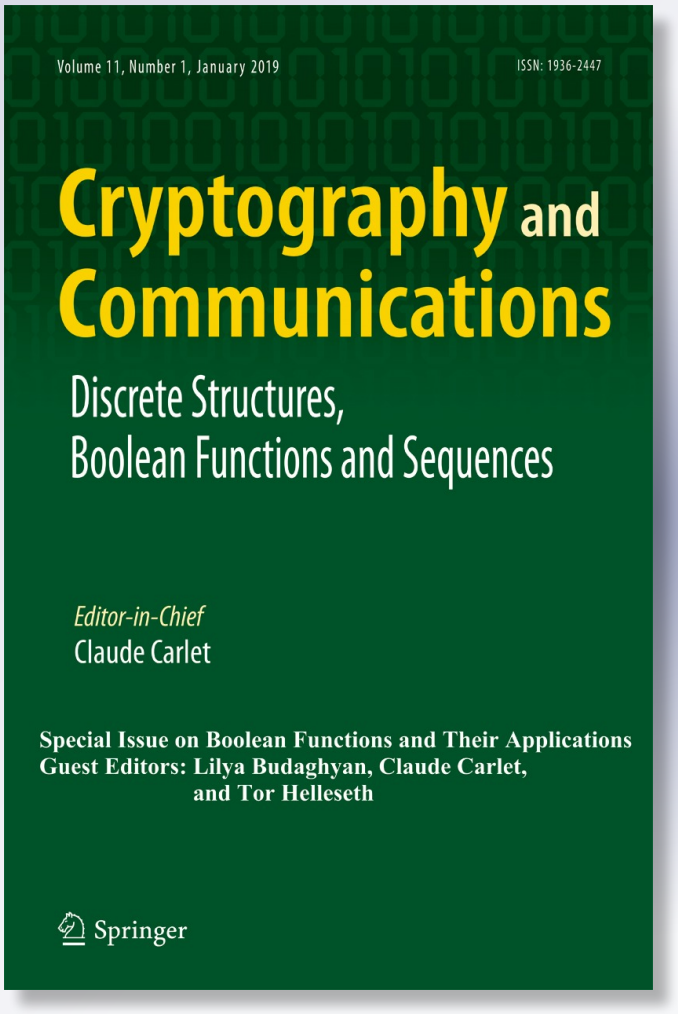
New classes of p-ary bent functions

Bimal Mandal, Pantelimon Stănică & Sugata Gangopadhyay

Cryptography and Communications
Discrete Structures, Boolean Functions and Sequences

ISSN 1936-2447
Volume 11
Number 1

Cryptogr. Commun. (2019) 11:77-92
DOI 10.1007/s12095-018-0290-9



Springer

Cryptogr. Commun. (2019) 11:77–92
https://doi.org/10.1007/s12095-018-0290-9

New classes of p-ary bent functions

Bimal Mandal[1] · **Pantelimon Stănică**[2] · **Sugata Gangopadhyay**[3]

Received: 12 October 2017 / Accepted: 28 February 2018 / Published online: 7 March 2018

Abstract In this paper, we consider the p-ary functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, where p is an odd prime. We characterize the subspace sum concept (depending upon the derivative) and give many of its properties. In particular, we show that the subspace sum of p-ary functions with respect to a subspace of $\mathbb{F}_p^n$ is an affine invariant. Further, we construct two new classes of p-ary bent functions, which do not contain one another.

Keywords Subspace sum · p-ary bent functions · Affine invariance

Mathematics Subject Classification (2010) 06E30 · 94C10

1 Introduction

Rothaus introduced the notion of bent Boolean functions concept in the 1960's, although his paper was not published until ten years later [22]. Bent functions are of interest since

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

✉ Pantelimon Stănică
pstanica@nps.edu

Bimal Mandal
bimalmandal90@gmail.com

Sugata Gangopadhyay
gsugata@gmail.com

[1] Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee 247667, India

[2] Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216, USA

[3] Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, Roorkee 247667, India

they are maximum Hamming distance away from the set of affine functions and have very nice combinatorial properties. Several classes of bent functions were constructed by Dillon [9], Rothaus [22], and Dobbertin [10]. Carlet [4] constructed two (so-called $\mathcal{D}$, $\mathcal{C}$) classes of bent Boolean functions by modifying the Maiorana–McFarland bent functions. Kumar et al. [17] introduced the concept of generalized bent functions $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$, where $q > 1$ is a positive integer and gave constructions for every possible q and n, except when n is odd and $q \equiv 2 \pmod 4$. Later, generalized bent functions over the finite field were studied by Ambrosimov [1]. There has been a renewed interest in this area, with new constructions being displayed, characterizations, and even connecting them to certain combinatorial objects such as partial difference sets, strongly regular graphs, association schemes and orthogonal frequency-division multiplexing (OFDM) (see [7, 15, 21, 23, 24]). For efficient wireless communication, generalized bent functions are used for large signal sets with low maximum crosscorrelation [11, 12, 16, 20, 26]. In 2006, Helleseth et al. [13] identified some monomial and quadratic bent functions over the finite fields of odd characteristic. In 2012, Budaghyan et al. [3] found some non-quadratic p-ary bent functions which do not belong to the complete p-ary Maiorana–McFarland class and proved that the complete p-ary Maiorana–McFarland class does not cover all quadratic bent functions, which is not the case in the characteristic two environment.

The rest of this article is organized as follows. In Section 1, some basic definitions and known results related to p-ary function, group algebra and generalized Reed–Muller code are given. In Section 2.1, we introduce the subspace sum concept (depending upon the derivative) and give many of its properties. In Section 2.2, we construct two new classes of p-ary bent functions (so-called $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$), which do not contain one another. In Section 2.3, we investigate conditions on $\mathcal{C}^p$ classes of bent functions for two classes of permutations and suitable linear subspaces of dimension ≤ 2 for $p = 3$.

1.1 Preliminary results

Let $\mathbb{F}_p$ and $\mathbb{F}_{p^n}$ be the prime field of characteristic p and the extension field of degree n over $\mathbb{F}_p$, respectively. Let $\mathbb{F}_p^n$ be the vector space of all n-tuples of elements of $\mathbb{F}_p$, i.e., $\mathbb{F}_p^n = \{x = (x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}_p, i = 1, 2, \ldots, n\}$, with the usual operations. Any $x \in \mathbb{F}_{p^n}$ can be written as

$$x = c_1x_1 + c_2x_2 + \cdots + c_nx_n,$$

where $x_i \in \mathbb{F}_p$, $1 \leq i \leq n$ and $c = \{c_1, c_2, \ldots, c_n\}$ is a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. A function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ (or, equivalently from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$) is called a *p-ary function* (also called a generalized function) in n variables. The set of all p-ary functions in n variables is denoted by $\mathcal{B}_n^p$. For $p = 2$, we obtain the classical Boolean functions, whose set is denoted by $\mathcal{B}_n$. Any $f \in \mathcal{B}_n^p$ can be uniquely expressed [14] as a polynomial in $\mathbb{F}_p[x_1, x_2, \ldots, x_n]/\langle x_1^p - x, \ldots, x_n^p - x\rangle$ of the form

$$f(x_1, x_2, \ldots, x_n) = \sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_p^n} \mu_a \left(\prod_{i=1}^{n} x_i^{a_i}\right),$$

where $\mu_a \in \mathbb{F}_p$. The *algebraic degree* of f, denoted by $\deg(f)$, is defined as $\deg(f) = \max_{a\in\mathbb{F}_p^n} \left\{\sum_{i=1}^n a_i : \mu_a \neq 0\right\}$, where $a = (a_1, \ldots, a_n) \in \mathbb{F}_p^n$, the sum being over $\mathbb{Z}$, the

ring of integers. The *generalized Walsh–Hadamard transform* of a function $f \in \mathcal{B}_n^p$ at $a \in \mathbb{F}_p^n$ is defined by

$$\mathcal{H}_f(a) = \sum_{x \in \mathbb{F}_p^n} \zeta^{f(x)-a\cdot x},$$

where $\zeta = e^{\frac{2\pi i}{p}}$ is the complex p^{th} root of unity and $a \cdot x$ denotes an inner product on $\mathbb{F}_p^n$. According to [17], a function $f \in \mathcal{B}_n^p$ is called a *p-ary bent function* if

$$|\mathcal{H}_f(a)| = p^{\frac{n}{2}} \text{ for all } a \in \mathbb{F}_p^n.$$

A p-ary bent function f is called *regular* (see [17, Definition 3] and [14, page 576]) if $\mathcal{H}_f(a) = p^{\frac{n}{2}} \zeta^{\tilde{f}(a)}$ for all $a \in \mathbb{F}_p^n$, where $\tilde{f} \in \mathcal{B}_n^p$. Here $\tilde{f}$ is called the *dual* of f. It is known that a function $f \in \mathcal{B}_n^p$ is a p-ary bent function [17, page 96] if for any nonzero $a \in \mathbb{F}_p^n$, the (autocorrelation) sum

