Generalized Rothaus construction and non-weakly regular bent functions

Wilfried Meidl
Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Atenbergerstrasse 69,
4040-Linz, Austria
meidlwilfried@gmail.com

Abstract

In this article a construction of bent functions from an n-dimensional vector space V_n over $\mathbb{F}_p$ to $\mathbb{F}_p$ is presented for arbitrary primes p and dimensions $n \geq 5$. The construction can be seen as generalization of the Rothaus construction for Boolean bent functions. Since vectorial bent functions are used, we recall some classes of vectorial bent functions and employ them to obtain both, weakly regular and non-weakly regular bent functions. The suggested construction provides the second known procedure to design non-weakly regular bent functions.

1 Introduction

Let p be a prime and let f be a function from an n-dimensional vector space V_n over the prime field $\mathbb{F}_p$ into $\mathbb{F}_p$. The *Walsh transform* of f is the complex valued function on V_n defined as

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

where $\langle u, x\rangle$ denotes a (nondegenerate) inner product in V_n. The classical representations of V_n are $\mathbb{F}_p^n$, the vector space of the n-tuples over $\mathbb{F}_p$, where $\langle u, x\rangle = u \cdot x$ is the conventional dot product, and $\mathbb{F}_{p^n}$, the finite field with p^n elements, where the standard inner product is $\langle u, x\rangle = \mathrm{Tr_n}(ux)$, the absolute trace of $ux \in \mathbb{F}_{p^n}$.

A function $f : V_n \to \mathbb{F}_p$ is called a *bent function* if the Walsh transform $\widehat{f}(u)$ of f at u, which we call the *Walsh coefficient* of u, has magnitude $p^{n/2}$ for all $u \in V_n$. The term bent function was introduced by Rothaus in [23] for Boolean functions. Bent functions in odd characteristic were first considered in [18]. Since then the area of bent functions and related functions has developed into a prominent research area, due to applications

in cryptography and coding and rich connections to many mathematical objects like (relative) difference sets, Hadamard matrices, graphs ....

For a Boolean bent function we obviously have $\widehat{f}(u) = (-1)^{f^*(u)}2^{n/2}$ for a Boolean function f^*, called the dual of f. Note that differently to the case where p is odd, Boolean bent functions can only exist for even dimension n. When p is odd, then a bent function f satisfies (cf. [16])

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

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

Several constructions of weakly regular bent functions are known. The first construction of infinite classes of non-weakly regular bent functions was introduced in [5] and further analysed in [6, 7, 8, 9]. Until then, only sporadic examples of non-weakly regular bent functions have been known, see [8].

Let V_n, V_m be vector spaces over $\mathbb{F}_p$ of dimension n and m, respectively, and let F be a function from V_n to V_m. For a nonzero $\gamma \in V_m$ the function $f_\gamma : V_n \to \mathbb{F}_p$ defined as

$$f_\gamma(x) = \langle \gamma, F(x) \rangle$$

is called a *component function* of F. The function F is called a *vectorial bent function* if all non-zero component functions of F are bent. Note that the set of component functions together with the zero-function then forms an m-dimensional vector space of bent functions. If $p = 2$, then m is at most $n/2$, if p is odd, then we have $m \leq n$, see [22]. Vectorial bent functions for which $m = n$, are called *PN-functions (perfect nonlinear functions)*. Examples of vectorial bent functions are vectorial *Maiorana-McFarland* bent functions, vectorial *partial spread* bent functions, where $m = n/2$, the *Dembowski-Ostrom* PN-polynomials and the *Coulter-Matthews* PN-function.

In this article we introduce a construction of bent functions from V_n to $\mathbb{F}_p$ for an arbitrary prime p and integer $n \geq 5$, which employs component functions of vectorial bent functions. In Section 2 we present the construction and show its correctness. We point out that the construction can be seen as a generalization of Rothaus' construction of Boolean bent functions in [23]. Though being comparatively simple, the construction turns out to

be very powerful. In Section 3 we apply the construction with some classes of vectorial bent functions and obtain both, weakly regular and non-weakly regular bent functions. After the construction in [5], this is the second procedure to design non-weakly regular bent functions. We conclude Section 3 with a comparison of the construction in this paper with the construction in [5].

