Bent functions stemming from Maiorana-McFarland class being provably outside its completed version

Fengrong Zhang[*], Nastja Cepak[†], Enes Pasalic[‡], Yongzhuang Wei[§]

Abstract

In early nineties Carlet [1] introduced two new classes of bent functions, both derived from the Maiorana-McFarland ($\mathcal{M}$) class, and named them $\mathcal{C}$ and $\mathcal{D}$ class, respectively. Apart from a subclass of $\mathcal{D}$, denoted by $\mathcal{D}_0$ by Carlet, which is provably outside two main (completed) primary classes of bent functions, little is known about their efficient constructions. More importantly, both classes may easily remain in the underlying $\mathcal{M}$ class which has already been remarked in [21]. Assuming the possibility of specifying a bent function f that belongs to one of these two classes (apart from $\mathcal{D}_0$), the most important issue is then to determine whether f is still contained in the known primary classes or lies outside their completed versions. In this article, we further elaborate on the analysis of the set of sufficient conditions given in [27] concerning the specification of bent functions in $\mathcal{C}$ and $\mathcal{D}$ which are provably outside $\mathcal{M}$. It is shown that these conditions, related to bent functions in class $\mathcal{D}$, can be relaxed so that even those permutations whose component functions admit linear structures still can be used in the design. It is also shown that monomial permutations of the form x^{2^r+1} have inverses which are never quadratic for $n > 4$, which gives rise to an infinite class of bent functions in $\mathcal{C}$ but outside $\mathcal{M}$. Similarly, using a relaxed set of sufficient conditions for bent functions in $\mathcal{D}$ and outside $\mathcal{M}$, one explicit infinite class of such bent functions is identified. We also extend the inclusion property of certain subclasses of bent functions in $\mathcal{C}$ and $\mathcal{D}$, as addressed initially in [1, 21], that are ultimately within the completed $\mathcal{M}$ class. Most notably, we specify *another generic and explicit subclass* of $\mathcal{D}$, which we call $\mathcal{D}_2^\star$, whose members are bent functions provably outside the completed $\mathcal{M}$ class.

Keywords: Bent functions, $\mathcal{C}$ and $\mathcal{D}$ class, Completed Maiorana-McFarland class, Class membership.

Mathematics Subject Classification: 94C10 · 06E30

[*]School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu 221116, China, and State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China, and Mine Digitization Engineering Research Center of Minstry of Education of the People's Republic of China, China University of Mining and Technology, Xuzhou, Jiangsu 221116, China, email:zhfl203@cumt.edu.cn

[†]University of Primorska, FAMNIT, Koper, Slovenia email:nastja.cepak@gmail.com

[‡]University of Primorska, FAMNIT & IAM, Koper, Slovenia, email:enes.pasalic6@gmail.com

[§]Guilin University of Electronic Technology, Guilin, P.R. China, email:walker_wei@msn.com

1 Introduction

Bent functions were introduced by Rothaus [24] as discrete structures having close connection to certain combinatorial objects such as difference sets and strongly regular graphs. Moreover, bent functions gained a wide range of practical applications in error correcting codes, sequences, symmetric design and cryptography. An early theoretical analysis related to their properties and construction methods goes back to the works of Dillon [13] and McFarland [20]. The most significant impact of these works is the definition of two generic primary classes of bent functions which are referred to as partial spread ($\mathcal{PS}$) class due to Dillon and the Maiorana-McFarland ($\mathcal{M}$) class [20]. Another generic and primary class $\mathcal{H}$ was proposed by Dobbertin [14] which includes both $\mathcal{M}$ and the only explicit subclass of $\mathcal{PS}$, due to Dillon [13], commonly denoted by $\mathcal{PS}_{ap}$. In 1993, Carlet [1] introduced two additional secondary classes of bent functions, so-called $\mathcal{C}$ and $\mathcal{D}$, which are derived through a suitable modification of bent functions in the $\mathcal{M}$ class. The term secondary construction (class) generally refers to the fact that such design methods require suitable bent functions as initial functions in order to generate "new" bent functions (possibly not belonging to the same class as initial functions). There has been an extensive research effort to provide several different secondary constructions, see for instance [9, 8, 2, 7, 6, 15, 26, 25, 23, 22, 17, 29, 28]. For a survey of the main known secondary constructions of bent functions the reader is referred to [3] whereas an exhaustive survey on bent functions can be found in [5]. Both these primary and secondary classes greatly contribute to enumeration and classification of bent functions even though a complete solution to these problems seems to be elusive. This is also evident from the work of Hou and Langevin [19], where the number of bent functions in eight variables that belong to the two main primary classes is only a small fraction (of size 2^{76}) of the whole space containing 2^{106} bent functions.

The main purpose of this paper is to provide a more accurate extended classification of bent functions which belong to the secondary classes of bent functions $\mathcal{C}$ and $\mathcal{D}$ introduced by Carlet [1]. These classes are derived from the $\mathcal{M}$ class (see (2), (1) and property (C) below) by adding a characteristic (indicator) function of suitably chosen vector subspaces to the functions in the $\mathcal{M}$ class. Nevertheless, apart from an explicit subclass $\mathcal{D}_0$ identified by Carlet [1], the bent conditions in terms of the selection of a vector subspace L and a permutation π (used to define the initial function $f(x, y) = x \cdot \pi(y)$ in $\mathcal{M}$, where $x, y \in \mathbb{F}_2^n$) are rather hard to satisfy. Due to its simple definition, using relatively simple arguments, Carlet showed that the class $\mathcal{D}_0$ lies outside both completed primary classes. The problem of specifying bent functions in $\mathcal{C}$ was recently addressed in [21]. The hardness of satisfying the (C) property (thus identifying a suitable permutation and related vector subspace) was confirmed true in [21] since 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 $f^* \in \mathcal{C}$ [21, Theorem 3.3]. On the other hand, for some other classes of permutations and associated linear subspaces of the same dimension (where the above permutations are inefficient) it could be verified that the property (C) is indeed satisfied [21]. Thus, given the existence of bent functions $f^* \in \mathcal{C}$ the most fundamental issue is to determine whether these functions are essentially contained in the known primary classes (which gives nothing new in

that case) or these functions potentially lie outside the known classes. It should be remarked that certain choices of the indicator functions used to define f^* from $f \in \mathcal{M}$ are provably non-efficient in this context, thus giving rise to bent functions f^* that still remain in the $\mathcal{M}$ class.

This article further refines the work [27], where a set of sufficient conditions for the choice of the permutation π and the corresponding linear subspace was provided so that a bent function f^* that belongs either to $\mathcal{C}$ or $\mathcal{D}$ is outside the completed $\mathcal{M}$ class. The derived sufficient conditions in [27] are relatively simple and the main constraint relates to the choice of permutations that do not admit linear structures. Even though the proofs of main results in [27] implicitly use the assumption that the component functions of a permutation (linear combinations of its coordinate functions) are without linear structures, the statements are given using a weaker (in general incorrect) formulation that the permutation does not admit linear structures. This refined and stronger condition then excludes the use of quadratic monomial permutations in the design since their component functions inevitably admit linear structures. Nevertheless, related to $\mathcal{D}$ class, we show that this condition can be relaxed thus allowing that a certain number of component functions may admit linear structures though such permutations still can be employed to generate bent functions outside $\mathcal{M}$. In connection to this, we derive an infinite class of bent functions which belongs to $\mathcal{D}$ but its members are provably outside $\mathcal{M}$.

Similarly, concerning the $\mathcal{C}$ class of bent functions, we show that monomial permutations of the form x^{2^r+1} have inverses which are never quadratic for $n > 4$ which also give rise to an infinite class of bent functions in $\mathcal{C}$ but outside $\mathcal{M}$. Though we mainly consider monomial permutations (being easier to analyze in this context), we address the use of some infinite classes of non-monomial permutations for the same purpose. We also extend the inclusion property of certain subclasses of bent functions in $\mathcal{C}$ and $\mathcal{D}$, as addressed initially in [1, 21], that are ultimately within the completed $\mathcal{M}$ class. Most notably, we specify *another generic and explicit subclass* of $\mathcal{D}$, which we call $\mathcal{D}_2^\star$, whose members are bent functions provably outside the completed $\mathcal{M}$ class.

However, we could not establish whether bent functions outside $\mathcal{M}$ identified in this paper are also outside the completed $\mathcal{PS}$ class. This is mainly due to a rather involved definition of the permutations and the associated linear subspaces and consequently we could not apply a similar technique as the one used by Carlet for the class $\mathcal{D}_0$. The existence of similar indicators as for the $\mathcal{M}$ class seems to be the essential obstacle towards more precise classification. In this direction, we provide some simple graph theoretic arguments (based on the hardness of identifying cliques in a graph) that the problem of specifying an efficient indicator for the $\mathcal{PS}$ class might be NP-hard in general.

The rest of this article is organized as follows. In Section 2 we provide some basic definitions related to Boolean (and in particular bent) functions along with the exact definitions of $\mathcal{C}$ and $\mathcal{D}$ classes. Sufficient conditions that bent functions in $\mathcal{C}$ or $\mathcal{D}$ do not belong to the completed $\mathcal{M}$ class are given in Section 3. In Section 4, we demonstrate that some instances of bent functions in $\mathcal{C}$, identified in [21], do not belong to the completed $\mathcal{M}$ class. Sufficient conditions ensuring that bent functions in $\mathcal{D}$ are outside the completed $\mathcal{M}$ class are shown to be relatively easily satisfied in Section 4.2. In Section 5, we provide sufficient conditions on

the choice of defining indicator subspaces so that certain subclasses of $\mathcal{C}$ and $\mathcal{D}$ intersect with $\mathcal{M}$. Another generic and explicit subclass of $\mathcal{D}$, whose members are bent functions provably outside the completed $\mathcal{M}$ class, is specified in Section 6. Some concluding remarks are given in Section 7.

2 Preliminaries

Let $\mathbb{F}_2$ denote the binary field and let the n-dimensional vector space spanned over $\mathbb{F}_2$ be denoted by $\mathbb{F}_2^n = \{x = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_2, \text{ for } i = 1, \ldots, n\}$. The extension of the Galois field of degree n over $\mathbb{F}_2$ is denoted 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 called a *Boolean function* on n variables and 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 [3, 4], and Cusick and Stănică [11]. For the convenience of the reader, we recall some basic notions below. For any binary string x, the (Hamming) *weight* of x, denoted by $wt(x)$, is defined as the number of nonzero entries of x. By abuse of notation, we sometimes write $wt(d)$ for a positive integer d and mean that d is implicitly represented as a binary string. The *algebraic normal form* (ANF) of a Boolean function $f \in \mathfrak{B}_n$ is

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

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 standard inner (dot) product of two vectors $u, x \in \mathbb{F}_2^n$ is defined as $u \cdot x := \sum_{i=1}^n u_i x_i$. Once the basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is fixed one can isomorphically identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$. The degree of a mapping $f(x) = \sum_{i=0}^{2^n-1} a_i x^i$ over $\mathbb{F}_{2^n}$ is the largest Hamming weight of exponent i for which $a_i \in \mathbb{F}_{2.}$ is nonzero.

