An analysis of the $\mathcal{C}$ class of bent functions

Bimal Mandal[1] Pantelimon Stănică[2] Sugata Gangopadhyay[3]
Enes Pasalic[4]

[1]Department of Mathematics
Indian Institute of Technology Roorkee, INDIA
bimalmandal90@gmail.com
[2]Department of Applied Mathematics
Naval Postgraduate School, Monterey, CA 93943–5216, USA
pstanica@nps.edu
[3]Department of Computer Science and Engineering
Indian Institute of Technology Roorkee, INDIA
sugatfcs@iitr.ac.in
[4]University of Primorska, Faculty of Mathematics, Natural Sciences
and Information Technologies (Famnit), SLOVENIA
enes.pasalic6@gmail.com

June 14, 2015

Abstract

Two (so-called $\mathcal{C}, \mathcal{D}$) classes of permutation-based bent Boolean functions were introduced by Carlet two decades ago, but without specifying some explicit construction methods for their construction (apart from the subclass $\mathcal{D}_0$). In this article, we look in more detail at the $\mathcal{C}$ class, and derive some existence and nonexistence results concerning the bent functions in the $\mathcal{C}$ class for many of the known classes of permutations over $\mathbb{F}_{2^n}$. Most importantly, the existence results induce generic methods of constructing bent functions in class $\mathcal{C}$ which possibly do not belong to the completed Maiorana-McFarland class. The question whether the specific permutations and related subspaces we identify in this article indeed give bent functions outside the completed Maiorana-McFarland class remains open.

Keywords: Boolean functions; bent functions; permutation polynomials.
MSC 2010: 05A05, 06E30, 11T55, 94C10

1 Introduction

Boolean functions are used in many domains such as sequences, cryptography and designs. The Boolean functions that are used as cryptographic primitives must resist affine approximation, which is achieved by having high nonlinearity. The *bent functions* defined on an even number of variables (although not directly usable as cryptographic primitives due to not being balanced) have the maximum nonlinearity, that is, they offer maximum resistance to affine approximation. Bent functions hold an interest among researchers, since they have maximum Hamming distance from the set of all affine Boolean functions and have very nice combinatorial properties. Several classes of bent functions were constructed by Rothaus [18], Dillon [9], Dobbertin [10], and Carlet [4].

Rothaus studied these objects in the 1960's, although his paper was not published until ten years later [18]. In print, bent functions appear in a preprint of Dillon from 1972, and in his Ph.D. thesis [9]. The class of bent functions found by Dillon is known as Partial Spread ($\mathcal{PS}$) class, and a subclass known as $\mathcal{PS}_{ap}$ allows an explicit mathematical description. The Maiorana-McFarland ($\mathcal{M}$) class introduced in [16] and further investigated in [9] is the other generic class of bent functions discovered around the same time. Dobbertin [10] proposed another set of bent functions which includes both $\mathcal{M}$ and $\mathcal{PS}$. These three classes are also referred to as the primary constructions, whereas the classes $\mathcal{C}$ and $\mathcal{D}$ introduced by Carlet [4] belong to secondary constructions obtained by modifying the class $\mathcal{M}$, see Section 3 for their definitions.

Even though both classes $\mathcal{C}$ and $\mathcal{D}$ are specified (see (2), (3) and property (C) below) by adding the indicator functions of suitably chosen vector subspaces to the functions in the $\mathcal{M}$ class, apart from an explicit subclass denoted by $\mathcal{D}_0$, the bent conditions in terms of the selection of vector subspaces and permutations (used to define the initial function in $\mathcal{M}$) are rather hard to satisfy. Certainly, as indicated in Remark 3.2, one could construct bent functions in the $\mathcal{C}$ class, but such an approach does not give us an *explicit* construction. The purpose of this article is to *fix* the permutation (from some known classes of permutations) and investigate these bent conditions in more detail, and to derive certain (non)existence results concerning the possibility of selecting appropriate subspaces so that the bent functions in the $\mathcal{C}$ class may be constructed. Most notably, for some classes of permutation polynomials there are no suitable linear subspaces of certain dimension for which the modification of $f \in \mathcal{M}$ would give a bent function $f^* \in \mathcal{C}$. On the other hand, some explicit conditions and the existence results could be derived for other classes of permutations. We also extend the original analysis of bent conditions of Carlet in terms of the Walsh-Hadamard spectra and show, for instance, that the modification (addition of the indicator of a linear subspace) of quadratic bent functions in $\mathcal{M}$ only result in bent functions within the completed class $\mathcal{M}$.

The rest of this article is organized as follows. In Section 2 some basic definitions related to Boolean (and in particular bent) functions are given. The definition of $\mathcal{C}$ and $\mathcal{D}$ classes along with one motivating result for the analysis in this article are given in Section 3. The analysis of bent conditions of the $\mathcal{C}$ class of bent functions in terms of their Walsh-Hadamard spectra is given in Section 4. The main results related to (non)existence of linear subspaces of certain dimension for some particular classes of permutations are deduced in Section 5. Some concluding remarks are given in Section 6.

2 Preliminaries

Let $\mathbb{Z}$ be the ring of integers and $\mathbb{F}_2$ be the prime field of characteristic 2. Let $\mathbb{F}_2^n = \{x = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_2, \text{ for all } i = 1, 2, \ldots, n\}$. We denote the extension field of degree n over $\mathbb{F}_2$ by $\mathbb{F}_{2^n}$, and the unit group therein by $\mathbb{F}_{2^n}^*$. Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ (or, equivalently from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$) is said to be a *Boolean function* on n variables. The set of all Boolean functions on n variables is denoted by $\mathfrak{B}_n$.

For a detailed study of Boolean functions we refer to Carlet [5, 6], and Cusick and Stănică [7]. For the convenience of the reader, we recall some basic notions below. For any $x \in \mathbb{F}_2^n$, the

(Hamming) *weight* of x is the integer sum $\mathrm{wt}(x) = \sum_{i=1}^{n} x_i$. The *algebraic normal form* (ANF) of a Boolean function $f \in \mathfrak{B}_n$ is

$$f(x_1, \dots, x_n) = \sum_{a=(a_1,\dots,a_n)\in\mathbb{F}_2^n} \mu_a x_1^{a_1} \dots x_n^{a_n},$$

where $\mu_a \in \mathbb{F}_2$, for all $a \in \mathbb{F}_2^n$. The *algebraic degree* of f is $\deg(f) = \max_{a\in\mathbb{F}_2^n}\{\mathrm{wt}(a) : \mu_a \neq 0\}$. The inner product $u \cdot x := \sum_{i=1}^{n} u_i x_i$, for all $u = (u_1, \dots, u_n), x = (x_1, \dots, x_n) \in \mathbb{F}_2^n$. We also identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ (as vector spaces) and take the inner product $u \cdot x := Tr_1^n(ux)$, where $Tr_1^n(a) := a + a^2 + a^{2^2} + \dots + a^{2^{n-1}}$, for all $a \in \mathbb{F}_{2^n}$, is the absolute trace on $\mathbb{F}_{2^n}$.

The *Walsh-Hadamard transform* of $f \in \mathfrak{B}_n$ at $u \in \mathbb{F}_2^n$ is

$$W_f(u) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)}(-1)^{u\cdot x}.$$

The multiset

$$[W_f(u) : u \in \mathbb{F}_2^n] \tag{1}$$

is said to be the *Walsh-Hadamard spectrum* of f. The *derivative* of $f \in \mathfrak{B}_n$ at $a \in \mathbb{F}_2^n$, denoted by $D_a f$, is a Boolean function defined by

$$D_a f(x) = f(x + a) + f(x), \text{ for all } x \in \mathbb{F}_2^n.$$

The notion of derivative of a Boolean function is extended to higher orders as follows. Suppose $\{a_1, a_2, \dots, a_k\}$ is a basis of a k-dimensional subspace V of $\mathbb{F}_2^n$ (we write $\dim(V) = k$). The *k-th derivative* of f with respect to V, denoted by $D_V f$, is a Boolean function defined by

$$D_V f(x) = D_{a_k} D_{a_{k-1}} \dots D_{a_1} f(x), \text{ for all } x \in \mathbb{F}_2^n.$$

It is to be noted that $D_V f$ is independent of the choice of the basis of V.

A Boolean function $f \in \mathfrak{B}_n$, where n is an even positive integer, is said to be a *bent function* if its Walsh-Hadamard spectrum (1) consists of values from the set $\{-2^{n/2}, 2^{n/2}\}$.

3 Towards an explicit specification of Carlet's $\mathcal{C}$-class

The Maiorana-McFarland class $\mathcal{M}$ is the set of m-variable ($m = 2n$) Boolean functions of the form

$$f(x, y) = x \cdot \pi(y) + g(y), \text{ for all } x, y \in \mathbb{F}_2^n,$$

where π is a permutation on $\mathbb{F}_2^n$, and g is an arbitrary Boolean function on $\mathbb{F}_2^n$. All such functions are bent and their duals (also bent) have the form $\widetilde{f}(x, y) = y \cdot \pi^{-1}(x) + g(\pi^{-1}(x))$ (where π^{-1} is the inverse function for π). Dillon constructed another class of bent functions called *partial spreads*, whose supports are union of "disjoint" $n = m/2$ dimensional subspaces of $\mathbb{F}_2^m$. For the details of the construction of bent functions in $\mathcal{PS}$ we refer to [8, 9].