$$\sum_{x \in \mathbb{F}_p^n} \zeta^{f(x+a)-f(x)} = 0.$$

The group of all invertible $\mathbb{F}_p$-linear transformations on $\mathbb{F}_p^n$ is denoted by $GL(n, \mathbb{F}_p)$. Two p-ary functions $f, g \in \mathcal{B}_n^p$ are said to be *affine equivalent* if and only if there exist $A \in GL(n, \mathbb{F}_p)$ and $b \in \mathbb{F}_p^n$ such that $g(x) = f(xA + b)$ for all $x \in \mathbb{F}_p^n$. The affine general linear group $AGL(n, \mathbb{F}_p)$ consists all the elements of the form $(A, b) \in GL(n, \mathbb{F}_p) \times \mathbb{F}_p^n$. Two p-ary functions $f, g \in \mathcal{B}_n^p$ are said to be *equivalent* if and only if there exist $(A, b) \in AGL(n, \mathbb{F}_p)$, $u \in \mathbb{F}_p^n$ and $\varepsilon \in \mathbb{F}_p$ such that

$$g(x) = f(xA + b) + u \cdot x + \varepsilon \text{ for all } x \in \mathbb{F}_p^n.$$

Let $\mathcal{A}$ be a group algebra of $\mathbb{F}_p^n$ over the field $\mathbb{F}_p$. An element $x \in \mathcal{A}$ is a formal sum

$$x = \sum_{g \in \mathbb{F}_p^n} x_g X^g, \text{ where } x_g \in \mathbb{F}_p.$$

For any $x, y \in \mathcal{A}$ and $c \in \mathbb{F}_p$, addition and scalar multiplication can be defined as

$$\begin{aligned} x + y &= \textstyle\sum_{g \in \mathbb{F}_p^n} x_g X^g + \sum_{g \in \mathbb{F}_p^n} y_g X^g = \sum_{g \in \mathbb{F}_p^n} z_g X^g, \text{ where } z_g = x_g + y_g \in \mathbb{F}_p \\ \text{and} \quad cx &= c \textstyle\sum_{g \in \mathbb{F}_p^n} x_g X^g = \sum_{g \in \mathbb{F}_p^n} (cx_g) X^g = \sum_{g \in \mathbb{F}_p^n} w_g X^g, \text{ where } w_g = cx_g \in \mathbb{F}_p. \end{aligned}$$

Using the polynomial multiplication $X^g X^h = X^{g+h}$, the multiplication in the group algebra $\mathcal{A}$ is defined by

$$xy = \textstyle\sum_{g \in \mathbb{F}_p^n} x_g X^g \sum_{h \in \mathbb{F}_p^n} y_h X^h = \sum_{\ell \in \mathbb{F}_p^n} \left(\sum_{g \in \mathbb{F}_p^n} x_g y_{\ell - g} \right) X^\ell.$$

Note that X^0 is the multiplicative unit of $\mathcal{A}$ as $X^0 a = a X^0 = a$ for all $a \in \mathcal{A}$. Consider the mapping $\psi : \mathcal{A} \longrightarrow \mathbb{F}_p$ defined by

$$x = \sum_{g \in \mathbb{F}_p^n} x_g X^g \longmapsto \sum_{g \in \mathbb{F}_p^n} x_g \text{ for all } x \in \mathcal{A}.$$

Then the set $\mathcal{P} = \{x \in \mathcal{A} : \psi(x) = 0\} = \{x \in \mathcal{A} : \sum_{g \in \mathbb{F}_p^n} x_g = 0\}$ is the unique maximal ideal of $\mathcal{A}$, and

$$\mathcal{A} = \mathcal{P}^0 \supset \mathcal{P} \supset \mathcal{P}^2 \supset \ldots \supset \mathcal{P}^{n(p-1)} = \mathbb{F}_p,$$

where $\mathcal{P}^i\mathcal{P}^j = \mathcal{P}^{i+j}$ and $\mathcal{P}^{n(p-1)+1} = \{0\}$. A p-ary function $f \in \mathcal{B}_n^p$ can be identified with a codeword $\Omega_f = \sum_{g\in\mathbb{F}_p^n} f(g)X^g$ of length p^n consisting of all values of $f(x), x \in \mathbb{F}_p^n$. The *support* of Ω_f, denoted by $supp(\Omega_f)$, is defined by $supp(\Omega_f) = \{x \in \mathbb{F}_p^n : f(x) \neq 0\}$. The generalized Reed–Muller code, $\mathcal{R}_p(r, n)$, is the set of codewords Ω_f, where $f \in \mathcal{B}_n^p$ and $\deg(f) \leq r$, $0 \leq r \leq n(p-1)$. If $f \in \mathcal{B}_n^p$ with $\deg(f) = r$, then Ω_f is in $\mathcal{P}^{n(p-1)-r}$. Further, we refer to [2].

The *derivative* of $f \in \mathcal{B}_n^p$ with respect to $a \in \mathbb{F}_p^n$, denoted by $D_a f$, is defined by

$$D_a f(x) = f(x + a) - f(x) \text{ for all } x \in \mathbb{F}_p^n.$$

The kth order derivative of $f \in \mathcal{B}_n^p$ with respect to $u_1, u_2, \ldots, u_k \in \mathbb{F}_p^n$ is defined by $D_{u_1,u_2,\ldots,u_k} f(x) = D_{u_1} D_{u_2} \ldots D_{u_k} f(x)$ for all $x \in \mathbb{F}_p^n$. If $u_1 = u_2 = \ldots = u_k =: u$, for easy easiness, we write $D_u^k f(x)$ in lieu of $\underbrace{D_u D_u \ldots D_u}_{k-\text{times}} f(x)$.

In what follows, p denotes an (arbitrary, but fixed) odd prime number. Let $a, b \in \mathbb{F}_p^n$ and E be a linear subspace of $\mathbb{F}_p^n$. It is known that

$$\sum_{x\in a+E} \zeta^{b\cdot x} = \zeta^{a\cdot b}|E|\phi_{E^\perp}(b),$$

where $\zeta = e^{\frac{2\pi i}{p}}$ is the p^{th} complex root of unity and $\phi_{E^\perp}(b) = 1$ if $b \in E^\perp$, otherwise 0.

Theorem 1 ([17, Theorem 1]) *Let $m = 2n$ and $f : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p$ be a p-ary function of the form*

$$f(x, y) = x \cdot \pi(y) + g(y),$$

where π is an arbitrary permutation polynomial over $\mathbb{F}_p^n$ and $g \in \mathcal{B}_n^p$. Then f is a regular bent function and the dual of f is $\tilde{f}(x, y) = y \cdot \pi^{-1}(x) + g(\pi^{-1}(x))$ (see [8]).

The bent functions defined as in Theorem 1 are called *p-ary Maiorana–McFarland bent* functions and their set is denoted by $\mathcal{M}^p$.

Definition 2 A class of bent functions is said to be complete if it is globally invariant under the action of the general affine group and under the addition of affine functions.

In the binary case, the completed Maiorana–McFarland class contains all quadratic bent functions which are the simplest and best understood. However, this does not hold in the p-ary case, $p \geq 3$.

Lemma 3 ([4, Generalization of Lemma 1]) *Let E be any linear subspace of $\mathbb{F}_p^n$ and $f \in \mathcal{B}_n^p$ be a regular bent function. Then, for any $a, b \in \mathbb{F}_p^n$, we have*

$$\sum_{x\in -a+E} \zeta^{f(x)-b\cdot x} = p^{\dim E - \frac{n}{2}} \zeta^{a\cdot b} \sum_{x\in b+E^\perp} \zeta^{\tilde{f}(x)-a\cdot x},$$

where $\zeta = e^{\frac{2\pi i}{p}}$ is the p^{th} complex root of unity and $\tilde{f}$ is the dual of f.

Suppose $a = b = 0$ and $\dim E = \frac{n}{2}$ ($\dim E$ denotes the dimension of a vector space E). From Lemma 3, we get

$$\sum_{x \in E} \zeta^{f(x)} = \sum_{x \in E^{\perp}} \zeta^{\tilde{f}(x)}.$$

Therefore, if the restriction $f_{/E}$ of f to E is i, then also the restriction $\tilde{f}_{/E^{\perp}}$ of $\tilde{f}$ to $E^{\perp}$ is i, where $i \in \{0, 1, \ldots, p-1\}$.

We now state the generalization (due to Charpin [5, 6]) of Berman's Theorem.

