing that every quadratic p-ary bent function is a component of a vectorial bent function, in fact of a planar function. In the main part of the section, we show for three (not quadratic) classes of p-ary bent monomials and binomials, that they are actually vectorial bent functions.

Let $n = 2m$ be even and $U_0, U_1, \ldots, U_{p^m}$ be a spread of $\mathbb{V}_n$, i.e., a set of $p^m + 1$ subspaces of dimension m which intersect pairwise trivially. We define a function $F : \mathbb{V}_n \to \mathbb{V}_k$ for some $k \leq m$ by

(i) $F(x) = 0$ (w.l.o.g.) for $x \in U_0$,
(ii) F is constant on the nonzero elements of U_i, $1 \leq i \leq p^m$, such that for every $c \in \mathbb{V}_k$ the nonzero elements of exactly p^{m-k} of the U_i's are mapped to c.

F is then a (vectorial) bent function from $\mathbb{V}_n$ to $\mathbb{V}_k$. We are here mostly interested in p-ary functions, where $k = 1$, and in vectorial bent functions with maximal $k = m$. In the latter case every element of $\mathbb{V}_m$ is the image of the nonzero elements of exactly one spread element U_i, $1 \leq i \leq p^m$, the elements of U_0 are additionally mapped to 0 (w.l.o.g.).

Let f be a p-ary spread function. We may order the elements of the spread so that the nonzero elements of $U_1, \ldots, U_{p^{m-1}}$ are mapped to 0, the nonzero elements of $U_{p^{m-1}+1}, \ldots, U_{2p^{m-1}}$ to 1, ..., those of $U_{(p-1)p^{m-1}+1}, \ldots, U_{p^m}$ to $p-1$, and U_0 is mapped to 0. We now define a vectorial spread bent function F from $\mathbb{V}_n$ to $\mathbb{F}_{p^m}$ with the one-to-one correspondence of $U_1, \ldots, U_{p^m}$ with the elements of $\mathbb{F}_{p^m}$ as follows. The p^{m-1} elements $z \in \mathbb{F}_{p^m}$ with $\mathrm{Tr}_m(z) = 0$ are assigned (one-to-one) to $U_1, \ldots, U_{p^{m-1}}$, the elements $z \in \mathbb{F}_{p^m}$ with $\mathrm{Tr}_m(z) = 1$ to $U_{p^{m-1}+1}, \ldots, U_{2p^{m-1}}$, ..., the elements with $\mathrm{Tr}_m(z) = p - 1$ to $U_{(p-1)p^{m-1}+1}, \ldots, U_{p^m}$. Clearly, $f(x) = \mathrm{Tr}_m(F(x))$, thus f is a component function of F. Hence it is easy to build a vectorial spread bent function with a given p-ary spread bent function as component.

We now turn our attention to quadratic p-ary bent functions. First recall that when n is even, then a quadratic bent function $Q : \mathbb{F}_p^n \to \mathbb{F}_p$, p odd, is EA-equivalent either to $x_1^2 + x_2^2 + \cdots + x_n^2$ or to $dx_1^2 + x_2^2 + \cdots + x_n^2$ for some fixed nonsquare $d \in \mathbb{F}_p$, one of which is regular, the other one is weakly regular but not regular (depending on p and n), see [13, Theorem 1]. If n is odd, then EA-equivalence can change the sign of the Walsh coefficient (see [13, Theorem 1]), and hence every quadratic bent function is EA-equivalent to $x_1^2 + x_2^2 + \cdots + x_n^2$. For every n there exists a quadratic planar function F (the simplest one is $F(x) = x^2$ on $\mathbb{F}_{p^n}$).

As is well known, F has then regular component functions as well as weakly regular but not regular ones if $p^n \equiv 1 \bmod 4$. If $p^n \equiv 3 \bmod 4$, then F has component functions for which $\zeta = i$ and component functions for which $\zeta = -i$ (where ζ is defined as in (1)). For details on the value distribution of the Walsh transform of planar functions we may refer to [14]. Since planarity is invariant under EA-equivalence, we have the following

Fact 1 *Every p-ary quadratic bent function is a component function of some planar function.*

Given the above arguments we can restrict ourselves to the analysis of vectorial bentness for functions which are not quadratic, not Coulter-Matthews, not in the (completed) Maiorana-McFarland class and not a p-ary partial spread bent function (defined on a complete spread). There are many secondary constructions of p-ary bent functions, i.e., procedures of constructing new bent functions from known ones, by which one can construct a huge number of bent functions. There are not many primary examples besides from those mentioned above. The following have been presented and analysed in [1, 8, 15]:

(i) $f_1 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_1(x) = \mathrm{Tr}_n\left(ax^{r(3^m-1)}\right)$, $n = 2m$, $\gcd(r, 3^m + 1) = 1$ with the condition that the Kloosterman sum $K\left(a^{3^m+1}\right) = \sum_{z\in\mathbb{F}_{3^n}} \epsilon_3^{\mathrm{Tr}_n\left(z+a^{3^m+1}/z\right)}$, where $1/0 := 0$, vanishes;

(ii) $f_2 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_2(x) = \mathrm{Tr}_n\left(ax^{\frac{3^n-1}{4}+3^m+1}\right)$, $n = 2m$, m odd, $a = \alpha^{(3^m+1)/4}$ for a primitive element α of $\mathbb{F}_{3^n}$;

(iii) $f_3 : \mathbb{F}_{p^n} \to \mathbb{F}_p$, $f_3(x) = \mathrm{Tr}_n\left(x^{p^{3k}+p^{2k}-p^k+1} + x^2\right)$, $n = 4k$.

We remark that it is shown in [16], that these functions do not belong to the completed Maiorana-McFarland class.