Two new classes of bent functions were derived by Carlet in [4]. The class $\mathcal{D}$ consists of bent functions of the form

$$f(x, y) = x \cdot \pi(y) + 1_{E_1}(x)1_{E_2}(y) \tag{2}$$

with π a permutation on $\mathbb{F}_2^n$ and E_1, E_2 two linear subspaces of $\mathbb{F}_2^n$ such that $\pi(E_2) = E_1^\perp$ (1_E is the indicator function of the space E). An explicit subclass of $\mathcal{D}$, denoted by $\mathcal{D}_0$, contains all elements of the form $x \cdot \pi(y) + \delta_0(x)$ ($\delta_0(x)$ is the Dirac symbol, which is 1 if $x = 0$, and 0, otherwise). It has been shown that $\mathcal{D}_0$ strictly includes the $\mathcal{M}$ and $\mathcal{PS}$ classes [4, 10]. The second Carlet class $\mathcal{C}$ of bent functions (one we will concentrate on) contains all functions of the form

$$f(x, y) = x \cdot \pi(y) + 1_{L^\perp}(x) \tag{3}$$

where L is any linear subspace of $\mathbb{F}_2^n$ and π is any permutation on $\mathbb{F}_2^n$ such that:

(C) $\phi(a + L)$ is a flat (affine subspace), for all $a \in \mathbb{F}_2^n$, where $\phi := \pi^{-1}$.

We will often say that (ϕ, L) *has property* (C).

Certainly, if L has dimension 1, then $\pi^{-1}(a + L) = \phi(a + L)$ is always a one-dimensional flat: if $L = \{0, u\}$ is a one-dimensional subspace, then $\phi(a + L) = \{\phi(a), \phi(a + u)\} = \phi(a) + \{0, \phi(a) + \phi(a + u)\}$, where $\phi(a) + \phi(a + u) \neq 0$. So, we will assume from now on that L has dimension ≥ 2. We will identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$, and we denote $\phi := \pi^{-1}$. We have the following characterization of a subspace L of dimension ≤ 2.

Lemma 3.1. *Suppose $u, v, w, z \in \mathbb{F}_{2^n}$. A set $L = \{u, v, w, z\}$ is a flat of $\mathbb{F}_{2^n}$ of dimension ≤ 2 if and only if $u + v + w + z = 0$.*

Proof. If L is a subspace, then without loss of generality, we can assume that $L = \{0, u, v, u+v\}$, which satisfies $0+u+v+u+v = 0$. Reciprocally, we assume that the set $L = \{u, v, w, z\}$ satisfies $u+v+w+z = 0$, and so, $z = u+v+w$. It follows that $u+L = \{0, u+v, u+w, u+(u+v+w) = v + w\}$, which is easily seen to be a subspace of dimension 0, if $u = v = w (= z)$, of dimension 1, if $u \neq v = w$, and of dimension 2, if v and w are independent. $\square$

Remark 3.2. *The fact that we can construct many bent functions in the $\mathcal{C}$ class of bent functions is not difficult. One could take two subspaces L, M in $\mathbb{F}_2^n$ of the same dimension and partition $\mathbb{F}_2^n$ into $\cup_{a\in A}(a+L)$ and $\cup_{b\in B}(b+M)$, with A, B subsets of $\mathbb{F}_2^n$ of the same cardinality $|A| = |B|$, and then take any permutation ϕ that maps the elements of $\{a + L \,|\, a \in A\}$ onto the elements of $\{b + M \,|\, b \in B\}$. The pair (ϕ, L) would satisfy property (C).*

However, our goal here is to fix the permutation π (many times among classes of known ones) and identify the subspaces L such that the property (C) is satisfied. We will refer to a $\mathcal{C}$ type function of the form $f(x, y) = x \cdot \pi(y) + 1_{L^\perp}(x)$ as the $\mathcal{C}$ type function associated to the permutation ϕ, where $\phi = \pi^{-1}$.

To illustrate the hardness of the underlying problem we consider one specific class of permutations $\{\pi\}$ proposed by Hou [12, Theorem B] and the existence of a 2-dimensional linear subspace L for which the function $x \cdot \pi(y) + 1_{L^\perp}(x)$ is a bent function in $\mathcal{C}$.

Theorem 3.3. *Let $n \geq 1$ and $\phi(x) = ax + bx^{2^n} + x^{2^{n+1}-1}$ be a permutation polynomial over $\mathbb{F}_{2^n}$ (see Hou* [12, Theorem B] *for explicit criteria). Then there exists no 2-dimensional linear subspace, L, of $\mathbb{F}_{2^n}$ such that (ϕ, L) has property (C).*

Proof. Suppose $L = \langle u, v \rangle$ is a 2-dimensional subspace of $\mathbb{F}_{2^n}$. Then for any $c \in \mathbb{F}_{2^n}$, $\phi(c+L)$ is a flat if and only if

$$\begin{aligned}
0 &= \phi(c) + \phi(c+u) + \phi(c+v) + \phi(c+u+v) \\
&= ac + bc^{2^n} + c^{2^{n+1}-1} + a(c+u) + b(c+u)^{2^n} + (c+u)^{2^{n+1}-1} \\
&+ a(c+v) + b(c+v)^{2^n} + (c+v)^{2^{n+1}-1} \\
&+ a(c+u+v) + b(c+u+v)^{2^n} + (c+u+v)^{2^{n+1}-1} \\
&= c^{2^{n+1}-1} + (c+u)^{2^{n+1}-1} + (c+v)^{2^{n+1}-1} + (c+u+v)^{2^{n+1}-1}
\end{aligned}$$

for all $c \in \mathbb{F}_{2^n}$. Therefore, multiplying the above identity by $c+u+v$ and using the binomial theorem (in characteristic 2) we obtain

$$(u+v)c^{2^{n+1}-1} + v(c+u)^{2^{n+1}-1} + u(c+v)^{2^{n+1}-1} = \sum_{j=0}^{2^{n+1}-2} \left(v\, u^{2^{n+1}-1-j} + u\, v^{2^{n+1}-1-j} \right) c^j = 0,$$

for all $c \in \mathbb{F}_{2^{2n}}$, implying that the polynomial $\displaystyle\sum_{j=0}^{2^{n+1}-2} \left(v\, u^{2^{n+1}-1-j} + u\, v^{2^{n+1}-1-j} \right) X^j \in \mathbb{F}_{2^{2n}}[X]$ has all of its coefficients 0, that is, $v\, u^{2^{n+1}-1-j} + u\, v^{2^{n+1}-1-j} = 0$, for all $0 \le j \le 2^{n+1}-2$. In particular, for $j = 2^{n+1}-3$,

$$u^2 v + uv^2 = 0 \Longleftrightarrow u^2 v = uv^2 \Longleftrightarrow u = v.$$

Thus there is no 2-dimensional subspace, L, which satisfies the required property. $\square$

4 Some general bent conditions related to $\mathcal{C}$ and $\mathcal{D}$ classes

Assuming that f is bent (not necessarily of the form $x \cdot \pi(y)$), two equivalent (and more general) conditions for the function $f^*(x) = f(x) + 1_L(x)$ to be bent were given in [4, Theorem]. The first condition states that, if $L = b + L'$ is any flat in $\mathbb{F}_2^m$, then the function $f^*(x) = f(x) + 1_L(x)$ is bent if and only if $f(x) + f(x+a)$ is balanced on L, for any $a \in \mathbb{F}_2^m \setminus L'$. That is, the derivatives of f restricted to L are balanced so that $\sum_{x \in L} (-1)^{f(x)+f(x+a)} = 0$, for all $a \in \mathbb{F}_2^m \setminus L'$. Also, the dimension of L is necessarily larger or equal to n if this condition is satisfied. The class $\mathcal{D}$ was derived using the result that for an n-dimensional subspace L of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ satisfying $f(x,y) = x \cdot \pi(y) = 0$ for any $(x,y) \in L$, the function $x \cdot \pi(y) + 1_L(x,y)$ is bent (cf. [4, Corollary 1]). The subclass named $\mathcal{D}_0$ (which is not contained in $\mathcal{M}$ or in $\mathcal{PS}$), deduced by Carlet, corresponds to a special choice of $L = \{0\} \times \mathbb{F}_2^n$.

Nevertheless, the fact that $x \cdot \pi(y) + 1_L(x,y)$ is bent for $L = \{0\} \times \mathbb{F}_2^n$ can also be easily deduced using the condition related to the derivatives of f restricted to L. On the other hand, by taking $L = \mathbb{F}_2^n \times \{0\}$, it is obvious that the function $f^*(x,y) = x \cdot \pi(y) + 1_L(x,y) = x \cdot \pi(y) + \prod_{i=1}^n (y_i + 1) = x \cdot \pi(y) + g(y)$ is bent, but no new bent functions can be obtained through this selection of L, since $f^* \in \mathcal{M}$. More generally, for the same reason the function $f^*(x,y) = x \cdot \pi(y) + 1_L(x,y)$ is also in $\mathcal{M}$, for $L = \mathbb{F}_2^n \times E$ where E is k-dimensional linear subspace of $\mathbb{F}_2^n$, $0 \le k \le n$. Thus, the case $L = \mathbb{F}_2^n \times E$ is of no interest to us and it is not treated further.

4.1 The analysis for arbitrary π and $L = E \times \mathbb{F}_2^n$

Let us extend our investigation for $f^*(x,y) = x \cdot \pi(y) + 1_L(x,y)$ to the case when π is any permutation on $\mathbb{F}_2^n$, and $L = E \times \mathbb{F}_2^n$. Notice that this particular choice of L implies that $1_L(x,y) = 1_L(x)$ and therefore we are considering the class $\mathcal{C}$. Assuming $f(x,y) = x \cdot \pi(y)$, we have

$$\begin{aligned}
0 &= \sum_{(x,y)\in L} (-1)^{f(x,y)+f(x+b,y+c)} \\
&= \sum_{(x,y)\in L} (-1)^{x\cdot\pi(y)+(x+b)\cdot\pi(y+c)} \\
&= \sum_{x\in E}\sum_{y\in\mathbb{F}_2^n} (-1)^{b\cdot\pi(y+c)+x\cdot(\pi(y)+\pi(y+c))} \\
&= \sum_{y\in\mathbb{F}_2^n}\sum_{x\in E} (-1)^{x\cdot(\pi(y)+\pi(y+c))+b\cdot\pi(y+c)}. \qquad (4)
\end{aligned}$$

Notice that $(b,c) \neq (0,0)$ and in particular $b \neq 0$, whereas c can be equal to zero. We consider two cases, namely $c = 0$ and $c \neq 0$. If $c = 0$, then the above sum becomes

$$\sum_{x\in E}\sum_{y\in\mathbb{F}_2^n} (-1)^{b\cdot\pi(y)},$$

which is zero as $b \neq 0$.