Theorem 4 ([2, Theorem 5.19]) *Let $\mathcal{R}_p(r, n)$ be generalized Reed–Muller codes, where $0 \le r \le n(p-1)$. Then $\mathcal{R}_p(r, n)$ is equal to $\mathcal{P}^{n(p-1)-r}$.*

Let $t = k(p-1)$, where k is a positive integer. From [2, Corollary 4.12], we know that $\mathcal{P}^t$ is a subspace generated by the codewords whose support is a k-dimensional subspace of $\mathbb{F}_p^n$.

2 Main results

In this section, we define the subspace sum (denoted by $\mathcal{S}_V f$) of a p-ary function $f \in \mathcal{B}_n^p$ with respect to a subspace V of $\mathbb{F}_p^n$ and prove that if $f, g \in \mathcal{B}_n^p$ are affine equivalent, then so are $\mathcal{S}_V f$ and $\mathcal{S}_V g$. Further, we extend to characteristic $p > 2$ a binary result of Dillon [9], concerning the vanishing subspace sum of any Maiorana–McFarland bent functions. Budaghyan at el. [3, Proposition 1] proved that if $f \in \mathcal{B}_n^p$ belongs to the complete p-ary Maiorana–McFarland class, then there exists a subspace of $\mathbb{F}_p^n$ with dimension $\frac{n}{2}$ such that all second derivatives vanishes, where n is even. We also derive a necessary condition for p-ary Maiorana–McFarland bent functions using the subspace sum.

In the binary case, the kth order derivative of a Boolean function $f \in \mathcal{B}_n$ with respect to $a_1, a_2, \ldots, a_k \in \mathbb{F}_2^n$ is same as the sum of the values of f on the coset $x + V$, where V is a k-dimensional subspace generated by $a_1, a_2, \ldots, a_k$. However, if $p \ge 3$ and $f \in \mathcal{B}_n^p$, the above two quantities may be different. Prompted by this observation, we introduce and study the subspace sum concept and its connection to affine invariance.

2.1 The subspace sum of a function

Let $f \in \mathcal{B}_n^p$ and V be any k-dimensional subspace of $\mathbb{F}_p^n$. Then, there exist k linearly independent elements $a_1, a_2, \ldots, a_k \in \mathbb{F}_p^n$ such that

$$V = \langle a_1, a_2, \ldots, a_k \rangle = \{a \in \mathbb{F}_p^n : a = \textstyle\sum_{i=1}^{k} c_i a_i, \text{ where } c_i \in \mathbb{F}_p, 1 \le i \le k\}.$$

Definition 5 The subspace sum of $f \in \mathcal{B}_n^p$ with respect to a subspace V of $\mathbb{F}_p^n$ is a p-ary function $\mathcal{S}_V f$, defined by

$$\mathcal{S}_V f(x) = \sum_{v \in V} f(x + v) \text{ for all } x \in \mathbb{F}_p^n.$$

More precisely, $\mathcal{S}_V f(x)$ is the sum of the values of f on the coset $x + V$ which depends on V, not only on the dimension of V. The functions $\mathcal{S}_{V_1} f$ and $\mathcal{S}_{V_2} f$ may be different even though the dimensions of two distinct subspaces V_1 and V_2 of $\mathbb{F}_p^n$ are equal. For example, $V_1 = \langle (1, 0, 0) \rangle$, $V_2 = \langle (0, 1, 0) \rangle$ and $f \in \mathcal{B}_3^3$ be defined as $f(x_1, x_2, x_3) = x_1^2 x_2$, for

all $x_i \in \mathbb{F}_3$, $1 \le i \le 3$. Then $\mathcal{S}_{V_1} f(x_1, x_2, x_3) = 2x_2$ and $\mathcal{S}_{V_2} f(x_1, x_2, x_3) = 0$, for all $x_i \in \mathbb{F}_3$, $1 \le i \le 3$.

Lemma 6 *Let $f \in \mathcal{B}_n^p$ and $V = \langle a \rangle$ be a one dimensional subspace of $\mathbb{F}_p^n$ generated by a, and $j \in \mathbb{F}_p$. Then $\mathcal{S}_V f(x) = \mathcal{S}_V f(x + ja)$, for all $x \in \mathbb{F}_p^n$. Further, if $0 < k \le p$, then for any $a \in \mathbb{F}_p^n$,*

$$D_a^k f(x) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} f(x + (k-i)a) \text{ for all } x \in \mathbb{F}_p^n. \tag{1}$$

Further, if $k = p$, then $D_a^k f(x) = 0$.

Proof The result can be shown by a direct computation or by applying Newton's binomial formula to $D_a = s_a - I$ (I is the identity operator and $s_a f(x) = f(x + a)$). □

Theorem 7 *Let $V = \langle a \rangle$ be an arbitrary one dimensional subspace of $\mathbb{F}_p^n$ generated by a and $f \in \mathcal{B}_n^p$. Then*

$$\mathcal{S}_V f(x) = D_a^{p-1} f(x) \text{ for all } x \in \mathbb{F}_p^n.$$

Furthermore, for any $r \in \{0, 1, 2, \ldots, p-1\}$

$$r\mathcal{S}_V f(x) = D_{ra} D_a^{p-2} f(x) \text{ for all } x \in \mathbb{F}_p^n.$$

Moreover, if $V = \langle a_1, a_2, \ldots, a_k \rangle$ be a k-dimensional subspace of $\mathbb{F}_p^n$ generated by $a_1, a_2, \ldots, a_k$ and $f \in \mathcal{B}_n^p$. Then

$$\mathcal{S}_V f(x) = D_{a_1}^{p-1} \ldots D_{a_k}^{p-1} f(x) \text{ for all } x \in \mathbb{F}_p^n.$$

Proof Using the previous lemma and the known elementary number theory congruence

$$\binom{p-1}{i} \equiv (-1)^i \pmod{p},$$

where p is an odd prime and $0 \le i \le p-1$, we get the first claim.

Let $r \in \{0, 1, 2, \ldots, p-1\}$ and $V = \langle a \rangle$ be an one dimensional subspace of $\mathbb{F}_p^n$. Suppose $g(x) = D_a^{p-2} f(x)$ for all $x \in \mathbb{F}_p^n$. Then by using Lemma 6 and the first claim of Theorem 7, we get

$$\begin{aligned} D_{ra} D_a^{p-2} f(x) &= D_{ra} g(x) = g(x + ra) - g(x) \\ &= g(x + ra) - g(x + (r-1)a) + \cdots + g(x + a) - g(x) \\ &= D_a g(x + (r-1)a) + D_a g(x + (r-2)a) + \cdots + D_a g(x) \\ &= \mathcal{S}_V f(x + (r-1)a) + \mathcal{S}_V f(x + (r-2)a) + \cdots + \mathcal{S}_V f(x) \\ &= \mathcal{S}_V f(x) + \mathcal{S}_V f(x) + \cdots + \mathcal{S}_V f(x) \text{ (sum with } r \text{ terms)} \\ &= r\mathcal{S}_V f(x). \end{aligned}$$

To show the last claim, without loss of generality, let $V_r = \langle a_1, a_2, \ldots, a_r \rangle$, $1 \le r \le k$, be an r-dimensional subspace of $\mathbb{F}_p^k$ and for $r = k$, $V_k = V$. The result is true for $k = 1$, so we now let $k = 2$. Let

$$g(x) = D_{a_2}^{p-1} f(x) = \sum_{i_2=0}^{p-1} f(x + i_2 a_2) \text{ for all } x \in \mathbb{F}_p^n.$$

Then

$$D_{a_1}^{p-1} D_{a_2}^{p-1} f(x) = D_{a_1}^{p-1} g(x) = \sum_{i_1=0}^{p-1} g(x+i_1 a_1) = \sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} f(x+i_2 a_2+i_1 a_1) = \mathcal{S}_{V_2} f(x).$$

We now assume that the result is true for $k = r$, that is, for all $x \in \mathbb{F}_p^n$,

$$\mathcal{S}_{V_r} f(x) = D_{a_1}^{p-1} \dots D_{a_r}^{p-1} f(x) = \sum_{i_1=0}^{p-1} \dots \sum_{i_r=0}^{p-1} f(x + i_r a_r + \dots + i_1 a_1).$$

Then

$$\begin{aligned} &D_{a_{r+1}}^{p-1} D_{a_1}^{p-1} \dots D_{a_r}^{p-1} f(x) = \textstyle\sum_{i_{r+1}=0}^{p-1} \mathcal{S}_{V_r} f(x + i_{r+1} a_{r+1}) \\ &= \textstyle\sum_{i_{r+1}=0}^{p-1} \sum_{i_1=0}^{p-1} \dots \sum_{i_r=0}^{p-1} f(x + i_{r+1} a_{r+1} + i_r a_r + \dots + i_1 a_1) = \mathcal{S}_{V_{r+1}} f(x), \end{aligned}$$

and the theorem is shown. □

As an example, let $p = 3$ and V be an one dimensional subspace generated by $a \in \mathbb{F}_3^n$. Then

$$\begin{aligned} \mathcal{S}_V f(x) &= f(x+2a) + f(x+a) + f(x) = D_a D_a f(x) \\ 2\mathcal{S}_V f(x) &= 2 D_a D_a f(x) = D_{2a} D_a f(x) = D_a D_{2a} f(x). \end{aligned}$$

