Cryptography and Communications (2019) 11:1233–1245
https://doi.org/10.1007/s12095-019-00370-w

Generalized bent functions into $\mathbb{Z}_{p^k}$ from the partial spread and the Maiorana-McFarland class

Wilfried Meidl[1] · **Alexander Pott**[2]

Received: 5 October 2018 / Accepted: 6 May 2019 / Published online: 21 May 2019

Abstract
Functions f from $\mathbb{F}_p^n$, $n = 2m$, to $\mathbb{Z}_{p^k}$ for which the character sum $\mathcal{H}_f^k(p^t, u) = \sum_{x\in\mathbb{F}_p^n} \zeta_{p^k}^{p^t f(x)} \zeta_p^{u\cdot x}$ (where $\zeta_q = e^{2\pi i/q}$ is a q-th root of unity), has absolute value p^m for all $u \in \mathbb{F}_p^n$ and $0 \le t \le k-1$, induce relative difference sets in $\mathbb{F}_p^n \times \mathbb{Z}_{p^k}$ hence are called bent. Functions only necessarily satisfying $|\mathcal{H}_f^k(1, u)| = p^m$ are called generalized bent. We show that with spreads we not only can construct a variety of bent and generalized bent functions, but also can design functions from $\mathbb{F}_p^n$ to $\mathbb{Z}_{p^m}$ satisfying $|\mathcal{H}_f^m(p^t, u)| = p^m$ if and only if $t \in T$ for any $T \subset \{0, 1 \ldots, m-1\}$. A generalized bent function can also be seen as a Boolean (p-ary) bent function together with a partition of $\mathbb{F}_p^n$ with certain properties. We show that the functions from the completed Maiorana-McFarland class are bent functions, which allow the largest possible partitions.

Keywords Bent function · Generalized bent function · Partial spread · Maiorana-McFarland · Walsh transform · Relative difference set

Mathematics Subject Classification (2010) 06E30 · 05B10 · 94C10

1 Introduction

Let $(A, +_A)$, $(B, +_B)$ be finite abelian groups. A function f from A to B is called a *bent function* if

$$|\sum_{x\in A} \chi(x, f(x))| = \sqrt{|A|} \tag{1}$$

This article is part of the Topical Collection on *Special Issue on Boolean Functions and Their Applications*

✉ Wilfried Meidl
meidlwilfried@gmail.com

Alexander Pott
alexander.pott@ovgu.de

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

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

for every character χ of $A \times B$ which is nontrivial on B. Alternatively, $f : A \to B$ is bent if and only if for all nonzero $a \in A$ the function $D_a f(x) = f(x +_A a) -_B f(x)$ is balanced, i.e. every value in B is taken on the same number $|A|/|B|$ times. The graph $G = \{(x, f(x)) : x \in A\}$ of f is then a relative difference set in $A \times B$, see [15]. For background on relative difference sets we refer to [16].

In this article we are interested in generalized Boolean functions and in generalized p-ary functions. Let p be a prime, let $\mathbb{V}_n$ be an n-dimensional vector space over the finite field $\mathbb{F}_p$, and for an integer q, let $\mathbb{Z}_q$ be the ring of integers modulo q. By '$+$' and '$-$' we respectively denote addition and subtraction modulo q, whereas '$\oplus$' denotes the addition in a vector space over $\mathbb{F}_2$ (or $\mathbb{F}_p$). We call a function from $\mathbb{V}_n$ to $\mathbb{Z}_{p^k}$ a *generalized p-ary function*, and in the case $p = 2$ a *generalized Boolean function* in n variables. We denote the set of all generalized p-ary respectively Boolean functions by $\mathcal{GB}_n^{p^k}$. For a function in $f \in \mathcal{GB}_n^{p^k}$ the character sum (1) is of the form

$$\mathcal{H}_f^k(\alpha, u) = \sum_{x \in \mathbb{V}_n} \zeta_{p^k}^{\alpha f(x)} \zeta_p^{u \cdot x}, \quad \zeta_q = e^{2\pi i/q},$$

where $u \cdot x$ denotes a nondegenerate inner product on $\mathbb{V}_n$. Accordingly we call $f \in \mathcal{GB}_n^{p^k}$ bent if $|\mathcal{H}_f^k(\alpha, u)| = p^{n/2}$ for all $u \in \mathbb{V}_n$ and all nonzero $\alpha \in \mathbb{Z}_{p^k}$. For $k = 1$, the bent condition is then $|\mathcal{H}_f^1(\alpha, u)| = |\mathcal{W}_f(-u)| = p^{n/2}$, where

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{V}_n} \zeta_p^{f(x) - u \cdot x}$$

is the *Walsh transform* of f. The function f from $\mathbb{V}_n$ to $\mathbb{F}_p$ is then a classical p-ary (Boolean) bent function. Note that when $k = 1$ it is sufficient to impose the condition for $\alpha = 1$. Whereas many classes and constructions of Boolean and p-ary bent functions are known, when $k \geq 3$ it seems not easy to find bent functions in $\mathcal{GB}_n^{p^k}$ different from functions obtained via the standard construction from a spread, see Section 3.

In [18] a generalization of bent functions in $\mathcal{GB}_n^{2^k}$ was defined satisfying a weaker condition. We give the definition more general for functions in $\mathcal{GB}_n^{p^k}$, see [11]. A function $f \in \mathcal{GB}_n^{p^k}$ is called a *generalized bent function* if the *generalized Walsh transform*

$$\mathcal{H}_f^k(1, u) = \mathcal{H}_f^k(u) = \sum_{x \in \mathbb{V}_n} \zeta_{p^k}^{f(x)} \zeta_p^{u \cdot x}$$

has absolute value $p^{n/2}$ for all $u \in \mathbb{V}_n$.