2 The construction

In this section we present a construction of bent functions in dimension $n+2$ from three bent functions f, g, h from V_n to $\mathbb{F}_p$, for which every nontrivial linear combination

$$\Omega_{\lambda_1,\lambda_2,\lambda_3}(x) := \lambda_1 f(x) + \lambda_2 g(x) + \lambda_3 h(x), \quad \lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_p,$$

is also bent. At first view it seems not easy to find functions f, g, h which satisfy this condition. However, for f, g, h one can take component functions of a vectorial bent function $F : V_n \to V_m$, $m \geq 3$, which are linearly independent over $\mathbb{F}_p$. Note that then $\{f, g, h\}$ forms a basis of a 3-dimensional subspace of the vector space of the component functions of F, i.e. $H(x) = (f(x), g(x), h(x))$ is a vectorial bent function from V_n to $\mathbb{F}_p^3$.

Theorem 1 *Let $f, g, h : V_n \to \mathbb{F}_p$ be linearly independent component functions of a vectorial bent function, and let a, b, c be elements of $\mathbb{F}_p$. The function G from $V_n \times \mathbb{F}_p^2 = V_{n+2}$ to $\mathbb{F}_p$ given by*

$$\begin{aligned} G(x,y,z) &= f^2(x) - f(x)g(x) + g(x)h(x) - f(x)h(x) + af(x) + bg(x) \\ &\quad + ch(x) + (g(x) - f(x))y + (h(x) - f(x))z + yz \end{aligned} \tag{1}$$

is bent if and only if $a + b + c \neq 0$.

Proof. Let $u \in V_n$, and $v, w \in \mathbb{F}_p$. Putting $f^2(x) - f(x)g(x) + g(x)h(x) - f(x)h(x) + af(x) + bg(x) + ch(x) := \phi(x)$ we have

$$\begin{aligned} \widehat{G}(u,v,w) &= \sum_{\substack{x \in V_n \\ y,z \in \mathbb{F}_p}} \epsilon_p^{\phi(x)+(g(x)-f(x))y+(h(x)-f(x))z+yz-\langle u,x\rangle - vy - wz} \\ &= \sum_{x \in V_n} \epsilon_p^{\phi(x)-\langle u,x\rangle} \sum_{y \in \mathbb{F}_p} \epsilon_p^{(g(x)-f(x)-v)y} \sum_{z \in \mathbb{F}_p} \epsilon_p^{(h(x)-f(x)-w+y)z} \\ &= \sum_{x \in V_n} \epsilon_p^{\phi(x)-\langle u,x\rangle} \epsilon_p^{(g(x)-f(x)-v)(f(x)-h(x)+w)} p \end{aligned}$$

where in the last step we use that the last sum vanishes if $y \neq f(x)-h(x)+w$. With the definition of ϕ this yields

$$\begin{aligned}\widehat{G}(u,v,w) &= p\epsilon_p^{-vw} \sum_{x\in V_n} \epsilon_p^{(a-v-w)f(x)+(b+w)g(x)+(c+v)h(x)-\langle u,x\rangle} \\ &= p\epsilon_p^{-vw}\widehat{\Omega_{\lambda_1,\lambda_2,\lambda_3}}(u), \end{aligned} \tag{2}$$

for $\lambda_1 = a-v-w, \lambda_2 = b+w, \lambda_3 = c+v$. If not $\lambda_1 = \lambda_2 = \lambda_3 = 0$, then $\Omega_{\lambda_1,\lambda_2,\lambda_3}$ is bent. Hence $|\widehat{\Omega_{\lambda_1,\lambda_2,\lambda_3}}(u)| = p^{n/2}$ for all $u \in V_n$, and as a consequence $|\widehat{G}(u,v,w)| = p^{(n+2)/2}$. Therefore G is bent if and only if $a-v-w=0, b+w=0, c+v=0$ does not have a solution v,w, which is equivalent to $a+b+c \neq 0$ □

Remark 1 *As one can see from Equation* (2)*, Theorem 1 has a more general version, as for G to be bent it is sufficient that $(a-v-w)f(x)+(b+w)g(x)+(c+v)h(x)$ is bent for all values for $v,w \in \mathbb{F}_p$. This is equivalent to the condition that $\lambda_1 f(x)+\lambda_2 g(x)+\lambda_3 h(x) = \Omega_{\lambda_1,\lambda_2,\lambda_3}(x)$ is bent for all $\lambda_1,\lambda_2,\lambda_3 \in \mathbb{F}_p$ for which $\lambda_1+\lambda_2+\lambda_3 = a+b+c$. However, the easiest way to find functions f,g,h which satisfy this condition is to employ vectorial bent functions.*