If $c \neq 0$, then rewriting (4) as $\sum_{y\in\mathbb{F}_2^n}(-1)^{b\cdot\pi(y+c)}\sum_{x\in E}(-1)^{x\cdot(\pi(y)+\pi(y+c))}$, one easily deduces the following result.

Lemma 4.1. *Let $f \in \mathfrak{B}_m$ be a bent function given by $f(x,y) = x\cdot\pi(y)$, where π is a permutation over $\mathbb{F}_2^n$, and $L = E\times\mathbb{F}_2^n$ where $\dim(E) = k$, for $k = 1,\ldots,n$. Then, the necessary and sufficient condition that $f^*(x,y) = f(x,y) + 1_L(x,y)$ is a bent function in class $\mathcal{C}$ is that,*

$$\sum_{y\in\mathbb{F}_2^n:\pi(y)+\pi(y+c)\in E^\perp} (-1)^{b\cdot\pi(y+c)} = 0,$$

for any $(b,c) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \setminus L$.

Remark 4.2. *The above condition ensures that even though $\sum_{x\in E}(-1)^{x\cdot(\pi(y)+\pi(y+c))} \neq 0$ for some fixed $y \in \mathbb{F}_2^n$ (which happens exactly when $\pi(y)+\pi(y+c) \in E^\perp$) the double sum still equals to zero. The cases $dim(E) \in \{n-1,n\}$ are trivial and correspond to addition of a constant ($dim(E) = n$) and affine function ($dim(E) = n-1$).*

Remark 4.3. *Though taking $f(x,y) = x\cdot\pi(y)$ is just a special case of considering f to be a bent function in $\mathcal{M}$, most notably the condition on balancedness of the derivatives on E is now related to the balancedness of the derivatives of π on $E^\perp$, as mentioned above.*

Even though the condition of Lemma 4.1 appears to be hard one can easily find a permutation π and a suitable subspace E that satisfy the above condition.

Example 4.4. *Let $n = 3$ and $E = \{000, 010\}$ thus $dim(E) = 1$. Then, $E^{\perp} = \{000, 001, 101, 100\}$. Let us define a nonlinear permutation $\pi : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ and compute the differentials for $c = (001)$:*

$y_3y_2y_1$	$\pi(y)$	$\pi(y+001)$	$\pi(y)+\pi(y+001)$
000	000	001	001
001	001	000	001
010	011	010	001
011	010	011	001
100	111	110	001
101	110	111	001
110	101	100	001
111	100	101	001

This c is obviously a linear structure of π (thus $\pi(y) + \pi(y + 001) = 001$ for all $y \in \mathbb{F}_2^3$) and since $(001) \in E^{\perp}$ we have:

$$\sum_{y \in \mathbb{F}_2^n : \pi(y)+\pi(y+001) \in E^{\perp}} (-1)^{b\cdot\pi(y+001)} = \sum_{y \in \mathbb{F}_2^n} (-1)^{b\cdot\pi(y+001)} = 0,$$

where the last equality is due to the fact that π is a permutation and $b \neq 0$. For other (nonzero) values of $c \in \mathbb{F}_2^3$ it turns out that either $Im(\pi(y)+\pi(y+c)) \subseteq E^{\perp}$ or $Im(\pi(y)+\pi(y+c)) \cap E^{\perp} = \emptyset$. For instance, one may check that $Im(\pi(y) + \pi(y + 011)) = \{010, 011\}$ and the intersection with $E^{\perp}$ is the empty set.

In both cases $\sum_{y \in \mathbb{F}_2^n : \pi(y)+\pi(y+c) \in E^{\perp}} (-1)^{b\cdot\pi(y+c)} = 0$, thus $f(x, y) = x \cdot \pi(y) + 1_L(x, y)$, where $L = E \times \mathbb{F}_2^3$, is a bent function on $\mathbb{F}_2^6$. For instance, one may check that $Im(\pi(y)+\pi(y+011)) = \{010, 011\}$.

It is also of interest to investigate the relation between the spectral values of $f(x, y) = x\cdot\pi(y)$ and $f^*(x, y) = f(x, y) + 1_L(x, y)$. Then, requiring that $f^*(x, y)$ is bent implies the following identity

$$\begin{aligned} W_{f^*}(u, v) &= \sum_{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n} (-1)^{x\cdot\pi(y)+1_L(x,y)+(u,v)\cdot(x,y)} \\ &= W_f(u, v) - 2 \sum_{(x,y) \in L} (-1)^{x\cdot\pi(y)+(u,v)\cdot(x,y)} \\ &= \pm 2^n - 2 \sum_{(x,y) \in L} (-1)^{x\cdot\pi(y)+(u,v)\cdot(x,y)}, \end{aligned}$$

and if f^* is to be bent then we must have $W_{f_{|L}}(u, v) = \sum_{(x,y) \in L} (-1)^{x\cdot\pi(y)+(u,v)\cdot(x,y)} \in \{0, \pm 2^n\}$, for any $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$. If $L = E \times \mathbb{F}_2^n$, we have $W_{f_{|L}}(u, v) = \sum_{x \in E} (-1)^{u\cdot x} \sum_{y \in \mathbb{F}_2^n} (-1)^{x\cdot\pi(y)+v\cdot y}$ and $W_{f_{|L}}(u, 0) = 2^n$, for any $u \in \mathbb{F}_2^n$. This is because for any fixed $x \neq 0$ and $v = 0$, the inner sum $\sum_{y \in \mathbb{F}_2^n} (-1)^{x\cdot\pi(y)} = 0$, unless $x = 0$ and the sum equals then to 2^n.

The next result is now immediate.

Proposition 4.5. *Let $f \in \mathfrak{B}_m$ be a bent function given by $f(x, y) = x \cdot \pi(y)$, where π is a permutation over $\mathbb{F}_2^n$. Let $L = E \times \mathbb{F}_2^n$. If $f^*(x, y) = f(x, y) + 1_L(x, y)$ is a bent function, then $W_f(u, 0) = 2^n$, for any $u \in \mathbb{F}_2^n$.*

Proof. Assuming $L = E \times \mathbb{F}_2^n$, we only need to prove that $W_f(u, 0) = 2^n$, for any $u \in \mathbb{F}_2^n$, is always satisfied. Indeed,

$$W_f(u,0) = \sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{x\cdot\pi(y)+(u,v)\cdot(x,y)} = \sum_{x\in\mathbb{F}_2^n} (-1)^{u\cdot x} \sum_{y\in\mathbb{F}_2^n} (-1)^{x\cdot\pi(y)} = 2^n,$$

which must be true for all $u \in \mathbb{F}_2^n$. Notice that the inner sum $\sum_{y\in\mathbb{F}_2^n}(-1)^{x\cdot\pi(y)} = 0$ for any fixed x, unless $x = 0$ (since π is a permutation), and therefore $W_f(u, 0) = 2^n$, for all $u \in \mathbb{F}_2^n$. $\square$

4.2 The subcase when π is a linear permutation and $L = E \times \mathbb{F}_2^n$

In this section we consider $f^*(x, y) = x\cdot\pi(y)+1_L(x, y)$ when $\pi(y) = yA$ is a linear permutation over $\mathbb{F}_2^n$, $L = E \times \mathbb{F}_2^n$ for some k-dimensional linear subspace E, for $0 \leq k \leq n$, and A is an invertible matrix over $\mathbb{F}_2$ of size $n \times n$ (that is $A \in GL(n, \mathbb{F}_2)$). It will be shown that f^* is always bent regardless the choice of E, but nevertheless f^* is in the completed class $\mathcal{M}^*$.

Theorem 4.6. *Let $f^*(x, y) = x \cdot \pi(y) + 1_L(x, y)$ be a function on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ and $\pi(y) = yA$, $A \in GL(n, \mathbb{F}_2)$, a linear permutation over $\mathbb{F}_2^n$ so that $f(x, y) = x\cdot\pi(y)$ is bent. Furthermore, let L be of the form $L = E \times \mathbb{F}_2^n$ where E is a k-dimensional linear subspace of $\mathbb{F}_2^n$, for $0 \leq k \leq n$. Then, f^* is a bent function.*

Proof. Since f^* is bent if and only if $f(x, y) + f(x + b, y + c)$ is balanced on $L = E \times \mathbb{F}_2^n$ for any $(b, c) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \setminus L$ we have,

$$\begin{aligned}\sum_{(x,y)\in L}(-1)^{f(x,y)+f(x+b,y+c)} &= \sum_{(x,y)\in L}(-1)^{x\cdot\pi(y)+(x+b)\cdot\pi(y+c)}\\ &= \sum_{x\in E;y\in\mathbb{F}_2^n}(-1)^{x\cdot yA+(x+b)\cdot(yA+cA)}\\ &= \sum_{x\in E}(-1)^{(x+b)\cdot cA}\sum_{y\in\mathbb{F}_2^n}(-1)^{b\cdot yA}\end{aligned}$$

which must equal to zero if f^* is bent. Now, since $\pi(y) = yA$ is a permutation over $\mathbb{F}_2^n$ then $\sum_{y\in\mathbb{F}_2^n}(-1)^{bA\cdot y} = 0$, for any $b \neq 0$. Noticing that $b \neq 0$ since $(b, c) \notin L$, we have that $\sum_{(x,y)\in L}(-1)^{f(x,y)+f(x+b,y+c)} = 0$, thus f^* is bent. $\square$

However, it turns out that the functions given by $f^*(x, y) = x\cdot y+1_L(x, y)$ (π being a linear permutation) are embedded in $\mathcal{M}$.