Proposition 8 *Let V be a k-dimensional subspace of $\mathbb{F}_p^n$ generated by $a_1, a_2, \dots, a_k$. Let $f \in \mathcal{B}_n^p$ be any function of degree r and $h(x) = \mathcal{S}_V f(x)$ for all $x \in \mathbb{F}_p^n$. Then $\left(\sum_{v \in V} X^v\right) \Omega_f$ is the associated codeword of $\mathcal{S}_V f$, that is,*

$$\Omega_h = \left(\sum_{v \in V} X^v \right) \Omega_f.$$

Proof Let $f \in \mathcal{B}_n^p$ and $a \in \mathbb{F}_p^n$. Then

$$X^a \Omega_f = X^a \textstyle\sum_{g \in \mathbb{F}_p^n} f(g) X^g = \sum_{g \in \mathbb{F}_p^n} f(g) X^{g+a} = \sum_{g \in \mathbb{F}_p^n} f(g-a) X^g.$$

Since any $v \in V$ can be written as $v = \sum_{i=1}^k c_i a_i$, where $c_i \in \mathbb{F}_p$, $i \in \{1, 2 \dots, k\}$, then

$$\begin{aligned} \left(\textstyle\sum_{v \in V} X^v\right) \Omega_f &= \textstyle\sum_{g \in \mathbb{F}_p^n} \left(\sum_{v \in V} f(g-v)\right) X^g = \sum_{g \in \mathbb{F}_p^n} \left(\sum_{v \in V} f(g+v)\right) X^g \\ &= \textstyle\sum_{g \in \mathbb{F}_p^n} \mathcal{S}_V f(g) X^g = \Omega_{\mathcal{S}_V f} = \Omega_h. \end{aligned}$$

□

Proposition 9 *Let V be a k-dimensional subspace of $\mathbb{F}_p^n$ and $f \in \mathcal{B}_n^p$ of degree r. Then the degree of $\mathcal{S}_V f$ is less than or equal to $r - k(p-1)$. In particular, the subspace sum of f with respect to any one dimensional subspace of $\mathbb{F}_p^n$ has degree at most $r - p + 1$.*

Proof Let V be a k-dimensional subspace generated by $a_1, a_2, \dots, a_k \in \mathbb{F}_p^n$ and let $y = \sum_{v \in V} X^v$ be the codeword of support V. Then

$$y \Omega_f = \left(\sum_{v \in V} X^v \right) \Omega_f = \sum_{g \in \mathbb{F}_p^n} \mathcal{S}_V f(g) X^g.$$

Further, y is a minimum codeword of $\mathcal{P}^{k(p-1)}$. Since $f \in \mathcal{B}_n^p$ is of degree r. Then Ω_f is in $\mathcal{P}^{n(p-1)-r}$, which does not depends on y. Thus, the codeword $y\Omega_f$ is in $\mathcal{P}^{k(p-1)}\mathcal{P}^{n(p-1)-r} = \mathcal{P}^{n(p-1)-r+k(p-1)}$, which is $\{0\}$ for $r \leq k(p-1)-1$. When $r = k(p-1)+d, d \geq 0$, the degree of $\mathcal{S}_V f$ is at most $d = r - k(p-1)$. □

Theorem 10 *Let $m = 2n$ and f be a p-ary Maiorana–McFarland bent function defined as in Theorem* 1. *Then there exists an n-dimensional subspace E of $\mathbb{F}_p^n \times \mathbb{F}_p^n$ such that:*

(*i*) *the subspace sum of f with respect to any one dimensional subspace of E is 0 if p is odd.*

(*ii*) *the subspace sum of f with respect to any two dimensional subspace of E is 0 if $p = 2$.*

Proof Let V be a subspace of $\mathbb{F}_p^n \times \mathbb{F}_p^n$. The *subspace sum* of f with respect to V is

$$\mathcal{S}_V f(x, y) = \sum_{(u,v)\in V} f(x+u, y+v) = \sum_{(u,v)\in V} ((x+u)\cdot\pi(y+v) + g(y+v)). \quad (2)$$

Let $v = 0$. Then V is a subspace of $E = \mathbb{F}_p^n \times \{0\}$ and from (2), we get

$$\mathcal{S}_V f(x, y) = \sum_{(u,0)\in V} (x+u)\cdot\pi(y) + |V|g(y) = \sum_{(u,0)\in V} (x+u)\cdot\pi(y).$$

Let p be an odd prime and $V = \langle (a, 0)\rangle$ be an one dimensional subspace of E. Then

$$\mathcal{S}_V f(x, y) = p\left(x + \frac{p-1}{2}a\right)\cdot\pi(y) = 0 \text{ for all } (x, y) \in \mathbb{F}_p^n \times \mathbb{F}_p^n.$$

Let $p = 2$ and $V = \langle (a, 0), (c, 0)\rangle$ be a two dimensional subspace of E, then

$$\mathcal{S}_V f(x, y) = 0 \text{ for all } (x, y) \in \mathbb{F}_p^n \times \mathbb{F}_p^n.$$

□

If $p = 2$, then the subspace sum of a Boolean function with respect to a k-dimensional subspace is same as its kth order derivative, and therefore our previous theorem naturally extends the binary case. Next, we generalize a result of Dillon [9].

Theorem 11 *Let $f \in \mathcal{B}_n^p$ and $\mathcal{S}_k[f]$ denote the multiset of subspace sum of f with respect to each k-dimensional subspace of $\mathbb{F}_p^n$. If $f, h \in \mathcal{B}_n^p$ are affine equivalent, then so are $\mathcal{S}_k[f]$ and $\mathcal{S}_k[h]$. Precisely, if a nonsingular affine transformation A (operating on $\mathbb{F}_p^n$) maps f onto h, then it also maps $\mathcal{S}_k[f]$ onto $\mathcal{S}_k[h]$.*

Proof Suppose that, $h(x) = f(xA + b)$ for all $x \in \mathbb{F}_p^n$, where $A \in GL(n, \mathbb{F}_p)$ and $b \in \mathbb{F}_p^n$. Let E be an arbitrary k-dimensional subspace of $\mathbb{F}_p^n$. For all $x \in \mathbb{F}_p^n$

$$\begin{aligned}\mathcal{S}_E h(x) &= \textstyle\sum_{a\in E} h(x+a) = \sum_{a\in E} f(xA + aA + b)\\ &= \textstyle\sum_{a\in E} f(xA + b + aA) = \sum_{c\in E_1} f(xA + b + c), \text{ where } E_1 = \{c : c = aA, a \in E\}\\ &= \mathcal{S}_{E_1} f(xA + b),\end{aligned}$$

since the maps $a \longrightarrow aA$ is a permutation of the k-dimensional subspace E of $\mathbb{F}_p^n$. The theorem is shown. □

Corollary 12 *If P is any affine invariant for $\mathcal{B}_n^p$, then*

$$f \longrightarrow P\{\mathcal{S}_k[f]\}$$

is also an affine invariant for $\mathcal{B}_n^p$.

Helleseth and Kholosha [13] verified the following fact by computer calculations, however, proving this result theoretically and probably finding the whole class of similar functions remains an open problem.

Fact 13 ([13, Fact 1]) *Any ternary function f from $\mathbb{F}_{3^6}$ to $\mathbb{F}_3$ of the form*

$$f(x) = Tr_1^6(\alpha^7 x^{98})$$

is bent and not weakly regular bent, where α is a primitive element of $\mathbb{F}_{3^6}$.