Remark 2 *If $a+b+c=0$, the Walsh spectrum of G, i.e. the multiset $\{\widehat{G}(u,v,w) \mid u \in V_n, v,w \in \mathbb{F}_p\}$ contains $(p^2-1)p^n$ elements with absolute value $p^{(n+2)/2}$, one element with absolute value p^{n+1} and p^n-1 times the 0.*

Remark 3 *For $p=2$, where G is bent whenever (a,b,c) has an odd Hamming weight, with the choice $a=1, b=c=0$ we obtain Rothaus' construction of Boolean bent functions in [23] as a special case. Note that for this case it is sufficient that with f,g,h also $f+g+h$ is bent.*

There are several other constructions of Boolean bent functions which have been generalized to p-ary versions. The p-ary Maiorana-McFarland class was presented in [18] where p-ary bent functions were introduced (actually even for arbitrary p, not necessarily a prime), the partial spread class was generalized to p-ary functions in [17, 20]. The construction of p-ary bent functions in [5, 7] can be seen as a generalization of a construction of Boolean bent functions in [11, 19]. On the other hand, as poined out in [10], Dillon's class H (see [14]) does not have a p-ary equivalent. Also the constructions of Boolean bent functions in [3, 21] do not seem to have a p-ary version, as in these constructions the property $(-1)^{f(x)} = 1-2f(x)$ of a Boolean function f plays an important role, which does not have a (obvious) p-ary equivalent.

3 Weakly regular and non-weakly regular examples

In this section we apply Theorem 1 to some classes of vectorial bent functions. In particular, we use knowledge about some classes of PN-functions to construct non-weakly regular bent functions. After the construction presented in [5] this is the second construction of non-weakly regular bent functions.

Vectorial Maiorana-McFarland functions

The most convenient way to describe vectorial Maiorana-McFarland bent functions is to use a representation via finite fields. Let $n = 2m$, let π be a permutation of $\mathbb{F}_{p^m}$ and let g be a function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$. The function F from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$ given by

$$F(x_1, x_2) = x_1\pi(x_2) + g(x_2)$$

is a vectorial bent function, i.e. for every nonzero $\beta \in \mathbb{F}_{p^m}$, the component function

$$f_\beta(x_1, x_2) = \mathrm{Tr}_m(\beta(x_1\pi(x_2) + g(x_2)))$$

is a Maiorana-McFarland bent function. To apply Theorem 1 we choose three nonzero elements $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_{p^m}$, which are linearly independent over $\mathbb{F}_p$ and define

$$\begin{aligned} f(x_1, x_2) &= \mathrm{Tr}_m(\beta_1 F(x_1, x_2)), \quad g(x_1, x_2) = \mathrm{Tr}_m(\beta_2 F(x_1, x_2)), \\ h(x_1, x_2) &= \mathrm{Tr}_m(\beta_3 F(x_1, x_2)). \end{aligned}$$

Then

$$\Omega_{\lambda_1,\lambda_2,\lambda_3}(x_1, x_2) = \mathrm{Tr}_m((\lambda_1\beta_1 + \lambda_2\beta_2 + \lambda_3\beta_3)F(x_1, x_2))$$

is bent for all $(\lambda_1, \lambda_2, \lambda_3) \neq (0, 0, 0)$, and we can construct a bent function G in dimension $n + 2$ given as in Equation (1). As Maiorana-McFarland bent functions are always regular (see [18]), i.e. $\widehat{\Omega_{\lambda_1,\lambda_2,\lambda_3}}(u_1, u_2) = p^{n/2}\epsilon_p^j$ for some j (depending on u_1, u_2), by (2) the resulting bent function G is also regular.

A procedure to obtain (quadratic) vectorial Maiorana-McFarland bent functions in multivariate form has been presented by Nyberg in [22]:
Pick a primitive polynomial in $\mathbb{F}_p[x]$ of degree $n/2 = m$, and let A be the state transition matrix of the corresponding maximal length sequence. The matrix A then describes a linear permutation of $\mathbb{F}_p^m$. As well known, every non-trivial linear combination of $I, A, A^2, \ldots, A^{m-1}$ is a power of A and

hence also a permutation. We obtain then a vectorial Maiorana-McFarland bent function from $\mathbb{F}_p^m \times \mathbb{F}_p^m$ to $\mathbb{F}_p^m$ as $F = (f_1, f_2, \ldots, f_m)$ with $f_j(x_1, x_2) = A^{j-1}x_1 \cdot x_2$, $1 \leq j \leq m$.
For our construction we may pick three distinct powers $A^{j_1}, A^{j_2}, A^{j_3}$ of A and define

$$f(x_1, x_2) = A^{j_1}x_1 \cdot x_2, \quad g(x_1, x_2) = A^{j_2}x_1 \cdot x_2, \quad h(x_1, x_2) = A^{j_3}x_1 \cdot x_2.$$

Finally we remark that in [4] a method to obtain multivariate Boolean Maiorana-McFarland bent functions f, g, h such that $f + g + h$ is bent has been presented, which uses orthomorphic permutations. The objective in [4] is to use those functions for Rothaus' construction, which as observed in Remark 3 is a special case of the construction in Theorem 1 when $p = 2$.