We denote by $Tr(\cdot)$ the absolute trace on $\mathbb{F}_{2^n}$ and by $T_k^n(\cdot)$ the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$, where k divides n:

$$T_k^n(\beta) = \beta + \beta^{2^k} + \cdots + \beta^{2^{(n/k-1)k}}.$$

The isomorphism between the vector space $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ (using a suitable basis) implies that $u \cdot x$ corresponds to $Tr(ux)$.

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

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

Higher order derivatives of a Boolean function refer to k-dimensional vector subspaces, where $k > 1$. Suppose $\{a_1, a_2, \ldots, a_k\}$ 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

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

It should 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 $W_f(u) \in \{-2^{n/2}, 2^{n/2}\}$, for all $u \in \mathbb{F}_2^n$.

2.1 Bent functions in $\mathcal{C}$ and $\mathcal{D}$

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 $\mathbb{F}_2^n$. From this class Carlet [1] derived the $\mathcal{C}$ class of bent functions that contains all functions of the form

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

where L is any linear subspace of $\mathbb{F}_2^n$, $1_{L^\perp}$ is the indicator function of the space $L^\perp$, and π is any permutation on $\mathbb{F}_2^n$ such that:

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

The permutation ϕ and the subspace L are then said to satisfy the (C) property, or for short (ϕ, L) *has property* (C).

Another class introduced by Carlet [1], called $\mathcal{D}$, is defined similarly as

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

where π is a permutation on $\mathbb{F}_2^n$ and E_1, E_2 two linear subspaces of $\mathbb{F}_2^n$ such that $\pi(E_2) = E_1^\perp$.

A special subclass of the $\mathcal{C}$ and $\mathcal{D}$ classes is the $\mathcal{D}_0$ subclass. It contains all functions of the form

$$f(x, y) = x \cdot \pi(y) + \delta_0(x),$$

where $\delta_0(x) = \prod_{i=1}^n (x_i + 1)$ so that it corresponds to the case $E_1 \times E_2 = \{0\} \times \mathbb{F}_2^n$.

Definition 1 *A class of bent functions $\{f\} \in \mathcal{B}_n$ is* complete *if it is globally invariant under the action of the general affine group (the group of all invertible matrices of size $n \times n$ over $\mathbb{F}_2$) and under the addition of affine functions. The* completed class *is the smallest possible class that properly includes the class under consideration.*

3 Sufficient conditions for functions in $\mathcal{C}$ and $\mathcal{D}$ to be outside $\mathcal{M}^\#$

A useful indicator for the purpose of establishing whether a given bent function belongs to the completed Maiorana-McFarland class ($\mathcal{M}^\#$) is given below.

Lemma 1 *[13, p. 102] An m-variable bent function f, $m = 2n$, belongs to $\mathcal{M}^\#$ if and only if there exists an n-dimensional linear subspace V of $\mathbb{F}_2^m$ such that the second order derivatives*

$$D_\alpha D_\beta f(x) = f(x) + f(x+\alpha) + f(x+\beta) + f(x+\alpha+\beta)$$

vanish (thus $D_\alpha D_\beta f(x) = 0$ for all $x \in \mathbb{F}_2^n$) for any $\alpha, \beta \in V$.

In [27], the authors provided sufficient conditions for bent functions in $\mathcal{C}$ and $\mathcal{D}$ not to belong to $\mathcal{M}^\#$. One of the two conditions requires that "π has no nonzero linear structure" and is present in both [27, Theorem 1] and [27, Theorem 2], referring to $\mathcal{C}$ and $\mathcal{D}$ class respectively. However, the proofs of both theorems essentially use a correct condition which can be stated as "$u \cdot \pi$ has no nonzero linear structure for all $u \in \mathbb{F}_2^n \backslash \{0_n\}$". Hence, the results in [27] should be restated in a more precise manner as follows.

Theorem 1 *[27, Theorem 1] Let $m = 2n \geq 8$ be an even integer and let $f(x, y) = \pi(y) \cdot x + 1_{L^\perp}(x)$, where L is any linear subspace of $\mathbb{F}_2^n$ and π is a permutation on $\mathbb{F}_2^n$ such that (π, L) has property (C). If (π, L) satisfies:*

1) $\dim(L) \geq 2$*;*

2) $u \cdot \pi$ has no nonzero linear structure for all $u \in \mathbb{F}_2^n \backslash \{0_n\}$,

then f does not belong to $\mathcal{M}^\#$.

Theorem 2 *[27, Theorem 2] Let $m = 2n > 6$ be an even integer and let $f(x, y) = \pi(y) \cdot x + 1_{E_1}(x) 1_{E_2}(y)$, where π is a permutation on $\mathbb{F}_2^n$, and E_1, E_2 are two linear subspaces of $\mathbb{F}_2^n$ such that $\pi(E_2) = E_1^\perp$. If (E_1, E_2, π) satisfies:*

1) $\dim(E_1) \geq 2$ *and* $\dim(E_2) \geq 2$*;*

2) $u \cdot \pi$ has no nonzero linear structure for all $u \in \mathbb{F}_2^n \backslash \{0_n\}$;

3) $\deg(\pi) \leq n - \dim(E_2)$*,*

then f is a bent function in $\mathcal{D}$ and it does not belong to $\mathcal{M}^\#$.

In this section, using the above criterion, we derive a slightly relaxed set of sufficient conditions for bent functions in $\mathcal{D}$ not to belong to the completed $\mathcal{M}$ class. The main difference compared to Theorem 2 is the possibility of defining bent functions outside $\mathcal{M}^\#$ using certain classes of permutations whose components (thus $u \cdot \pi(y)$) may admit linear structures. This is in particular useful when considering quadratic permutations which are not covered by the following result which is a direct consequence of [10, Theorem 5].

Proposition 1 *Let $\pi(x) = x^d$ be a monomial permutation over $\mathbb{F}_{2^n}$. Then none of the component functions of $\pi(x)$ will admit a linear structure if and only if $wt(d) \geq 3$.*

Proof. The result follows from [10, Theorem 5] which states that $Tr(ux^d) : \mathbb{F}_2^n \to \mathbb{F}_2$ admits a linear structure only if $wt(d) \in \{1, 2\}$. Furthermore, if $wt(d) \in \{1, 2\}$ there will always exist (at least) one $u \in \mathbb{F}_{2^n}^*$ so that $Tr(ux^d)$ has a linear structure. Thus, selecting $\pi(x) = x^d$ so that $wt(d) \geq 3$ (thus π is at least cubic since $wt(d) \geq 3$) gives the result. $\diamond$

3.1 Sufficient conditions for class $\mathcal{D}$

We know show that even though a certain number of component functions of π may admit linear structures, such permutations can still be used for defining bent functions in $\mathcal{D}$. The following preparatory result will be frequently used when dealing with the second order derivatives of indicators of $(n-2)$-dimensional subspaces.

Lemma 2 *Let n be a positive integer. Let E_1 be a subspace of $\mathbb{F}_2^n$ such that $\dim(E_1) = n-2$. If $a^{(1)}, b^{(1)} \notin E_1$ and $a^{(1)} + b^{(1)} \notin E_1$, then*

$$D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) = 1.$$

If $a^{(1)}, b^{(1)} \notin E_1$ and $a^{(1)} + b^{(1)} \in E_1$, then

$$D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) = 0.$$

Furthermore, $D_{a^{(1)}} 1_{E_1}(x) = 0$ if $a^{(1)} \in E_1$ and $\deg\left(D_{a^{(1)}} 1_{E_1}(x)\right) = 1$ when $a^{(1)} \in \mathbb{F}_2^n \setminus E_1$.

Proof. We know $\sup(1_{E_1}(x)) = E_1$ and $\sup(1_{E_1}(x + a^{(1)})) = E_1 + a^{(1)}$, where $\sup(1_{E_1}(x))$ denotes the support of the function 1_{E_1}. For shortness, define $E_1^a = E_1 + a^{(1)}$,$E_1^b = E_1 + b^{(1)}$ and $E_1^{a,b} = E_1 + a^{(1)} + b^{(1)}$. Then, it can be easily verified that

$$\sup\left(D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x)\right) = \{E_1 \cup E_1^a \cup E_1^b \cup E_1^{a,b}\} \bmod 2,$$

where in the multi-set $\sup(D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x))$ we remove vectors appearing even number of times. FR: I feel we can use *mod* 2 instead of mod 2 Now if $a^{(1)}, b^{(1)} \notin E_1$ and $a^{(1)} + b^{(1)} \notin E_1$, the four cosets of E_1 partition the space $\mathbb{F}_2^n$, i.e., $\{E_1 \cup E_1^a \cup E_1^b \cup E_1^{a,b}\} \bmod 2 = \mathbb{F}_2^n$ since $\dim(E_1) = n-2$. This implies that $D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) = 1$.

If $a^{(1)}, b^{(1)} \notin E_1$ and $a^{(1)} + b^{(1)} \in E_1$, then $E_1 = E_1^{a,b}$ and also $E_1^a = E_1^b$ since $E_1 + a^{(1)} + b^{(1)} = E_1$ implies that $E_1 + a^{(1)} = E_1 + b^{(1)}$. Hence, $D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) = 0$.

If $a^{(1)} \in E_1$, then $D_{a^{(1)}} 1_{E_1}(x) = 0$. If $a^{(1)} \notin E_1$, then $\sup\left(D_{a^{(1)}} 1_{E_1}(x)\right) = \{E_1 \cup E_1^a\} \bmod 2$ is an $(n-1)$-dimensional subspace of $\mathbb{F}_2^n$. Hence, for $a^{(1)} \notin E_1$, $\deg\left(D_{a^{(1)}} 1_{E_1}(x)\right) = 1$. $\diamond$

Theorem 3 *Let $m = 2n \geq 8$ be an even integer and let $f(x, y) = \pi(y) \cdot x + 1_{E_1}(x) 1_{E_2}(y)$, where π is a permutation on $\mathbb{F}_2^n$, and E_1, E_2 are two linear subspaces of $\mathbb{F}_2^n$ such that $\pi(E_2) = E_1^{\perp}$. If (E_1, E_2, π) satisfies:*

1. $\dim(E_2) = 2$;
2. *For any subspace Λ of $\mathbb{F}_2^n$ of dimension $n-3$ and any nonzero vector $\nu \in \mathbb{F}_2^n$, there always exists at least one vector $\alpha \in \Lambda \setminus \{0_n\}$ such that $D_\nu(\alpha \cdot \pi) \neq const.$;*
3. $\deg(\pi) \leq n-2$,

then f does not belong to $\mathcal{M}^{\#}$.