In the remainder of this section, we also show that these classes of p-ary bent functions are vectorial bent functions, i.e., each of the functions f_i, $i = 1, 2, 3$, is a component of some vectorial bent function.

(i) $\mathbf{f_1(x) = \mathrm{Tr}_n\left(ax^{r(3^m-1)}\right)}$.

The bentness of the monomial function f_1 was shown in [1], a binomial which can be seen as a generalization of f_1, and of which the bentness also depends on a condition involving Kloosterman sums, has been dealt with in the articles [17, 18]. Both bent functions are functions with "Dillon type exponents", hence are constant on the nonzero elements of the elements of the Desarguesian spread of $\mathbb{F}_{3^n}$, i.e., the set of subspaces $\{\gamma\mathbb{F}_{3^m} : \gamma \in \mathcal{C}\}$, where $\mathcal{C}$ is a set of coset representatives of the multiplicative subgroup $\mathbb{F}_{3^m}^*$ of $\mathbb{F}_{3^n}^*$. As shown in Theorem 3.3 in [19], every such bent function is a spread bent function. Immediately we infer that both functions are a component function of some vectorial spread bent function from $\mathbb{F}_{3^n}$ to $\mathbb{F}_{3^m}$.

(ii) $\mathbf{f_2(x) = \mathrm{Tr}_n\left(ax^{\frac{3^n-1}{4}+3^m+1}\right)}$.

The bentness of this monomial was conjectured in [1], in [8, Theorem 1.4] it is then proven that f_2 is a weakly regular but not regular bent function. To show the following theorem on the vectorial bentness of this monomial, one can apply a p-ary version of Lemma 1 and Proposition 1 in [9] on vectorial bentness of monomial Boolean bent functions. By Tr_m^n we denote the relative trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. We first state the version of Lemma 1 in [9] for odd primes p, and give its proof for completeness.

Lemma 1 *Let n, m be positive integers such that $m|n$, $t = 1 + p^m + p^{2m} + \cdots + p^{n-m} = (p^n - 1)/(p^m - 1)$, and d be a positive integer. Then*

$$(1)\ \gcd(d, p^n - 1)|t \Leftrightarrow (2)\ \mathbb{F}_{p^m}^* \subseteq \{x^d : x \in \mathbb{F}_{p^n}^*\} \Leftrightarrow (3)\ \gcd\left(\frac{d}{\gcd(d,t)}, p^m - 1\right) = 1.$$

Proof Let α be a primitive element of $\mathbb{F}_{p^n}$, then α^t is a primitive element of $\mathbb{F}_{p^m}$, i.e., $\mathbb{F}_{p^m}^* = \langle \alpha^t \rangle$. With $\{x^d : x \in \mathbb{F}_{p^n}^*\} = \langle \alpha^d \rangle = \langle \alpha^{\gcd(d, p^n-1)} \rangle$, we have (1) $\Leftrightarrow$ (2), and (2) $\Leftrightarrow$ (3) holds since

$$\mathbb{F}_{p^m}^* \subseteq \{x^d : x \in \mathbb{F}_{p^n}^*\} \Leftrightarrow \langle \alpha^t \rangle \cap \langle \alpha^d \rangle = \langle \alpha^t \rangle \Leftrightarrow \langle \alpha^{lcm(t,d)} \rangle = \langle \alpha^t \rangle$$

$$\Leftrightarrow \gcd(lcm(t, d), p^n - 1) = t \Leftrightarrow \gcd\left(\tfrac{d}{\gcd(d,t)}, p^m - 1\right) = 1.$$

□

The next lemma is the p-ary version of Proposition 1 in [9].

Lemma 2 *Let $f(x) = Tr_n(ax^d)$ be a monomial bent function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ with d satisfying one of the equivalent conditions in Lemma 1 for some divisor m of n. Then the function $F(x) = Tr_m^n(ax^d)$ is a vectorial bent function.*

Proof We have to show that $F_\lambda(x) = \mathrm{Tr}_n(\lambda a x^d)$ is bent for all nonzero $\lambda \in \mathbb{F}_{p^m}$. If (1),(2),(3) in Lemma 1 hold, then $\lambda = \beta^d$ for some $\beta \in \mathbb{F}_{p^n}$, hence $\mathrm{Tr}_n(\lambda a x^d) = \mathrm{Tr}_n(a(\beta x)^d)$, which is EA-equivalent to the original function $\mathrm{Tr}_n(ax^d)$, thus bent as well. □

Theorem 1 *Let $n = 2m$, m odd, $a = \alpha^{(3^m+1)/4}$ for a primitive element α of $\mathbb{F}_{3^n}$. Then $F : \mathbb{F}_{3^n} \to \mathbb{F}_{3^m}$, $F(x) = Tr_m^n\left(ax^{\frac{3^n-1}{4}+3^m+1}\right)$ is a vectorial bent function with component functions all of which are weakly regular but not regular.*

Proof For $d = \frac{3^n-1}{4} + 3^m + 1$ and $n/2 = m$ is odd, we easily see that $\gcd(d, 3^n - 1) = (3^m + 1)/2$, which divides $t = 3^m + 1$. Hence with Lemma 2, the function $F(x) = \mathrm{Tr}_m^n\left(ax^{\frac{3^n-1}{4}+3^m+1}\right)$ is a vectorial bent function. Moreover, from the proof of Lemma 2 we know that every component function of F is EA-equivalent to f_2. Since EA-equivalence does not change regularity when n is even (see [13, Theorem 1]), all components are weakly regular but not regular. □

(iii) $\mathbf{f_3(x) = \mathrm{Tr}_n\left(x^{p^{3k}+p^{2k}-p^k+1} + x^2\right)}$. In [15] it has been shown that f_3 is a weakly regular but not regular bent function. We next show that f_3 is a component of a vectorial bent function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^{2k}}$ ($n = 4k$).