VECTORIAL PARTIAL SPREAD FUNCTIONS

The famous class of *partial spread* bent functions was introduced by Dillon in his thesis [14] for $p = 2$. In [17, 20] a generalization of partial spread functions for arbitrary primes p was presented. As for the Boolean case, one can distinguish between PS+ and PS- partial spread bent functions. For a precise definition of the PS+ and the PS- class, we refer to [14] respectively [20].

We here consider partial spread bent functions in arbitrary characteristic p. First of all we point out that similarly as for the case $p = 2$, we can define a vectorial bent function from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$, for which all component functions are partial spread bent functions, by using a complete spread of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

We consider a spread of $\mathbb{F} = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ (or $\mathbb{F}_{p^{2m}}$) with elements $U_0, U_1, \ldots, U_{p^m}$, and define a function $F : \mathbb{F} \to \mathbb{F}_{p^m}$ by

$$F(z) = \gamma_i \text{ if } z \in U_i, z \neq 0, 1 \leq i \leq p^m, \text{ and } F(z) = \gamma_0 \text{ if } z \in U_0 \qquad (3)$$

for a permutation $i \to \gamma_i$ from $\{1, 2, \ldots, p^m\}$ to $\mathbb{F}_{p^m}$ and an element $\gamma_0 \in \mathbb{F}_{p^m}$.

Lemma 1 *The function F in (3) is a vectorial bent function, for which all component functions are partial spread bent functions. If $\gamma_0 \neq 0$, then $(p-1)p^{m-1}$ component functions of F are PS+, $p^{m-1}-1$ are PS-. If $\gamma_0 = 0$ then all component functions are PS-.*

Proof. For a nonzero $\beta \in \mathbb{F}_{p^m}$, the component function f_β of F is given by $f_\beta(z) = \mathrm{Tr_m}(\beta\gamma_i)$ for nonzero $z \in U_i$, $0 \leq i \leq p^m$, and $f_\beta(0) = \mathrm{Tr_m}(\beta\gamma_0)$. First suppose that $\mathrm{Tr_m}(\beta\gamma_0) = 0$. Let $j \in \mathbb{F}_p^*$. Since γ_i, $i = 1, 2, \ldots, p^m$,

runs through all elements of $\mathbb{F}_{p^m}$, the preimage $f_\beta^{-1}(j)$ is the union of p^{m-1} spread elements (without the 0 which is mapped to $\mathrm{Tr_m}(\beta\gamma_0) = 0$). By [20, Theorem 3.3], f_β is a partial spread bent function belonging to the family PS-.
Now suppose that $\mathrm{Tr_m}(\beta\gamma_0) = t \neq 0$. Then for every (nonzero) $j \neq t$, the preimage $f_\beta^{-1}(j)$ is the union of p^{m-1} spread elements (without the 0 which is mapped to $\mathrm{Tr_m}(\beta\gamma_0) = t$), and the preimage of t is the union of $p^{m-1}+1$ spread elements. By [20, Theorem 3.6], f_β is a partial spread bent function belonging to the family PS+. With the observation that $\mathrm{Tr_m}(\beta\gamma_0) = 0$ always applies if $\gamma_0 = 0$, and otherwise it applies for exactly $p^{m-1} - 1$ nonzero $\beta \in \mathbb{F}_{p^m}$, we obtain the last statement of the lemma. □

Lemma 1 yields a large number of candidates from the partial spread class for the construction in Theorem 1. Again choosing $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_{p^m}$ linearly independent over $\mathbb{F}_p$, we can take the component functions $f = f_{\beta_1}$, $g = f_{\beta_2}$, $h = f_{\beta_3}$ of F defined as in (3) for our construction. As all partial spread bent functions are regular (see [20]), the resulting bent function G will also be regular.

