Cryptography and Communications (2022) 14:1229–1256
https://doi.org/10.1007/s12095-022-00566-7

Constructing new superclasses of bent functions from known ones

Amar Bapić[1,2] · Enes Pasalic[1,2] · Fengrong Zhang[3,4] · Samir Hodžić[1]

Received: 19 October 2021 / Accepted: 9 February 2022 / Published online: 28 March 2022

Abstract
Some recent research articles (Zhang et al. in Lecture Notes in Computer Science, 10194, 298-313. (2017), Zhang et al. in Discret. Appl. Math. 285(1), 458-472. (2020)) addressed an explicit specification of indicators that specify bent functions in the so-called $\mathcal{C}$ and $\mathcal{D}$ classes, derived from the Maiorana-McFarland ($\mathcal{M}$) class by C. Carlet in 1994 (Carlet in In Lecture Notes in Computer Science 765, 77–101. (1993)). Many of these bent functions that belong to $\mathcal{C}$ or $\mathcal{D}$ are provably outside the completed $\mathcal{M}$ class. Nevertheless, these modifications are performed on affine subspaces, whereas modifying bent functions on suitable subsets may provide us with further classes of bent functions. In this article, we exactly specify new families of bent functions obtained by adding together indicators typical for the $\mathcal{C}$ and $\mathcal{D}$ class, thus essentially modifying bent functions in $\mathcal{M}$ on suitable subsets instead of subspaces. It is shown that the modification of certain bent functions in $\mathcal{M}$ gives rise to new bent functions which are provably outside the completed $\mathcal{M}$ class. Moreover, we consider the so-called 4-bent concatenation (using four different bent functions on the same variable space) of the (non)modified bent functions in $\mathcal{M}$ and show that we can generate new bent functions in this way which do not belong to the completed $\mathcal{M}$ class either. This result is obtained by specifying explicitly the duals of four constituent bent functions used in the concatenation. The question whether these bent functions are also excluded from the completed versions of $\mathcal{PS}$, $\mathcal{C}$ or $\mathcal{D}$ remains open and is considered difficult due to the lack of membership indicators for these classes.

Keywords $\mathcal{C}$ class · $\mathcal{D}$ class · Completed Maiorana-McFarland class $\mathcal{M}^{\#}$ · $\mathcal{CD}$ class · Weakly normal bent functions · Bent duals · 4-bent decomposition

Mathematics Subject Classification (2010) 94A60 · 06E30

1 Introduction

An important class of Boolean functions was introduced by Rothaus [4] in 1976, which are defined in even number of variables having the maximum possible Hamming distance to the set of all affine functions. These functions are called *bent* functions. Bent functions

✉ Amar Bapić
amar.bapic@famnit.upr.si

Extended author information available on the last page of the article

have been exhaustively studied in the past four decades because of their applications in cryptography, coding theory, graph theory, association schemes, etc. For more details on bent functions, their characterizations and design methods we refer to the textbooks [5–9].

When considering classes of bent functions, there are two primary classes referred to as partial spread ($\mathcal{PS}$) class due to Dillon [9] and the Maiorana-McFarland ($\mathcal{M}$) class [10]. The term primary refers to the design that does not employ known bent functions to generate new ones (giving rise to the so-called secondary methods), it rather uses a suitable set of affine functions (typical for the Maiorana-McFarland method [10]) or a collection of disjoint $n/2$-dimensional subspaces to construct a bent function on $GF(2)^n$ (typical for the partial spread class introduced by Dillon [9]). Another generic class, denoted by $\mathcal{N}$, was proposed by Dobbertin [11] and it includes both $\mathcal{M}$ and a subclass of $\mathcal{PS}$ commonly denoted $\mathcal{PS}_{ap}$. In 1993, Carlet [3] introduced two additional secondary classes of bent functions, denoted by $\mathcal{C}$ and $\mathcal{D}$, which are derived through a suitable modification of bent functions in the $\mathcal{M}$ class. One explicit class derived by Carlet, containing instances that do not belong to $\mathcal{M}$ or $\mathcal{PS}$, is named $\mathcal{D}_0$ and its cardinality is of approximately the same size as of $\mathcal{M}$. This does not substantially help in achieving a complete classification of bent functions, as the two primary classes stand only for a portion of $\approx 2^{76}$ of bent functions on $\mathbb{F}_2^8$, whereas their totality is around 2^{106} [12]. In recent articles [1, 2, 13], the analysis of these two secondary classes has been taken further towards specifying a sufficient set of conditions so that the resulting bent functions are also provably outside $\mathcal{M}^{\#}$, where the superscript "#" in general denotes a completed version of the considered class. Due to the hardness of overall conditions, ensuring that at the same time the specified bent functions are indeed in $\mathcal{C}$ or $\mathcal{D}$ and additionally outside $\mathcal{M}^{\#}$ (possibly also outside $\mathcal{PS}^{\#}$) is a rather difficult task. In [14], the authors extend the results in [2] to vectorial bent functions and introduce the concept of *weakly* and *strongly* outside a completed (given) primary class (more specifically $\mathcal{M}^{\#}$).