Proof. Let $a^{(1)}, b^{(1)}, a^{(2)}, b^{(2)} \in \mathbb{F}_2^n$. We prove that f does not belong to $\mathcal{M}^{\#}$, by using Lemma 1. We need to show that there does not exist $V \subset \mathbb{F}_2^m$, with $\dim(V) = n$, such that

$$D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f = 0,$$

for any $(a^{(1)}, a^{(2)})$, $(b^{(1)}, b^{(2)}) \in V$.

In the following, we will directly use the fact that $\dim(E_2) = \dim(E_1^{\perp})$ and $\deg(1_{E_1}(x)) = \dim(E_2)$ since E_1, E_2 are two linear subspaces of $\mathbb{F}_2^n$ such that $\pi(E_2) = E_1^{\perp}$. On the other hand, we have $\deg(1_{E_2}(y)) = n - \dim(E_2)$. The second derivative of f with respect to a and b can be written as,

$$\begin{aligned}
& D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x,y) \\
= \;& x \cdot (D_{a^{(2)}} D_{b^{(2)}} \pi(y)) + a^{(1)} \cdot D_{b^{(2)}} \pi(y + a^{(2)}) \\
& + b^{(1)} \cdot D_{a^{(2)}} \pi(y + b^{(2)}) + D_a D_b 1_{E_1}(x) 1_{E_2}(y) \\
= \;& x \cdot (D_{a^{(2)}} D_{b^{(2)}} \pi(y)) + a^{(1)} \cdot D_{b^{(2)}} \pi(y + a^{(2)}) + b^{(1)} \cdot D_{a^{(2)}} \pi(y + b^{(2)}) \\
& + 1_{E_1}(x) D_{a^{(2)}} D_{b^{(2)}} 1_{E_2}(y) + 1_{E_2}(y + a^{(2)}) D_{a^{(1)}} 1_{E_1}(x) \\
& + 1_{E_2}(y + b^{(2)}) D_{b^{(1)}} 1_{E_1}(x) + 1_{E_2}(y + a^{(2)} + b^{(2)}) D_{a^{(1)} + b^{(1)}} 1_{E_1}(x).
\end{aligned} \tag{3}$$

We denote the set $\{(x, 0_n) \mid x \in \mathbb{F}_2^n\}$ by Δ, and consider two cases $V = \Delta$ and $V \neq \Delta$.

1. For $V = \Delta$, we can find two vectors $(a^{(1)}, 0_n), (b^{(1)}, 0_n) \in \Delta$ such that

   $$D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) \neq 0,$$

   since $\deg(1_{E_1}(x)) = \dim(E_2) = 2$. Further, using $a^{(2)} = b^{(2)} = 0_n$, (3) gives

   $$\begin{aligned}
   D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x,y) &= 1_{E_2}(y)(D_{a^{(1)}} 1_{E_1}(x) + D_{b^{(1)}} 1_{E_1}(x) + D_{a^{(1)}+b^{(1)}} 1_{E_1}(x)) \\
   &= 1_{E_2}(y) D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) \neq 0
   \end{aligned}$$

   since $\deg(1_{E_2}(y)) = n - 2$.

2. For $V \neq \Delta$, we have $1 \leq |V \cap \Delta| \leq 2^{n-1}$ since $V \cap \Delta$ is also a subspace. Further, we have $|V \cap \Delta| = 2^i$, where $i = 0, 1, \cdots, n-1$. We set $V = \left\{(v_1^{(1)}, v_2^{(1)}), (v_1^{(2)}, v_2^{(2)}), \ldots, (v_1^{(2^n)}, v_2^{(2^n)})\right\}$ and split the proof into three cases depending on the cardinality of $V \cap \Delta$:

   (a) When $1 \leq |V \cap \Delta| < 2^{n-3}$, we have $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\}| > 8$. This is because $V \cap \Delta$ is an additive subgroup of V and from the definition of Δ and Lagrange's theorem, we know $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\}| = |V|/|V \cap \Delta| > \frac{2^n}{2^{n-3}} = 8$. Thus, there exist $a, b \in V$ such that $a^{(2)}, b^{(2)} \notin E_2$ and $a^{(2)} + b^{(2)} \notin E_2$. Then, by Lemma 2,

   $$D_{a^{(2)}} D_{b^{(2)}} 1_{E_2}(y) \neq 0$$

   since $\dim(E_2) = 2$. Because $\deg(1_{E_1}(x)) = 2$, we have $D_a D_b f(x,y) \neq 0$ since the term $1_{E_1}(x) D_{a^{(2)}} D_{b^{(2)}} 1_{E_2}(y)$ cannot be cancelled in (3).

(b) When $2^{n-3} \leq |V \cap \Delta| \leq 2^{n-1}$, we have $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\}| \geq 2$. For any nonzero vector $b = (b^{(1)}, b^{(2)}) \in V$ such that $b^{(2)} \neq 0_n$, we can always find a vector $a^{(1)} \in |V \cap \Delta|$ such that the term $a^{(1)} \cdot D_{b^{(2)}}\pi(y) \neq const.$ in (3) . This comes from our assumption that there is at least one vector $\alpha \in \Lambda$ such that $D_\nu(\alpha \cdot \pi) = \alpha \cdot D_\nu \pi \neq const.$ for any Λ, with $\dim(\Lambda) = n-3$, and any given nonzero $\nu \in \mathbb{F}_2^n$.

We select $a = (a^{(1)}, 0_n) \in V \cap \Delta$ and $b = (b^{(1)}, b^{(2)}) \in V$. Thus, with $a^{(2)} = 0_n$, (3) becomes:

$$\begin{aligned} & D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x,y) \\ = \; & a^{(1)} \cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y) D_{a^{(1)}} 1_{E_1}(x) \\ + \; & 1_{E_2}(y + b^{(2)}) D_{b^{(1)}} 1_{E_1}(x) + 1_{E_2}(y + b^{(2)}) D_{a^{(1)}+b^{(1)}} 1_{E_1}(x) \qquad (4) \\ = \; & a^{(1)} \cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y) D_{a^{(1)}} 1_{E_1}(x) + 1_{E_2}(y + b^{(2)}) D_{a^{(1)}} 1_{E_1}(x + b^{(1)}). \end{aligned}$$

There are five cases to be considered.

i) If $a^{(1)}, b^{(1)} \in E_1$, implying $D_{a^{(1)}} 1_{E_1}(x) = 0$ and $D_{a^{(1)}} 1_{E_1 + b^{(1)}}(x) = 0$, then

$$D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x,y) = a^{(1)} \cdot D_{b^{(2)}}\pi(y) \neq 0$$

since $a^{(1)} \cdot D_{b^{(2)}}\pi(y) \neq const.$

ii) If $a^{(1)} \in E_1$ and $b^{(1)} \notin E_1$, then $D_{a^{(1)}} 1_{E_1}(x) = 0$ and $D_{a^{(1)}} 1_{E_1 + b^{(1)}}(x) = D_{b^{(1)}} 1_{E_1}(x) \neq 0$, by Lemma 2. It means that (4) does not equal zero since

$$a^{(1)} \cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y + b^{(2)}) D_{a^{(1)}} 1_{E_1}(x + b^{(1)})$$

cannot be canceled as $D_{a^{(1)}} 1_{E_1}(x + b^{(1)})$ depends (linearly) on x.

iii) The case $a^{(1)} \notin E_1$ and $b^{(1)} \in E_1$ is similar to ii), this time $D_{a^{(1)}} 1_{E_1}(x)$ depends (linearly) on x and thus $D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x,y) \neq 0$.

iv) If $a^{(1)}, b^{(1)}, a^{(1)} + b^{(1)} \notin E_1$, we have $D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) = 1$ by Lemma 2. Then

$$\begin{aligned} & D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x,y) \\ = \; & a^{(1)} \cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y) D_{a^{(1)}} 1_{E_1}(x) + 1_{E_2}(y + b^{(2)}) D_{a^{(1)}} 1_{E_1}(x + b^{(1)}) \\ = \; & a^{(1)} \cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y) D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) + D_{b^{(2)}} 1_{E_2}(y) D_{a^{(1)}} 1_{E_1}(x + b^{(1)}) \\ = \; & a^{(1)} \cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y) + D_{b^{(2)}} 1_{E_2}(y) D_{a^{(1)}} 1_{E_1}(x + b^{(1)}) \neq 0, \qquad (5) \end{aligned}$$

since $\deg(\pi) \leq n-2 = \deg(1_{E_2}(y))$ implying $\deg(a^{(1)} \cdot D_{b^{(2)}}\pi(y)) < n-2$.

v) If $a^{(1)}, b^{(1)} \notin E_1$ and $a^{(1)} + b^{(1)} \in E_1$, by Lemma 2, $D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) = 0$.

Further,

$$
\begin{aligned}
& D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x,y) \\
= \;& a^{(1)}\cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x) + 1_{E_2}(y+b^{(2)})D_{a^{(1)}}1_{E_1}(x+b^{(1)}) \\
= \;& a^{(1)}\cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x) \\
& +1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x+b^{(1)}) + 1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x+b^{(1)}) \qquad (6)\\
& +1_{E_2}(y+b^{(2)})D_{a^{(1)}}1_{E_1}(x+b^{(1)}) \\
= \;& a^{(1)}\cdot D_{b^{(2)}}\pi(y) + \Big(1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x) + 1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x+b^{(1)})\Big) \\
& + \Big(1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x+b^{(1)}) + 1_{E_2}(y+b^{(2)})D_{a^{(1)}}1_{E_1}(x+b^{(1)})\Big) \\
= \;& a^{(1)}\cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y)D_{a^{(1)}}D_{b^{(1)}}1_{E_1}(x) + D_{b^{(2)}}1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x+b^{(1)}) \\
= \;& a^{(1)}\cdot D_{b^{(2)}}\pi(y) + D_{b^{(2)}}1_{E_2}(y)D_{b^{(1)}}1_{E_1}(x) \neq 0
\end{aligned}
$$

since $D_{b^{(1)}}1_{E_1}(x) \neq const.$.

Combining items 1 and 2, we deduce that f does not belong to $\mathcal{M}^{\#}$. $\diamond$

From the proving process of Theorem 3, the condition that $\deg(\pi) \leq n-2$ is only used in item $2-(b)-iv)$. Now we provide an alternative condition which covers item $2-(b)-iv)$ of Theorem 3.

Corollary 1 *Let $m = 2n \geq 8$ be an even integer and let $f(x,y) = \pi(y)\cdot x + 1_{E_1}(x)1_{E_2}(y)$, where π is a permutation on $\mathbb{F}_2^n$, and E_1, E_2 are two linear subspaces of $\mathbb{F}_2^n$ such that $\pi(E_2) = E_1^{\perp}$. If (E_1, E_2, π) satisfies:*

1. $\dim(E_2) = 2$;
2. *For any subspace Λ of $\mathbb{F}_2^n$ of dimension $n-3$ and any given nonzero vector $\nu \in \mathbb{F}_2^n$, there always exists at least one vector $\alpha \in \Lambda \setminus \{0_n\}$ such that $D_\nu(\alpha\cdot\pi) \neq const.$;*
3. $\sup\left(D_\nu(\omega\cdot\pi)\right) \neq E_2$ *for any $\nu \in \mathbb{F}_2^n \setminus \{0_n\}$ and $\omega \notin E_1$;*

then f does not belong to $\mathcal{M}^{\#}$.