Theorem 4.7. *Let $f^*(x, y) = x\cdot\pi(y)+1_L(x, y)$ be a function on $\mathbb{F}_2^n\times\mathbb{F}_2^n$, and $\pi(y) = yA$ be a linear permutation over $\mathbb{F}_2^n$. Furthermore, let $L = E \times \mathbb{F}_2^n$, where E is a k-dimensional linear subspace of $\mathbb{F}_2^n$, for $0 \leq k \leq n$. Then, f^* belongs to $\mathcal{M}^*$.*

Proof. It is well-known that $f \in \mathcal{M}^*$ on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ if and only if there exists an n-dimensional subspace, say $U \subset \mathbb{F}_2^{2n}$, such that the second derivatives $D_\alpha D_\beta f(x, y) = 0$, for any $\alpha, \beta \in U$.

Notice that since $L = E \times \mathbb{F}_2^n$, the support of L does not depend on the y variables, and so, $1_L(x, y) = 1_L(x)$. Now, for $\alpha = (a, b)$ and $\beta = (c, d)$ where $(a, b),(c, d) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ we have,

$$D_\alpha D_\beta(x \cdot yA) = D_\beta(x \cdot bA + a \cdot yA + a \cdot bA),$$

and taking the derivative with respect to $\beta = (c, d)$ gives $D_\alpha D_\beta(x \cdot yA) = c \cdot bA + a \cdot dA$. So it is sufficient to show the existence of U such that both $D_\alpha D_\beta 1_L(x) = 0$ and $D_\alpha D_\beta(x \cdot yA) = 0$, for any $\alpha, \beta \in U$. Taking $U = \{0\} \times \mathbb{F}_2^n$ so that $a = c = 0$, we clearly have $D_\alpha D_\beta 1_L(x) = 0$ and $D_\alpha D_\beta(x \cdot y) = b \cdot c + aA \cdot d = 0$, for any $\alpha, \beta \in U$. □

5 k-linear split permutations

In this section we look for permutations π, where there are subspaces L such that (π, L) satisfies the property (C). In contrast to Theorem 3.3 which, for a particular class of permutations introduced by Hou [12] shows the nonexistence of a 2-dimensional linear subspace L, it turns out that our considered permutations do give rise to functions in the $\mathcal{C}$ class, and both necessary and sufficient conditions on L can be given.

It is known that any permutation on a finite field can be written as a polynomial. We consider those permutation polynomials which can be factored (split) into linearized polynomials.

Definition 5.1. *A linearized polynomial $\ell \in \mathbb{F}_{2^n}[X]$ is a polynomial of the shape*

$$\ell(X) = \sum_{i=0}^{n-1} a_i X^{2^i} \text{ with } a_i \in \mathbb{F}_{2^n}.$$

The set of all such polynomials is denoted by $\mathcal{L}(n)$.

The action of a pair of bijective linearized polynomials $(\ell_1, \ell_2) \in \mathcal{L}(n) \times \mathcal{L}(n)$ on $\mathbb{F}_{2^n}[X]$ is defined as $\ell_1 \circ \phi \circ \ell_2$ where $\phi \in \mathbb{F}_{2^n}[X]$. Two polynomials $\phi, \psi \in \mathbb{F}_{2^n}[X]$ are said to be *linearly equivalent* if there exist (bijective) $\ell_1, \ell_2 \in \mathcal{L}(n)$ such that $\ell_1 \circ \phi \circ \ell_2 = \psi$.

Lemma 5.2. *Suppose π and ϕ are two linearly equivalent permutations on $\mathbb{F}_{2^n}$ such that $\phi = \ell_1 \circ \pi \circ \ell_2$ where $\ell_1, \ell_2 \in \mathcal{L}(n)$, and L is a linear subspace of $\mathbb{F}_{2^n}$. If $\pi(a + L)$ is a flat for all $a \in \mathbb{F}_{2^n}$, then $\phi(a + \ell_2^{-1}(L))$ is a flat for all $a \in \mathbb{F}_{2^n}$.*

Proof. For any $a \in \mathbb{F}_{2^n}$ we have

$$\begin{aligned}\phi(a + \ell_2^{-1}(L)) &= \ell_1 \circ \pi \circ \ell_2(a + \ell_2^{-1}(L)) = \ell_1 \circ \pi(\ell_2(a + \ell_2^{-1}(L))) \\ &= \ell_1 \circ \pi(\ell_2(a) + L) = \ell_1(\pi(\ell_2(a) + L)).\end{aligned}$$

Since $\pi(\ell_2(a) + L)$ is a flat and ℓ_1 is a linear permutation, $\ell_1(\pi(\ell_2(a) + L))$ is a flat. □

Thus it is enough to consider $\mathcal{C}$ type constructions associated to linearly inequivalent permutations. In the spirit of Blokhuis, Coulter, Henderson and O'Keefe [2] and Laigle-Chapuy [13], we extend their construction in the next definition.

We call a polynomial $\phi \in \mathbb{F}_{2^n}[X]$ a *k-linear split* polynomial if it is of the form

$$\phi(X) = \pi_1(X)\pi_2(X)\cdots\pi_k(X) \text{ with } \pi_i \in \mathcal{L}(n), 1 \le i \le k.$$

Blokhuis et al. [2] and Laigle-Chapuy [13] refer to the case $k = 2$ as a bilinear polynomial (some authors prefer Dembowski-Ostrom polynomial), but the "bilinear" notion has a different meaning in too many areas, so we prefer to insert "split" into the definition. Certainly, if the function associated to the polynomial ϕ is bijective, we will refer to ϕ as a k-linear split permutation.

It is easy to see that using the transformation $Y = \pi_1(X)$, the polynomial ϕ is linearly equivalent to one of the type

$$\phi(Y) = Y\ell_1(Y)\cdots\ell_{k-1}(Y), \text{ where } \ell_i = \pi_i \circ \pi_1^{-1} \in \mathcal{L}(n), \tag{5}$$

so, we will only consider these forms from here on.

5.1 $\mathcal{C}$ type bent functions associated to bilinear split permutations

From our observation (5) (see also [2, Section 2]), it will be sufficient to investigate the $\mathcal{C}$ type bent functions (in this case) associated to bilinear split permutations of the shape

$$X\ell(X) = \sum_{i=0}^{n-1} a_i X^{2^i+1} \text{ with } a_i \in \mathbb{F}_{2^n}.$$

The set of all such polynomials is denoted by $\mathcal{B}(n)$.

Theorem 5.3. *Suppose $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a permutation defined by $\phi(x) = x\ell(x) + \ell_0(x)$, for all $x \in \mathbb{F}_{2^n}$, where $\ell, \ell_0 \in \mathcal{L}(n)$. Let $L = \langle u, v\rangle$ be a 2-dimensional subspace. Then (ϕ, L) satisfies the (C) property if and only if $\frac{\ell(u)}{u} = \frac{\ell(v)}{v}$.*

Proof. For L to satisfy the required condition for all $a \in \mathbb{F}_{2^n}$, we must have

$$\begin{aligned}
&\phi(a) + \phi(a+u) + \phi(a+v) + \phi(a+u+v)\\
&= a\ell(a) + \ell_0(a) + (a+u)\ell(a+u) + \ell_0(a+u) + (a+v)\ell(a+v) + \ell_0(a+v)\\
&\quad + (a+u+v)\ell(a+u+v) + \ell_0(a+u+v)\\
&= a\ell(a) + a\ell(a) + a\ell(u) + u\ell(a) + u\ell(u) + a\ell(a) + a\ell(v) + v\ell(a) + v\ell(v)\\
&\quad + a\ell(a) + a\ell(u) + a\ell(v) + u\ell(a) + u\ell(u) + u\ell(v) + v\ell(a) + v\ell(u) + v\ell(v)\\
&= u\ell(v) + v\ell(u) = 0.
\end{aligned}$$

Therefore the necessary and sufficient condition that a 2-dimensional linear subspace $L = \langle u, v\rangle$ has the required property is that $\frac{\ell(u)}{u} = \frac{\ell(v)}{v}$. □

Corollary 5.4. *Suppose $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, defined by $\phi(x) = x\ell(x) + \ell_0(x)$, for all $x \in \mathbb{F}_{2^n}$, where $\ell(X) = \sum_{i=0}^{n-1} a_i X^{2^i} \in \mathcal{L}(n)$. Then there exists a $\mathcal{C}$ type function associated to ϕ if and only if the function $x \mapsto \frac{\ell(x)}{x}$ on $\mathbb{F}_{2^n}^*$ is not a permutation.*

Proof. The proof follows easily from Theorem 5.3. □

The following result due to Payne [17] restated by Berger, Canteaut, Charpin and Laigle-Chapuy [1] provides a complete characterization of such linearized polynomials.

Theorem 5.5 ([1], Theorem 6)**.** *A polynomial in $\mathbb{F}_{2^n}[X]$ of the form*

$$Q(X) = \sum_{i=1}^{n-1} c_i X^{2^i-1}, c_i \in \mathbb{F}_{2^n}$$

cannot be a permutation polynomial unless $Q(X) = c_k X^{2^k-1}$ with $\gcd(k,n) = 1$ and $c_k \in \mathbb{F}_{2^n}^*$.

Let $Supp(\ell) = \{i : a_i \neq 0\}$ where $\ell \in \mathcal{L}(n)$. Then $P(X) = \frac{\ell(X)}{X}$ is not a permutation if any one of the following conditions are satisfied.