Theorem 2 *Let $n = 4k$ where k is an arbitrary positive integer. Then the function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^{2k}}$,*

$$F(x) = Tr_{2k}^{4k}\left(x^{p^{3k}+p^{2k}-p^k+1} + x^2\right)$$

is a vectorial bent function with all components weakly regular but not regular bent.

Proof Let ω be a primitive element of $\mathbb{F}_{p^{4k}}$, then the nonzero elements of $\mathbb{F}_{p^{2k}}$ are given by $\omega^{(p^{2k}+1)j}$, $j = 0, 1, \ldots, p^{2k}-2$. Observe that for $\gamma_j = \omega^{(p^{2k}+1)j/2}$, $j = 0, 1, \ldots, p^{2k}-2$, we have

$$\begin{aligned}\gamma_j^{p^{3k}+p^{2k}-p^k+1} &= \left(\omega^{(p^{2k}+1)j/2}\right)^{p^{3k}+p^{2k}-p^k+1} = \omega^{\frac{\left(p^{5k}-p^k+p^{3k}-p^{3k}+2p^{2k}+p^{4k}+1\right)j}{2}} \\ &= \omega^{(p^{2k}+1)j} = \gamma_j^2.\end{aligned}$$

Hence for the component function $f_j(x) = \mathrm{Tr}_{2k}\left(\omega^{(p^{2k}+1)j}F(x)\right)$ we obtain

$$\begin{aligned}f_j(x) &= \mathrm{Tr}_{2k}\left(\omega^{(p^{2k}+1)j}F(x)\right) \\ &= \mathrm{Tr}_{4k}(\omega^{(p^{2k}+1)j}(x^{p^{3k}+p^{2k}-p^k+1}+x^2)) \\ &= \mathrm{Tr}_{4k}((\gamma_j x)^{p^{3k}+p^{2k}-p^k+1}+(\gamma_j x)^2) = f_3(\gamma_j x).\end{aligned}$$

□

We close this section recalling an interesting result of Carlet and Leander, see [20, p.99] (see also [21]), on the vectorial bentness of the Boolean Kasami bent function. The result shows that also bent functions which behave different from the functions in the standard classes, may be components of vectorial bent functions. This also motivates our analysis in the following sections, where we investigate non-weakly regular and non-dual-bent functions.

Recall that the Kasami function $\mathrm{Tr}_n\left(\gamma x^{2^{2i}-2^i+1}\right)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, n even, is bent if and only if γ is not a cube in $\mathbb{F}_{2^n}$. Let $n = 2m$, where m is odd, then all elements in $\mathbb{F}_{2^m}$ are cubes in $\mathbb{F}_{2^n}$. For a non-cube $\beta \in \mathbb{F}_{2^n}$ the elements of the coset $\beta\mathbb{F}_{2^m}^*$ are non-cubes. Hence for a basis $\{\alpha_1, \ldots, \alpha_m\}$ of $\mathbb{F}_{2^m}$, the function

$$F(x) = \left(\mathrm{Tr}_n\left(\beta\alpha_1 x^{2^{2i}-2^i+1}\right), \ldots, \mathrm{Tr}_n\left(\beta\alpha_m x^{2^{2i}-2^i+1}\right)\right)$$

is a vectorial bent function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2^m$, with component functions all of which are Kasami bent functions.

In [22] it has been verified that some Kasami bent functions from $\mathbb{F}_{2^{14}}$ to $\mathbb{F}_2$ are non-weakly normal, and it was conjectured that all nonquadratic Kasami bent functions from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_2$, m odd and $m \geq 7$, are non-weakly normal (it also has been pointed out that m odd is a necessary condition for a Kasami function to be not normal). Hence, remarkably, non-weakly normal Boolean bent functions can be components of vectorial bent functions (even of largest possible dimension $m = n/2$). We conclude that the two "nice" properties of Boolean bent functions, (weak) normality and vectorial bentness seem to be not directly related.

Recall that weakly regular but not regular bent functions in dimension $n = 2m$ are never (weakly) normal, see [23, Theorem 6]. However all vectorial bent functions in odd characteristic investigated so far have component functions with "nice" properties. All of their components are regular or weakly regular, and hence dual-bent. In the next two sections we investigate if non-weakly regular and non-dual-bent functions can be component functions of a vectorial bent function.

3 Non-weakly regular, dual-bent functions

Based on a construction of Boolean bent functions in [24] (see also [25]), a procedure for constructing bent functions in odd characteristic was introduced in [10] and further analysed in [2, 13, 23]. As one of the main achievements in [10], this construction was used to obtain the first infinite classes of non-weakly regular bent functions. As pointed out in [2], the obtained functions belong to the class of dual-bent functions.

We start this section with a generalization of the construction in [10] to vectorial functions. For this purpose we represent $\mathbb{V}_{kn}$ by $\mathbb{F}_{p^k}^n$.

Theorem 3 *For every $y \in \mathbb{F}_{p^k}$ let g_y be a vectorial bent function from $\mathbb{F}_{p^k}^n$ to $\mathbb{F}_{p^k}$. Then the function $F : \mathbb{F}_{p^k}^{n+2} \to \mathbb{F}_{p^k}$ defined as*

$$F(x_1, \ldots, x_n, x_{n+1}, y) = g_y(x_1, \ldots, x_n) + yx_{n+1}$$

is a vectorial bent function.