A subclass of the vectorial partial spread bent functions, for which an explicit representation is known, is the class PS_{ap}. For a balanced function $G : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ with $G(0) = 0$ define $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ as

$$F(x_1, x_2) = G(x_1 x_2^{p^m-2}).$$

Then for every nonzero $\beta \in \mathbb{F}_{p^m}$ the component function

$$f_\beta(x_1, x_2) = \mathrm{Tr_m}(\beta G(x_1 x_2^{p^m-2}))$$

is a (p-ary) PS_{ap} bent function, see [14]. For our construction we can again choose linearly independent $\beta_1, \beta_2, \beta_3 \in \mathbb{F}_{p^m}$ and define

$$\begin{aligned} f(x_1, x_2) &= \mathrm{Tr_m}(\beta_1 G(x_1 x_2^{p^m-2})),\ g(x_1, x_2) = \mathrm{Tr_m}(\beta_2 G(x_1 x_2^{p^m-2})), \\ h(x_1, x_2) &= \mathrm{Tr_m}(\beta_3 G(x_1 x_2^{p^m-2})). \end{aligned}$$

DO-POLYNOMIALS

PN-functions, which only can exist for odd p, seem to be quite rare. Besides from one exception, only quadratic PN-functions are known, which can be represented by so called Dembowski-Ostrom polynomials (DO-polynomials) in $\mathbb{F}_{p^n}[x]$, (see [12, 13]). For examples of DO-polynomials which describe PN-functions we refer to [1, 2, 26, 27] and the references therein. Clearly, all of those PN-functions serve as a source for bent functions f, g, h for our construction.

The easiest example of a (quadratic) PN-function is the monomial function on $\mathbb{F}_{p^n}$ given by $F(x) = x^{p^j+1}$ with $n/\gcd(n,j)$ odd. We will employ this PN-function to construct non-weakly regular bent functions. We will use the following lemma, see Lemma 2 and Corollary 3 in [16]. By $\eta(\alpha)$ we denote the quadratic character of α in $\mathbb{F}_{p^n}$.

Lemma 2 *Let n and $0 \leq j \leq n$ be integers such that $n/\gcd(n,j)$ is odd. For a nonzero $\alpha \in \mathbb{F}_{p^n}$ let f_α be the function $f_\alpha(x) = \mathrm{Tr_n}(\alpha x^{p^j+1})$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then*

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

To use the PN-monomial x^{p^j+1} for the construction in Theorem 1, we choose nonzero $\alpha_1, \alpha_2, \alpha_3$ in $\mathbb{F}_{p^n}$ linearly independent over $\mathbb{F}_p$, and put $f(x) = \mathrm{Tr_n}(\alpha_1 x^{p^j+1})$, $g(x) = \mathrm{Tr_n}(\alpha_2 x^{p^j+1})$, $h(x) = \mathrm{Tr_n}(\alpha_3 x^{p^j+1})$. Then the function $G(x,y,z)$ from $\mathbb{F}_{p^n} \times \mathbb{F}_p^2 \to \mathbb{F}_p$ given as in Equation (1) is of the form

$$\begin{aligned} G(x,y,z) \quad = \quad & (\mathrm{Tr_n}(\alpha_1 x^{p^j+1}))^2 - \mathrm{Tr_n}(\alpha_1 x^{p^j+1})\mathrm{Tr_n}(\alpha_2 x^{p^j+1}) \\ & + \mathrm{Tr_n}(\alpha_2 x^{p^j+1})\mathrm{Tr_n}(\alpha_3 x^{p^j+1}) - \mathrm{Tr_n}(\alpha_1 x^{p^j+1})\mathrm{Tr_n}(\alpha_3 x^{p^j+1}) \\ & + \mathrm{Tr_n}((a\alpha_1 + b\alpha_2 + c\alpha_3)x^{p^j+1}) + \mathrm{Tr_n}((\alpha_2 - \alpha_1)x^{p^j+1}y) \\ & + \mathrm{Tr_n}((\alpha_3 - \alpha_1)x^{p^j+1}z) + yz. \end{aligned} \tag{4}$$

Corollary 1 *Let n and $0 \leq j \leq n$ be integers such that $n/\gcd(n,j)$ is odd, let $\alpha_1, \alpha_2, \alpha_3$ be linearly independent elements of $\mathbb{F}_{p^n}$ such that not all of them are squares respectively nonsquares in $\mathbb{F}_{p^n}$, and let $a, b, c \in \mathbb{F}_p$ such that $a+b+c \neq 0$. Then the function G given in Equation (4) is a non-weakly regular bent function.*