Theorem 14 *The function $f \in \mathcal{B}_6^3$ defined as in Fact 13 does not belong to the complete $\mathcal{M}^p$ class.*

Proof Let f be equivalent to a function from class $\mathcal{M}^p$. From Theorem 10, there exists a 3-dimensional subspace E of $\mathbb{F}_{3^6}$ such that the subspace sum of f with respect to any one dimensional subspace of E is 0. Let $V = \langle a \rangle$, where $a \in \mathbb{F}_{3^6}^*$. Then

$$\mathcal{S}_V f(x) = f(x) + f(x+a) + f(x+2a) = Tr_1^6(\alpha^7(x^{98} + (x+a)^{98} + (x+2a)^{98})). \quad (3)$$

The 3-ary representation of 98 is $(0, 1, 0, 1, 2, 2)$ as $98 = 3^4 + 3^2 + 2 \cdot 3 + 2$. Thus, all the monomials in $(x+a)^{98}$ are of the form x^d with

$$d = (0, d_4, 0, d_2, d_1, d_0), \quad (4)$$

where $d_4, d_2 \in \{0, 1\}$ and $d_1, d_0 \in \{0, 1, 2\}$. The coefficient of the monomial $x^{2\cdot 3+2}$ in $(x+a)^{98}$ is $a^{3^4+3^2}$. Thus, the coefficient of the monomial $x^{2\cdot 3+2}$ in (3) is

$$\alpha^7(a^{3^4+3^2} + (2a)^{3^4+3^2}) = (1 + 2^{3^4+3^2})\alpha^7 a^{3^4+3^2} = 2\alpha^7 a^{3^4+3^2}$$

as $2^{3^4+3^2} \equiv 1 \pmod 3$. Since $3^i(2 \cdot 3 + 2) \not\equiv 2 \cdot 3 + 2 \pmod{728}$ for all $1 \le i \le 5$. It is also obvious that $3^i d \not\equiv (0, 0, 0, 0, 2, 2) \pmod{728}$ for all $1 \le i \le 5$, where d defined as in (4) with $d \neq (0, 0, 0, 0, 2, 2)$. If $\mathcal{S}_V f(x) = 0$ for all $x \in \mathbb{F}_{3^6}$, then all coefficients of monomials in (3) must equal 0, and therefore $2\alpha^7 a^{3^4+3^2} = 0$, which is a contradiction. Thus, there cannot be a 3-dimensional subspace E of $\mathbb{F}_{3^6}$, such that the subspace sum of f with respect to any one dimensional subspace of E is 0. □

2.2 The construction of $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$ classes of bent functions

In [4], Carlet constructed two (so-called $\mathcal{D}, \mathcal{C}$) classes of bent Boolean functions by modifying the Maiorana–McFarland bent function and a generalized bent function over a modulus ring in the following way. Let q be any even positive integer and $\mathbb{Z}_q$ be the ring of integers modulo q. Let E be any subgroup of order q^n of $\mathbb{Z}_q^n \times \mathbb{Z}_q^n$ and π be any permutation on $\mathbb{Z}_q^n$ such that $x \cdot \pi(y) = 0$ for all $(x, y) \in E$. Then the function $f : \mathbb{Z}_q^n \times \mathbb{Z}_q^n \longrightarrow \mathbb{Z}_q$, defined as

$$f(x, y) = x \cdot \pi(y) + \frac{q}{2}\phi_E(x, y), \quad (5)$$

is bent.

We modify this construction (for the environment in consideration) in our next theorem, where we further show that the functions are also regular.

Theorem 15 *Let $E = E_1 \times E_2$, where $E_1, E_2 \subseteq \mathbb{F}_p^n$ with $\dim E_1 + \dim E_2 = n$ and $\varepsilon \in \mathbb{F}_p$. The p-ary function f on $\mathbb{F}_p^n \times \mathbb{F}_p^n$ of the form*

$$f(x, y) = x \cdot \pi(y) + \varepsilon\phi_E(x, y)$$

is a regular p-ary bent function, where π is a permutation polynomial over $\mathbb{F}_p^n$ such that $\pi(E_2) = E_1^{\perp}$.

Proof Let $\zeta = e^{\frac{2\pi i}{p}}$ be the complex p^{th} root of unity. From Theorem 1, we have

$$\sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} = p^n\zeta^{-b\cdot\pi^{-1}(a)} \text{ for all } (a, b) \in \mathbb{F}_p^n \times \mathbb{F}_p^n,$$

so

$$\begin{aligned}
\mathcal{H}_f(a, b) &= \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{x\cdot\pi(y)+\varepsilon\phi_E(x,y)-a\cdot x-b\cdot y} \\
&= \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n\setminus E} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} + \zeta^{\varepsilon} \sum_{(x,y)\in E} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} \\
&= \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} + (\zeta^{\varepsilon} - 1) \sum_{(x,y)\in E} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} \qquad (6) \\
&= p^n\zeta^{-b\cdot\pi^{-1}(a)} + (\zeta^{\varepsilon} - 1) \sum_{(x,y)\in E} \zeta^{-a\cdot x-b\cdot y} \\
&= p^n(\zeta^{-b\cdot\pi^{-1}(a)} + (\zeta^{\varepsilon} - 1)\phi_{E^{\perp}}(a, b)).
\end{aligned}$$

Let $(a, b) \notin E^{\perp}$. Then $\phi_{E^{\perp}}(a, b) = 0$, and we get

$$\mathcal{H}_f(a, b) = \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{f(x,y)-a\cdot x-b\cdot y} = p^n\zeta^{-b\cdot\pi^{-1}(a)} = p^n\zeta^{-b\cdot\pi^{-1}(a)+\varepsilon\phi_{E^{\perp}}(a,b)}. \qquad (7)$$

Let $(a, b) \in E^{\perp}$. Then $b \cdot \pi^{-1}(a) = 0$ (by Lemma 3) and $\phi_{E^{\perp}}(a, b) = 1$, so

$$\mathcal{H}_f(a, b) = \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{f(x,y)-a\cdot x-b\cdot y} = p^n\zeta^{\varepsilon} = p^n\zeta^{-b\cdot\pi^{-1}(a)+\varepsilon\phi_{E^{\perp}}(a,b)}. \qquad (8)$$

From (6), (7) and (8), we infer

$$\mathcal{H}_f(a, b) = p^n\zeta^{-b\cdot\pi^{-1}(a)+\varepsilon\phi_{E^{\perp}}(a,b)} \text{ for all } (a, b) \in \mathbb{F}_p^n \times \mathbb{F}_p^n.$$

Therefore, f is a regular p-ary bent function. □

Remark 16 The dual of f defined as in Theorem 15 is $\tilde{f}(x, y) = -y\cdot\pi^{-1}(x)+\varepsilon\phi_{E^{\perp}}(x, y)$ for all $(x, y) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$, and the set of all such functions f is denoted by $\mathcal{D}^p$.

Lemma 17 *Let p be an odd prime and $n = 2t$ be an even integer. Then for all $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_p^n$,*

$$\phi_{E_0}(x, y) = \prod_{i=1}^{n}\prod_{j=1}^{p-1}(x_i - j),$$

where $E_0 = \{0\} \times \mathbb{F}_p^n$.

Proof We know that

$$\phi_{E_0}(x, y) = \begin{cases} 1, & \text{if } x = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Let $x \neq 0$. Then there exist at least one $j \in \{1, 2, \ldots, n\}$ such that $x_j \neq 0$, so $\prod_{i=1}^{n} \prod_{j=1}^{p-1} (x_i - j) = 0$. Assume now that $x = 0$. Then

$$\prod_{i=1}^{n} \prod_{j=1}^{p-1} (0 - j) = \prod_{i=1}^{n} (p-1)! = 1 = ((p-1)!)^n = ((p-1)!)^{2t}, \tag{9}$$

using Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$, which renders

$$\prod_{i=1}^{n} \prod_{j=1}^{q-1} (x_i - j) = 1,$$

and the lemma is shown. □

For the special case of Theorem 15, we let $E_1 = \{0\}$, $E_2 = \mathbb{F}_p^n$ and $E_0 = \{0\} \times \mathbb{F}_p^n$, where n is even. Then the p-ary functions on $\mathbb{F}_p^n \times \mathbb{F}_p^n$ of the form

$$f(x, y) = x \cdot \pi(y) + \varepsilon \phi_{E_0}(x, y) = x \cdot \pi(y) + \varepsilon \prod_{i=1}^{n} \prod_{j=1}^{p-1} (x_i - j)$$

is a regular p-ary bent function. This class of bent functions will be denoted by $\mathcal{D}_0^p$ and it is a subclass of $\mathcal{D}^p$. Observe that if $f \in \mathcal{D}_0^p$ is an m variables p-ary function, then $m \equiv 0 \pmod 4$.

The next theorem surprisingly shows that $\mathcal{M}^p$ and $\mathcal{D}_0^p \subseteq \mathcal{D}^p$ are overlapping classes, but in general not included in one another.

Theorem 18 *In general, $\mathcal{D}_0^p$ and $\mathcal{D}^p$ are not included in the class $\mathcal{M}^p$. Further, the class $\mathcal{M}^p$ is in general not included in $\mathcal{D}_0^p$ and $\mathcal{D}^p$ classes.*

Proof Let $f \in \mathcal{D}^p$ written as

$$f(x, y) = x \cdot \pi(y) + \varepsilon \phi_E(x, y), \tag{10}$$

with $\varepsilon \in \mathbb{F}_p$, $E = E_1 \times E_2$, where $E_1, E_2 \subseteq \mathbb{F}_p^n$ of $\dim E_1 + \dim E_2 = n$ and π is a permutation over $\mathbb{F}_p^n$ such that $\pi(E_2) = E_1^{\perp}$.