Proof. The first two conditions are identical to those of Theorem 3. We use the third condition to show item $2-(b)-iv)$ of Theorem 3.

When $a^{(1)}, b^{(1)}, a^{(1)}+b^{(1)} \notin E_1$, we have $D_{a^{(1)}}D_{b^{(1)}}1_{E_1}(x) = 1$ by Lemma 2. From (5),

$$D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x,y) = a^{(1)}\cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y) + D_{b^{(2)}}1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x+b^{(1)}).$$

Since $\dim(E_2) = 2$, we have $wt(1_{E_2}(y)) = 4$. Due to the assumption that $\sup(D_\nu(\omega\cdot\pi)) \neq E_2$ for $\nu \in \mathbb{F}_2^n \setminus \{0_n\}$ and $\omega \notin E_1$, we have

$$a^{(1)}\cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y) \neq 0.$$

If $D_{b^{(2)}}1_{E_2}(y) \neq 0$, then $D_{b^{(2)}}1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x+b^{(1)})$ must depend on x since $a^{(1)} \notin E_1$. If $D_{b^{(2)}}1_{E_2}(y) = 0$, then $D_{b^{(2)}}1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x+b^{(1)}) = 0$. Hence, we have

$$D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x,y) = a^{(1)} \cdot D_{b^{(2)}}\pi(y) + 1_{E_2}(y) + D_{b^{(2)}}1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x+b^{(1)}) \neq 0.$$

$\diamond$

Remark 1 *The set of sufficient conditions in Theorem 1 can also be relaxed when the dimension of L is strictly greater than 2. In this case, the condition 2) of Theorem 1 becomes : $u \cdot \pi$ has no nonzero linear structure for all $u \in L^{\perp}\backslash\{0_n\}$, where $L^{\perp}\backslash\{0_n\} \neq \emptyset$. However, we do not consider the case $\dim(L) > 2$ and therefore we omit the proof of this result.*

4 Generic methods for bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside $\mathcal{M}^{\#}$

In this section we apply the criterion derived in the previous section to those bent functions given in [21] that satisfy the (C) property, and later we provide some examples of bent functions in $\mathcal{D}$ that are outside $\mathcal{M}^{\#}$.

4.1 Bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$

For convenience of the reader, we first recall a subset of bent functions given in [21] that satisfy the (C) property which are also outside the $\mathcal{M}^{\#}$ class as already demonstrated in [27].

Theorem 4 *[21, Theorem 5.8] Suppose $\phi(y) = y^{2^r+1}$, for all $y \in \mathbb{F}_{2^n}$, where $\gcd(r,n) = e$, n/e is odd (which implies $\gcd(2^n-1, 2^r+1) = 1$).*

(i) 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.

The following example specifies in detail a bent function lying in the $\mathcal{C}$ class and outside of $\mathcal{M}^{\#}$.

Example 1 *[27] Let $n = 2p$ where p is any odd prime, $r = 2$ and $e = \gcd(n,r) = 2$. Since n/e is odd, it is known that $\gcd(2^r+1, 2^n-1) = 1$. Therefore $\phi(y) = y^{2^r+1}$ is a permutation on $\mathbb{F}_{2^n}$. Let ζ be a primitive element of $\mathbb{F}_{2^n}$. Therefore, $\lambda = \zeta^{\frac{2^n-1}{2^e-1}} = \zeta^{\frac{2^n-1}{3}}$ is a generator of $\mathbb{F}_{2^e}$. Define a permutation $\pi(y) = \phi^{-1}(y) = y^{\gamma}$, where $\gamma(2^r+1) \equiv 1 \pmod{2^n-1}$. Given r and n, γ can be computed easily using the Euclidean algorithm. Consider a bent function $f(x,y) = x \cdot \pi(y) \in \mathcal{M}$, where $x, y \in \mathbb{F}_2^n$ and $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$. According to Theorem 4, if we*

choose $L = \langle 1, \lambda \rangle$ *then the function* $f^*(x, y) = x \cdot \pi(y) + 1_{L^\perp}(x)$ *is in* $\mathcal{C}$. *The bent function* f^* *can be explicitly written (over* $\mathbb{F}_{2^n}$*) as:*

$$\begin{aligned} f^*(x, y) &= Tr_1^n(xy^\gamma) + (Tr_1^n(x) + 1)(Tr_1^n(\lambda x) + 1) \\ &= Tr_1^n(xy^\gamma) + Tr_1^n(x)Tr_1^n(\lambda x) + Tr_1^n((1 + \lambda)x) + 1. \end{aligned} \tag{7}$$

We set $n = 6$ *and* $r = 2$. *Thus, from* $\gamma(2^r + 1) \equiv 1 \pmod{2^n - 1}$, *we have* $\gamma = 38$ *and* $\pi(y) = y^{38}$. *The permutation* π *is thus cubic and by Proposition 1 none of its component functions admit linear structures. Therefore, by Theorem 1, the function* f^* *is outside* $\mathcal{M}^\#$.

The above example can be generalized by ensuring that $wt(\gamma) \geq 3$, where γ satisfies $\gamma(2^r+1) \equiv 1 \pmod{2^n-1}$ for a given permutation $\phi(y) = y^{2^r+1}$ and $\pi(y) = \phi^{-1}(y) = y^\gamma$. The monomial permutation π needs to be at least cubic, so that by Proposition 1 its component functions $Tr(u\pi(x))$ do not admit linear structures.

Lemma 3 *Let* $n > 4$ *be a positive integer and let* r *satisfies the condition of Theorem 4. Then, the unique* $1 < \gamma < 2^n - 1$ *which satisfies* $\gamma(2^r + 1) \equiv 1 \pmod{2^n - 1}$ *is such that* $wt(\gamma) > 2$. *In other words, for any* $1 \leq i \neq j \leq n - 1$, *we always have*

$$(2^i + 2^j)(2^r + 1) \not\equiv 1 \mod (2^n - 1). \tag{8}$$

Proof. Without loss of generality, we set $i < j < n$. There are two cases to be considered.

1. If $i + r \geq n$ (that is $r \geq n - i$), then we have two cases to be considered.

   (a) If $i = n - 2$, then $j = n - 1$ (since $i < j < n$). We have

   $$\begin{aligned} (2^i + 2^j)(2^r + 1) &= 2^{i+r} + 2^{j+r} + 2^i + 2^j \\ &\equiv 2^{i+r-n} + 2^{j+r-n} + 2^i + 2^j \mod (2^n - 1) \\ &\equiv 2^{r-2} + 2^{r-1} + 2^{n-2} + 2^{n-1} \mod (2^n - 1). \end{aligned} \tag{9}$$

   There are also two cases to be considered.

   i. When $r = n - 1$, from (9), after substituting we get

   $$(2^i + 2^j)(2^r + 1) \equiv 2^{n-3} + 1 \not\equiv 1 \mod (2^n - 1).$$

   ii. When $r < n - 1$, that is, $r \leq n - 2$, from (9), we have

   $$2^{r-2} + 2^{r-1} + 2^{n-2} + 2^{n-1} \leq 2^{n-4} + 2^{n-3} + 2^{n-2} + 2^{n-1} < 2^n - 1,$$

   where the latter relation is true for $n > 4$ so that $(2^i + 2^j)(2^r + 1) \not\equiv 1 \pmod{2^n - 1}$.

   (b) If $i < n - 2$, that is $i \leq n - 3$, then we have

   $$\begin{aligned} 2^{i+r-n} + 2^{j+r-n} + 2^i + 2^j &\leq 2^{r-3} + 2^{(n-1)+(n-1)-n} + 2^{n-3} + 2^{n-1} \\ &\leq 2^{n-4} + 2^{n-2} + 2^{n-3} + 2^{n-1} \\ &< 2^n - 1 \end{aligned} \tag{10}$$

2. If $i + r < n$ (that is $r < n - i$), then we have two cases to be considered.

   (a) If $j + r < n$, then $(2^i + 2^j)(2^r + 1) = 2^{i+r} + 2^{j+r} + 2^i + 2^j$. There are three cases to be considered.

      i. When $j+r < n-1$ (that is, $i+r < n-2$), we have $2^{i+r}+2^{j+r}+2^i+2^j < 2^n-1$ and consequently $(2^i + 2^j)(2^r + 1) \not\equiv 1 \mod (2^n - 1)$.

      ii. When $j + r = n - 1$ and $i + r = n - 2$, there are two cases to be considered.

         A. For $r = 1$ and using (9), we get

$$2^{i+r}+2^{j+r}+2^i+2^j = 2^{n-2}+2^{n-1}+2^{n-3}+2^{n-2} \equiv 2^{n-3}+1 \mod (2^n-1).$$

         B. When $r > 1$ (that is, $r \geq 2$), we have

$$2^{i+r} + 2^{j+r} + 2^i + 2^j \leq 2^{n-2} + 2^{n-1} + 2^{n-4} + 2^{n-3} < 2^n - 1.$$

      iii. When $j+r = n-1$ and $i+r < n-2$, we know $i+r \leq n-3$ and $i \leq n-4$. We can conclude the same as in part B, thus $(2^i + 2^j)(2^r + 1) \not\equiv 1 \mod (2^n - 1)$.

   (b) If $j + r \geq n$, then

$$(2^i + 2^j)(2^r + 1) = 2^{i+r} + 2^{j+r-n} + 2^i + 2^j \mod (2^n - 1). \tag{11}$$

   There are two cases to be considered.

      i. When $r = n - 1$ (that is, $i = 0$ and $j \geq 2$ since $i + r < n$ and $j + r \geq n$ respectively), there are also two cases to be considered.

         A. When $j = n - 1$, setting $i = 0$ and $r = n - 1 = j$ in (11), we have $2^{n-1} + 2^{n-2} + 2^0 + 2^{n-1} = 2^{n-2} + 2 \not\equiv 1 \mod (2^n - 1)$.

         B. When $2 \leq j \leq n - 2$, using (11), we have

$$2^{i+r} + 2^{j+r-n} + 2^i + 2^j \leq 2^{n-1} + 2^{n-3} + 2^0 + 2^{n-2} < 2^n - 1.$$

      ii. When $r \leq n - 2$, there are also three cases to be considered.