As shown in [8], a generalized bent function $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ always satisfies $\mathcal{H}_f^k(u) = 2^{n/2} \zeta_{2^k}^{f^*(u)}$ for some $f^* \in \mathcal{GB}_n^{2^k}$, except for the case when $k = 2$ and n is odd. In accordance with the notation for Boolean bent functions we call f^* the *dual* of f. We remark that f^* is again a generalized bent function, see e.g. [9]. A similar result holds for a generalized bent function f from $\mathbb{V}_n$ to $\mathbb{Z}_{p^k}$, p odd, see [11, Lemma 3].

Similarly as for the Boolean case, bent functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$ can only exist for even n. This is different for generalized bent functions, which also when $p = 2$ do exist for even and for odd n. In this article we will investigate two classes of generalized bent functions which are defined for even n, the partial spread class and generalized bent functions from the Maiorana-McFarland class. Hence if not stated otherwise, $n = 2m$ will always be an even integer. Further we will mostly be interested in the case $p = 2$, but many results also apply for odd primes p, which then will be also included in this article.

Though generalized bent functions in general do not correspond to relative difference sets, they turned out to be very interesting functions with rich structural properties and interesting connections to Boolean respectively p-ary bent functions, see e.g. [4, 8, 11, 19]. In Section 2 we will summarize recent results on these connections. In Section 3, we study generalized bent functions obtained from spreads and Section 4 investigates generalized bent functions related to Maiorana-McFarland bent functions. As we will see both classes seem particularly interesting.

2 Preliminaries

To a function $f \in \mathcal{GB}_n^{p^k}$ we can associate a unique sequence of Boolean respectively p-ary functions a_i $(i = 0, 1, \ldots, k-1)$ such that

$$f(x) = a_0(x) + pa_1(x) + \cdots + p^{k-1}a_{k-1}(x), \text{ for all } x \in \mathbb{V}_n. \tag{2}$$

Further we associate to $f \in \mathcal{GB}_n^{p^k}$ given as in (2) the affine space of Boolean respectively p-ary functions

$$\mathcal{A} := a_{k-1} \oplus \langle a_0, a_1, \ldots, a_{k-2} \rangle. \tag{3}$$

Recall that "$\oplus$" denotes the addition in the vector space over $\mathbb{F}_p$ of Boolean respectively p-ary functions from $\mathbb{V}_n$ to $\mathbb{F}_p$ (in contrast to the addition in $\mathbb{Z}_{p^k}$ in (2)). If the function $f \in \mathcal{GB}_n^{p^k}$ is generalized bent, then all Boolean respectively p-ary functions in the corresponding affine space $\mathcal{A}$ are bent functions (see e.g. [4, 8, 19] for $p = 2$ and for the according result for odd p see [11]). For $p = 2$, more precisely, a function $f \in \mathcal{GB}_n^{2^k}$ is generalized bent if and only if all functions in the corresponding affine space $\mathcal{A}$ are bent, such that for any $h_0, h_1, h_2 \in \mathcal{A}$, $h_3 = h_0 \oplus h_1 \oplus h_2 \in \mathcal{A}$ we have $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$, where h^* denotes the dual of a bent function h, cf. [4]. By a secondary construction of Boolean bent functions proposed by Carlet in [2] (see also [12]), this is equivalent to the following statement: A function $f \in \mathcal{GB}_n^{2^k}$ is generalized bent if and only if for any $h_0, h_1, h_2 \in \mathcal{A}$ the function $h_0h_1 \oplus h_0h_2 \oplus h_1h_2$ is a bent function. Hence there is a strong relation between Carlet's construction and generalized bent functions $f \in \mathcal{GB}_n^{2^k}$. For details we refer to the treatment of octal generalized bent functions in [10] and to Corollaries 1 and 2 in [4].

The most comprehensive description of generalized bent functions which also works for functions $f \in \mathcal{GB}_n^{p^k}$, p odd, has been given in [11]. There, a generalized bent function is described as

- a Boolean (p-ary) bent function $a(x)$ from $\mathbb{V}_n$ to $\mathbb{F}_2$ ($\mathbb{F}_p$) with
- a partition $\mathcal{P}$ of $\mathbb{V}_n$

with the property that $a(x) \oplus C(x)$ is bent for every $C : \mathbb{V}_n \to \mathbb{F}_2$ ($C : \mathbb{V}_n \to \mathbb{F}_p$) which is constant on the elements of $\mathcal{P}$. This main result of [11] can be summarized more precisely as follows: Let $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$, n even, be given as in (2), and let $\mathcal{P}$ be the partition of $\mathbb{V}_n$ obtained by $\mathcal{P} = \{A(d) : 0 \le d \le p^{k-1} - 1\}$, where

$$A(d) = \left\{ x \in \mathbb{V}_n : \sum_{i=0}^{k-2} a_i(x)p^i = d \right\}, \tag{4}$$

(some of the $A(d)$ may be empty). Then we have the following theorem.

Theorem 1 *Let $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$, n even, be given as in (2). Then f is generalized bent if and only if $a_{k-1}(x) \oplus C(x)$ is bent for every Boolean (p-ary) function $C(x)$ which is constant on the elements $A(d)$ in (4) of the partition $\mathcal{P}$.*

For some alternative forms of the statement of Theorem 1, we refer to [11].

Remark 1 For an octal generalized bent function $f : \mathbb{V}_n \to \mathbb{Z}_8$, the corresponding affine space $\mathcal{A}$ contains exactly four bent functions h_0, h_1, h_2 and $h_3 = h_0 \oplus h_1 \oplus h_2$ with the property that $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$. With straightforward calculations one sees that the bent functions $h_0(x) \oplus C(x)$ of Theorem 1 are exactly the functions $\{h_0, h_1, h_2, h_3, h_0h_1 \oplus h_0h_2 \oplus h_1h_2, h_0h_1 \oplus h_0h_3 \oplus h_1h_3, h_0h_2 \oplus h_0h_3 \oplus h_2h_3, h_1h_2 \oplus h_1h_3 \oplus h_2h_3\} \oplus \{0, 1\}$, which are all obtained from h_0, h_1, h_2, h_3 with Carlet's secondary construction, [2].