Proof We have to show that for every nonzero $\beta \in \mathbb{F}_{p^k}$ the component function $\mathrm{Tr}_k(\beta F)$ is bent. Let $\alpha_1, \ldots, \alpha_n, \gamma, \delta$ be elements of $\mathbb{F}_{p^k}$. Then

$$\begin{aligned}
&\widehat{\mathrm{Tr}_k(\beta F)}(\alpha_1, \ldots, \alpha_n, \gamma, \delta) \\
&= \sum_{\substack{(x_1,\ldots,x_n)\in\mathbb{F}_{p^k}^n \\ x_{n+1},\, y\in\mathbb{F}_{p^k}}} \epsilon_p^{\mathrm{Tr}_k(\beta(g_y(x_1,\ldots,x_n)+x_{n+1}y)-\alpha_1x_1-\cdots-\alpha_nx_n-\gamma x_{n+1}-\delta y)} \\
&= \sum_{\substack{(x_1,\ldots,x_n)\in\mathbb{F}_{p^k}^n \\ y\in\mathbb{F}_{p^k}}} \epsilon_p^{\mathrm{Tr}_k(\beta(g_y(x_1,\ldots,x_n)))-\mathrm{Tr}_k(\sum_{i=1}^n \alpha_i x_i+\delta y)} \sum_{x_{n+1}\in\mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(x_{n+1}(\beta y-\gamma))} \\
&= p^k \epsilon_p^{-\mathrm{Tr}_k(\delta\gamma\beta^{-1})} \widehat{\mathrm{Tr}_k(\beta g_{\gamma\beta^{-1}})}(\alpha_1, \ldots, \alpha_n) \\
&= p^{\frac{(n+2)k}{2}} \zeta \epsilon_p^{\mathrm{Tr}_k(\beta g_{\gamma\beta^{-1}})^*(\alpha_1,\ldots,\alpha_n)-\mathrm{Tr}_k(\delta\gamma\beta^{-1})} \qquad (2)
\end{aligned}$$

for some $\zeta \in \{\pm 1, \pm i\}$ which may depend on γ (when $p = 2$ then $\zeta = 1$). In the last step we used that $g_{\gamma\beta^{-1}}$ is a vectorial bent function from $\mathbb{F}_{p^k}^n$ to $\mathbb{F}_{p^k}$ for every $\gamma \in \mathbb{F}_{p^k}$. □

By (2), for every fixed $\beta \in \mathbb{F}_{p^k}^*$, the dual function $\mathrm{Tr}_k(\beta F)^*$ of $\mathrm{Tr}_k(\beta F)$ is

$$\begin{aligned}
&(\mathrm{Tr}_k(\beta F))^*(x_1, \ldots, x_n, x_{n+1}, y) = \\
&(\mathrm{Tr}_k(\beta g_{\beta^{-1}x_{n+1}}))^*(x_1, \ldots, x_n) - \mathrm{Tr}_k(\beta^{-1}x_{n+1}y).
\end{aligned}$$

As one observes, $\mathrm{Tr}_k(\beta F)^*$ and $\mathrm{Tr}_k(\beta F)$ are of a similar shape. With the same calculations as in the proof above, one can show that $\mathrm{Tr}_k(\beta F)^*$ is bent as well, under the assumption that the duals of the component functions of g_y used in the construction in Theorem 3 are bent. So far, all known constructions of vectorial bent functions have weakly regular, hence dual-bent component functions. Consequently, Theorem 3 yields vectorial bent functions with dual-bent component functions.

The objective is now to obtain the first infinite class of vectorial bent functions from $\mathbb{V}_{kn}$ to $\mathbb{F}_{p^k}$ for which the component functions are non-weakly regular dual-bent functions. Hence for the remainder of this section, p is always an odd prime. We will use the following lemma from [1] on the Walsh transform of $\mathrm{Tr}_n(\alpha x^2)$.

Lemma 3 (**Corollary 3 in** [1]) *For a nonzero $\alpha \in \mathbb{F}_{p^n}$, let f_α be the function $f_\alpha(x) = Tr_n(\alpha x^2)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then*

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

where

$$f_\alpha^*(u) = -Tr_n\left(\frac{u^2}{4\alpha}\right),$$

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

Recall that every quadratic bent function is a component function of some planar function. Here we will utilize diagonal forms from $\mathbb{F}_{p^k}^n$ to $\mathbb{F}_{p^k}$. We will employ the following lemma on the Walsh transforms of such diagonal forms. For simplicity we suppose that k is even so that for a bent function $g : \mathbb{F}_{p^k}^n \to \mathbb{F}_{p^k}$ we always have $\widehat{g}(b) = \pm\epsilon_p^{g^*(b)} p^{kn/2}$. But all arguments apply in the same way to odd k.

Lemma 4 *For an odd prime p and integers n, k, the diagonal quadratic form $g(x_1, \ldots, x_n) \in \mathbb{F}_{p^k}[x_1, \ldots, x_n]$,*

$$g(x_1, x_2, \ldots, x_n) = a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2, \ a_i \in \mathbb{F}_{p^k}^*, 1 \le i \le n,$$

is a vectorial bent function from $\mathbb{F}_{p^k}^n$ to $\mathbb{F}_{p^k}$. For $\beta \in \mathbb{F}_{p^k}^*$ let

$$\Delta(\beta, a_1, \ldots, a_n) = \begin{cases} (-1)^n \eta(\beta^n) \prod_{i=1}^n \eta(a_i) & : \quad p \equiv 1 \bmod 4, \\ (-1)^{n(k+2)/2} \eta(\beta^n) \prod_{i=1}^n \eta(a_i) & : \quad p \equiv 3 \bmod 4. \end{cases}$$

If $\Delta(\beta, a_1, \ldots, a_n) = 1$, then the component function $Tr_k(\beta g)$ is regular, otherwise it is weakly regular but not regular.