         A. When $i + r \leq n - 2$, we have $i \leq n - 3$ since $r \geq 1$. Further,

$$2^{i+r} + 2^{j+r-n} + 2^i + 2^j \leq 2^{n-2} + 2^{j-(i+2)} + 2^{n-3} + 2^{n-1} < 2^n - 1.$$

         B. When $i + r = n - 1, j = n - 1$, we have

$$\begin{aligned} 2^{i+r} + 2^{j+r-n} + 2^i + 2^j &= 2^{n-1} + 2^{r-1} + 2^{n-r-1} + 2^{n-1} \\ &\equiv 2^{r-1} + 2^{n-r-1} + 1 \mod (2^n - 1) \\ &\not\equiv 1 \mod (2^n - 1). \end{aligned}$$

         C. When $i + r = n - 1, j \leq n - 2$, we have $r \geq 2$ since $j + r \geq n$. Then,

$$2^{i+r} + 2^{j+r-n} + 2^i + 2^j \leq 2^{n-1} + 2^{r-2} + 2^{n-r-1} + 2^{n-2}. \tag{12}$$

We know $2 \leq r \leq n-1$. There are three cases to be considered. When $r = 2$, we have

$$\begin{aligned} 2^{i+r} + 2^{j+r-n} + 2^i + 2^j \leq & \quad 2^{n-1} + 2^0 + 2^{n-3} + 2^{n-2} \\ < & \quad 2^n - 1. \end{aligned}$$

When $r = n-1$, we have

$$2^{i+r} + 2^{j+r-n} + 2^i + 2^j \leq 2^{n-1} + 2^{n-3} + 2^0 + 2^{n-2} < 2^n - 1.$$

When $2 < r < n-1$, we have $i \leq n-4$ (resp. $j + r - n \leq n-4$) since $i + r = n-1$ (resp. $j \leq n-2, r < n-1$). It gives

$$2^{i+r} + 2^{j+r-n} + 2^i + 2^j \leq 2^{n-1} + 2^{n-4} + 2^{n-4} + 2^{n-2} < 2^n - 1.$$

Combining items 1 and 2, we have $(2^i + 2^j)(2^r + 1) \not\equiv 1 \mod (2^n - 1)$ as claimed. $\diamond$

Theorem 5 *Let $\phi(y) = y^{2^r+1}$ be a permutation over $\mathbb{F}_{2^n}$ and $\pi(y) = \phi^{-1}(y) = y^\gamma$ be its inverse, for $n > 4$. In addition, assume that the conditions of Theorem 4 are satisfied with respect to the choice of L. Then, the bent function $f(x, y) = x \cdot \pi(y) + 1_{L^\perp}(x)$ belongs to $\mathcal{C}$ and is outside $\mathcal{M}^\#$.*

Proof. The proof follows from assumptions and the results given by Proposition 1, Lemma 3 and Theorem 1. $\diamond$

Remark 2 *Theorem 5 resembles the statement of Lemma 2 in [27]. However, Lemma 2 in [27] uses a weaker (in general incorrect) condition that π has no linear structures. Even though we mostly use monomial permutations on $\mathbb{F}_2^n$, whose component functions by Lemma 3 do not admit linear structures for $n > 4$, for instance when $n = 4$ a permutation $\phi(y) = y^{2^r+1}$ and its inverse can be quadratic so that the second condition of Theorem 1 is not satisfied.*

4.2 Bent functions in $\mathcal{D}$ outside $\mathcal{M}^\#$

The set of sufficient conditions related to class $\mathcal{D}$, given in Theorem 2, can be easily satisfied whenever we use monomial permutations $\pi(y) = y^d$ with $wt(d) \geq 3$. The following result was stated in [27, Proposition 1] and is based on Theorem 2. However, due to the existence of linear structures for quadratic monomial permutations, the condition that $\deg(\pi) \geq 3$ must be included.

Proposition 2 *[27] Let n be even. Then any monomial permutation $\pi(y) = y^d$, where $3 \leq deg(\pi) \leq n-2$, satisfies the required conditions in Theorem 2 for the 2-dimensional vector subspace $E_2 = \langle \zeta^{\frac{2^n-1}{3}}, \zeta^{\frac{2(2^n-1)}{3}} \rangle$, where ζ is a primitive element of $\mathbb{F}_{2^n}$. Thus, $f(x, y) = \pi(y) \cdot x + 1_{E_1}(x) 1_{E_2}(y)$, where $\pi(E_2) = E_2 = E_1^\perp$, is a bent function in $\mathcal{D}$ and outside $\mathcal{M}^\#$.*

Proof. The proof is similar to that of Proposition 1 in [27] and therefore omitted. $\diamond$

Remark 3 *Notice that Example 2 given in [27] is not affected by the above correction since it uses a cubic monomial permutation π.*

On the other hand, quadratic non-monomial permutations can be used in Theorem 3 as illustrated below.

Proposition 3 *Let $n = 2m, m = 3$, $\pi(y) = y^5 + y^{2^{m+4}} + y^{4\cdot 2^m+1} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Let E_2, E_1 be defined as in Proposition 2. Then $f(x, y) = \pi(y) \cdot x + 1_{E_1}(x)1_{E_2}(y)$ is a bent function in $\mathcal{D}$ and outside $\mathcal{M}^{\#}$.*

Proof. In Theorem 3.4 in [16], it was shown that any polynomial of the form $\pi(y) = y^5 + y^{2^{m+4}} + y^{4\cdot 2^m+1} : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ is a permutation over $\mathbb{F}_2^{2m}$, for odd m. Using the programming package Magma it was confirmed that $\pi(y)$ and its component functions do not admit linear structures. Therefore, using the same arguments as in the proof of Proposition 2 we have that $f(x, y) = \pi(y) \cdot x + 1_{E_1}(x)1_{E_2}(y)$ is a bent function in $\mathcal{D}$ and outside $\mathcal{M}^{\#}$. $\diamond$

Remark 4 *For reasonably large m, we could confirm (using MAGMA) that the component functions of the permutation π from [16, Theorem 3.4] do not admit linear structure. We conjecture that the result is true for any $n = 2m$, with m odd.*

As mentioned earlier, the main purpose of providing a relaxed set of sufficient conditions in Theorem 3, related to linear structures of a permutation π, is the possibility of employing quadratic monomial permutations π. We now provide a useful application of Theorem 3 to cover the case when π is a quadratic monomial permutation, thus $u\cdot\pi$ admits linear structures for any nonzero $u \in \mathbb{F}_2^n$, but still satisfying the set of sufficient conditions to generate bent functions outside $\mathcal{M}$.

Theorem 6 *Let $\pi(y) = y^d$ be a quadratic permutation over $\mathbb{F}_{2^n}$ ($n \geq 5$), where $d = 2^j(2^i+1)$ for $0 \leq i, j \leq n-1$ and $i \neq 0$, so that $\gcd(2^n - 1, 2^i + 1) = 1$. Let also $E_2 = \langle \zeta^a, \zeta^b \rangle$ be a 2-dimensional linear subspace of $\mathbb{F}_2^n$, where ζ is a primitive element of $\mathbb{F}_{2^n}$ and $0 \leq b < a \leq 2^n - 1$. If $\gcd(n, i) = 1$ and*

$$(a - b)(2^{i+j} - 2^j) \equiv 0 \mod (2^n - 1)$$

then $\pi(E_2) = E_1^{\perp}$ and π satisfies the conditions of Theorem 3. Thus, the function $f(x, y) = \pi(y) \cdot x + 1_{E_1}(x)1_{E_2}(y)$ is a bent function in $\mathcal{D}$ but outside $\mathcal{M}^*$.

Proof. Clearly, for $n \geq 5$ and $\deg(\pi) = 2$, the condition $\deg(\pi) \leq n - \dim(E_2)$ is satisfied.

We know show that the condition $(a-b)(2^{j+i} - 2^j) \equiv 0 \mod (2^n - 1)$ is sufficient so that the subspace E_2 is mapped to a subspace. Noting that $\zeta^a \mapsto \zeta^{ad}$ and $\zeta^b \mapsto \zeta^{bd}$, it is required that $\zeta^a + \zeta^b$ is mapped by π to $(\zeta^a + \zeta^b)^d = \zeta^{ad} + \zeta^{bd}$. Therefore

$$\begin{aligned}
(\zeta^a + \zeta^b)^{2^{j+i}+2^j} &= \zeta^{a(2^{j+i}+2^j)} + \zeta^{b(2^{j+i}+2^j)} \\
(\zeta^a + \zeta^b)^{2^{j+i}}(\zeta^a + \zeta^b)^{2^j} &= \zeta^{a(2^{j+i}+2^j)} + \zeta^{b(2^{j+i}+2^j)} \\
\zeta^{a(2^{j+i}+2^j)} + \zeta^{a2^{j+i}+b2^j} + \zeta^{b2^{j+i}+a2^j} + \zeta^{b(2^{j+i}+2^j)} &= \zeta^{a(2^{j+i}+2^j)} + \zeta^{b(2^{j+i}+2^j)} \\
\zeta^{a2^{j+i}+b2^j} &= \zeta^{b2^{j+i}+a2^j}.
\end{aligned}$$

It follows that

$$\begin{aligned} a2^{j+i} + b2^j &\equiv b2^{j+i} + a2^j \mod (2^n - 1), \\ 2^{j+i}(a-b) - 2^j(a-b) &\equiv 0 \mod (2^n - 1) \\ (a-b)(2^{j+i} - 2^j) &\equiv 0 \mod (2^n - 1). \end{aligned}$$

which implies $(a-b)(2^{j+i} - 2^j) \equiv 0 \mod (2^n - 1)$, as stated.

It remains to show that the condition 2) of Theorem 3 is satisfied. Let Λ be a subset of $\mathbb{F}_{2^n}$ such that $|\Lambda| \geq 2^{n-3}$. We want to show that given any $\nu \in \mathbb{F}_{2^n}^*$, we can always find (at least) one element $\alpha' \in \Lambda$ such that $Tr(\alpha'\pi(y)) + Tr(\alpha'\pi(y+\nu)) \neq const.$ Let $\alpha, \nu \in \mathbb{F}_{2^n}^*$. We have

$$\begin{aligned} Tr(\alpha\pi(y)) + Tr(\alpha\pi(y+\nu)) &= Tr(\alpha y^{2^j(2^i+1)}) + Tr(\alpha(y+\nu)^{2^j(2^i+1)}) \\ &= Tr(\alpha\nu^{2^j(2^i+1)}) + Tr(\alpha y^{2^{j+i}}\nu^{2^j}) + Tr(\alpha\nu^{2^{j+i}}y^{2^j}) \\ &= Tr(\alpha\nu^{2^j(2^i+1)}) + Tr(\alpha y^{2^{j+i}}\nu^{2^j} + \alpha^{2^i}\nu^{2^{j+2i}}y^{2^{j+i}}), \end{aligned} \tag{13}$$

and therefore $Tr(\alpha\pi(y)) + Tr(\alpha\pi(y+\nu)) = const.$ if and only if $\alpha\nu^{2^j} + \alpha^{2^i}\nu^{2^{j+2i}} = 0$, which is equivalent to $\alpha^{2^i-1}\nu^{2^j(2^{2i}-1)} = 1$. Since by assumption $\gcd(n,i) = 1$, implying that $\gcd(2^n - 1, 2^i - 1) = 1$, then α^{2^i-1} is a permutation. Then, for any fixed $\nu \in \mathbb{F}_{2^n}^*$ there is exactly one solution for $\alpha^{2^i-1}\nu^{2^j(2^{2i}-1)} = 1$ and therefore there always exist a nonzero $\alpha' \in \Lambda$ so that $Tr(\alpha'\pi(y)) + Tr(\alpha'\pi(y+\nu)) \neq const.$.