Let $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$ be given as $f(x) = \sum_{i=0}^{k-1} a_i(x)p^i$ be a generalized bent function and let $l \geq k$ be an integer. As pointed out in [11], as an immediate consequence of Theorem 1 the function $g : \mathbb{V}_n \to \mathbb{Z}_{p^l}$

$$\begin{aligned} g(x) \;=\; & c_0(a_0(x), \ldots, a_{k-2}(x)) + pc_1(a_0(x), \ldots, a_{k-2}(x)) + \cdots \\ & + p^{k-2}c_{k-2}(a_0(x), \ldots, a_{k-2}(x)) + \cdots \\ & + p^{l-2}c_{l-2}(a_0(x), \ldots, a_{k-2}(x)) + p^{l-1}a_{k-1}(x) \end{aligned} \tag{5}$$

is a generalized bent function for every choice of $c_i : \mathbb{F}_p^{k-1} \to \mathbb{F}_p$, $0 \leq i \leq l-2$. However this function, which formally maps into $\mathbb{Z}_{2^l}$, is only another instance of the same object, the bent function a_{k-1} with the partition already obtained from f above. One may say that g is obtained from f by "lifting and playing with the partition". In this connection it was already pointed out in [4], that only generalized bent functions given as in (2) for which $a_0, \ldots, a_{k-2}$ are linearly independent are relevant. Hence in [4] the dimension of a generalized bent function is defined as the dimension of the corresponding affine space (3), see [4] for the details. On the other hand, the partitions for two generalized bent functions represented by their affine spaces, $\mathcal{A}_1 = a \oplus \langle a_0, \ldots a_{r-1}\rangle$ and $\mathcal{A}_2 = a \oplus \langle a_0, \ldots a_{r-1}, a_r\rangle$ with $a_0, \ldots, a_{r-1}, a_r$ linearly independent, may still be the same. Easy examples are obtained with constant $a_r(x) = 1$ and $1 \notin \langle a_0, \ldots a_{r-1}\rangle$. The condition $1 \notin \langle a_0, \ldots a_{r-1}\rangle$ is, for instance, satisfied for the nontrivial octal examples in Remark 1. In the light of Theorem 1 they are the same objects, hence we now modify the concept of the dimension of a generalized bent function accordingly.

Lemma 1 *Let $g : \mathbb{V}_n \to \mathbb{Z}_{p^l}$, $g(x) = \sum_{i=0}^{l-1} b_i(x)p^i$ be a generalized bent function, and suppose that the partition $\{A(d) : 0 \leq d \leq p^{l-1} - 1\}$ of $\mathbb{V}_n$, defined as in (4), contains $p^{k-2} < \Omega \leq p^{k-1}$ nonempty sets. Then there exists a generalized bent function $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$ given as $\sum_{i=0}^{k-2} a_i(x)p^i + p^{k-1}b_{l-1}(x)$ with the same partition $\{A(d) : 0 \leq d \leq p^{k-1} - 1\}$ and necessarily linearly independent $a_0, \ldots, a_{k-2}$.*

Proof Pick Ω distinct elements $\delta_1, \ldots, \delta_\Omega \in \{0, \ldots, p^{k-1} - 1\}$, and denote the (nonempty) sets in the partition of $\mathbb{V}_n$ by $\{A(\delta_1), \ldots, A(\delta_\Omega)\}$. Then $a_0(x) + pa_1(x) + \cdots + p^{k-2}a_{k-2}(x) = \delta_j$ if and only if $x \in A(\delta_j)$, uniquely defines the p-ary functions a_i, $0 \leq i \leq k-2$. Since $\Omega > p^{k-2}$, the functions a_i must be linearly independent. With Theorem 1, $\sum_{i=0}^{k-2} a_i(x)p^i + p^{k-1}b_{l-1}(x)$ is generalized bent. Moreover it can be transformed to g described as in (5). □

We now can modify the definition of the dimension of a generalized bent function as follows. We state three equivalent versions.

- The dimension of a generalized bent function is $k-1$ if the corresponding partition $\mathcal{P}$ (defined as above) contains $p^{k-2}+1 \leq \Omega \leq p^{k-1}$ (nonempty) sets.
- The dimension of a generalized bent function f is $k-1$, if k is the smallest number for which there exists a generalized bent function $\tilde{f}(x) = \sum_{i=0}^{k-1} a_i(x) p^i$ from $\mathbb{V}_n$ to $\mathbb{Z}_{p^k}$, which induces the same partition of $\mathbb{V}_n$ as f. The coordinate functions $a_0, a_1, \ldots, a_{k-2}$ are then necessarily linearly independent, i.e., the affine space of bent functions $a_{k-1} \oplus \langle a_0, \ldots, a_{k-2} \rangle$ has dimension $k-1$.
- The dimension of a generalized bent function f is $k-1$ if k is the smallest number for which there exists a generalized bent function $\tilde{f} : \mathbb{V}_n \to \mathbb{Z}_{p^k}$ from which f can be obtained by "lifting and playing with the partition".

3 Designing functions from the PS class

Let $\mathbb{V}_{2m}$ be a $2m$-dimensional vector space over $\mathbb{F}_p$. As is well known, from a spread of $\mathbb{V}_{2m}$ one can construct bent functions from $\mathbb{V}_{2m}$ to $\mathbb{Z}_{p^k}$ respectively relative difference sets in $\mathbb{V}_{2m} \times \mathbb{Z}_{p^k}$ (relative to $\mathbb{Z}_{p^k}$). We recall the proof from which we then also will infer the conditions for obtaining generalized bent functions (which are weaker since generalized bentness is a more general concept).

Proposition 1 *Let $U_0, U_1, \ldots, U_{p^m}$ be the elements of a spread of $\mathbb{V}_n$, $n = 2m$, and $k \leq m$. Define a function $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ by*

(i) *$f(x) = 0$ 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 $c \in \mathbb{Z}_{2^k}$ the nonzero elements of exactly p^{m-k} of the U_i's are mapped to c.*

Then f is a bent function from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$.