Proof Since quadratic bent functions are (weakly) regular, it is sufficient to determine the Walsh transform of $\mathrm{Tr}_k(\beta g)$ at 0. With Lemma 3 and recursively applying that $\widehat{F}(a, b) = \widehat{f}(a)\widehat{h}(b)$ if $F(x, y) = f(x) + h(y)$ for two functions $f, h : \mathbb{F}_{p^k} \to \mathbb{F}_p$, for a nonzero $\beta \in \mathbb{F}_{p^k}$ we get

$$\widehat{\mathrm{Tr}_k(\beta g)}(0) = \begin{cases} (-1)^n \eta(\beta^n) \prod_{i=1}^n \eta(a_i) p^{nk/2} & : \quad p \equiv 1 \bmod 4, \\ (-1)^{n(k+2)/2} \eta(\beta^n) \prod_{i=1}^n \eta(a_i) p^{nk/2} & : \quad p \equiv 3 \bmod 4. \end{cases}$$

□

For each $y \in \mathbb{F}_{p^k}$ we choose a vectorial bent function g_y from $\mathbb{F}_{p^k}^n$ to $\mathbb{F}_{p^k}$ as

$$g_y(x_1, x_2, \ldots, x_n) = a_{y,1} x_1^2 + a_{y,2} x_2^2 + \cdots + a_{y,n} x_n^2, \ a_{y,i} \in \mathbb{F}_{p^k}^*, 1 \le i \le n,$$

such that for some $\bar{y}, \tilde{y} \in \mathbb{F}_{p^k}$ we have $\prod_{i=1}^{n} \eta(a_{\bar{y},i}) \neq \prod_{i=1}^{n} \eta(a_{\tilde{y},i})$, i.e., exactly one of $\mathrm{Tr}_k(g_{\bar{y}})$, $\mathrm{Tr}_k(g_{\tilde{y}})$ is regular. Now define $F : \mathbb{F}_{p^k}^{n+2} \to \mathbb{F}_{p^k}$ as

$$\begin{aligned} F(x_1, \ldots, x_n, x_{n+1}, y) &= g_y(x_1, \ldots, x_n) + y x_{n+1} \\ &= a_{y,1}x_1^2 + a_{y,2}x_2^2 + \cdots + a_{y,n}x_n^2 + y x_{n+1}. \end{aligned} \tag{3}$$

Theorem 4 *The function $F : \mathbb{F}_{p^k}^{n+2} \to \mathbb{F}_{p^k}$ defined as in (3) is a vectorial bent function for which every component function is a non-weakly regular dual-bent function.*

Proof By Theorem 3 and the discussion following it, the function F is a vectorial bent function with dual-bent component functions. Let β be a nonzero element of $\mathbb{F}_{p^k}$. By Equation (2),

$$\widehat{\mathrm{Tr}_k(\beta F)}(\alpha_1, \ldots, \alpha_n, \gamma, \delta) = \epsilon_p^{-\mathrm{Tr}_k(\delta\gamma\beta^{-1})} p^k \widehat{\mathrm{Tr}_k(\beta g_{\gamma\beta^{-1}})}(\alpha_1, \ldots, \alpha_n).$$

Choose $\bar{\gamma} = \beta\bar{y}$ and $\tilde{\gamma} = \beta\tilde{y}$. Then exactly one of the bent functions $\mathrm{Tr}_k(\beta g_{\bar{\gamma}\beta^{-1}})$ and $\mathrm{Tr}_k(\beta g_{\tilde{\gamma}\beta^{-1}})$ is regular. Hence $\widehat{\mathrm{Tr}_k(\beta F)}(\alpha_1, \ldots, \alpha_n, \bar{\gamma}, \delta)$ and $\widehat{\mathrm{Tr}_k(\beta F)}(\alpha_1, \ldots, \alpha_n, \tilde{\gamma}, \delta)$ have different signs, i.e., $\mathrm{Tr}_k(\beta F)$ is non-weakly regular. □

4 The semi-direct sum and vectorial bent functions with non-dual-bent component functions

The first published non-weakly regular bent function is the monomial function $k(x) = \mathrm{Tr}_6(\zeta^7 x^{98})$ from $\mathbb{F}_{3^6}$ to $\mathbb{F}_3$, where ζ is a primitive element of $\mathbb{F}_{3^6}$, (see Fact 1 in [1]), which was found via computer search. In [2] it was pointed out that k is a non-dual-bent function. With the notation of Lemma 1 we have $d = 98$, $n = 6$, and putting $m = 3$ we obtain $t = 28$. Since $\gcd(98, 728) = 14$ divides 28, by Lemma 2 we have the following

Fact 2 *The monomial function $K(x) = Tr_3^6(\zeta^7 x^{98})$ is a vectorial bent function from $\mathbb{F}_{3^6}$ to $\mathbb{F}_{3^3}$, with component functions all of which are non-dual-bent functions.*

We conclude the last statement from the fact that all component functions of K are linearly equivalent (see the proof of Lemma 2), and from the fact that the property of being non-dual-bent is invariant under EA-equivalence. We hence have a sporadic example of a vectorial bent function with non-dual-bent component functions.

In this section we present the first construction of vectorial bent functions with non-dual-bent components for arbitrary primes p. The procedure is based on the recent very first construction of non-dual-bent functions presented by the authors in [3]. The simplest secondary construction of bent functions is the direct sum of two bent functions $f : \mathbb{V}_m \to \mathbb{F}_p$, $g : \mathbb{V}_n \to \mathbb{F}_p$ given by $F(x, y) = f(x) + g(y)$. Recall that then $\widehat{F}(u, v) = \widehat{f}(u)\widehat{g}(v)$. In its vectorial form, f and g are two vectorial bent functions from $\mathbb{V}_m$ respectively from $\mathbb{V}_n$ to (w.l.o.g.) $\mathbb{F}_{p^k}$. Obviously, for every nonzero $\alpha \in \mathbb{F}_{p^k}$, the component function $\mathrm{Tr}_k(\alpha F(x, y)) = \mathrm{Tr}_k(\alpha(f(x) + g(y))) = \mathrm{Tr}_k(\alpha f(x)) + \mathrm{Tr}_k(\alpha g(y))$ is bent.