Thus, all three conditions imposed by Theorem 3 are satisfied and f is a bent function outside $\mathcal{M}^*$. $\diamond$

It was already noted in [27] that one can find many different tuples (a,b) such that $E_2 = \langle \zeta^a, \zeta^b \rangle$ is mapped to some 2-dimensional space by π. The additional condition $\gcd(n,i)$ in Theorem 6, compared to Proposition 2 in [27], does not affect the number of tuples (a,b) that define E_2, though it somewhat reduces the choices of (i,j) tuples.

4.3 Inclusion in the $\mathcal{PS}$ class

The so-called $\mathcal{PS}$ class, originally considered by Dillon [13], can be viewed as a union of $\mathcal{PS}^-$ and $\mathcal{PS}^+$. The former subclass corresponds to defining the support of f as a union of $2^{n/2-1}$ disjoint linear subspaces (intersecting trivially in 0) of dimension $n/2$ without including the all-zero vector. The subclass $\mathcal{PS}^+$ uses as a support a union of $2^{n/2-1}+1$ disjoint linear subspaces of dimension $n/2$ and includes the all-zero vector. In general, proving that a given bent function does not belong to the completed $\mathcal{PS}$ class is much harder than for the $\mathcal{M}$ class due to the lack of useful indicators. We translate the problem of determining whether a given function belongs to the $\mathcal{PS}$ class to a graph theoretical problem to show its difficulty.

In a graph, a clique is a set of vertices such that any two vertices are adjacent. A clique cover of a given undirected graph is a partition of the vertices of the graph into cliques.

Proposition 4 *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function and $G_f = (V,E)$ its corresponding graph, where $V = \sup(f) \setminus \{0\}, E = \{\{x,y\} \mid x,y \in V, x-y \in \sup(f)\}$. If the function*

$f \in \mathcal{PS}^-(\mathcal{PS}^+)$ then the graph G_f has a clique cover where all cliques are disjoint and of size $2^{n/2-1}(2^{n/2-1}+1)$. If the graph G_f has a clique cover where all cliques correspond to subspaces, which are disjoint and of size $2^{n/2-1}(2^{n/2-1}+1)$, then $f \in \mathcal{PS}^-(f \in \mathcal{PS}^+)$.

Proof. If a subset $H \cup \{0\}, H \subseteq V$, forms a subspace of $\mathbb{F}_2^n$, then any two $x, y \in H$ must be connected and therefore vertices corresponding to elements of H must form a clique. If $f \in \mathcal{PS}^-$, $\sup(f)$ is exactly a union of $2^{n/2-1}$ disjoint $\frac{n}{2}$-linear subspaces without the 0 vector. The graph G must therefore contain exactly $2^{n/2-1}$ cliques of size $2^{\frac{n}{2}}-1$ which cover the entire graph and are disjoint. If $f \in \mathcal{PS}^+$, $\sup(f)$ is exactly a union of $2^{n/2-1}+1$ disjoint $\frac{n}{2}$-linear subspaces. When defining the set of vertices V the 0 vector is removed. The graph G must therefore contain exactly $2^{n/2-1}+1$ cliques of size $2^{\frac{n}{2}}-1$ which again cover the entire graph and are disjoint.

If all the cliques contained in such a cover also correspond to subspaces and are disjoint, the converse is true as well. ◇

Therefore we can translate the initial problem into graph-theoretical terms in the following way: "Given a bent function f, does the graph G_f have a clique cover where all cliques correspond to subspaces, are disjoint, and of size $2^{\frac{n}{2}}-1$?"

In graph theory, the so-called Clique Cover Problem is very well known: "Given a graph G and an integer k, can the vertices of the graph be partitioned into k cliques?" It was proven in [18] that this is an NP-complete problem. A related problem of finding the minimum clique cover of a graph, that is, finding the minimum integer k for which there exists a clique cover with k cliques, is an NP-hard problem.

This, together with the fact that many other closely related problems in graph theory are proven to be either NP-hard or NP-complete, makes us believe that determining whether an arbitrary bent function f lies within the $\mathcal{PS}$ class is either an NP-hard or an NP-complete problem.

5 Sufficient conditions for functions in $\mathcal{C}$ and $\mathcal{D}$ to be in $\mathcal{M}^\#$

In this section, we will extend the results regarding some special choices of indicator functions of linear subspaces given in [21, 1] related to the class membership. In [21, Proposition 4.1], it was remarked that certain members of the class $\mathcal{C}$ intersect with $\mathcal{M}$ whenever L is selected as $L = E \times \mathbb{F}_2^n$ for some linear subspace E. We here show that some other nontrivial selections of the subspace L also lead to bent functions that are both in $\mathcal{C}$ and $\mathcal{M}$.

We first consider $f \in \mathcal{C}$ as defined by (1), thus the $\mathcal{C}$ class of functions. It is obvious that $f \in \mathcal{M}^\#$ if $\deg(\pi(y)) = 1$, hence we consider the case that $\deg(\pi(y)) > 1$. The *linear kernel* of f will denote the set of those vectors a such that $D_a f$ is a constant function, which forms a linear subspace of $\mathbb{F}_2^n$, see e.g. [11].

Theorem 7 *Let $m = 2n \geq 8$ be an even integer and let $f(x, y) = \pi(y) \cdot x + 1_{L^\perp}(x)$, where L is any linear subspace of $\mathbb{F}_2^n$ and π is a permutation on $\mathbb{F}_2^n$ such that (π, L) has property (C). Let S be a linear subspace of $\mathbb{F}_2^n$. If (S, π) satisfies:*

1) $S \subseteq L^{\perp}$*;*

2) For any $u \in S$*, there exists a linear subspace* K_0 *of* $\mathbb{F}_2^n$ *such that* $D_v(u \cdot \pi(y)) = 0$ *for any* $v \in K_0$*;*

3) $D_u D_v \pi(y) = 0$ *for* $u, v \in K_0$*;*

4) $\dim(S \times K_0) \geq n$*.*

then f *belongs to* $\mathcal{M}^{\#}$*.*

Proof. Let $a^{(1)}, b^{(1)}, a^{(2)}, b^{(2)} \in \mathbb{F}_2^n$. We prove that f belongs to $\mathcal{M}^{\#}$, by using Lemma 1. We need to show that there exists an n-dimensional subspace V of $\mathbb{F}_2^m$ such that

$$D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x,y) = 0,$$

for any $(a^{(1)}, a^{(2)})$, $(b^{(1)}, b^{(2)}) \in V$.

Let $V \subseteq S \times K_0$ and take $(a^{(1)}, a^{(2)})$, $(b^{(1)}, b^{(2)}) \in V$. We notice that $\dim(S \times K_0) \geq n$ and in particular if $\dim(S \times K_0) = n$ then $S \times K_0 = V$. We have

$$\begin{aligned} D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x,y) &= x \cdot (D_{a^{(2)}} D_{b^{(2)}} \pi(y)) + a^{(1)} \cdot D_{b^{(2)}} \pi(y + a^{(2)}) \\ &\quad + b^{(1)} \cdot D_{a^{(2)}} \pi(y + b^{(2)}) + D_{a^{(1)}} D_{b^{(1)}} 1_{L^{\perp}}(x). \end{aligned} \tag{14}$$

From (14), we have

$$D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x,y) = 0,$$

since $S \subseteq L^{\perp}$ and for any $u \in S$, by assumption, there exists a linear subspace K_0 of $\mathbb{F}_2^n$ such that $D_v(u \cdot \pi(y)) = 0$ for any $v \in K_0$.

$\diamond$

An example of application of Theorem 7, for the purpose of identifying bent functions that belong to both $\mathcal{C}$ and $\mathcal{M}^{\#}$, is given below and it utilizes a particular class of involutions over $\mathbb{F}_{2^n}$ (permutations having the property that $F \circ F(x) = x$).

Lemma 4 *[21] 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* $\leqslant 2$ *if and only if* $u + v + w + z = 0$*.*

Theorem 8 *Let* $n \geq 3$ *be an integer, and let* $\alpha^{(1)}, \alpha^{(2)} \in \mathbb{F}_2^n$*. Let* π *be an involution, defined as*

$$\pi(y) = \begin{cases} y, & y \in \mathbb{F}_2^n \setminus \{\alpha^{(1)}, \alpha^{(2)}\} \\ \alpha^{(1)}, & y = \alpha^{(2)} \\ \alpha^{(2)}, & y = \alpha^{(1)}. \end{cases}$$

Let $f(x,y) = \pi(y) \cdot x + 1_{L^{\perp}}(x)$*, where* $L = \{0, \alpha^{(1)}, \alpha^{(2)}, \alpha^{(1)} + \alpha^{(2)}\}$*. Then* f *belongs to both* $\mathcal{C}$ *and* $\mathcal{M}^{\#}$*.*

Proof. Since π is an involution, we have $\pi^{-1} = \pi$. Let $a \in \mathbb{F}_2^n$. From Lemma 4 and the definition of $\mathcal{C}$ class of bent functions, if

$$\pi(a) + \pi(\alpha^{(1)} + a) + \pi(\alpha^{(2)} + a) + \pi(\alpha^{(1)} + \alpha^{(2)} + a) = 0, \tag{15}$$

then (π, L) has property (C). From the definition of π, (15) holds and thus f belongs to $\mathcal{C}$.

Let $S = L^\perp$ and $K_0 = L$. By Theorem 7, it is sufficient to show that

$$D_v(u \cdot \pi(y))) = 0 \text{ for any } u \in L^\perp \text{ and } v \in L, \tag{16}$$

since only the item 2) of Theorem 7 needs to be verified. Now there are two cases to be considered.

1. If $y \in \mathbb{F}_2^n \setminus L$, then $(y + v) \in \mathbb{F}_2^n \setminus L$ for any $v \in L$ (since L is an additive group). Thus, we have
$$D_v(u \cdot \pi(y)) = u \cdot \pi(y) + u \cdot \pi(y + v)) = u \cdot v = 0,$$
for any $u \in L^\perp$ and $v \in L$. Notice that for $y \in \mathbb{F}_2^n \setminus L$ we have $\pi(y) = y$ and consequently $u \cdot \pi(y + v)) = u \cdot y + u \cdot v$.

2. If $y \in L$, then $\pi(y) \in L$. Thus $u \cdot \pi(y)) = 0$ since $u \in S = L^\perp$, that is, $D_v(u \cdot \pi(y)) = 0$ for any $u \in L^\perp$.