Proof Putting $f(x) = c_i$ if $x \in U_i^*$, $1 \leq i \leq p^m$, we have

$$\begin{aligned}\mathcal{H}_f^k(\alpha, u) &= \sum_{i=0}^{p^m} \sum_{z \in U_i \setminus \{0\}} \epsilon_{p^k}^{\alpha f(z)} \epsilon_p^{u \cdot z} + \epsilon_{p^k}^{\alpha f(0)} = \sum_{i=0}^{p^m} \sum_{z \in U_i} \epsilon_{p^k}^{\alpha c_i} \epsilon_p^{u \cdot z} - \sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i} \\ &= \sum_{i=0}^{p^m} \epsilon_{p^k}^{\alpha c_i} \sum_{z \in U_i} \epsilon_p^{u \cdot z} - \sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i}.\end{aligned}$$

Using that for all $u \in \mathbb{V}_n$, $u \neq 0$, the inner product $u \cdot z$ is trivial on exactly one spread element U_{i_u}, i.e. $u \cdot z = 0$ for all $z \in U_{i_u}$, we obtain

$$\begin{aligned}\mathcal{H}_f^k(\alpha, u) &= p^m \epsilon_{p^k}^{\alpha c_{i_u}} - \sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i} \quad \text{if } u \neq 0, \text{ and} \\ \mathcal{H}_f^k(\alpha, 0) &= p^m + (p^m - 1) \sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i}.\end{aligned}$$

With Condition (ii) we have $\sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i} = 0$ for all nonzero $\alpha \in \mathbb{Z}_{p^k}$, which completes the proof. □

Remark 2 We note that Proposition 1 also holds if we replace $\mathbb{Z}_{p^k}$ by any abelian group of order p^k.

Generalized bent functions need to satisfy $|\mathcal{H}_f^k(\alpha, u)| = p^m$ solely for $\alpha = 1$, hence only the weaker condition $\sum_{i=1}^{p^m} \epsilon_{p^k}^{c_i} = 0$ has to hold. Observing that this condition is satisfied if and only if in the sum $\sum_{i=1}^{p^m} \epsilon_{p^k}^{c_i}$ for every $0 \le c \le p^{k-1} - 1$ the elements $\epsilon_{p^k}^{c}, \epsilon_{p^k}^{c+p^{k-1}}, \epsilon_{p^k}^{c+2p^{k-1}}, \ldots, \epsilon_{p^k}^{c+(p-1)p^{k-1}}$ appear the same number of times, we immediately obtain

Corollary 1 *Let $U_0, U_1, \ldots, U_{p^m}$ be a spread of $\mathbb{V}_{2m}$, and let $f : \mathbb{V}_{2m} \to \mathbb{Z}_{p^k}$ be a function satisfying $f(x) = 0$ for $x \in U_0$, and f is constant on the nonzero elements of U_i, $1 \le i \le p^m$. Then f is generalized bent if and only if the number of U_i, $i \neq 0$, mapped to an arbitrary element in $\{c, c + p^{k-1}, c + 2p^{k-1}, \ldots, c + (p-1)p^{k-1}\}$ is the same for every $0 \le c \le p^{k-1} - 1$.*

Remark 3 For the special case $p = 2$ the condition in Corollary 1 implies that the number of spread elements mapped to c and to $c + 2^{k-1}$ has to be the same for every $0 \le c \le 2^{k-1} - 1$. This condition can also be deduced from the description of partial spread generalized bent functions into $\mathbb{Z}_{2^k}$ given in [9].

The most interesting case, also giving generalized bent functions of largest dimension, is the case that $k = m$. We collect some obvious observations on generalized bent functions $f : \mathbb{V}_{2m} \to \mathbb{Z}_{2^m}$ obtained from a spread, and on their partitions $\mathcal{P}$ of $\mathbb{V}_{2m}$ defined as in (4). We restrict ourselves to $p = 2$, similar observations hold for arbitrary p.

- $|\mathcal{P}| \le 2^{m-1}$, (hence $\mathcal{P} = \{A(d) : 0 \le d \le 2^{m-1} - 1\}$), and $|\mathcal{P}| = 2^{m-1}$ if and only if $f : \mathbb{V}_{2m} \to \mathbb{Z}_{2^m}$ is bent.
- All $A(d)$ but one ($A(0)$ w.l.o.g.) contain an even number of spread elements (without $0 \in \mathbb{V}_{2m}$). If f is bent, then $A(d)$ is the union of 2 spread elements (without the 0), $1 \le d \le 2^{m-1} - 1$, and $A(0)$ (w.l.o.g) contains 3.
- All functions $a_{m-1}(x) \oplus C(x)$ as defined in Theorem 1 are partial spread bent functions.
- Since the elements of the partition $\mathcal{P}$ of any (generalized) bent function obtained from a spread contains the (nonzero) elements of at least two spread elements, the spread is a finer partition than $\mathcal{P}$ for any (generalized) bent function obtained from a spread. From a spread one can obtain many (generalized) bent functions of (large) dimension $m - 1$ giving different partitions, hence are different in the light of Theorem 1.

The spread construction is thus very powerful, yielding bent functions in $\mathcal{GB}_{2m}^{p^m}$ consequently relative difference sets in $\mathbb{V}_{2m} \times \mathbb{Z}_{p^m}$, and many more generalized bent functions for which the character sum $\mathcal{H}_f(\alpha, u)$ must have absolute value p^m only for $\alpha = 1$ (and all u). Next we investigate the question if there are functions $f \in \mathcal{GB}_{2m}^{p^m}$ with $|\mathcal{H}_f(\alpha, u)| = p^m$ for several α without necessarily being bent.