1. The cardinality of $Supp(\ell)$, that is, $|Supp(\ell)| \geq 3$.
2. The coefficient $a_0 = 0$ and $|Supp(\ell)| = 2$.
3. The coefficient $a_0 \neq 0$ and $Supp(\ell) = \{0, k\}$ where $\gcd(k, n) \neq 1$.

In addition to Remark 3.2, it is possible to obtain explicitly $\mathcal{C}$ type bent functions, for a special class of explicit permutations. Thus, for effective construction of the functions in $\mathcal{C}$, there is a need to characterize linear subspaces such as L with respect to permutations over $\mathbb{F}_{2^n}$.

In Theorem 5.7 we consider the permutation $\phi(x) = x^{2^{t+1}+1} + x^3 + x$, for all $x \in \mathbb{F}_{2^n}$ where $n = 2t + 1$ (see [11]).

Lemma 5.6 ([3], Corollary 1). *Let d, n, s be positive integers satisfying $\gcd(n, s) = 1$ and let*

$$0 \neq g(X) = \sum_{i=0}^{d} r_i X^{2^{si}} \in \mathbb{F}_{2^n}[X].$$

Then the equation $g(X) = 0$ has at most 2^d solutions in $\mathbb{F}_{2^n}$.

Theorem 5.7. *Suppose $\phi(x) = x^{2^{t+1}+1}+x^3+x$, for all $x \in \mathbb{F}_{2^n}$, where $n = 2t+1$, $\gcd(t, n) = 1$. Then there exists at least one and at most $2(2^n - 2)$ two dimensional linear subspaces L such that $\phi(a + L)$ is flat for all $a \in \mathbb{F}_{2^n}$.*

Proof. Since, $\frac{\phi(x)-x}{x}$ is not a permutation, by Corollary 5.4 there exists at least one function in $\mathcal{C}$ associated to ϕ.

Let $L = \langle u, v\rangle$ be a 2-dimensional subspace of $\mathbb{F}_{2^n}$. The set $\phi(a + L)$ is a flat if and only if

$$\phi(a) + \phi(a + u) + \phi(a + v) + \phi(a + u + v) = u^{2^{t+1}} v + uv^{2^{t+1}} + u^2 v + uv^2 = 0.$$

Exponentiating both sides of the above equation by 2^{2t}, we obtain

$$\begin{aligned}
&(u^{2^{t+1}} v + uv^{2^{t+1}} + u^2 v + uv^2)^{2^{2t}} = 0 \\
\text{i.e.,}\quad & u^{2^{3t+1}} v^{2^{2t}} + u^{2^{2t}} v^{2^{3t+1}} + u^{2^{2t+1}} v^{2^{2t}} + u^{2^{2t}} v^{2^{2t}+1} = 0 \\
\text{i.e.,}\quad & (u^{2^{2t+1}})^{2^t} v^{2^{2t}} + u^{2^{2t}} (v^{2^{2t+1}})^{2^t} + u^{2^{2t+1}} v^{2^{2t}} + u^{2^{2t}} v^{2^{2t}+1} = 0 \\
\text{i.e.,}\quad & u^{2^t} v^{2^{2t}} + u^{2^{2t}} v^{2^t} + uv^{2^{2t}} + u^{2^{2t}} v = 0,\ \text{since } u, v \in \mathbb{F}_{2^n} \text{ where } n = 2t + 1 \\
\text{i.e.,}\quad & (u^{2^t} + u)v^{2^{2t}} + u^{2^{2t}} v^{2^t} + u^{2^{2t}} v = 0.
\end{aligned}$$

Therefore,

$$\sum_{i=0}^{2} c_i v^{2^{it}} = 0, \text{ where } c_2 = u^{2^t} + u, c_1 = c_0 = u^{2^{2t}}. \tag{6}$$

Since $\gcd(t, n) = 1$ where $n = 2t + 1$, the greatest common divisor $\gcd(2^t - 1, 2^{2t+1} - 1) = 1$. Thus $c_2 = u^{2^t} + u \neq 0$ if and only if $u = 1$. If $u = 1$, then (6) reduces to $v^{2^t} + v = 0$, which has only one solution $v = 1$. Equation (6) has at most $2^2 = 4$ solutions if $u \neq 1$, by Lemma 5.6

among them one solution is $v = 0$ and another is $v = u$. So, if $u \notin \{0, 1\} \subseteq \mathbb{F}_{2^n}$, we can obtain at most two values of v such that $\{u, v\}$ is linearly independent. Thus, we can obtain at most $2(2^n - 2)$ many subspaces L such that $\phi(a + L)$ is a flat for all $a \in \mathbb{F}_{2^n}$. If $u = 1$, then the only solution is $v = u = 1$; giving us no subspace L. So the total number of two dimensional subspace L such that $\phi(a + L)$ is flat for all $a \in \mathbb{F}_{2^n}$ is at most $2(2^n - 2)$. □

We now consider the case of a bilinear split permutation $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $\phi(x) = x^{2^i+1}$, for all $x \in \mathbb{F}_{2^n}$.

Theorem 5.8. *Suppose $\phi(x) = x^{2^r+1}$, for all $x \in \mathbb{F}_{2^n}$, where $\gcd(r, n) = e$.*

(i) We assume that n/e is odd. Then (ϕ, L) (where L is a subspace of $\dim(L) = 2$) satisfies the (C) property if and only if $L = \langle u, cu \rangle$ where $u \in \mathbb{F}_{2^n}^*$ and $1 \neq c \in \mathbb{F}_{2^e}^*$.

(ii) We assume that $e = \gcd(n, r) > 1$ and $L = \langle u_1, c_1u_1, \ldots, c_{s-1}u_1 \rangle$, $\dim(L) = s$, $c_i \in \mathbb{F}_{2^e}^*$, $1 \leq i \leq s - 1$, $s \geq 2$, and $u_1 \in \mathbb{F}_{2^n}^*$. Then (ϕ, L) satisfies the (C) property.

Proof. We first show (i). Suppose that $L = \langle u, v \rangle$ is a 2-dimensional subspace of $\mathbb{F}_{2^n}$. For any $a \in \mathbb{F}_{2^n}$ we have

$$a + L = \{a, a + u, a + v, a + u + v\}.$$

The set $\phi(a + L)$ is a flat if and only if

$$\phi(a) + \phi(a + u) + \phi(a + v) + \phi(a + u + v) = 0.$$

Therefore we have

$$\begin{aligned}
&\phi(a) + \phi(a + u) + \phi(a + v) + \phi(a + u + v) \\
&= a^{2^r+1} + (a + u)^{2^r+1} + (a + v)^{2^r+1} + (a + u + v)^{2^r+1} \\
&= a^{2^r+1} + a^{2^r+1} + au^{2^r} + a^{2^r}u + u^{2^r+1} + a^{2^r+1} + av^{2^r} + a^{2^r}v + v^{2^r+1} \\
&\quad + a^{2^r+1} + a(u + v)^{2^r} + a^{2^r}(u + v) + (u + v)^{2^r+1} \\
&= uv^{2^r} + u^{2^r}v \\
&= uv^{2^r} + u^{2^r}v = 0.
\end{aligned}$$

It follows that $(uv^{-1})^{2^r-1} = 1$. Combining with this the fact that $(uv^{-1})^{2^n-1} = 1$, for $u, v \in \mathbb{F}_{2^n}^*$, and $\gcd(2^n - 1, 2^r - 1) = 2^e - 1$ we obtain $(uv^{-1})^{2^e-1} = 1$. Therefore $L = \langle u, cu \rangle$ where $u \in \mathbb{F}_{2^n}^*$ and $c \in \mathbb{F}_{2^e}^*$.

We next show (ii). Assume that $L = \langle u_1, c_1u_1, \ldots, c_{s-1}u_1 \rangle$ is of dimension $s \geq 2$, where $u_1 \in \mathbb{F}_{2^n}^*, c_i \in \mathbb{F}_{2^e}^*$, $\gcd(2^r - 1, 2^n - 1) = 2^e - 1$. Then (ϕ, L) satisfies the (C) property, which is equivalent to the fact that for any $u, v \in L$ there exists $w \in L$ such that $\phi(a + u) + \phi(a + v) + \phi(a) + \phi(a + w) = 0$. To show this, we take $u = \alpha u_1, v = \beta u_1$, $\alpha, \beta \in \mathbb{F}_{2^e}^*$, and define $w := u + v = (\alpha + \beta)u_1 \in L$. Then

$$\begin{aligned}
&\phi(a + u) + \phi(a + v) + \phi(a) + \phi(a + w) \\
&= (a + u)^{1+2^r} + (a + v)^{1+2^r} + a^{1+2^r} + (a + u + v)^{1+2^r} \\
&= au^{2^r} + ua^{2^r} + av^{2^r} + va^{2^r} + a(u + v)^{2^r} + (u + v)a^{2^r} + uv^{2^r} + vu^{2^r} \\
&= uv^{2^r} + vu^{2^r} = \alpha u_1(\beta u_1)^{2^r} + \beta u_1(\alpha u_1)^{2^r} \\
&= \alpha\beta u_1^{1+2^r} + \alpha\beta u_1^{1+2^r} = 0,
\end{aligned}$$

where we used that $\alpha^{2^r} = \alpha, \beta^{2^r} = \beta$, since both $\alpha, \beta \in \mathbb{F}_{2^e}^*$. The claim is shown. □

From the above theorem we note that if $e = 1$ then there is no linear subspace of dimension 2 such that function in $\mathcal{C}$ can be constructed with respect to the class of permutations under consideration.

The following bilinear split permutations (all are linearly equivalent to each other) are constructed by Blokhuis et al. [2] on $\mathbb{F}_{2^n}$ where $0 < i < n$ and $e = \gcd(i, n)$ (see also Laigle-Chapuy [13]):

1. X^{2^i+1} where n/e is odd.
2. $X^{2^i+1} + aX^{2^{n-i}+1}$ where n/e is odd and $a^{(2^n-1)/(2^e-1)} \neq 1$.
3. $X^{2^{2i}+1} + (aX)^{2^i+1} + aX^2$ where $n = 3i$ and $a^{(2^n-1)/(2^e-1)} \neq 1$.