Combining items 1 and 2, we conclude that f belongs to $\mathcal{M}^\#$. ◇

In his pioneering work [1], Carlet defined an explicit class of bent functions called $\mathcal{D}_0$ which corresponds to the case $E_1 = \{0_n\}$ and $E_2 = \mathbb{F}_2^n$. Furthermore, it was also remarked [1, Remark, pg. 9] that considering the case $E_1 = \mathbb{F}_2^n$ and $E_2 = \{0_n\}$ only leads to bent functions in $\mathcal{D}$ that are provably in $\mathcal{M}$. We show that the same conclusion is valid when $\dim E_2 = 1$, thus excluding this case for possible further analysis.

Proposition 5 *Let $m = 2n$ be an even integer and let $f(x, y) = \pi(y) \cdot x + 1_{E_1}(x)1_{E_2}(y)$, where π is a permutation on $\mathbb{F}_2^n$, and E_1, E_2 are two linear subspaces of $\mathbb{F}_2^n$ such that $\pi(E_2) = E_1^\perp$. If $\dim(E_2) = 1$, then f belongs to $\mathcal{M}^\#$.*

Proof. According to Lemma 1, we need to show that there exist an n-dimensional subspace V such that

$$D_{(a^{(1)}, a^{(2)})} D_{(b^{(1)}, b^{(2)})} f = 0,$$

for any $(a^{(1)}, a^{(2)})$, $(b^{(1)}, b^{(2)}) \in V$. Set $V = \{(x, 0_n) \mid x \in \mathbb{F}_2^n\}$. Since $\dim(E_2) = 1$ and $\pi(E_2) = E_1^\perp$, we have $D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) = 0$ for any $a^{(1)}$, $b^{(1)} \in \mathbb{F}_2^n$. Therefore, we have

$$\begin{aligned} & D_{(a^{(1)}, a^{(2)})} D_{(b^{(1)}, b^{(2)})} f(x, y) \\ = \; & 1_{E_2}(y)(D_{a^{(1)}} 1_{E_1}(x) + D_{b^{(1)}} 1_{E_1}(x) + D_{a^{(1)} + b^{(1)}} 1_{E_1}(x)) \\ = \; & 1_{E_2}(y) D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) = 0 \end{aligned}$$

for any $(a^{(1)}, a^{(2)})$, $(b^{(1)}, b^{(2)}) \in V$, which shows that f belongs to $\mathcal{M}^\#$. ◇

6 An explicit class of bent functions $\mathcal{D}_2^\star$ outside $\mathcal{M}^\#$

Whereas our sufficient conditions, related to non-inclusion in the completed $\mathcal{M}$ class, could be specified for certain permutation monomials, we now largely extend these specific instances by specifying *two generic explicit subclass* of $\mathcal{D}$, which we call $\mathcal{D}_2^\star$ and $\mathcal{D}_1^\star$, whose members are bent functions provably outside the completed $\mathcal{M}$ class.

Due to the selection of the 0-dimensional subspace E_1, thus $E_1 = \{0_n\}$ and consequently $E_2 = \mathbb{F}_2^n$, the explicit class $\mathcal{D}_0$ of bent functions introduced by Carlet [1] does not impose any additional conditions on the choice of a permutation π. On the other hand, as already remarked, when $\dim(E_2) \in \{0, 1\}$ (hence $\dim(E_1) \in \{n, n-1\}$) such bent functions in $\mathcal{D}$ are provably within $\mathcal{M}^\#$. In what follows, we first consider the case $\dim(E_2) = n-2$ and define an explicit class $\mathcal{D}_2^\star$ of bent functions where the subscript actually refers to the fact that $\dim(E_1) = 2$. For this purpose, we employ a class of permutations on $\mathbb{F}_2^n$ derived from the identity permutation given by:

$$\pi^\star(y) = \begin{cases} y, & y \notin \{e^{(l)}, e^{(t)}\}; \\ e^{(l)}, & y = e^{(t)}; \\ e^{(t)}, & y = e^{(l)}, \end{cases} \tag{17}$$

where $l, t \in \{1, 2, \ldots, n\}$ with $l \neq t$, and furthermore $e^{(l)}, e^{(t)} \in \mathbb{F}_2^n$ denote elements in the canonical basis of $\mathbb{F}_2^n$. More precisely, $e_i^{(l)} = 1$ if and only if $i = l$, otherwise $e_i^{(l)} = 0$. It can be readily verified that selecting $E_1 = \langle e^{(l)}, e^{(t)} \rangle$ and $E_2 = E_1^\perp$, implies that $\pi^\star(E_2) = E_2 = E_1^\perp$. Thus, the function $f(x, y) = \pi^\star(y) \cdot x + 1_{E_1}(x)1_{E_2}(y)$ is a bent function which belongs to $\mathcal{D}$, where $x, y \in \mathbb{F}_2^n$.

Lemma 5 *Let $k > 2$ be an integer and $f \in \mathfrak{B}_k$. If $wt(f) = 1$ so that $f(x) = 1_\alpha(x)$ for some $\alpha \in \mathbb{F}_2^k$, then we have*

$$D_a D_b f \neq const.,$$

for any two different nonzero vectors $a, b \in \mathbb{F}_2^k$. Further, $\deg(D_a D_b f) = k - 2$.

Proof. For any nonzero vector $a \in \mathbb{F}_2^k$, we always have $wt(D_a f) = 2$ when $wt(f) = 1$. Further, we have $wt(D_a D_b f) = 4$ for any nonzero vectors $a, b \in \mathbb{F}_2^k$, where $b \neq a$, since $||\{\alpha, \alpha + a, \alpha + b, \alpha + a + b\}|| = 4$ when $f(x) = 1_\alpha(x)$. Since $k > 2$ we conclude that $D_a D_b f \neq const.$ for any two different nonzero vectors $a, b \in \mathbb{F}_2^k$.

From $wt(D_a D_b f) = 4$, we have

$$\deg(D_a D_b f) \geq k - 2. \tag{18}$$

If $wt(a) = t$, we have $a_{i_1} = 1, \ldots, a_{i_t} = 1$ for some $1 \leq i_1 < \cdots < i_t \leq k$. . Further, the terms of the maximum degree in $\prod_{i=1}^{k}(x_i + \alpha_i + 1) + \prod_{i=1}^{k}(x_i + \alpha_i + a_i + 1)$ are $x_1 \cdots x_{i_1 - 1} x_{i_1 + 1} \cdots x_k$, $x_1 \cdots x_{i_2 - 1} x_{i_2 + 1} \cdots x_k, \cdots, x_1 \cdots x_{i_t - 1} x_{i_t + 1} \cdots x_k$, which equal that of $\prod_{i=1}^{k}(x_i + \alpha_i + b_i + 1) +$

$\prod_{i=1}^{k}(x_i+a_i+b_i+\alpha_i+1)$ since $\alpha+(\alpha+a)+(\alpha+b)+(\alpha+a+b)=0_k$. Thus, we have

$$\deg(D_aD_bf)\le k-2. \tag{19}$$

Hence, combing (18) and (19), we have $\deg(D_aD_bf)=k-2$.

$\diamond$

Theorem 9 *Let $n\ge 5$ be a positive integer and $\pi^\star(y)$ be a permutation over $\mathbb{F}_2^n$ given by (17). Let l,t be two positive integers such that $1\le l<t\le n$. Define $f(x,y)=\pi^\star(y)\cdot x+1_{E_1}(x)1_{E_2}(y)$, with $x,y\in\mathbb{F}_2^n$, where $E_1=\langle e^{(l)},e^{(t)}\rangle$ and $E_2=E_1^\perp$ so that $\dim(E_2)=n-2$. Then f is a bent function outside $\mathcal{M}^\#$.*

Proof. According to the definition of $\mathcal{D}$ class bent functions, it is obvious that f is a bent function.

From Lemma 1, it is sufficient to show for any n-dimensional linear subspace V of $\mathbb{F}_2^{2n}$, we always find two distinct vectors $a,b\in\mathbb{F}_2^{2n^*}$ such that $D_aD_bf\neq 0$.

Without loss of generality, we set $l=1,t=2$ so that $e^{(1)}=(1,0,0,\ldots,0)$ and $e^{(2)}=(0,1,0,\ldots,0)$. Then,

$$\begin{aligned}
f(x,y)= &\ \pi^\star(y)\cdot x+1_{E_1}(x)1_{E_2}(y)\\
= &\ \left(y+\left(\prod_{i=1}^{n}(y_i+e_i^{(1)}+1)+\prod_{i=1}^{n}(y_i+e_i^{(2)}+1)\right)(e^{(1)}+e^{(2)})\right)\cdot x+1_{E_1}(x)1_{E_2}(y)\\
= &\ \left(y+\left((y_1+y_2)\prod_{i=3}^{n}(y_i+1)\right)(1,1,0,\ldots,0)\right)\cdot x+1_{E_1}(x)1_{E_2}(y)\\
= &\ x\cdot y+(x_1+x_2)(y_1+y_2)\prod_{i=3}^{n}(y_i+1)+(y_1+1)(y_2+1)\prod_{i=3}^{n}(x_i+1).
\end{aligned}$$

For any two nonzero vectors $a,b\in\{0_2\}\times\mathbb{F}_2^n\times\{0_{n-2}\}$, we have

$$D_aD_bf(x,y)=c+0+D_aD_b\left((y_1+1)(y_2+1)\prod_{i=3}^{n}(x_i+1)\right)$$

where $c\in\mathbb{F}_2$ is a constant. For any two nonzero vectors $a=(0_2,\widehat{a},0_{n-2}),b=(0_2,\widehat{b},0_{n-2})\in\{0_2\}\times\mathbb{F}_2^n\times\{0_{n-2}\}$, we have

$$\begin{aligned}
D_aD_bf(x,y)= &\ c+0+D_aD_b\left((y_1+1)(y_2+1)\prod_{i=3}^{n}(x_i+1)\right)\\
= &\ c+0+D_{\widehat{a}}D_{\widehat{b}}\left((y_1+1)(y_2+1)\prod_{i=3}^{n}(x_i+1)\right)
\end{aligned}$$

where $c\in\mathbb{F}_2$ is a constant. Then, by Lemma 5, we have

$$\begin{aligned}
\deg\left(D_aD_b\left(1_{E_1}(x)1_{E_2}(y)\right)\right)= &\ \deg\left(D_aD_b\left((y_1+1)(y_2+1)\prod_{i=3}^{n}(x_i+1)\right)\right)\\
= &\ \deg\left(D_{\widehat{a}}D_{\widehat{b}}\big((y_1+1)(y_2+1)\prod_{i=3}^{n}(x_i+1)\big)\right)=n-2,
\end{aligned} \tag{20}$$

for any nonzero $a, b \in \{0_2\} \times \mathbb{F}_2^n \times \{0_{n-2}\}$. Hence, $D_aD_bf(x,y) \neq const.$ for any nonzero $a, b \in \{0_2\} \times \mathbb{F}_2^n \times \{0_{n-2}\}$. Similarly, we have $D_aD_bf(x,y) \neq const.$ for any nonzero $a, b \in \{0_{2+n}\} \times \mathbb{F}_2^{n-2}$.