The procedure in [3] by which we obtained non-dual-bent functions, is a generalization of the direct sum, which we call *semi-direct sum*. Theorem 5 below extends the semi-direct sum to vectorial functions. For $k = 1$ it is Theorem 1 in [3].

Theorem 5 *Let $f : \mathbb{V}_m \to \mathbb{F}_{p^k}$ and $g : \mathbb{V}_n \to \mathbb{F}_{p^k}$ be vectorial bent functions, and let h be a function from $\mathbb{V}_m$ to $\mathbb{V}_n$. The function $F : \mathbb{V}_m \times \mathbb{V}_n \to \mathbb{F}_{p^k}$ defined as*

$$F(x, y) = f(x) + g(y + h(x))$$

is vectorial bent if and only if for all $b \in \mathbb{V}_n$ and nonzero $\alpha \in \mathbb{F}_{p^k}$ the function $G_{b,\alpha} : \mathbb{V}_m \to \mathbb{F}_p$

$$G_{b,\alpha}(x) = Tr_k(\alpha f(x)) + \langle b, h(x)\rangle_n$$

is a bent function.

Proof For a nonzero element $\alpha \in \mathbb{F}_{p^k}$, let $F_\alpha(x, y) = \mathrm{Tr}_k(\alpha F(x, y))$. Then for $a \in \mathbb{V}_m$ and $b \in \mathbb{V}_n$ we have

$$\begin{aligned}
\widehat{F_\alpha}(a, b) &= \sum_{x\in\mathbb{V}_m, y\in\mathbb{V}_n} \epsilon_p^{\mathrm{Tr}_k(\alpha(f(x)+g(y+h(x))))-\langle a,x\rangle_m-\langle b,y\rangle_n} \\
&= \sum_{x\in\mathbb{V}_m} \epsilon_p^{\mathrm{Tr}_k(\alpha f(x))-\langle a,x\rangle_m} \sum_{y\in\mathbb{V}_n} \epsilon_p^{\mathrm{Tr}_k(\alpha g(y+h(x)))-\langle b,y\rangle_n} \\
&= \sum_{x\in\mathbb{V}_m} \epsilon_p^{\mathrm{Tr}_k(\alpha f(x))-\langle a,x\rangle_m} \sum_{y\in\mathbb{V}_n} \epsilon_p^{\mathrm{Tr}_k(\alpha g(y))-\langle b,y-h(x)\rangle_n} \\
&= \sum_{x\in\mathbb{V}_m} \epsilon_p^{\mathrm{Tr}_k(\alpha f(x))+\langle b,h(x)\rangle_n-\langle a,x\rangle_m} \sum_{y\in\mathbb{V}_n} \epsilon_p^{\mathrm{Tr}_k(\alpha g(y))-\langle b,y\rangle_n} \\
&= \widehat{G_{b,\alpha}}(a)\widehat{g_\alpha}(b).
\end{aligned}$$

Since g is vectorial bent, i.e., $\widehat{g_\alpha}(b) = \zeta p^{n/2}\epsilon_p^{g_\alpha^*(b)}$ for some $\zeta \in \{\pm 1, \pm i\}$ (which is 1 if $p = 2$, otherwise may depend on b and α), the function F is bent if and only if $|\widehat{G_{b,\alpha}}(a)| = p^{m/2}$ for all $a \in \mathbb{V}_m$, $b \in \mathbb{V}_n$, and nonzero $\alpha \in \mathbb{F}_{p^k}$. Equivalently, $G_{b,\alpha}$ is bent for all $b \in \mathbb{V}_n$ and nonzero $\alpha \in \mathbb{F}_{p^k}$. □

Remark 1 *With the observation that*

$$\widehat{F_\alpha}(a, b) = \zeta p^{(m+n)/2}\epsilon_p^{G_{b,\alpha}^*(a)+g_\alpha^*(b)}$$

for some $\zeta \in \{\pm 1, \pm i\}$ (which is 1 if $p = 2$, otherwise may depend on a, b and α), the formula for the dual of the component function F_α of F is

$$F_\alpha^*(x, y) = G_{y,\alpha}^*(x) + g_\alpha^*(y).$$

Corollary 1 *For some integers m, n, l, k with $n + k = l \le m$, let $\mathcal{F}(x) = (f_1(x), \ldots, f_l(x))$, be a vectorial bent function from $\mathbb{V}_m$ to $\mathbb{V}_l$, and let g be a vectorial bent function from $\mathbb{V}_n$ to $\mathbb{V}_k$. Let f be the projection of $\mathcal{F}$ to $\mathbb{V}_k$ given by $f(x) = (f_1(x), \ldots, f_k(x))$, hence a vectorial bent function from $\mathbb{V}_m$ to $\mathbb{V}_k$. Then*

$$F(x, y) = f(x) + g(y_1 + f_{k+1}(x), y_2 + f_{k+2}(x), \ldots, y_n + f_l(x)) \tag{4}$$

is a vectorial bent function from $\mathbb{V}_m \times \mathbb{V}_n$ to $\mathbb{V}_k$. For nonzero $\alpha \in \mathbb{V}_k$, the dual F_α^* of $F_\alpha(x, y) = \langle\alpha, F(x, y)\rangle_k$ is

$$F_\alpha^*(x, y) = G_{y,\alpha}^*(x) + g_\alpha^*(y),$$

where for every $y = (y_1, \ldots, y_n) \in \mathbb{V}_n$, the function $G_{y,\alpha}^*(x)$ is the dual of the bent function

$$G_{y,\alpha}(x) = \alpha_1 f_1(x) + \cdots + \alpha_k f_k(x) + y_1 f_{k+1}(x) + \cdots + y_n f_l(x). \tag{5}$$