First observe that $|\mathcal{H}_f^k(2^t, u)| = 2^m$ is equivalent to $2^t f$ being a generalized bent function, and $|\mathcal{H}_f^k(2^t, u)| = 2^m$ implies $|\mathcal{H}_f^k(2^t r, u)| = 2^m$ for all odd r (i.e. only the order of

the character matters), which is a consequence of the regularity of generalized bent functions defined as in [7] (see [8]). The according statement also holds for odd primes p (for the regularity of generalized bent functions when p is odd, we refer to [11, Lemma 3]). Accordingly, our objective is to construct functions $f \in \mathcal{GB}_{2m}^{p^m}$ such that for a given subset $T \subset \{0, 1, \ldots, m-1\}$ we have $|\mathcal{H}_f^m(p^t, u)| = p^m$ for all $u \in \mathbb{V}_{2m}$ if and only if $t \in T$. We describe a procedure for $p = 2$, which can easily be adapted for any prime p.

Lemma 2 *For a spread $U_0, U_1, \ldots, U_{2^m}$ of $\mathbb{V}_{2m}$, let f be a function from $\mathbb{V}_{2m}$ to $2^{t+1}\mathbb{Z}_{2^m}$ with $f(x) = 0$ for all $x \in U_0$, and f is constant on the nonzero elements of every U_j, $1 \le j \le 2^m$. Suppose that for every $c \in 2^{t+1}\mathbb{Z}_{2^m}$ the number of U_i, $1 \le i \le 2^m$, of which the (nonzero) elements are mapped to c is either zero or 2^{l_c}, $l_c \ge t+1$. Construct from f a function $g \in \mathcal{GB}_{2m}^{2^m}$ and a function $h \in \mathcal{GB}_{2m}^{2^m}$, both taking values in $2^t\mathbb{Z}_{2^m}$, as follows.*

A *For every $c \in 2^{t+1}\mathbb{Z}_{2^m}$ the function g maps 2^{l_c-1} of the 2^{l_c} spread elements which f maps to c to the element $c/2$. The other 2^{l_c-1} of these spread elements the function g maps to $c/2 + 2^{m-1}$.*

B *For every $c \in 2^{t+1}\mathbb{Z}_{2^m}$, the function h maps either*

(i) *2^{l_c-1} of the 2^{l_c} spread elements which f maps to c to the element $c/2$, and the other 2^{l_c-1} of these spread elements the function h maps to $c/2 + 2^{m-1}$, or*

(ii) *all of the 2^{l_c} spread elements which f maps to c the function h maps to one of $c/2$ and $c/2 + 2^{m-1}$.*

For at least one $c \in 2^{t+1}\mathbb{Z}_{2^m}$ the second situation occurs.

Then $2g = f$, $2h = f$, the function g is a generalized bent function, the function h is not a generalized bent function.

Proof Clearly both g and h take values in $2^t\mathbb{Z}_{2^m}$, and $2g = f$, $2h = f$ obviously holds. The function g satisfies the conditions in Corollary 1, hence is generalized bent. Since for h, situation (ii) described in the lemma occurs at least once, h does not satisfy the conditions in Corollary 1, hence it is not generalized bent. □

Lemma 2 is the basis of the algorithm we sketch below to construct a function $f \in \mathcal{GB}_{2m}^{2^m}$ obtained from a spread $U_0, U_1, \ldots, U_{2^m}$ of $\mathbb{V}_{2m}$ for which $|\mathcal{H}_f(2^t, u)| = 2^m$ if and only if $t \in T$ for any prescribed subset T of $\{0, 1, \ldots, m-1\}$.

Algorithm

Input: $m \ge 2$, a subset T of $\{0, 1, \ldots, m-1\}$

Output: A function $f \in \mathcal{GB}_{2m}^{2^m}$ with $|\mathcal{H}_f(2^t, u)| = 2^m$ if and only if $t \in T$

$f(x) = 0$ for all $x \in \mathbb{V}_{2m}$

While $m > 1$

If $m - 1 \in T$, construct from f a function g as in Lemma 2 A,

$g \to f$ *(used for f in the next round)*

else construct from f a function h as in Lemma 2 B,

$h \to f$ *(used for f in the next round)*

$m \to m - 1$ **Output** f

Example $f : \mathbb{V}_{10} \to \mathbb{Z}_{32}$, $T = \{0, 2, 4\}$

In this example c denotes the elements of $\mathbb{Z}_{32}$, the symbol # denotes the number of spread elements different from U_0 which are mapped by f to the element c above. W.l.o.g., U_0 is mapped to 0.

c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	1	0	2	2	1	0	1	2	1	0	0	2	1	0	1	2
c :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	1	0	2	2	1	0	1	2	1	0	0	2	1	0	1	2

From the distribution of the spread elements assigned to the elements of $\mathbb{Z}_{32}$, the distribution for $2f, 4f, 8f, 16f$ of course follows. It is given in the tables below.

c :	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
# :	2	0	$\underline{4}$	4	2	0	2	4	2	0	$\underline{0}$	4	2	0	2	4

c :	0	4	8	12	16	20	24	28
# :	4	0	4	8	4	0	4	8

c :	0	8	16	24
# :	8	$\underline{0}$	8	$\underline{16}$

c :	0	16
# :	17	16

.

As we see, f, $4f$, $16f$ are generalized bent, whereas $2f$, $8f$ are not (the positions at which the condition in Corollary 1 is violated are underlined). Equivalently, $\mathcal{H}_f^5(1, u)$, $\mathcal{H}_f^5(4, u)$, $\mathcal{H}_f^5(16, u)$ have absolute value 2^5 for all $u \in \mathbb{V}_{10}$, whereas this does not apply for $\mathcal{H}_f^5(2, u)$, $\mathcal{H}_f^5(8, u)$. For constructing the function f, one reads the tables from down to up. One first chooses $16f$ by assigning 17 spread elements (including U_0) to 0 and 16 spread elements to 16. As one wants $8f$ not to be generalized bent, for $8f$ all these 16 spread elements are assigned to 24 and none to 8. In the next step one can then "repair" the function and obtain the generalized bent function $4f$. Observe that the value set of the function f has cardinality 22, the corresponding partition contains 11 nonempty sets. Hence the dimension of f is in fact $m - 1 = 4$. In this connection we remark that in the case of $m - 1 \in T$, we have two options in the first step of our algorithm. We either assign all spread elements to 0, or all but U_0 to 2^{m-1}. In the fist case, the resulting function maps only into $2\mathbb{Z}_{2^m} \simeq \mathbb{Z}_{2^{m-1}}$, hence the second choice is to prefer.