By Theorem 5.8 and Lemma 5.2 we can derive explicit choices of L which yield $\mathcal{C}$ class bent functions associated to the above permutations.

5.2 $\mathcal{C}$ type bent functions associated to k-linear split permutations

We next look at $\mathcal{C}$ type bent functions associated to trilinear split permutations.

Theorem 5.9. *Suppose $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a permutation of the form $\phi(x) = x\ell_1(x)\ell_2(x)$, for all $x \in \mathbb{F}_{2^n}$, where $\ell_1(X) = \sum_{i=0}^{n-1} a_i X^{2^i}, \ell_2(X) = \sum_{i=0}^{n-1} b_i X^{2^i} \in \mathcal{L}(n)$ ($a_i, b_i \in \mathbb{F}_{2^n}$), and $L = \langle u, v\rangle$ is a 2-dimensional subspace of $\mathbb{F}_{2^n}$. Then $\phi(a + L)$ is a flat for all $a \in \mathbb{F}_{2^n}$ if and only if*

$$\begin{aligned}
&\sum_{1\le i,j\le n-1} a_i b_j \left(u^{2^i} v^{2^j} + v^{2^i} u^{2^j}\right) + \sum_{j=0}^{n-1} (a_0 b_j + a_j b_0)\left(uv^{2^j} + u^{2^j} v\right) = 0,\\
&\sum_{j=0}^{n-1} (a_i b_j + a_j b_i)\left(uv^{2^j} + u^{2^j} v\right) = 0, \quad \text{for all } i = 1, \dots, n-1, \\
&\sum_{0\le i,j\le n-1} a_i b_j \left((u+v)\left(u^{2^i} v^{2^j} + v^{2^i} u^{2^j}\right) + uv^{2^i+2^j} + vu^{2^i+2^j}\right) = 0.
\end{aligned} \tag{7}$$

Proof. Using Lemma 3.1, we see that $\phi(a + L)$ is a flat for all $a \in \mathbb{F}_{2^n}$ if and only if

$$\begin{aligned}
&\phi(a) + \phi(a + u) + \phi(a + v) + \phi(a + u + v)\\
&= a[\ell_1(u)\ell_2(v) + \ell_1(v)\ell_2(u)] + \ell_1(a)[u\ell_2(v) + v\ell_2(u)]\\
&+ \ell_2(a)[u\ell_1(v) + v\ell_1(u)] + u\ell_1(u)\ell_2(v) + u\ell_1(v)\ell_2(u)\\
&+ u\ell_1(v)\ell_2(v) + v\ell_1(u)\ell_2(u) + v\ell_1(u)\ell_2(v) + v\ell_1(v)\ell_2(u) = 0
\end{aligned} \tag{8}$$

for all $a \in \mathbb{F}_{2^n}$. Substituting ℓ_1, ℓ_2 in (8) we obtain

$$\begin{aligned}
&\left(\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}(a_i b_j + a_j b_i)u^{2^i} v^{2^j}\right) a + \sum_{i=0}^{n-1} a_i \left(\sum_{j=0}^{n-1}(uv^{2^j} + u^{2^j} v) b_j\right) a^{2^i}\\
&\qquad + \sum_{i=0}^{n-1} b_i \left(\sum_{j=0}^{n-1}(uv^{2^j} + u^{2^j} v) a_j\right) a^{2^i}\\
&+ u\ell_1(u)\ell_2(v) + u\ell_1(v)\ell_2(u) + u\ell_1(v)\ell_2(v) + v\ell_1(u)\ell_2(u) + v\ell_1(u)\ell_2(v) + v\ell_1(v)\ell_2(u)
\end{aligned}$$

$$= \left(\sum_{0\le i,j\le n-1} (a_ib_j + a_jb_i)u^{2^i}v^{2^j} \right) a + \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} (uv^{2^j} + u^{2^j}v) \right) (a_ib_j + a_jb_i)\, a^{2^i}$$
$$+ (u+v) \sum_{0\le i,j\le n-1} a_ib_ju^{2^i}v^{2^j} + (u+v) \sum_{0\le i,j\le n-1} a_ib_ju^{2^i}v^{2^j}$$
$$+ u \sum_{0\le i,j\le n-1} a_ib_jv^{2^i+2^j} + v \sum_{1\le i,j\le n-1} a_ib_ju^{2^i+2^j}$$
$$= \left(\sum_{1\le i,j\le n-1} (a_ib_j + a_jb_i)u^{2^i}v^{2^j} + \left(\sum_{j=0}^{n-1} (uv^{2^j} + u^{2^j}v) \right) (a_0b_j + a_jb_0) \right) a$$
$$+ \sum_{i=1}^{n-1} \left(\sum_{j=0}^{n-1} (uv^{2^j} + u^{2^j}v) \right) (a_ib_j + a_jb_i)\, a^{2^i}$$
$$+ (u+v) \sum_{0\le i,j\le n-1} a_ib_j(u^{2^i}v^{2^j} + v^{2^i}u^{2^j}) + \sum_{0\le i,j\le n-1} a_ib_j(uv^{2^i+2^j} + vu^{2^i+2^j}) = 0,$$

for all $a \in \mathbb{F}_{2^n}$. Thus, in order to construct $\mathcal{C}$ type bents associated to the permutation ϕ with $L = \langle u, v\rangle$, we must obtain linearly independent vectors in $u, v \in \mathbb{F}_{2^n}$ satisfying the system of equations (7). $\square$

Corollary 5.10. *Let us consider the case when $\phi(x) = x^{1+2^r+2^s}$, for all $x \in \mathbb{F}_{2^n}$, where $1 < r < s$. Then there is no 2-dimensional subspace $L = \langle u, v\rangle$ satisfying the (C) property.*

Proof. By the previous theorem, the system of equations (7) reduces to

$$\begin{aligned}
&a_rb_s(u^{2^r}v^{2^s} + u^{2^s}v^{2^r}) = 0\\
&(uv^{2^s} + u^{2^s}v)a_rb_s = 0\\
&(uv^{2^r} + u^{2^r}v)a_rb_s = 0\\
&u^{1+2^r}v^{2^s} + u^{1+2^s}v^{2^r} + uv^{2^s+2^r} + u^{2^s+2^r}v + u^{2^r}v^{1+2^s} + u^{2^s}v^{1+2^r} = 0.
\end{aligned}$$

Since $a_r \neq 0$ and $b_s \neq 0$ we obtain the system

$$\begin{aligned}
&u^{2^r}v^{2^s} + u^{2^s}v^{2^r} = 0\\
&uv^{2^s} + u^{2^s}v = 0\\
&uv^{2^r} + u^{2^r}v = 0\\
&u^{1+2^r}v^{2^s} + u^{1+2^s}v^{2^r} + uv^{2^s+2^r} + u^{2^s+2^r}v + u^{2^r}v^{1+2^s} + u^{2^s}v^{1+2^r} = 0
\end{aligned} \tag{9}$$

that is, $(uv^{-1})^{2^{n+s-r}-1} = 1$, $(uv^{-1})^{2^s-1} = 1$ and $(uv^{-1})^{2^r-1} = 1$. Let

$$\gcd\left(2^n - 1, 2^{n+s-r} - 1, 2^r - 1, 2^s - 1\right) = 2^e - 1$$

(it is immediate that if L exists, then we must have $e > 1$). Then $uv^{-1} \in \mathbb{F}_{2^e}$. Since $e > 1$, there exists $1 \neq c \in \mathbb{F}_{2^e}^*$ such that $v = cv$. Substituting $v = cu$ in the last equation of (9) we obtain

$$cu^{1+2^r+2^s} + cu^{1+2^r+2^s} + c^2u^{1+2^s+2^r} + cu^{1+2^s+2^r} + c^2u^{1+2^r+2^s} + c^2u^{1+2^r+2^s} = 0,$$

that is, $(c+c^2)u^{1+2^r+2^s}=0$, implying $c\in\{0,1\}$, which is a contradiction. Therefore, there are no trilinear split permutation of the above form for which we can construct a 2-dimensional subspace $L=\langle u,v\rangle$ with the required conditions. $\square$

We can extend the previous theorem to the general case of k-linear split permutations, showing in our next theorem a nonexistence result.

Theorem 5.11. *If $\phi(x)=x^{\sum_{i=0}^k 2^{r_i}}$ $(k\geq 2)$, for all $x\in\mathbb{F}_{2^n}$, where $r_0=0<r_1<\ldots<r_k<n$, then there is no 2-dimensional subspace L such that (ϕ,L) satisfies the (C) property.*

Proof. We assume that L exists, and so, there exists $u,v\in\mathbb{F}_{2^n}$ that are $\mathbb{F}_2$–linearly independent such that (ϕ,L) satisfies the (C) property. For a subset $A\subseteq\{0,1,\ldots,k\}$ (for convenience, we write the set $\{0,1,\ldots,k\}$ as $[0,k]$), we denote by $R_A:=\sum_{i\in A}2^{r_i}$ and $\bar{A}=[0,k]\setminus A$, with the convention that if $A=\emptyset$, then $R_A=0$.