Proof Observe that $G_{y,\alpha}$ in (5) is a component function of the vectorial bent function $\mathcal{F}$, hence bent. By Theorem 5, F in (4) is a vectorial bent function from $\mathbb{V}_m \times \mathbb{V}_n$ to $\mathbb{V}_k$. The expression for the dual follows from Remark 1. □

Since our objective is to construct vectorial bent functions with non-dual-bent component functions, for the remainder of this section, p is an odd prime. We employ Corollary 1 choosing $m = 3k$, $n = 2k$, for $\mathcal{F}$ the planar function $\mathcal{F}(x) = x^2$ on $\mathbb{F}_{p^m}$, and for g the Maiorana-McFarland bent function $g(x, y) = xy$ from $\mathbb{F}_{p^k} \times \mathbb{F}_{p^k}$ to $\mathbb{F}_{p^k}$.

Theorem 6 *Let $m = 3k$, and let $\{1, \gamma_1, \gamma_2\}$ be a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^k}$. Then the function F from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^k} \times \mathbb{F}_{p^k}$ to $\mathbb{F}_{p^k}$,*

$$F(x, y_1, y_2) = Tr_k^m(x^2) + (y_1 + Tr_k^m(\gamma_1 x^2))(y_2 + Tr_k^m(\gamma_2 x^2))$$

is a vectorial bent function. For every nonzero $\alpha \in \mathbb{F}_{p^k}$ the dual of the component function $F_\alpha(x, y_1, y_2) = Tr_k(\alpha F(x, y_1, y_2))$ is

$$F_\alpha^*(x, y_1, y_2) = -Tr_m\left(\frac{x^2}{4(\alpha + y_1\gamma_1 + y_2\gamma_2)}\right) - Tr_k(y_1 y_2/\alpha).$$

Proof Since $\{1, \gamma_1, \gamma_2\}$ are linearly independent over $\mathbb{F}_{p^k}$, for every $\alpha, b_1, b_2 \in \mathbb{F}_{p^k}$, the function

$$\begin{aligned} G_{b_1,b_2,\alpha}(x) &= \mathrm{Tr}_k(\alpha \mathrm{Tr}_k^m(x^2)) + \mathrm{Tr}_k(b_1 \mathrm{Tr}_k^m(\gamma_1 x^2)) + \mathrm{Tr}_k(b_2 \mathrm{Tr}_k^m(\gamma_2 x^2)) \\ &= \mathrm{Tr}_m((\alpha + b_1\gamma_1 + b_2\gamma_2)x^2) \end{aligned}$$

is bent. Hence by Theorem 5, the function $F(x, y_1, y_2)$ is bent. The formula for the dual follows from Remark 1 with Lemma 3 and the fact that the dual of the Maiorana-McFarland function $\mathrm{Tr}_k(\alpha y_1 y_2)$ is $-\mathrm{Tr}_k(y_1 y_2/\alpha)$, see [5]. □

Our next objective is to demonstrate that in general the components F_α of F are not dual-bent. Therefore we determine $\widehat{F_\alpha^*}(0, 0, 0)$. We will use that

$$\begin{aligned} G_{b_1,b_2,\alpha}^{**}(x) &= G_{b_1,b_2,\alpha}(-x) = \mathrm{Tr}_m((\alpha + b_1\gamma_1 + b_2\gamma_2)x^2) \\ &= G_{b_1,b_2,\alpha}(x). \end{aligned}$$

Then for the Walsh coefficient of F_α^* at $(0, 0, 0) = (\mathbf{0})$ we have

$$\begin{aligned} \widehat{F_\alpha^*}(\mathbf{0}) &= \sum_{\substack{x \in \mathbb{F}_{p^m} \\ y_1, y_2 \in \mathbb{F}_{p^k}}} \epsilon_p^{G_{y_1,y_2,\alpha}^*(x) - \mathrm{Tr}_k(y_1 y_2/\alpha)} \\ &= \sum_{y_1, y_2 \in \mathbb{F}_{p^k}} \epsilon_p^{-\mathrm{Tr}_k(y_1 y_2/\alpha)} \sum_{x \in \mathbb{F}_{p^m}} \epsilon_p^{G_{y_1,y_2,\alpha}^*(x)} \\ &= \sum_{y_1, y_2 \in \mathbb{F}_{p^k}} \epsilon_p^{-\mathrm{Tr}_k(y_1 y_2/\alpha)} \widehat{G_{y_1,y_2,\alpha}^*}(0) \\ &= \zeta p^{m/2} \sum_{y_1, y_2 \in \mathbb{F}_{p^k}} \epsilon_p^{-\mathrm{Tr}_k(y_1 y_2/\alpha)} \eta(\alpha + y_1\gamma_1 + y_2\gamma_2) \epsilon_p^{G_{y_1,y_2,\alpha}^{**}(0)} \\ &= \zeta p^{m/2} \sum_{y_1, y_2 \in \mathbb{F}_{p^k}} \eta(\alpha + y_1\gamma_1 + y_2\gamma_2) \epsilon_p^{-\mathrm{Tr}_k(y_1 y_2/\alpha)}, \end{aligned} \tag{6}$$

where $\zeta \in \{\pm 1, \pm i\}$ only depends on p and m, see Lemma 3. From Equation (6), we obtain a necessary condition for $\widehat{F_\alpha^*}(\mathbf{0})$ to have absolute value $p^{m/2+k}$, i.e., for the bentness of F_α^*. We hence have the following corollary.