Proof. By Theorem 1 the function G in (4) is a bent function. We solely have to show that G is non-weakly regular. Suppose that $\eta(\alpha_1) \neq \eta(\alpha_2)$. We compare the Walsh coefficients $\widehat{G}(u,-c,-b)$ and $\widehat{G}(u,-c,a+c)$. With Equation (2) putting $a+b+c := k$ we get

$$\widehat{G}(u,-c,-b) = p\epsilon_p^{-bc} \sum_{x \in V_n} \epsilon_p^{(a+b+c)f(x) - \langle u,x \rangle} = p\epsilon_p^{-bc}\widehat{kf}(u) = p\epsilon_p^{-bc}\widehat{f_{k\alpha_1}}(u)$$

and

$$\widehat{G}(u,-c,a+c) = p\epsilon_p^{c(a+c)} \sum_{x \in V_n} \epsilon_p^{(a+b+c)g(x) - \langle u,x \rangle} = p\epsilon_p^{c(a+c)}\widehat{kg}(u) = p\epsilon_p^{c(a+c)}\widehat{f_{k\alpha_2}}(u).$$

With the assumption that $\eta(k)\eta(\alpha_1) \neq \eta(k)\eta(\alpha_2)$, by Lemma 2 the bent function G is non-weakly regular.
Similarly one observes that the Walsh coefficients $\widehat{G}(u,-c,-b)$ and $\widehat{G}(u,a+b,-b)$ have opposite signs if $\eta(\alpha_1) \neq \eta(\alpha_3)$, and $\widehat{G}(u,-c,a+c)$ and $\widehat{G}(u,a+b,-b)$ have opposite signs if $\eta(\alpha_2) \neq \eta(\alpha_3)$. □

We note that one may choose $\alpha_1 = 1$, $\alpha_2 = \omega$, $\alpha_2 = \omega^2$ for a primitive element ω of $\mathbb{F}_{p^n}$, and obtain for all odd p a description of a non-weakly regular bent function for infinitely many finite fields $\mathbb{F}_{p^n}$ (of course ω and the trace function are defined in the respective finite field $\mathbb{F}_{p^n}$).

Remark 4 *To design a non-weakly regular bent function by Corollary 1 it is sufficient to choose $\alpha_1, \alpha_2, \alpha_3$ with not all the same quadratic character in $\mathbb{F}_{p^n}$. However, this condition is not necessary for obtaining a non-weakly regular bent function. From Equation* (2) *one can deduce that the bent function G in* (4) *is non-weakly regular whenever $(a-v-w)\alpha_1+(b+w)\alpha_2+(c+v)\alpha_3$ does not have one and the same quadratic character for all combinations of $v, w \in \mathbb{F}_q$. By Remark 1 this holds if and only if $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \lambda_3\alpha_3$ does not have one and the same quadratic character for all combinations of $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_p$ for which $\lambda_1 + \lambda_2 + \lambda_3 = a + b + c$.*

Coulter-Matthews PN-function

We finally want to use the knowledge on the *Coulter-Matthews* PN-function $F : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n}$,

$$F(x) = x^{\frac{3^k+1}{2}}, \quad k \text{ odd and } \gcd(n,k) = 1,$$

yet the only known not quadratic PN-function, to construct non-weakly regular bent functions. The following Lemma follows from [15, Lemma 3], see Proposition 2 in [9].

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

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

where η represents the quadratic character in $\mathbb{F}_{3^n}$.

Corollary 2 *Let n, k be integers such that $\gcd(2n,k) = 1$, let $\alpha_1, \alpha_2, \alpha_3$ be linearly independent elements of $\mathbb{F}_{3^n}$ such that not all of them are squares*

respectively nonsquares in $\mathbb{F}_{3^n}$*, and let* $a, b, c \in \mathbb{F}_3$ *such that* $a+b+c \neq 0$*. Then the function* $G : \mathbb{F}_{3^n} \times \mathbb{F}_3^2 \to \mathbb{F}_3$*,*

$$\begin{aligned} G(x,y,z) &= (\mathrm{Tr_n}(\alpha_1 x^{\frac{3^k+1}{2}}))^2 - \mathrm{Tr_n}(\alpha_1 x^{\frac{3^k+1}{2}})\mathrm{Tr_n}(\alpha_2 x^{\frac{3^k+1}{2}}) \\ &\quad + \mathrm{Tr_n}(\alpha_2 x^{\frac{3^k+1}{2}})\mathrm{Tr_n}(\alpha_3 x^{\frac{3^k+1}{2}}) - \mathrm{Tr_n}(\alpha_1 x^{\frac{3^k+1}{2}})\mathrm{Tr_n}(\alpha_3 x^{\frac{3^k+1}{2}}) \\ &\quad + \mathrm{Tr_n}((a\alpha_1 + b\alpha_2 + c\alpha_3)x^{\frac{3^k+1}{2}}) + \mathrm{Tr_n}((\alpha_2 - \alpha_1)x^{\frac{3^k+1}{2}} y) \\ &\quad + \mathrm{Tr_n}((\alpha_3 - \alpha_1)x^{\frac{3^k+1}{2}} z) + yz \end{aligned} \tag{5}$$

is a non-weakly regular bent function.