Further, since $n \geq 5$, there must exist $l' \in \{3, 4, \ldots, n\}$ such that $D_aD_b\left(1_{E_1}(x)1_{E_2}(y)\right)$ depends on the variable $x_{l'}$ if $D_aD_b\left(1_{E_1}(x)1_{E_2}(y)\right) \neq const.$ for any $a, b \in \mathbb{F}_2^{2n*}$. From the ANF of f and the definition of $\pi^\star$, $D_aD_b\left(x \cdot y + (x_1 + x_2)(y_1 + y_2)\prod_{i=3}^{n}(y_i + 1)\right)$ can not depend on the variable $x_{l'}$. Hence, we have

$$D_aD_bf \neq const. \;\; if \;\; D_aD_b\left(1_{E_1}(x)1_{E_2}(y)\right) \neq const.. \tag{21}$$

Similarly, there must exist $t' \in \{3, 4, \ldots, n\}$ such that $D_aD_b\left((x_1 + x_2)(y_1 + y_2)\prod_{i=3}^{n}(y_i + 1)\right)$ depends on the variable $y_{t'}$ if $D_aD_b\left((x_1 + x_2)(y_1 + y_2)\prod_{i=3}^{n}(y_i + 1)\right) \neq const.$ for any $a, b \in \mathbb{F}_2^{2n*}$ (using that $n \geq 5$). From the ANF of f and the definition of $\pi^\star$, $D_aD_b\left(x \cdot y + 1_{E_1}(x)1_{E_2}(y)\right)$ cannot depend on the variable $y_{t'}$. Hence, we have

$$D_aD_bf \neq const. \; if \; D_aD_b\left((x_1 + x_2)(y_1 + y_2)\prod_{i=3}^{n}(y_i + 1)\right) \neq const.. \tag{22}$$

Let V be an arbitrary n-dimensional subspace $\mathbb{F}_2^{2n}$. Denote by $\widehat{V} = \{(v_3, \ldots, v_{n+2}) | v \in V\}$ and $\widehat{U} = \{(v_{n+3}, \ldots, v_{2n}) | v \in V\}$. We have

$$\dim(\widehat{V}) + \dim(\widehat{U}) \geq \dim(\widehat{V} \times \widehat{U}) \geq n - 2,$$

where $\widehat{V} \times \widehat{U}$ denotes the Cartesian product of $\widehat{V}$ and $\widehat{U}$. There are two cases to be considered.

1. If $||\widehat{V} \cap \mathbb{F}_2^n|| \geq 4$, we can select two vectors $a, b \in V$ such that $(a_3, a_4, \ldots, a_{n+1}, a_{n+2}) \neq 0_n$, $(b_3, b_4, \ldots, b_{n+1}, b_{n+2}) \neq 0_n$ and $(a_3, a_4, \ldots, a_{n+1}, a_{n+2}) \neq (b_3, b_4, \ldots, b_{n+1}, b_{n+2})$. Thus, $D_aD_b\left(1_{E_1}(x)1_{E_2}(y)\right) \neq constant.$ From (21), we have $D_aD_bf \neq const.$.
2. If $||\widehat{V} \cap \mathbb{F}_2^n|| < 4$, then $\dim(\widehat{V}) \leq 1$. Thus, we have $\dim(\widehat{U}) \geq n - 3$, that is, $||\widehat{U} \cap \mathbb{F}_2^{n-2}|| \geq 4$ since $n > 5$. We can select two different vectors $a, b \in V$ such that $(a_{n+3}, a_{n+4}, \ldots, a_{2n}) \neq 0_{n-2}$, $(b_{n+3}, b_{n+4}, \ldots, b_{2n}) \neq 0_{n-2}$ and $(a_{n+3}, a_{n+4}, \ldots, a_{2n}) \neq (b_{n+3}, b_{n+4}, \ldots, b_{2n})$. Thus, $D_aD_b\left((x_1 + x_2)(y_1 + y_2)\prod_{i=3}^{n}(y_i + 1)\right) \neq const.$. From (22), we have $D_aD_bf \neq const.$.

$\diamond$

We denote the class of bent functions, specified by means of Theorem 9, by $\mathcal{D}_2^\star$ to indicate that $\dim(E_1) = 2$ and the superscript "$\star$" emphasizes the fact that there exist other permutations π (apart from $\pi^\star$) that can be used for the same purpose when E_1 is a 2-dimensional subspace.

7 Conclusions

Two secondary classes of bent functions, that possibly provide instances of bent functions outside the standard primary classes, were introduced by Carlet more than two decades ago and a single class named $\mathcal{D}_0$ was shown to be outside $\mathcal{PS}^{\#}$ and $\mathcal{M}^{\#}$. We further refine sufficient conditions for the members of $\mathcal{C}$ and $\mathcal{D}$ class to be outside $\mathcal{M}^{\#}$ compared to [27] and identify a few infinite subclasses of bent functions that do not belong to the completed $\mathcal{M}$ class. More importantly, another explicit subclass of bent functions in $\mathcal{D}$, denoted by $\mathcal{D}_2^{\star}$, has been introduced and it is shown that its members are strictly outside $\mathcal{M}^{\#}$. The question whether these functions are also outside the completed $\mathcal{PS}$ class (the inclusion in this class being equivalent to the NP-hard problem of identifying cliques in a graph, cf. Section 4.3) remains open and is quite difficult due to the lack of indicators.

8 Acknowledgements

Yongzhuang Wei is supported in part by the Natural Science Foundation of China (61572148, 61872103), in part by the Guangxi Science and Technology Foundation (Guike AB18281019). Fengrong Zhang is supported in part by the Natural Science Foundation of China (61972400) and in the part by the Jiangsu Natural Science Foundation (BK20181352). Enes Pasalic is partly supported by the Slovenian Research Agency (research program P1-0404 and research project J1-1694). Nastja Cepak is supported in part by the Slovenian Research Agency (research program P1-0404 and research project J1-1694).

References

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

[2] C. Carlet. On the secondary constructions of resilient and bent functions. *Proceedings of the Workshop on Coding, Cryptography and Combinatorics 2003*, published by Birkhuser Verlag, PCS vol. 23, pp. 3–28, 2004.

[3] 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.), Available: `http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html`, pp. 257–397 (2010).

[4] 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`, pp. 398–469 (2010).

[5] C. Carlet, S. Mesnager. Four decades of research on bent functions. *Designs, Codes and Cryptography*, vol. 78 (1), pp. 5–50 (2016).

[6] C. Carlet, G. Gao, W. Liu. A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions. *Journal of Combinatorial Theory, Series A*, vol. 127, pp. 161–175, 2014.

[7] C. Carlet, S. Mesnager. On Dillon's class H of bent functions, Niho bent functions and o-polynomials. *Journal of Combinatorial Theory, Series A*, vol. 118, no. 8, pp. 2392–2410, 2011.

[8] C. Carlet, J. L. Yucas. Piecewise constructions of bent and almost optimal Boolean functions. *Designs, Codes and Cryptography*, vol. 37, no. 3, pp. 449–464, 2005.

[9] C. Carlet, F. Zhang, Y. Hu. Secondary constructions of bent functions and their enforcement. *Advances in Mathematics of Communications*, vol. 6, no. 3, pp. 305–314, 2012.

[10] P. Charpin and G. Kyureghyan. Monomial functions with linear structure and permutation polynomials. *Finite Fields: Theory and Applications FQ9*, vol. 518, AMS, pp. 99–111, 2010.

[11] Cusick, T. W., Stănică, P.: Cryptographic Boolean functions and applications. Elsevier–Academic Press, (2009)

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

[13] J. F. Dillon. Elementary Hadamard difference sets. *In proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing*, Utility Mathematics, Winnipeg, pp. 237–249 (1975).

[14] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. *Fast Software Encryption '94*, LNCS 1008, Springer-Verlag, pp. 61–74 (1995).

[15] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, P. Gaborit. Construction of bent functions via Niho power functions. *Journal of Combinatorial Theory, Series A*, vol. 113, no. 5, pp. 779-798, 2006.

[16] R. Gupta, R.K. Sharma. Some new classes of permutation trinomials over finite fields with even characteristic. *Finite Fields and Their Applications*, vol. 41, pp. 89–C96, 2016.

[17] X.-D. Hou, P. Langevin. Results on bent functions. *Journal of Combinatorial Theory, Series A*, vol. 80, no. 2, pp. 232–246, 1997.

[18] R.M. Karp. Reducibility among combinatorial problems, *Complexity of computer computations*, Springer, Boston, MA, 1972, pp. 85–103.

[19] P. Langevin, G. Leander. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Designs Codes and Cryptography*, vol. 59, no. 1-3, pp. 193–225, 2011.

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

[21] B. Mandal, P. Stanica, S. Gangopadhyay, E. Pasalic. An analysis of $\mathcal{C}$ class of bent functions. *Fundamenta Informaticae*, vol. 147 (3), pp. 271–292 (2016).

[22] S. Mesnager. Further constructions of infinite families of bent functions from new permutations and their duals. *Cryptography and Communications*, vol. 8, no. 2, pp. 229–246, 2016.

[23] S. Mesnager. Several new infinite families of bent functions and their duals. *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 4397–4407, 2014.

[24] O. S. Rothaus. On bent functions. *J. Combinatorial Theory, Ser. A*, vol. 20, pp. 300–305 (1976).

[25] F. Zhang, C. Carlet, Y. Hu, T.-J. Cao. Secondary constructions of highly nonlinear Boolean functions and disjoint spectra plateaued functions. *Information Sciences*, vol. 283, pp. 94–106, 2014.

[26] F. Zhang, C. Carlet, Y. Hu, W. Zhang. New secondary constructions of bent functions. *Applicable Algebra in Engineering, Communication and Computing*, vol. 27, no. 5, pp. 413–434, 2016.

[27] F. Zhang, E. Pasalic, N. Cepak, Y. Wei. Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana-McFarland class. *Codes, Cryptology and Information Security*, C2SI, LNCS 10194, Springer-Verlag, pp. 298–313 (2017).

[28] F. Zhang, E. Pasalic, Y. Wei, N. Cepak. Constructing bent functions outside the Maiorana-McFarland class using a general form of Rothaus. *IEEE Transactions on Information Theory*, vol. 63, no. 8, pp. 5336 – 5349, 2017.

[29] F. Zhang, Y. Wei, E. Pasalic. Constructions of bent-negabent functions and their relation to the completed Maiorana - McFarland class. *IEEE Transactions on Information Theory*, vol. 61, no. 3, pp. 1496–1506, 2015.