Assume that $f \in \mathcal{M}^p$, and so, f can be expressed as

$$f(x, y) = x \cdot \pi_1(y) + g(y), \tag{11}$$

where π_1 is a permutation over $\mathbb{F}_p^n$ and $g \in \mathcal{B}_n^p$. Putting $x = 0$ in both (10) and (11), we get $g(y) = \varepsilon \phi_E(0, y)$, and so,

$$x \cdot (\pi(y) - \pi_1(y)) = \varepsilon(\phi_E(0, y) - \phi_E(x, y)). \tag{12}$$

Observe now that the left hand side of (12) is linear with respect to the variable x, as opposed to the right hand side of (12) which may not be linear with respect to the variable x (by choosing a suitable nonlinear function $\phi_E(x, y)$ and $\varepsilon \neq 0$). Thus, in general, the classes $\mathcal{D}_0^p$ and $\mathcal{D}^p$ are not included in class $\mathcal{M}^p$.

For example, if $p = 3$ and $n = 4$, we let $f : \mathbb{F}_3^4 \times \mathbb{F}_3^4 \to \mathbb{F}_3$,

$$f(x, y) = x \cdot \pi(y) + \varepsilon(x_1 - 1)(x_1 - 2)(x_2 - 1)(x_2 - 2)(x_3 - 1)(x_3 - 2)(x_4 - 1)(x_4 - 2),$$

where $x = (x_1, x_2, x_3, x_4)$, $y = (y_1, y_2, y_3, y_4) \in \mathbb{F}_3^4$ and $\varepsilon \in \mathbb{F}_3$. The previous nonlinearity

condition on $\phi_E(0, y) - \phi_E(x, y)$ is obviously satisfied, and so $f \in \mathcal{D}_0^p$ does not belong to $\mathcal{M}^p$.

Conversely, let $f \in \mathcal{M}^p$, and assume that it also belongs to $\mathcal{D}^p$. Thus, for all $(x, y) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$

$$f(x, y) = x \cdot \psi(y) + g(y) = x \cdot \psi_1(y) + \varepsilon\phi_E(x, y),$$

where ψ and ψ_1 are permutations over $\mathbb{F}_p^n$ and $E = E_1 \times E_2$, where $E_1, E_2 \subseteq \mathbb{F}_p^n$ of $\dim E_1 + \dim E_2 = n$ and $\psi_1(E_2) = E_1^\perp$. Then $g(y) = \varepsilon\phi_E(0, y) \in \{0, \varepsilon\}$ for all $y \in \mathbb{F}_p^n$, that is, the range set of g contain at most two distinct elements. Therefore, if the range set of g contains at least three distinct elements, the corresponding $\mathcal{M}^p$ function f does not belong to $\mathcal{D}^p$, and our theorem is shown. □

Recall the following result of Carlet [4] introducing the $\mathcal{C}$ class of bent functions.

Theorem 19 ([4, Corollary 4]) *Let L be a linear subspace of $\mathbb{F}_2^n$ and π be any permutation on $\mathbb{F}_2^n$ such that for any element λ of $\mathbb{F}_2^n$, the set $\pi^{-1}(\lambda + L)$ is a flat. The function f on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ defined by*

$$x \cdot \pi(y) + \phi_{L^\perp}(x)$$

is bent.

We now generalize Carlet's result.

Theorem 20 *Let L be any linear subspace of $\mathbb{F}_p^n$ and π be any permutation on $\mathbb{F}_p^n$, such that for any element λ of $\mathbb{F}_p^n$, the set $\pi^{-1}(\lambda + L)$ is a flat. Then the function f on $\mathbb{F}_p^n \times \mathbb{F}_p^n$, defined by*

$$f(x, y) = x \cdot \pi(y) + \varepsilon\phi_{L^\perp}(x),$$

where $\varepsilon \in \mathbb{F}_p$, is a p-ary bent function.

Proof Let $E = L^\perp \times \mathbb{F}_p^n$. For any $(a, b) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$,

$$\begin{aligned}
\mathcal{H}_f(a, b) &= \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{x\cdot\pi(y)+\varepsilon\phi_{L^\perp}(x)-a\cdot x-b\cdot y} \\
&= \sum_{y\in\mathbb{F}_p^n} \left(\sum_{x\in\mathbb{F}_p^n\setminus L^\perp} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} + \zeta^\varepsilon \sum_{x\in L^\perp} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} \right) \\
&= \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} + (\zeta^\varepsilon - 1) \sum_{(x,y)\in L^\perp\times\mathbb{F}_p^n} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} \\
&= p^n\zeta^{-b\cdot\pi^{-1}(a)} + (\zeta^\varepsilon - 1)|L^\perp| \sum_{x\in a+L} \zeta^{-b\cdot\pi^{-1}(x)} \text{ (using Lemma 3)} \\
&= p^n \left(\zeta^{-b\cdot\pi^{-1}(a)} + \tfrac{(\zeta^\varepsilon-1)}{|L|} \sum_{x\in\pi^{-1}(a+L)} \zeta^{-b\cdot x} \right).
\end{aligned}$$

Let $E_1 = \{\pi^{-1}(a + u) : u \in L\}$. Since $\pi^{-1}(a + L)$ is a flat for all $a \in \mathbb{F}_p^n$. If $b \notin E_1^\perp$, then $\sum_{x\in\pi^{-1}(a+L)} \zeta^{-b\cdot x} = 0$, and from (13), we get

$$\mathcal{H}_f(a, b) = p^n(-1)^{-b\cdot\pi^{-1}(a)} = p^n\zeta^{-b\cdot\pi^{-1}(a)+\varepsilon\phi_{E_1^\perp}(b)}. \tag{13}$$

If $b \in E_1^{\perp}$, then $b \cdot \pi^{-1}(a) = 0$ and $\sum_{x \in \pi^{-1}(a+L)} \zeta^{-b \cdot x} = \sum_{x \in E_1} \zeta^{-b \cdot x} = |L|$. From (13) we get

$$\mathcal{H}_f(a, b) = p^n \zeta^{\varepsilon} = p^n \zeta^{-b \cdot \pi^{-1}(a) + \varepsilon \phi_{E_1^{\perp}}(b)}. \tag{14}$$

Therefore, from (13), (13) and (14) we get

$$\mathcal{H}_f(a, b) = p^n \zeta^{-b \cdot \pi^{-1}(a) + \varepsilon \phi_{E_1^{\perp}}(b)} \quad \text{for all } (a, b) \in \mathbb{F}_p^n \times \mathbb{F}_p^n,$$

and the theorem is shown. □

The class of bent functions defined as in Theorem 20 will be denoted by $\mathcal{C}^p$. If $L = \mathbb{F}_p^n$, the class $\mathcal{C}^p$ contains the class $\mathcal{D}_0^p$, and so, also $\mathcal{C}^p$ is not included in the $\mathcal{M}^p$ class.

2.3 Existence and nonexistence of $\mathcal{C}^3$ class bent functions

For the construction of p-ary bent functions defined as in Theorem 20, one needs to consider a permutation polynomial π on $\mathbb{F}_p^n$ such that $\pi^{-1}(a + L)$ is a flat for any $a \in \mathbb{F}_p^n$. In [18], Mandal et al. derived some existence and nonexistence results concerning the bent functions in the $\mathcal{C}$ class for many of the known classes of permutations over $\mathbb{F}_{2^n}$. We investigate below these conditions for two classes of permutations and suitable linear subspaces of dimension less than or equal to 2, for $p = 3$.

Lemma 21 *Let $u_1, u_2, u_3 \in \mathbb{F}_3^n$. A set $L = \{u_1, u_2, u_3\}$ is flat of $\mathbb{F}_3^n$ of dimension ≤ 1 if and only if $u_1 + u_2 + u_3 = 0$.*

Proof If L is a subspace, without loss of generality, we may assume that $L = \{0, u_1, 2u_1\}$, which satisfies $0 + u_1 + 2u_1 = 0$. Conversely let $L = \{u_1, u_2, u_3\}$ with $u_1 + u_2 + u_3 = 0$, i.e., $u_3 = 2u_1 + 2u_2$. It follows that $2u_1 + L = \{0, u_2 + 2u_1, u_1 + 2u_2\} = \langle u_1 + 2u_2 \rangle$. The lemma is proved. □

Theorem 22 *Consider the permutation polynomial over $\mathbb{F}_{3^4}$, $\phi(x) = x + x^{17}$ [25]. Then there is no 1-dimensional subspace L of $\mathbb{F}_{3^4}$ such that $\phi(a + L)$ is flat for all $a \in \mathbb{F}_{3^4}$.*

Proof Let $L = \{0, u, 2u\}$, $u \in \mathbb{F}_{3^4}^*$. Then for any $a \in \mathbb{F}_{3^4}$, $\phi(a + L)$ is flat if and only if

$$\begin{aligned} &\phi(a) + \phi(a + u) + \phi(a + 2u) = 0 \Longleftrightarrow a^{17} + (a + u)^{17} + (a + 2u)^{17} = 0 \\ \Longleftrightarrow\ &2a^{15}u^2 + 2a^{13}u^4 + 2a^{11}u^6 + 2a^9u^8 + a^7u^{10} + a^5u^{12} + a^3u^{14} + au^{16} = 0. \end{aligned} \tag{15}$$