Proof. The function G in (5) is bent by Theorem 1. The proof of the non-weak regularity resembles the proof of Corollary 1 and is hence omitted. □

We close this section with a comparison of the construction of Theorem 1 and the construction presented in [5], which both enable the design of non-weakly regular bent functions. We remark that once one obtained a non-weakly regular bent function, one can recursively generate more non-weakly regular bent functions as the direct sum of a weakly regular and a non-weakly regular bent function, see [25]. We start with recalling the construction in [5].

Let $f_0, f_1, \ldots, f_{p-1}$ be bent functions from V_n to $\mathbb{F}_p$, then the function $G : V_n \times \mathbb{F}_p^2 \to \mathbb{F}_p$ defined as

$$G(x,y,z) = f_z(x) + yz$$

is again a bent function. As shown in [5], it is non-weakly regular if some of the bent functions f_i, $0 \leq i \leq p-1$, are regular and some are weakly regular but not regular.

We observe that both methods employ bent functions in dimension n to obtain a bent function in dimension $n+2$. Whereas the method in this paper can be seen as a generalization of the Rothaus construction, the method in [5] can be seen as a generalization of a construction of Boolean bent functions in [11, 19], which follows a construction principle suggested by Siegenthaler [24] to obtain correlation-immune Boolean functions.
The method in [5] does not impose properties on the p bent functions $f_0, f_1, \ldots, f_{p-1}$ used for the construction. The construction in this paper on the other hand requires that (certain) nontrivial linear combinations over $\mathbb{F}_p$ of the three used bent functions f, g, h are bent as well. As a consequence,

vectorial bent functions can play a crucial role, serving as a source for the components f, g, h for the construction.

As easily can be seen, the algebraic degree of the bent function G obtained with the construction in [5] is upper bounded by $d + (p-1)$ if d is the maximum of the algebraic degrees of the employed bent functions $f_0, f_1, \ldots, f_{p-1}$. We will show that this is not the case for the construction in this paper.

Consider the Coulter-Matthews PN-function x^{14} from $\mathbb{F}_{3^7} \to \mathbb{F}_{3^7}$, and let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{3^7}$ be linearly independent over $\mathbb{F}_3$. Recalling that the algebraic degree is the maximum of the p-ary weights of an exponent in a polynomial representation, we observe that the component functions $\mathrm{Tr}_7(\alpha_i x^{14})$, $i = 1, 2, 3$, have algebraic degree 4. As one can easily determine, the coefficient of x^{1148} in the polynomial representation of our resulting bent function G in dimension 9

$$\begin{aligned} G(x,y,z) &= (\mathrm{Tr_n}(\alpha_1 x^{14}))^2 - \mathrm{Tr_n}(\alpha_1 x^{14})\mathrm{Tr_n}(\alpha_2 x^{14}) + \mathrm{Tr_n}(\alpha_2 x^{14})\mathrm{Tr_n}(\alpha_3 x^{14}) \\ &\quad -\mathrm{Tr_n}(\alpha_1 x^{14})\mathrm{Tr_n}(\alpha_3 x^{14}) + \mathrm{Tr_n}((a\alpha_1 + b\alpha_2 + c\alpha_3)x^{14}) \\ &\quad +\mathrm{Tr_n}((\alpha_2 - \alpha_1)x^{14}y) + \mathrm{Tr_n}((\alpha_3 - \alpha_1)x^{14}z) + yz \end{aligned} \tag{6}$$

is

$$C_{1148} = \alpha_1^{3^4}(2\alpha_1 - \alpha_2 - \alpha_3) + \alpha_2^{3^4}(\alpha_3 - \alpha_1) + \alpha_3^{3^4}(\alpha_2 - \alpha_1).$$