Lemma 2 and Algorithm can easily be adapted for odd primes p. In the following ternary example, a function from $\mathbb{V}_6$ to $\mathbb{Z}_{27}$ is designed for which $|\mathcal{H}_f^3(3^t, u)| = 3^3$ for all u, for $t = 0, 2$ but not for $t = 1$.

Example $f : \mathbb{V}_6 \to \mathbb{Z}_{27}$

c :	0	1	2	3	4	5	6	7	8
# :	1	2	1	1	1	1	1	0	1

c :	9	10	11	12	13	14	15	16	17
# :	1	2	1	1	1	1	1	0	1

c :	18	19	20	21	22	23	24	25	26
# :	1	2	1	1	1	1	1	0	1

With this choice the distribution for $3f, 9f$ is as follows:

$$\begin{array}{l} c: 0\ 3\ 6\ 9\ 12\ 15\ 18\ 21\ 24 \\ \#: 3\ \underline{6}\ 3\ 3\ \underline{3}\ \ 3\ \ 3\ \ \underline{0}\ \ 3 \end{array}$$

$$\begin{array}{l} c: 0\ 9\ 18 \\ \#: 9\ 9\ \ 9 \end{array}$$

Summarizing, in this section we gave a constructive proof of

Theorem 2 *For every integer $m \geq 2$ and subset T of $\{0, 1, \ldots, m-1\}$ there exist functions from $\mathbb{V}_{2m}$ to $\mathbb{Z}_{p^m}$ such that $\mathcal{H}_f^m(p^t, u)$ has absolute value p^m for all $u \in \mathbb{V}_{2m}$ if and only if $t \in T$.*

Remark 4 We note that it is in general difficult to find a function f if only the absolute values of the Walsh transform are known. Therefore, Theorem 2 is quite remarkable. The reason why we can construct a function given the absolute values of the Walsh transform heavily rely on the nice properties of the underlying spread.

4 The Maiorana-McFarland class and generalized bent functions of largest dimension

As seen in the previous section, from a spread of $\mathbb{V}_{2m}$ one can obtain various bent and generalized bent functions from $\mathbb{V}_{2m}$ to $\mathbb{Z}_{p^m}$ (with large dimension $m-1$, i.e. the cardinality Ω of the corresponding partition $\mathcal{P}$ of $\mathbb{V}_{2m}$ satisfies $p^{m-2}+1 \leq \Omega \leq p^{m-1}$). Note that when $p = 2$, for a bent function from $\mathbb{V}_{2m}$ to $\mathbb{Z}_{2^k}$, the largest value for k is m, cf. [13, 17]. In this section we will see that generalized bent functions can have an even finer partition. More precisely, we will show that there exist generalized bent functions from $\mathbb{V}_{2m}$ to $\mathbb{Z}_{p^{m+1}}$ for which the corresponding partition $\mathcal{P}$ of $\mathbb{V}_{2m}$ has cardinality larger than p^m. We show that the cardinality of the partition of a generalized bent function from $\mathbb{V}_{2m}$ into a cyclic group is upper bounded by p^{m+1}. This upper bound can be attained with functions obtained from the completed Maiorana-McFarland class.

We require some results from the literature. For a subset A of $\mathbb{V}_n$ we denote the indicator function of A by $I(A)$, i.e.,

$$I(A)(x) = \begin{cases} 1 & : \quad x \in A, \\ 0 & : \quad \text{otherwise.} \end{cases}$$

In [3], Carlet presented the following secondary construction of Boolean bent functions which can easily be generalized to p-ary bent functions, see [14]:

Lemma 3 *If g is a bent function from $\mathbb{V}_n$ to $\mathbb{F}_p$ which is affine on an $n/2$-dimensional affine subspace A of $\mathbb{V}_n$, then for all $c \in \mathbb{F}_p$, the function $g \oplus cI(A)$ is again a bent function.*

In [5, 6], Kolomeec further analysed this observation and used it to investigate the graph of minimal distances of bent functions. We will use the following lemma, see [5] and Proposition 1 in [6], and for the p-ary version [14].

Lemma 4 *Two bent functions from $\mathbb{V}_n$ to $\mathbb{F}_p$ differ at least at $p^{n/2}$ positions. Two bent functions with minimal distance $p^{n/2}$ always differ on an affine subspace (of dimension $n/2$), restricted to which they are affine functions.*

With Lemma 4, we can show some properties of the partition $\mathcal{P}$ corresponding to a generalized bent function in $\mathcal{GB}_n^{p^k}$.

Theorem 3 *Let $f \in \mathcal{GB}_n^{p^k}$, $f(x) = \sum_{i=0}^{k-1} a_i(x)p^i$, be a generalized bent function with the partition $\mathcal{P} = \{A(d) : 0 \le d \le p^{k-1} - 1\}$ of $\mathbb{V}_n$ defined as in (4). Then*

(i) *$|A(d)| \ge p^{n/2}$ (or $A(d) = \emptyset$), and if $|A(d)| = p^{n/2}$, then $A(d)$ is an affine subspace of $\mathbb{V}_n$ on which a_{k-1} is affine,*
(ii) *there are at most $p^{n/2}$ integers $0 \le d \le p^{k-1} - 1$ such that $A(d) \ne \emptyset$.*

Proof (i) If f is generalized bent, then $a_{k-1}(x) \oplus C(x)$ is bent for every Boolean (p-ary) function which is constant on $A(d)$ for all $0 \le d \le p^{k-1} - 1$. In particular this applies if $C(x) = I(A(d))$, where $I(A(d))$ is the indicator function of $A(d)$ for a fixed $0 \le d \le p^{k-1} - 1$. Since by Lemma 4 two bent functions differ at least at $p^{n/2}$ positions, we must have $|A(d)| \ge p^{n/2}$ for all $0 \le d \le p^{k-1} - 1$ (or $A(d) = \emptyset$). Furthermore, by Lemma 4, two bent functions with minimal distance $p^{n/2}$ always differ on an affine subspace (of dimension $n/2$), restricted to which they are affine functions. This shows the second statement in (i).