Corollary 2 *Let $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^k} \times \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ be the bent function in Theorem 6. If for some nonzero $\alpha \in \mathbb{F}_{p^k}$ we have*

$$\left| \sum_{y_1, y_2 \in \mathbb{F}_{p^k}} \eta(\alpha + y_1\gamma_1 + y_2\gamma_2)\epsilon_p^{-Tr_k(y_1 y_2/\alpha)} \right| \neq p^k, \tag{7}$$

then F_α^* is not bent, and consequently F is a vectorial bent function which has non-dual-bent component functions.

Remark 2 *Condition (7) combines the additive and the multiplicative structure of the finite field and is therefore not easy to analyse. With a random choice of α and of γ_1 and γ_2, one would expect a chaotic behaviour of the character sum in (7). In particular, experimental results indicate that its absolute value is mostly different from p^k, so that it is easy to find examples of vectorial bent functions with non-dual-bent component functions. For a discussion on the case $k = 1$ we also refer to* [3].

Acknowledgement W.M. is supported by the FWF Project P 30966.

References

1. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inform. Theory **52**, 2018–2032 (2006)
2. Çeşmelioğlu, A., Meidl, W., Pott, A.: On the dual of (non)-weakly regular bent functions and self-dual bent functions. Advances in Mathematics of Communications **7**, 425–440 (2013)
3. Çeşmelioğlu, A., Meidl, W., Pott, A.: There are infinitely many bent functions for which the dual is not bent. IEEE Trans. Inform. Theory **62**, 5204–5208 (2016)
4. Nyberg, K.: Perfect nonlinear S-boxes. In: Advances in cryptology–EUROCRYPT '91 (Brighton, 1991), Lecture Notes in Comput. Sci., 547, pp. 378–386. Springer, Berlin (1991)
5. Dillon, J.F.: Elementary Hadamard difference sets. Ph.D. dissertation, University of Maryland (1974)
6. Carlet, C., Mesnager, S.: Sihem On Dillon's class H of bent functions, Niho bent functions and o-polynomials. J. Combin. Theory Ser. A **118**, 2392–2410 (2011)
7. Çeşmelioğlu, A., Meidl, W., Pott, A.: Bent functions, spreads, and o-polynomials. SIAM J. Discrete Math **29**, 854–867 (2015)
8. Helleseth, T., Hollmann, H., Kholosha, A., Wang, Z., Xiang, Q.: Proofs of two conjectures on ternary weakly regular bent functions. IEEE Trans. Inform. Theory **55**, 5272–5283 (2009)
9. Xu, Y., Carlet, C., Mesnager, S., Wu, C.: Classification of bent monomials, constructions of bent multinomials and upper bounds on the nonlinearities of vectorial functions. IEEE Trans. Inform. Theory **64**, 367–383 (2018)
10. Çeşmelioğlu, A., McGuire, G., Meidl, W.: A construction of weakly and non-weakly regular bent functions. J. Comb. Theory, Series A **119**, 420–429 (2012)
11. Tokareva, N., Functions, B.: Results and Applications to Cryptography. Academic Press, San Diego, CA (2015)
12. Tokareva, N.: On the number of bent functions from iterative constructions: lower bounds and hypothesis. Adv. Math. Commun **5**, 609–621 (2011)
13. Çeşmelioğlu, A., Meidl, W.: A construction of bent functions from plateaued functions. Des. Codes Cryptogr **66**, 231–242 (2013)
14. Feng, K., Luo, J.: Value distributions of exponential sums from perfect nonlinear functions and their applications. IEEE Trans. Inform. Theory **53**, 3035–3041 (2007)

15. Helleseth, T., Kholosha, A.: New binomial bent functions over the finite fields of odd characteristic. IEEE Trans. Inform. Theory **56**, 4646–4652 (2010)
16. Budaghyan, L., Carlet, C., Helleseth, T., Kholosha, A.: Generalized bent functions and their relation to Maiorana-McFarland class: 2012 IEEE Int. Symp. on Inform. Theory Proceedings, pp. 1212–1215 (2012)
17. Jia, W., Zeng, X., Helleseth, T., Li, C.: A class of binomial bent functions over the finite fields of odd characteristic. IEEE Trans. Inform. Theory **58**, 6054–6063 (2012)
18. Zheng, D., Yu, L., Hu, L.: On a class of binomial bent functions over the finite fields of odd characteristic. Appl. Algebra Engrg. Comm. Comput **24**, 461–475 (2013)
19. Lisonek, P., Lu, H.Y.: Bent functions on partial spreads. Des. Codes Cryptogr **73**, 209–216 (2014)
20. Carlet, C.: Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Des Codes Cryptogr **59**, 89–109 (2011)
21. Pasalic, E., Zhang, W.G.: On multiple output bent functions. Inform. Process. Lett **112**, 811–815 (2012)
22. Canteaut, A., Daum, M., Dobbertin, H., Leander, G.: Finding nonnormal bent functions. Discrete Appl Math **154**, 202–218 (2006)
23. Çeşmelioğlu, A., Meidl, W., Pott, A.: Generalized Maiorana-McFarland class and normality of p-ary bent functions. Finite Fields Appl **24**, 105–117 (2013)
24. Leander, G., McGuire, G.: Construction of bent functions from near-bent functions. J. Combin. Theory Ser. A **116**, 960–970 (2009)
25. Charpin, P., Pasalic, E., Tavernier, C.: On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inform. Theory **51**, 4286–4298 (2005)