Since $1148 = 3^6 + 3^5 + 2 \cdot 2^4 + 2^2 + 3 + 2$ has 3-ary weight 8, the algebraic degree of G in (6) is 8 if $\alpha_1, \alpha_2, \alpha_3$ are chosen such that $C_{1148} \neq 0$. For instance one may choose $\alpha_1 = 1$, $\alpha_2 = \omega$, $\alpha_3 = \omega^2$, where ω is one of the 1092 primitive elements of $\mathbb{F}_{3^7}$. The coefficient C_{1148} is then nonzero if ω is not a root of $x^{163} + 2x^{162} + x^{83} + 2x^{81} + 2x^2 + 2x + 2$. Observe that the bent function G in (6) of algeraic degree 8 cannot be obtained from Coulter-Matthews functions $\mathrm{Tr}_7(\alpha x^{14})$ of algebraic degree 4 with the construction in [5].

4 Acknowledgement

This research is supported by the FWF Lise Meitner program under the project number M 1767-N26.

References

[1] J. Bierbrauer, New semifields, PN and APN functions, Des. Codes Cryptogr. 54 (2010), 189–200.

[2] L. Budaghyan, T. Helleseth, New perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p, in: S.E. Golomb, M.G. Parker, A. Pott, A. Winterhof (Eds.), Sequences and their applications–SETA 2008, Lecture Notes in Comput. Sci., 5203, Springer, Berlin, 2008, pp. 403–414.

[3] C. Carlet, On bent and highly nonlinear balanced/resilient functions and their algebraic immunities, in: M. Fossorier et al. (Eds.), AAECC 2006, Lecture Notes in Comput. Sci. 3857, Springer, Berlin, 2006, pp. 1–28.

[4] C. Carlet, F. Zhang, Y. Hu, Secondary constructions of bent functions and their enforcement, Advances in Mathematics of Communications 6 (2012), 305–314.

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

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

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

[8] 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), 425–440.

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

[10] A. Çeşmelioğlu, W. Meidl, A. Pott, Bent functions, spreads, and o-polynomials, SIAM J. Discrete Math. 29 (2015), 854–867

[11] P. Charpin, E. Pasalic, C. Tavernier, On bent and semi-bent quadratic Boolean functions, IEEE Trans. Inform. Theory 51 (2005), 4286–4298.

[12] R. S. Coulter, R. W. Matthews, Planar functions and planes of Lenz-Barlotti class II, Des. Codes Cryptogr. 10 (1997), 167–184.

[13] P. Dembowski, T.G. Ostrom, Planes of order n with collineation groups of order n^2, Math. Z. 103 (1968), 239–258.

[14] J.F. Dillon, Elementary Hadamard difference sets, Ph.D. dissertation, University of Maryland, 1974.

[15] K. Feng, J. Luo, Value distributions of exponential sums from perfect nonlinear functions and their applications, IEEE Trans. Inform. Theory 53 (2007), 3035–3041.

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

[17] W. Kantor, Bent functions generalizing Dillon's partial spread functions, arXiv:1211.2600v1.

[18] P.V. Kumar, R.A. Scholtz, L.R. Welch, Generalized bent functions and their properties, J. Combin. Theory Ser. A 40 (1985), 90–107.

[19] G. Leander, G. McGuire, Construction of bent functions from near-bent functions, J. Combin. Theory Ser. A 116 (2009), 960–970.

[20] P. Lisonek, H.Y. Lu, Bent functions on partial spreads, Des. Codes Cryptogr. 73 (2014), 209–216.

[21] S. Mesnager, Several new infinite families of bent functions and their duals, IEEE Trans. Inform. Theory 60 (2014), 4397–4407.

[22] K. Nyberg, Perfect nonlinear S-boxes, in: D.W. Davies (Ed.), Advances in cryptology, EUROCRYPT '91 (Brighton, 1991), Lecture Notes in Comput. Sci. 547, Springer, Berlin, 1991, pp. 378–386.

[23] O.S. Rothaus, On "bent" functions, J. Combin. Theory Ser. A 20 (1976), 300–305.

[24] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. Inform. Theory 30 (1984), 776–780.

[25] Y. Tan, J. Yang, X. Zhang, A recursive approach to construct p-ary bent functions which are not weakly regular, in: Y. Yang (Ed.), Proceedings of IEEE International Conference on Information Theory and Information Security, Beijing, 2010, pp. 156–159.

[26] Z. Zha, G. Kyureghyan, X. Wang, Perfect nonlinear binomials and their semifields, Finite Fields Appl. 15 (2009), 125–133.

[27] Z. Zha, X. Wang, New families of perfect nonlinear polynomial functions, J. Algebra 322 (2009), 3912–3918.