(ii) follows immediately from the fact that every nonempty set $A(d)$ in the partition of $\mathbb{V}_n$ has cardinality at least $p^{n/2}$. □

Bent functions in dimension n which are affine on many $n/2$-dimensional affine subspaces are the Maiorana-McFarland bent functions. The following characterization of the completed Maiorana-McFarland class is well known, see e.g. [6, Proposition 11]

Lemma 5 *A bent function $f : \mathbb{V}_n \to \mathbb{F}_p$ is in the completed Maiorana-McFarland class if and only if there exists an $n/2$-dimensional affine subspace Λ of $\mathbb{V}_n$ such that f is affine on each coset of Λ.*

With Lemmas 3 and 5 we obtain the following theorem.

Theorem 4 *Let $f : \mathbb{V}_{2m} \to \mathbb{Z}_{p^{m+1}}$ be a generalized bent function for which the corresponding partition $\mathcal{P} = \{A(d) : 0 \le d \le p^m - 1\}$ defined as in (4) attains the upper bound $|\mathcal{P}| = p^m$ (hence for all $0 \le d \le p^m - 1$ the set $A(d)$ is not empty and $|A(d)| = p^m$), and the affine subspaces in $\mathcal{P} = \{A(d) : 0 \le d \le p^m - 1\}$ are parallel. Then $f(x) = a_0(x) + \cdots + p^{m-1}a_{m-1}(x) + p^m a_m(x)$ for a bent function a_m in the completed Maiorana-McFarland class. Conversely, for every bent function in the completed Maiorana-McFarland class we have such an extremal generalized bent function.*

Proof If $|A(d)| = p^m$ for all d, then by Theorem 3, $\mathbb{V}_{2m}$ is partitioned by $\mathcal{P} = \{A(d) : 0 \le d \le p^m - 1\}$ into affine subspaces. We assume that these are parallel. Consequently, $\mathcal{P}$ must be the set of all cosets of an $n/2$-dimensional subspace of $\mathbb{V}_n$. Again by Theorem 3, the bent function $a_m(x)$ is then affine on all of these cosets. (Note that the dimension of f is

m, and f has a representation as given in the theorem.) By Lemma 5, a_m is in the completed Maiorana-McFarland class.

Let now $a : \mathbb{V}_{2m} \to \mathbb{F}_p$ be in the completed Maiorana-McFarland class, i.e. $a(x)$ is affine on the cosets of an m-dimensional linear subspace of $\mathbb{V}_{2m}$. These cosets form then a partition $\mathcal{P} = \{A(d) : 0 \le d \le p^m - 1\}$ of $\mathbb{V}_{2m}$. It remains to show that then $a(x) \oplus C(x)$ is bent for all $C : \mathbb{V}_{2m} \to \mathbb{F}_p$ which are constant on $A(d)$ for all d. This follows by repeatedly applying Carlet's construction of bent functions in Lemma 3 using the affine subspaces $A(d)$. □

Remark 5 The fact that the sets in $\mathcal{P} = \{A(d) : 0 \le d \le p^m - 1\}$ are affine subspaces does not imply that they are parallel. As shown in [1], there even exist partitions of $\mathbb{V}_n$ into affine subspaces all of dimension r, $1 \le r \le n-2$, no two of which are parallel.

We close with a result for $p = 2$ which is related to vertices of maximum degree in the graph of minimal distances of bent functions, see [6]. It shows that for a Maiorana-McFarland bent function, we can have many such maximal partitions $\mathcal{P}$. Most of such partitions we have for the quadratic bent function.

Theorem 5 *Let $q : \mathbb{V}_n \to \mathbb{F}_2$ be a quadratic bent function. Then there are $K = (2^1 + 1)(2^2 + 1) \cdot \cdots \cdot (2^{\frac{n}{2}} + 1)$ distinct linear subspaces of $\mathbb{V}_n$ of dimension $n/2$ such that q is constant on any of the cosets. This yields K distinct partitions of $\mathbb{V}_n$ for generalized bent functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^{n/2+1}}$, i.e. K different generalized bent functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^{n/2+1}}$. This is the maximal number of such partitions a bent function can have.*

Proof The proof uses the following results of [6].

(i) [6, Theorem 1]: The only bent function $f : \mathbb{V}_n \to \mathbb{F}_2$ with the properties

I f is affine on some $n/2$-dimensional affine subspace of $\mathbb{V}_n$,
II if f is affine on an $n/2$-dimensional affine subspace L of $\mathbb{V}_n$, then f is affine on every coset of L,

is the quadratic bent function (invariant under EA-equivalence).

(ii) The number of the m-dimensional affine subspaces, $m = n/2$, on which the quadratic bent function is affine is $2^m(2^1 + 1)(2^2 + 1) \cdot \cdots \cdot (2^m + 1)$, [6, Theorem 2]. (In the language of [6] this is the maximum degree of a vertex in the graph of minimal distances of bent functions.)

(iii) Every not quadratic bent function is affine on a smaller number of such affine subspaces, [6, Theorem 2].

By (ii) and (i) there are K distinct linear subspaces of $\mathbb{V}_n$ of dimension $n/2$ such that q is constant on any of the cosets, which by (i) yield K distinct partitions of $\mathbb{V}_n$ for generalized bent functions. With (iii), K is the maximal number of such partitions a bent function can have. □

5 Perspectives

A generalized bent function from $\mathbb{V}_{2m}$ to $\mathbb{Z}_{p^k}$ (of dimension $k-1$), which satisfies $|\mathcal{H}_f^k(1,u)| = p^m$, can be also viewed as a bent function $a : \mathbb{V}_{2m} \to \mathbb{F}_p$, for which

additionally there exists a partition $\mathcal{P}$ of $\mathbb{V}_{2m}$ of cardinality $p^{k-2}+1 \leq \Omega \leq p^{k-1}$ such that $a(x) \oplus C(x)$ is also bent for every function C which is constant on the elements of $\mathcal{P}$. Generalized bent functions (for $k \geq 3$) are harder to find than conventional bent functions since the image set is contained in a cyclic group rather than an elementary abelian group.