Equation (15) holds for all $a \in \mathbb{F}_{3^4}$ if and only if $u = 0$, which contradicts $\dim L = 1$. □

Remark 23 We can certainly construct functions in $\mathcal{C}^3$. For example, consider the permutation polynomial $\phi(x) = x + 1$ over $\mathbb{F}_{3^4}$ [19, Theorem 1.1]. Then for any 1-dimensional

subspace L of $\mathbb{F}_{3^4}$, $\phi(a+L)$ is flat for all $a \in \mathbb{F}_{3^4}$, since, for $L = \{0, u, 2u\}$, $u \in \mathbb{F}_{3^4}^*$, then $\phi(a) + \phi(a+u) + \phi(a+2u) = 0$, for all $a \in \mathbb{F}_{3^4}$. If $L = \langle u, v\rangle$ is a 2-dimensional subspace of $\mathbb{F}_{3^4} \times \mathbb{F}_{3^4}$ and $a \in \mathbb{F}_{3^4}$, then

$$\begin{aligned}\phi(a+L) = \{&\phi(a), \phi(a+u), \phi(a+v), \phi(a+u+v), \phi(a+2u), \phi(a+2v),\\ &\phi(a+2u+v), \phi(a+u+2v), \phi(a+2u+2v)\} = 1 + a + L.\end{aligned}$$

Theorem 24 *Let ϕ be a permutation polynomial defined as in* [25] *on $\mathbb{F}_{3^4}$ of the form*

$$\phi(x) = x(x^{16}+1) = x^{17} + x.$$

Then, there is no 2-dimensional subspace $L = \langle u, v\rangle$ such that $\phi(a+L)$ is flat for all $a \in \mathbb{F}_{3^4}$.

Proof Let $a \in \mathbb{F}_{3^4}$. If $\phi(a+L)$ is a flat, then

$$\begin{aligned}&\phi(a) + \phi(a+u) + \phi(a+v) + \phi(a+u+v) + \phi(a+2u) + \phi(a+2v)\\ &+\phi(a+2u+v) + \phi(a+u+2v) + \phi(a+2u+2v) = 0.\end{aligned} \tag{16}$$

The linear part of (16) certainly sums to 0. Furthermore,

$$\begin{aligned}
(a+u)^{17} &= a^{17} + 2a^{16}u + a^{15}u^2 + 2a^{14}u^3 + a^{13}u^4 + 2a^{12}u^5 + a^{11}u^6 + 2a^{10}u^7 + a^9u^8\\
&\quad + a^8u^9 + 2a^7u^{10} + a^6u^{11} + 2a^5u^{12} + a^4u^{13} + 2a^3u^{14} + a^2u^{15} + 2au^{16} + u^{17},\\
(a+v)^{17} &= a^{17} + 2a^{16}v + a^{15}v^2 + 2a^{14}v^3 + a^{13}v^4 + 2a^{12}v^5 + a^{11}v^6 + 2a^{10}v^7 + a^9v^8\\
&\quad + a^8v^9 + 2a^7v^{10} + a^6v^{11} + 2a^5v^{12} + a^4v^{13} + 2a^3v^{14} + a^2v^{15} + 2av^{16} + v^{17},\\
(a+u+v)^{17} &= a^{17} + 2a^{16}(u+v) + a^{15}(u+v)^2 + 2a^{14}(u+v)^3 + a^{13}(u+v)^4\\
&\quad + 2a^{12}(u+v)^5 + a^{11}(u+v)^6 + 2a^{10}(u+v)^7 + a^9(u+v)^8 + a^8(u+v)^9 + 2a^7(u\\
&\quad + v)^{10} + a^6(u+v)^{11} + 2a^5(u+v)^{12} + a^4(u+v)^{13} + 2a^3(u+v)^{14} + a^2(u+v)^{15}\\
&\quad + 2a(u+v)^{16} + (u+v)^{17},\\
(a+2u)^{17} &= a^{17} + 2a^{16}(2u) + a^{15}(2u)^2 + 2a^{14}(2u)^3 + a^{13}(2u)^4 + 2a^{12}(2u)^5\\
&\quad + a^{11}(2u)^6 + 2a^{10}(2u)^7 + a^9(2u)^8 + a^8(2u)^9 + 2a^7(2u)^{10} + a^6(2u)^{11}\\
&\quad + 2a^5(2u)^{12} + 2a^3(2u)^{14} + a^2(2u)^{15} + 2a(2u)^{16} + (2u)^{17},\\
(a+2v)^{17} &= a^{17} + 2a^{16}(2v) + a^{15}(2v)^2 + 2a^{14}(2v)^3 + a^{13}(2v)^4 + 2a^{12}(2v)^5\\
&\quad + a^{11}(2v)^6 + 2a^{10}(2v)^7 + a^9(2v)^8 + a^8(2v)^9 + 2a^7(2v)^{10} + a^6(2v)^{11}\\
&\quad + 2a^5(2v)^{12} + a^4(2v)^{13} + 2a^3(2v)^{14} + a^2(2v)^{15} + 2a(2v)^{16} + (2v)^{17},\\
(a+2u+v)^{17} &= a^{17} + 2a^{16}(2u+v) + a^{15}(2u+v)^2 + 2a^{14}(2u+v)^3 + a^{13}(2u+v)^4\\
&\quad + 2a^{12}(2u+v)^5 + a^{11}(2u+v)^6 + 2a^{10}(2u+v)^7 + a^9(2u+v)^8 + a^8(2u+v)^9\\
&\quad + 2a^7(2u+v)^{10} + a^6(2u+v)^{11} + 2a^5(2u+v)^{12} + a^4(2u+v)^{13} + 2a^3(2u+v)^{14}\\
&\quad + a^2(2u+v)^{15} + 2a(2u+v)^{16} + (2u+v)^{17},\\
(a+u+2v)^{17} &= a^{17} + 2a^{16}(u+2v) + a^{15}(u+2v)^2 + 2a^{14}(u+2v)^3\\
&\quad + a^{13}(u+2v)^4 + 2a^{12}(u+2v)^5 + a^{11}(u+2v)^6 + 2a^{10}(u+2v)^7 + a^9(u+2v)^8\\
&\quad + a^8(u+2v)^9 + 2a^7(u+2v)^{10} + a^6(u+2v)^{11} + 2a^5(u+2v)^{12} + a^4(u+2v)^{13}\\
&\quad + 2a^3(u+2v)^{14} + a^2(u+2v)^{15} + 2a(u+2v)^{16} + (u+2v)^{17},\\
(a+2u+2v)^{17} &= a^{17} + 2a^{16}(2u+2v) + a^{15}(2u+2v)^2 + 2a^{14}(2u+2v)^3\\
&\quad + a^{13}(2u+2v)^4 + 2a^{12}(2u+2v)^5 + a^{11}(2u+2v)^6 + 2a^{10}(2u+2v)^7 + a^9(2u+2v)^8\\
&\quad + a^8(2u+2v)^9 + 2a^7(2u+2v)^{10} + a^6(2u+2v)^{11} + 2a^5(2u+2v)^{12} + a^4(2u+2v)^{13}\\
&\quad + 2a^3(2u+2v)^{14} + a^2(2u+2v)^{15} + 2a(2u+2v)^{16} + (2u+2v)^{17}.
\end{aligned}$$