Since, $\phi(a+L)$ is a flat, then $\phi(a)+\phi(a+u)+\phi(a+v)+\phi(a+u+v)=0$, and so,

$$\begin{aligned}
0 &= a^{R_{[0,k]}}+(a+u)^{R_{[0,k]}}+(a+v)^{R_{[0,k]}}+(a+u+v)^{R_{[0,k]}}\\
&= a^{R_{[0,k]}}+\prod_{i=0}^{k}(a+u)^{2^{r_i}}+\prod_{i=0}^{k}(a+v)^{2^{r_i}}+\prod_{i=0}^{k}(a+u+v)^{2^{r_i}}
\end{aligned}$$

$$\begin{aligned}
&= a^{R_{[0,k]}}+\prod_{i=0}^{k}\left(a^{2^{r_i}}+u^{2^{r_i}}\right)+\prod_{i=0}^{k}\left(a^{2^{r_i}}+v^{2^{r_i}}\right)+\prod_{i=0}^{k}\left(a^{2^{r_i}}+(u+v)^{2^{r_i}}\right)\\
&= a^{R_{[0,k]}}+\sum_{A\subseteq[0,k]}a^{R_A}u^{R_{\bar{A}}}+\sum_{A\subseteq[0,k]}a^{R_A}v^{R_{\bar{A}}}+\sum_{A\subseteq[0,k]}a^{R_A}(u+v)^{R_{\bar{A}}}\\
&= \sum_{A\subsetneqq[0,k]}\left(u^{R_{\bar{A}}}+v^{R_{\bar{A}}}+(u+v)^{R_{\bar{A}}}\right)a^{R_A},
\end{aligned}$$

for all $a\in\mathbb{F}_{2^n}$. That is, the polynomial

$$\sum_{A\subsetneqq[0,k]}\left(u^{R_{\bar{A}}}+v^{R_{\bar{A}}}+(u+v)^{R_{\bar{A}}}\right)X^{R_A}$$

has 2^n roots, but its degree is $\leq R_{[0,k]}=\sum_{i=0}^k 2^{r_i}<2^n$, and therefore all its coefficients must be 0. Hence (replacing $\bar{A}$ by A, under the condition $A\neq\emptyset$), we have

$$u^{R_A}+v^{R_A}+(u+v)^{R_A}=0,\ \text{for all } A\subseteq[0,k], A\neq\emptyset. \tag{10}$$

Now, taking $A=\{0,i\},1\leq i\leq k$, and simplifying, we get

$$vu^{2^{r_i}}+uv^{2^{r_i}}=0,\ \text{for all } 1\leq i\leq k,$$

and so, $vu^{-1}\in\mathbb{F}_{2^{r_i}}^*,1\leq i\leq k$. Thus, if $2^e-1=\gcd(2^n-1,2^{r_1}-1,\ldots,2^{r_k}-1)$ (certainly, if L of dimension 2 exists, it is necessary that $e>1$), then $v=cu$, for some $c\in\mathbb{F}_{2^e}^*\setminus\{1\}$. Substituting $v=cu$ in (10) with $A=\{0,1,2\}$, we obtain

$$cu^{1+2^{r_1}+2^{r_2}}+cu^{1+2^{r_1}+2^{r_2}}+c^2u^{1+2^{r_2}+2^{r_1}}+cu^{1+2^{r_2}+2^{r_1}}+c^2u^{1+2^{r_1}+2^{r_2}}+c^2u^{1+2^{r_1}+2^{r_2}}=0,$$

that is,

$$(c+c^2)u^{1+2^{r_1}+2^{r_2}}=0,$$

implying $c\in\{0,1\}$, which is a contradiction. Therefore, there are no 2-dimensional subspaces L for which we can construct $\mathcal{C}$ type bent functions corresponding to k-linear split monomial permutations. $\square$

For permutations on $\mathbb{F}_{2^n}$ of the form $\phi(x)=x^{\sum_{i=1}^{k}2^{r_i}}$ $(k\ge 2)$, we can inquire whether there are subspaces of dimension >2 associated to $\mathcal{C}$ type bent functions. While in general we cannot answer that question, we can certainly derive some necessary conditions.

Theorem 5.12. *Let ϕ be a monomial permutation of degree k, that is, $\phi(x)=x^{\sum_{i=1}^{k}2^{r_i}}$, $0=r_1<\ldots<r_k<n$, $k\ge 2$. A necessary condition for (ϕ,L) (with L of dimension $s\ge 2$) to satisfy the (C) property is*

$$\sum_{u\in L}u^{R_A}=0,\ \text{for all } \emptyset\ne A\subseteq[0,k]. \tag{11}$$

Moreover, if (ϕ,L) with L of dimension $s\ge 2$ satisfies the property (C), then both $2^s-1, 2^n-2^s$ must be in $\mathbb{N}p_1+\cdots+\mathbb{N}p_\ell$, where $2^n-1=\prod_{i=1}^{\ell}p_i^{e_i}$ is the prime power factorization (we adopt the convention that $0\in\mathbb{N}$).

Proof. Since for subspaces or flats of dimension $s\ge 2$ the sum of all elements must be zero, we can infer (as we have done in the proof of our previous theorem) that for all $a\in\mathbb{F}_{2^n}$,

$$\begin{aligned}
0 &= \sum_{u\in L}\phi(a+u)=\sum_{u\in L}\prod_{i=1}^{k}(a+u)^{2^{r_i}}\\
&= \sum_{u\in L}\sum_{A\subseteq[0,k]}u^{R_A}a^{R_{\bar{A}}}\\
&= \sum_{\emptyset\ne A\subseteq[0,k]}\left(\sum_{u\in L}u^{R_A}\right)a^{R_{\bar{A}}}.
\end{aligned}$$

As before, the polynomial $\sum_{\emptyset\ne A\subseteq[0,k]}\left(\sum_{u\in L}u^{R_A}\right)X^{R_{\bar{A}}}$ with degree $<2^n$ and has 2^n roots, and so, all coefficients must be zero (the terms $X^{R_{\bar{A}}}$ are all distinct for different $\bar{A}$ by the uniqueness of binary representations), from which we infer the first claim.

It is well-known (see Lam and Leung [14, 15] and Sivek [19]) that a sum of k distinct m-th roots of unity is zero (we say that m is k-balancing) if and only if both k and $m-k$ are in $\mathbb{N}p_1+\cdots+\mathbb{N}p_\ell$, where $m=\prod_{i=1}^{\ell}p_i^{e_i}$ is the prime power factorization. Since the elements $u\in L\subseteq\mathbb{F}_{2^n}$ are (2^n-1)-th roots of unity, condition (11) shows that (2^n-1) is (2^s-1)-balancing (since the cardinality of L^* is 2^s-1). Expressing $2^n-1=\prod_{i=1}^{\ell}p_i^{e_i}$, then the previous result forces both 2^s-1 and 2^n-2^s to be in $\mathbb{N}p_1+\cdots+\mathbb{N}p_\ell$. $\square$

Using some elementary number theory arguments, we can easily get several results regarding the nonexistence of subspaces as in property (C). Let $\mathbf{p}(N)$ denote the smallest prime factor of N.

Corollary 5.13. *With the notations of Theorem 5.12, the following statements are true:*

(*i*) *If* $1 < s < \log_2(\mathbf{p}(2^n - 1))$, *or* $\log_2(2^n - \mathbf{p}(2^n - 1)) < s < n$, *then there are no pairs* (ϕ, L) *satisfying the* (C) *property, where* $\dim(L) = s$ *and* ϕ *is a monomial permutation.*

(*ii*) *Let* $n = P$ *be a prime number. If* $2^n - 1 = p$ *is a Mersenne prime, or* $2^n - 1 = p\,q$, *a product of two primes, then there are no subspaces of dimension* $1 < s < n$ *satisfying the* $\mathcal{C}$ *type bent condition* (C) *for a monomial permutation* ϕ *of degree* $k \geq 3$.

Proof. The first claim follows easily observing that, by Theorem 5.12, if $s < \log_2(\mathbf{p}(2^n - 1))$, then $2 \leq 2^s - 1 < \mathbf{p}(2^n - 1) \in \{p_1, \ldots, p_\ell\}$, and so, $2^s - 1 \notin \mathbb{N}p_1 + \cdots + \mathbb{N}p_\ell$; if $s > \log_2(2^n - \mathbf{p}(2^n - 1))$, then $2^n - 2^s < \mathbf{p}(2^n - 1)$, and so, $2^n - 2^s \notin \mathbb{N}p_1 + \cdots + \mathbb{N}p_\ell$.

Regarding claim (*ii*), if $2^n - 1 = p$ is a Mersenne prime, then, by Theorem 5.12, $2^n - 1$ is $(2^s - 1)$-balancing, and so, one needs $2^s - 1 = ap$ and $2^n - 2^s = Ap$, for some nonnegative integers a, A. Thus, $2^n - 1 = (A + a)p = p$, which implies that $(a, A) \in \{(0, 1), (1, 0)\}$, therefore, either $s = 0$, or $s = n$, which contradicts our assumption that $2 \leq s < n$.

To show the second part of claim (*ii*), observe that by Theorem 5.12, there exist nonnegative integers a, b, A, B such that

$$\begin{aligned} 2^n - 1 &= p\,q, \\ 2^s - 1 &= ap + bq, \\ 2^n - 2^s &= Ap + Bq, \end{aligned}$$

from which we derive that $(A + a)p + (B + b)q = p\,q$, and so, $A + a \equiv 0 \pmod q, B + b \equiv 0 \pmod p$. If $ab \neq 0$, since A, B, a, b are nonnegative and $A < q, a < q, B < p, b < p$, then $A = q - a, B = p - b$. But then, $2^n - 2^s = Ap + Bq = 2pq - (ap + bq) = pq + (pq - 2^s + 1) > 2^n$, which is a contradiction. Thus, $ab = 0$, and without loss of generality, we assume that $b = 0$, but then $B = 0$, as well. Thus, $2^s - 1 = ap, 2^n - 2^s = (q - a)p$. It is well-known that $\gcd(2^n - 1, 2^s - 1) = 2^{\gcd(n,s)} - 1$. Since $p | 2^n - 1, p | 2^s - 1$ and n is prime (thus, for $2 \leq s < n$, $\gcd(n, s) = 1$), then $p | 2^{\gcd(n,s)} - 1 = 1$, which is a contradiction. ☐

5.3 $\mathcal{C}$ class functions from $x(Tr_l^n(x) + ax)$

We consider bilinear split permutations of the form

$$\phi(x) = x(Tr_l^n(x) + ax) \tag{12}$$

where $l > 1$, $a \in \mathbb{F}_{2^l} \setminus \mathbb{F}_2$ and $Tr_l^n(x) = \sum_{i=0}^{k-1} x^{2^{li}}$. For details we refer to [2, 13]. We show here that bent functions in the $\mathcal{C}$ class, corresponding to ϕ, can be constructed by adding indicator functions of subspaces of codimension 2. The number of such subspaces is also obtained.