We first showed that with spreads we not only can construct bent functions f from $\mathbb{V}_{2m}$ to $\mathbb{Z}_{p^m}$ (satisfying $|\mathcal{H}_f^m(p^t,u)| = p^m$ for all $0 \leq t \leq m-1$ (and all $u \in \mathbb{V}_{2m}$)), and a large variety of generalized bent functions, i.e. functions for which $|\mathcal{H}_f^m(1,u)| = p^m$, but we can also design functions $f \in \mathcal{GB}_{2m}^{p^m}$ for which $|\mathcal{H}_f^m(p^t,u)| = p^m$ if and only if $t \in T$ for any subset T of $\{0,1,\ldots,m-1\}$.

For a bent function from $\mathbb{V}_{2m}$ to $\mathbb{Z}_{2^k}$, the value $k=m$, which is attained by spread bent functions, is maximal possible. We show that the weaker generalized bent functions can even have dimension m, i.e. there are Boolean (p-ary) bent functions which allow an even finer partition than the spread partition. Bent functions with the finest possible partition are the functions in the completed Maiorana-McFarland class. Note that by Remark 5, we cannot exclude the existence of other such bent functions.

There are many further interesting questions to investigate, some of which may be the following:

- Note that there are bent functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^{n/2}}$ and from $\mathbb{V}_n$ to $\mathbb{Z}_{p^{n/2}}$. As far as we know, the only examples of such bent functions rely on spreads in $\mathbb{V}_n$. Try to prove that this has to be the case, or find a counter example. Note that our Theorem 4 shows that there are other constructions in the generalized bent case.
- Find bent functions $\mathbb{V}_n \to \mathbb{Z}_{p^k}$ (p prime) which are not related to spreads. This problem is, of course, related to the problem of proving inequivalence of relative difference sets, which might be difficult. One potential example is the function in [10, Corollary 3] (based on Theorem 14 in [12]), of which one can show that it is a bent function from $\mathbb{V}_n$ to $\mathbb{Z}_8$ (obtained from Maiorana-McFarland functions), which is not obtained from a spread as described in Section 3 for some $n \geq 12$. In fact, the concrete example obtained by choosing $m=6$ and $e=5$ in Table 1 in [12] yields a bent function in $\mathcal{GB}_{12}^8$ for which the components have algebraic degree 3. The components of all generalized bent functions obtained from the spread construction have degree m.
- Find "best partitions" $\mathcal{P}$ for classes of bent functions other than spread or Maiorana-McFarland bent functions. This, of course, means to construct, first, other examples of generalized bent functions.

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

References

1. Baum, L., Neuwirth, L.: Decompositions of vector spaces over GF(2) into disjoint equidimensional affine spaces. J. Combin. Theory Ser. A **18**, 88–100 (1975)
2. Carlet, C., et al.: On bent and highly non-linear balanced/resilient functions and their algebraic immunities. In: Fossorier, M.P.C. (ed.) AAECC, Lecture notes in computer science 3857, pp. 1–28. Springer-Verlag, New York (2006)
3. Carlet, C.: Two new classes of bent functions. In: Advances in Cryptology–EUROCRYPT93, Lecture Notes Comput. Sci 765, pp.77–101, Springer-Verlag (1994)
4. Hodzić, S., Meidl, W., Pasalic, E.: Full characterization of generalized bent functions as (semi)-bent spaces, their dual, and the Gray image. IEEE Trans. Inform. Theory **64**, 5432–5440 (2018)

5. Kolomeec, N.: Enumeration of the bent functions of least deviation from a quadratic bent function. J. Appl. Ind. Math. **6**, 306–317 (2012)
6. Kolomeec, N.: The graph of minimal distances of bent functions and its properties. Des. Codes Cryptogr. **85**, 395–410 (2017)
7. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Combin. Theory Ser. A **40**, 90–107 (1985)
8. Martinsen, T., Meidl, W., Stanica, P.: Generalized bent functions and their gray images. In: Arithmetic of finite fields, Lecture Notes in Comput. Sci., 10064, pp. 160–173. Springer, Cham (2016)
9. Martinsen, T., Meidl, W., Stanica, P.: Partial spread and vectorial generalized bent functions. Des. Codes Cryptogr. **85**, 1–13 (2017)
10. Meidl, W.: A secondary construction of bent functions, octal gbent functions and their duals. Math. Comput. Simulation **143**, 57–64 (2018)
11. Mesnager, S., Tang, C., Qi, Y., Wang, L., Wu, B., Feng, K.: Further results on generalized bent functions and their complete characterization. IEEE Trans. Inform. Theory **64**, 5441–5452 (2018)
12. Mesnager, S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inform. Theory **60**(7), 4397–4407 (2014)
13. 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)
14. Potapov, V.: On minimal distance of q-ary bent functions. In: Problems of redundancy in information and control systems, pp. 115–116, IEEE (2016)
15. Pott, A.: Nonlinear functions in abelian groups and relative difference sets. Discret. Appl. Math. **138**, 177–193 (2004)
16. Pott, A.: A survey on relative difference sets. Groups, difference sets, and the Monster. In: Ohio State Univ. Math. Res. Inst. Publ., 4, pp. 195–232, de Gruyter, Berlin (1996)
17. Schmidt, B.: On (p^a, p^b, p^a, p^{a-b})-relative difference sets. J. Algebraic Combin. **6**, 279–297 (1997)
18. Schmidt, K.U.: Quaternary constant-amplitude codes for multicode CDMA. IEEE Trans. Inform. Theory **55**, 1824–1832 (2009)
19. Tang, C., Xiang, C., Qi, Y., Feng, K.: Complete characterization of generalized bent and 2k-bent Boolean functions. IEEE Trans. Inform. Theory **63**, 4668–4674 (2017)