Adding all these equations, and collecting powers of a, we obtain

$$
\begin{aligned}
&9a^{17} = 0,\\
&2a^{16}\,(u+v+(u+v)+2u+2v+(2u+v)+(u+2v)+(2u+2v)) = 0,\\
&a^{15}\left(u^2+v^2+(u+v)^2+(2u)^2+(2v)^2+(2u+v)^2+(u+2v)^2+(2u+2v)^2\right) = 0,\\
&2a^{14}\left(u^3+v^3+(u+v)^3+(2u)^3+(2v)^3+(2u+v)^3+(u+2v)^3+(2u+2v)^3\right) = 0,\\
&a^{13}\left(u^4+v^4+(u+v)^4+(2u)^4+(2v)^4+(2u+v)^4+(u+2v)^4+(2u+2v)^4\right) = 0,\\
&2a^{12}\left(u^5+v^5+(u+v)^5+(2u)^5+(2v)^5+(2u+v)^5+(u+2v)^5+(2u+2v)^5\right) = 0,\\
&a^{11}\left(u^6+v^6+(u+v)^6+(2u)^6+(2v)^6+(2u+v)^6+(u+2v)^6+(2u+2v)^6\right) = 0,\\
&2a^{10}\left(u^7+v^7+(u+v)^7+(2u)^7+(2v)^7+(2u+v)^7+(u+2v)^7+(2u+2v)^7\right) = 0,\\
&a^{9}\left(u^8+v^8+(u+v)^8+(2u)^8+(2v)^8+(2u+v)^8+(u+2v)^8+(2u+2v)^8\right)\\
&\qquad\qquad = a^9(u^6v^2+u^4v^4+u^2v^6),\\
&a^{8}\left(u^9+v^9+(u+v)^9+(2u)^9+(2v)^9+(2u+v)^9+(u+2v)^9+(2u+2v)^9\right) = 0,\\
&2a^{7}\left(u^{10}+v^{10}+(u+v)^{10}+(2u)^{10}+(2v)^{10}+(2u+v)^{10}+(u+2v)^{10}+(2u+2v)^{10}\right) = 0,\\
&a^{6}\left(u^{11}+v^{11}+(u+v)^{11}+(2u)^{11}+(2v)^{11}+(2u+v)^{11}+(u+2v)^{11}+(2u+2v)^{11}\right) = 0,\\
&2a^{5}\left(u^{12}+v^{12}+(u+v)^{12}+(2u)^{12}+(2v)^{12}+(2u+v)^{12}+(u+2v)^{12}+(2u+2v)^{12}\right) = 0,\\
&a^{4}\left(u^{13}+v^{13}+(u+v)^{13}+(2u)^{13}+(2v)^{13}+(2u+v)^{13}+(u+2v)^{13}+(2u+2v)^{13}\right) = 0,\\
&2a^{3}\left(u^{14}+v^{14}+(u+v)^{14}+(2u)^{14}+(2v)^{14}+(2u+v)^{14}+(u+2v)^{14}+(2u+2v)^{14}\right)\\
&\qquad\qquad = 2a^3(u^{12}v^2+2u^{10}v^4+2u^4v^{10}+u^2v^{10}),\\
&a^{2}\left(u^{15}+v^{15}+(u+v)^{15}+(2u)^{15}+(2v)^{15}+(2u+v)^{15}+(u+2v)^{15}+(2u+2v)^{15}\right) = 0,\\
&2a\left(u^{16}+v^{16}+(u+v)^{16}+(2u)^{16}+(2v)^{16}+(2u+v)^{16}+(u+2v)^{16}+(2u+2v)^{16}\right)\\
&\qquad\qquad = 2a(2u^{12}v^4+u^{10}v^6+u^6v^{10}+2u^4v^{12}),\\
&u^{17}+v^{17}+(u+v)^{17}+(2u)^{17}+(2v)^{17}+(2u+v)^{17}+(u+2v)^{17}+(2u+2v)^{17} = 0.
\end{aligned}
$$

From (16), we get that if $\phi(a+L)$ is flat, then

$$
\begin{aligned}
&a(u^{12}v^4+2u^{10}v^6+2u^6v^{10}+u^4v^{12})\\
&\quad +a^3(2u^{12}v^2+u^{10}v^4+u^4v^{10}+2u^2v^{10})+a^9(u^6v^2+u^4v^4+u^2v^6) = 0,
\end{aligned}
$$

which is satisfied for all $a \in \mathbb{F}_{3^4}$, only when $u^{12}v^4+2u^{10}v^6+2u^6v^{10}+u^4v^{12} = 0$, $2u^{12}v^2+u^{10}v^4+u^4v^{10}+2u^2v^{10} = 0$, $u^6v^2+u^4v^4+u^2v^6 = 0$. Since

$$
\begin{aligned}
&u^6v^2+u^4v^4+u^2v^6 = 0 \iff u^4+u^2v^2+v^4 = 0, \quad \text{as } u, v \neq 0\\
&\iff (2u^2+v^2)^2 = 0 \ \text{ or } \ (u^2+2v^2)^2 = 0 \iff u = v \ \text{ or } \ u = 2v,
\end{aligned}
$$

which is not possible as u and v are linearly independent. □

3 Summary

In this paper we define and characterize the subspace sum concept for p-ary bent functions, and derive its connection to affine invariance and vanishing properties for any p-ary Maiorana–McFarland bent functions. Further, two new classes of p-ary bent functions, $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$, are constructed, one of which, D^p, consists of p-ary regular bent functions. Lastly, the existence and nonexistence of functions in the $\mathcal{C}^p$ class for two known permutations and specific suitable subspaces is investigated.

Acknowledgments We thank the referees for the very useful comments that has immensely helped us to significantly improve both technical and editorial quality of the paper. The first two authors thank the Centre of Excellence in Cryptology (CoEC) and R. C. Bose Centre for Cryptology and Security of Indian Statistical Institute, Kolkata, for supporting their visits at the Indian Statistical Institute, Kolkata, during which period the above work was carried on.

References

1. Ambrosimov, A.C.: Properties of the Bent functions of q-Ary logic over finite fields. Discret Math **6:3**, 50–60 (1994)
2. Assmus, E.F., Key, J.: Polynomial codes and finite geometries. In: Pless, V.S., Huffman, W.C., Brualdi, R.A. (eds.) Handbook of Coding Theory–Part 2: Connections, pp. 1269–1343. Elsevier, Amsterdam (1998). Ch. 16
3. Budaghyan, L., Carlet, C., Helleseth, T., Kholosha, A.: Generalized Bent functions and their relation to Maiorana-McFarland class. In: International Symposium on Information Theory, pp. 1212–1215 (2012)
4. Carlet, C.: Two new classes of Bent functions. In: Adv. Crypt. – Eurocrypt'93, LNCS, vol. 765, pp. 77–101 (1994)
5. Charpin, P.: Codes cycliques étendus invariants sous le groupe affine. Thèse de Doctorat d'État Université Paris VII (1987)
6. Charpin, P.: Une generalisation de la construction de Berman des codes de Reed et Muler p-aires. Commun Algebra **16:11**, 2231–2246 (1988)
7. Chee, Y.M., Tan, Y., Zhang, X.D.: Strongly regular graphs constructed from p-ary Bent functions. J. Alg. Combinat. **34:2**, 251–266 (2011)
8. Dillon, J.F.: Elementary Hadamard difference sets. University of Maryland, Ph.D. dissertations (1974)
9. Dillon, J.F.: Elementary Hadamard difference sets. In: Proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, p. 237–249. Winnipeg (1975)
10. Dobbertin, H.: Construction of bent functions and balanced Boolean functions with high nonlinearity. Fast Software Encryption, Leuven 1994, LNCS 1008, pp. 61–74. Springer-Verlag (1995)
11. Golomb, S.M., Gong, G.: Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge University Press, Cambridge (2005)
12. Helleseth, T., Kumar, P.V.: Sequences with low correlation. In: Handbook of Coding Theory II, pp. 1765–1853. North-Holland (1998)
13. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52:5**, 2018–2032 (2006)
14. Hou, X.-D.: p-ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields Applic. **10:4**, 555–582 (2004)
15. Hyun, J.Y., Lee, H., Lee, Y.: Necessary conditions for the existence of regular p-ary Bent functions. IEEE Trans. Inf. Theory **60:3**, 1665–1672 (2014)
16. Kim, S.H., No, J.S.: New families of binary sequences with low correlation. IEEE Trans. Inf. Theory **49:11**, 3059–3065 (2003)
17. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Combinat. Theory Ser. A **40:1**, 90–107 (1985)
18. Mandal, B., Stanica, P., Gangopadhyay, S., Pasalic, E.: An Analysis of the C Class of Bent Functions. Fundamenta Informaticae **146:3**, 271–292 (2016)
19. Matthews, R.: Permutation properties of polynomials permutation properties of polynomials $1 + x + \cdots + x^k$ over a finite field. Proc. Amer. Math. Soc. **120:1**, 47–51 (1994)
20. Olsen, J.D., Scholtz, R.A., Welch, L.R.: Bent-function sequences. IEEE Trans. Inf. Theory **28:6**, 858–864 (1982)
21. Pott, A., Tan, Y., Feng, T., Ling, S.: Association schemes arising from Bent functions. Des Codes Cryptograph **59:1**, 319–331 (2011)
22. Rothaus, O.S.: On Bent functions. J. Combinat. Theory Ser. A **20:3**, 300–305 (1976)
23. Stinchcombe, T.E.: Aperiodic correlations of length 2^m sequences, complementarity, and power control for OFDM, Ph.D. dissertation, Univ. London, London U.K. (2000)
24. Tan, Y., Pott, A., Feng, T.: Strongly regular graphs associated with ternary Bent functions. J. Combinat. Theory Ser. A **117:6**, 668–682 (2010)
25. Wang, L.: On permutation polynomials. Finite Fields Applic. **8:3**, 311–322 (2002)
26. Zhou, Z., Tang, X.: New nonbinary sequence families with low correlation, large size, and large linear span. Appl. Math. Lett. **24:7**, 1105–1110 (2011)