Theorem 5.14. *Let* $n = kl$ *where* k *be odd and* l *be any positive integer. Consider* ϕ *as given in* (12). *Then the total number of* 2*-dimensional linear subspaces of* $\mathbb{F}_{2^n}$ *which satisfy the condition* (C) *required for the construction of* $\mathcal{C}$ *type bent functions is* $(2^n - 1)(2^l - 2) + (2^{n-l} - 1)(2^{n-l} - 2)$.

Proof. Let $L = \langle u, v \rangle$ be any two dimensional subspace of $\mathbb{F}_{2^n}$. We know that for any $c \in \mathbb{F}_{2^n}$, $\phi(c + L)$ is flat if and only if $\phi(c) + \phi(c + u) + \phi(c + v) + \phi(c + u + v) = 0$, that is,

$$\begin{aligned} &c(Tr_l^n(c) + ac) + (c + u)(Tr_l^n(c + u) + a(c + u)) + (c + v)(Tr_l^n(c + v) \\ &+a(c + v)) + (c + u + v)(Tr_l^n(c + u + v) + a(c + u + v)) = 0. \end{aligned} \tag{13}$$

Since $a(c^2+(c+u)^2+(c+v)^2+(c+u+v)^2)=0$ and (13) can be rewritten as

$$\begin{aligned} 0 &= cTr_l^n(c)+cTr_l^n(c)+cTr_l^n(u)+uTr_l^n(c)+uTr_l^n(u)+cTr_l^n(c)+cTr_l^n(v)+vTr_l^n(c)+ \\ &\quad vTr_l^n(v)+cTr_l^n(c)+c(Tr_l^n(u)+Tr_l^n(v))+(u+v)Tr_l^n(c)+(u+v)(Tr_l^n(u)+Tr_l^n(v)) \\ &= uTr_l^n(u)+vTr_l^n(v)+uTr_l^n(u)+uTr_l^n(v)+vTr_l^n(u)+vTr_l^n(v)=uTr_l^n(v)+vTr_l^n(u), \end{aligned}$$

then $\phi(c+L)$ is flat if and only if $uTr_l^n(v)+vTr_l^n(u)=0$, that is, $\frac{Tr_l^n(u)}{u}=\frac{Tr_l^n(v)}{v}$.

Therefore, $\mathcal{C}$ type functions associated to ϕ exist if and only if the function $x\mapsto\frac{Tr_l^n(x)}{x}$ is not a permutation on $\mathbb{F}_{2^n}$. We know that a polynomial in $\mathbb{F}_{2^n}[x]$ of the form $Q(x)=\sum_{i=0}^{n-1}c_ix^{2^i-1}$, $c_i\in\mathbb{F}_{2^n}$ can not be a permutation polynomial unless $Q(x)=c_kx^{2^k-1}$ with $\gcd(k,n)=1$ and $c_k\in\mathbb{F}_{2^n}^*$.

Let $k=1$ then $Tr_l^n(x)=x$. It is obvious that $x\mapsto\frac{Tr_l^n(x)}{x}=1$ not a permutation. If $k\ge 3$ then it is not a permutation polynomial, where k is odd. Thus for the permutation ϕ we can find at least one 2-dimensional subspace of $\mathbb{F}_{2^n}$ which satisfies the condition (C). Let $\alpha=Tr_l^n(u)$ and $\beta=Tr_l^n(v)$.

Case I: Let $\alpha\neq 0$ and $\beta\neq 0$. Then $\phi(c+L)$ is flat if and only if $\alpha v+\beta u=0\Rightarrow v=\frac{\beta}{\alpha}u$, that is, $v=\lambda u$ where $\lambda=\frac{\beta}{\alpha}\in\mathbb{F}_{2^l}^*$ and $\lambda\neq 1$ as $u\neq v$. Therefore, for any $u\in\mathbb{F}_{2^n}^*$, we can choose v in 2^l-2 ways. Thus, the total number of 2-dimensional subspaces is $(2^n-1)(2^l-2)$.

Case II: Let $\alpha=0$ and $\beta\neq 0$. Then, $\alpha v+\beta u=0$ implies $\beta u=0$, and thus $u=0$ (since $\beta\neq 0$), which is not possible. The case $\alpha\neq 0$ and $\beta=0$ implies that $v=0$, which is also not possible.

Case III: Let $\alpha=0$ and $\beta=0$. Then, $\phi(c+L)$ is flat if and only if $u,v\in\ker(Tr_l^n)\setminus\{0\}$ with $u\neq v$ where $\ker(Tr_l^n)=\{x\in\mathbb{F}_{2^n}:Tr_l^n(x)=0\}$. Therefore, the dimension of $\ker(Tr_l^n)$ is $kl-l$. Thus, u can be chosen in $2^{kl-l}-1$ ways and v in $2^{kl-l}-2$ ways. Hence the total number of 2-dimensional subspaces is $(2^{kl-l}-1)(2^{kl-l}-2)$.

To summarize, for any value of $l>1$, the total number of 2-dimensional subspaces of $\mathbb{F}_{2^n}$ which satisfies the condition (C) required for the construction of $\mathcal{C}$ type bent functions is $(2^n-1)(2^l-2)+(2^{n-l}-1)(2^{n-l}-2)$. □

6 Conclusions

The problem of specifying suitable linear subspaces of low dimension for some generic classes of permutations related to the derivation of new bent functions in $\mathcal{C}$ has been partially addressed. The results clearly indicate the hardness of this problem due to the fact that whereas some "suitable" permutations may finally yield bent functions within class $\mathcal{C}$ for other permutations such functions simply cannot exist. It appears that additional efforts are needed for getting a better understanding and deriving more explicit subclasses within the $\mathcal{C}$ and $\mathcal{D}$ class. Also, the question whether the classes of permutations specified here and related subspaces indeed give rise to bent functions outside $\mathcal{M}$ (and possibly outside $\mathcal{PS}$ as well) remains to be addressed.

Acknowledgment. Part of this paper was written during an enjoyable visit of S. G. at the Applied Mathematics Department of Naval Postgraduate School, supported in part by VSP award no. N62909-13-1-V105 (Department of the US Navy, ONR-Global). B. M. thanks IIT Roorkee for supporting his research.

References

[1] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy, *Almost perfect nonlinear functions over* $\mathbb{F}_{2^n}$, IEEE Trans. Inform. Theory 52 (2006), 4160–4170.

[2] A. Blokhuis, R. S. Coulter, M. Henderson and C. M. O'Keefe, *Permutations amongst the Dembowski–Ostrom polynomials*, in: 1999 Finite Fields and Applications, pp. 37–42. Springer, Berlin (2001).

[3] C. Bracken, E. Byrne, N. Markin and G. McGuire, *Determining the nonlinearity of a new family of APN functions*, AAECC 2007, LNCS 4851, pp. 72–79, 2007.

[4] C. Carlet, *Two New Classes of Bent Functions*, in: Eurocrypt '93, LNCS, Vol. 765 (1994), pp. 77–101.

[5] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the monograph: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge University Press, Yves Crama and Peter L. Hammer (eds.) (2010), 257–397. Available: `http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html`.

[6] C. Carlet, *Vectorial Boolean functions for cryptography*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 398–469, 2010. Available: `http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html`.

[7] T. W. Cusick, P. Stănică, Cryptographic Boolean functions and applications, Elsevier–Academic Press, 2009.

[8] J. F. Dillon, *Elementary Hadamard Difference Sets*, PhD Thesis, University of Maryland, 1974.

[9] J. F. Dillon, *Elementary Hadamard Difference Sets*, in: proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, (1975) pp. 237–249.

[10] H. Dobbertin, *Construction of bent functions and balanced Boolean functions with high nonlinearity*, Fast Software Encryption, Leuven 1994 (1995), LNCS 1008, Springer-Verlag, pp. 61–74.

[11] H. Dobbertin, *Almost Perfect Nonlinear Power Functions on* $GF(2^n)$*: The Welch Case*, IEEE Trans. Inf. Theory 45:4 (1999), 1271–1275.

[12] X.-d. Hou, *Determination of a type of permutation trinomial over finite fields I, II*, manuscripts, 2013, 2014: available at `http://arxiv.org/abs/1309.3530` and `http://arxiv.org/abs/1404.1822`.

[13] Y. Laigle-Chapuy, *A note on a class of quadratic permutations over* $\mathbb{F}_{2^n}$, AECC (2007), LNCS 4851, pp. 130–137.

[14] T. Y. Lam, K.H. Leung, *On vanishing sums of mth roots of unity in finite fields*, Finite Fields Appl. 2 (1996), 422–438.

[15] T. Y. Lam, K.H. Leung, *On vanishing sums of roots of unity*, J. Algebra 224 (2000), 91–109.

[16] R. L. McFarland, *A family of noncyclic difference sets*, J. Combinatorial Theory, Ser. A 15 (1973), 1–10.

[17] S. Payne, *Complete determination of translation ovoids in finite Desarguian planes*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. 51 (1971), 328–331.

[18] O. S. Rothaus, *On Bent Functions*, J. Combinatorial Theory, Ser. A 20 (1976), 300–305.

[19] G. Sivek, *On vanishing sums of distinct roots of unity*, Integers 10 (2010), 365–368.