In the first part of this article, we further extend the initiative taken in [15], where it was shown that under certain conditions it is possible to construct a superclass of bent functions that stems from $\mathcal{D}_0$ and $\mathcal{C}$, named as the $\mathcal{SC}$ class. This class of functions uses the addition of indicators typical to $\mathcal{D}_0$ and $\mathcal{C}$ and therefore their overall effect is a modification of a bent function on a suitable subset instead on a subspace. We show that, apart from adding the indicators of $\mathcal{D}_0$ and $\mathcal{C}$, the only remaining possibility of ensuring the bentness of the resulting functions corresponds to the addition of suitable indicators used in the definition of $\mathcal{C}$ and $\mathcal{D}$ classes (\, for instance adding indicators of $\mathcal{D}_0$ and $\mathcal{D}$ cannot give bent functions), which results in a superclass $\mathcal{CD}$ of bent functions. We then give sufficient conditions which ensure that bent functions in $\mathcal{CD}$ lie outside $\mathcal{M}^{\#}$ and provide two generic methods for specifying these objects, see Proposition 2 and 3. We also partially address the normality of these functions and in this context we further refine the constraints on functions in $\mathcal{CD}$ to be outside the completed $\mathcal{PS}^{+}$ class. This problem of finding non(weakly)-normal bent functions is intrinsically difficult and it remains open whether there are instances of bent functions in $\mathcal{CD}$ which are non(weakly)-normal.

In the second part of this article, we consider the problem of specifying suitable selections of four bent functions so that their concatenation is again a bent function. This approach is closely related to the so-called 4-decomposition [16] of bent functions. More precisely, there are three possibilities of decomposing bent functions on $\mathbb{F}_2^n$ as four restrictions to the cosets of some $(n-2)$-dimensional linear subspace. In general, these restrictions are either all bent, semi-bent or 5-valued spectra functions [16]. We show that suitable $(n-2)$-variable bent functions in $\mathcal{C}, \mathcal{D}, \mathcal{CD}$ and $\mathcal{M}$ can be concatenated to provide new bent functions in n variables. Most notably, the resulting bent functions are also provably outside the $\mathcal{M}^{\#}$ class. The bentness of these functions is established using the necessary

and sufficient condition given in [17] that the duals of its restrictions must satisfy. This implies that for the first time, we explicitly determine the duals of certain functions in $\mathcal{C}$ and $\mathcal{D}$ (implying the exact specification of the duals of bent functions in $\mathcal{SC}$ and $\mathcal{CD}$), which is in general considered as a difficult problem. Moreover, the fact that the 4-bent concatenation, that employs bent functions stemming from different classes, gives instances of bent functions provably outside the $\mathcal{M}^{\#}$ class is quite interesting. More precisely, we believe that the gap between the total space of bent functions and their portion that comes from the primary classes (as mentioned above) exactly originates in the lack of understanding of 4-bent decomposition. In other words, having only three possibilities of concatenating suitable objects on an $(n-2)$-dimensional space to achieve the bentness on $\mathbb{F}_2^n$, we need to analyze the behaviour and class inclusion of these objects in more depth.

This article is organized as follows. In Sect. 2, we recall some relevant notions and definitions related to Boolean functions and in particular we specify the main primary and secondary classes of bent functions. A superclass of bent functions which employs the addition of indicators typical to classes $\mathcal{C}$ and $\mathcal{D}$, named $\mathcal{CD}$, is introduced in Sect. 3. In Sect. 4, we specify sufficient conditions for bent functions in $\mathcal{CD}$ to lie outside the completed $\mathcal{M}$ class and provide two generic methods (Propositions 2 and 3) of constructing such functions. We then consider the problem of concatenating four suitable $(n-2)$-variable bent functions, taken form different classes, for the purpose of generating new bent functions in n variables. It is shown that our superclass $\mathcal{CD}$ provides such instances and furthermore the resulting bent functions are again provably outside the completed $\mathcal{M}$ class. This is achieved by specifying explicitly the duals of certain functions in $\mathcal{C}$ and $\mathcal{D}$ which also allows us to determine the duals of bent functions in $\mathcal{SC}$ and $\mathcal{CD}$. Some concluding remarks are given in Sect. 6.

2 Preliminaries

With $|S|$ we denote the cardinality of a finite set S. The vector space $\mathbb{F}_2^n$ is the space of all n-tuples $\mathbf{x} = (x_1, \ldots, x_n)$, where $x_i \in \mathbb{F}_2$. For $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$ the usual scalar (dot) product over $\mathbb{F}_2$ is defined as $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 \oplus \cdots \oplus x_n y_n$. With $\mathbb{F}_2^{n^*}$ we denote the set $\mathbb{F}_2^n \setminus \{\mathbf{0}_n\}$ and with $\mathbb{F}_{2^n}^*$ we denote the multiplicative cyclic group of a finite filed $\mathbb{F}_{2^n}$ which consists of the $2^n - 1$ nonzero elements of $\mathbb{F}_{2^n}$. For convenience, we will sometimes identify the vector space $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$. Any element $\mathbf{x} \in \mathbb{F}_2^n$ uses a bold face letter, whereas the standard letters are reserved for finite field elements. Throughout the paper, if $t|m$ then we treat $\mathbb{F}_{2^t}$ as a subfield of $\mathbb{F}_{2^m}$. A polynomial $F(x) \in \mathbb{F}_{2^n}[x]$ is called a *permutation polynomial*, if the induced evaluation $\{F(x) : x \in \mathbb{F}_{2^n}\}$ permutes the elements of $\mathbb{F}_{2^n}$.

Moreover, any (n, n)-function F can be uniquely expressed as a *univariate polynomial* of degree at most $2^n - 1$:

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i, \quad a_i \in \mathbb{F}_{2^n}.$$

For the 2-adic expansion $i = i_0 + i_1 2 + i_2 2^2 + \cdots + i_{n-1} 2^{n-1}$, the algebraic degree of F is defined as

$$\deg(f) = \max\{\mathrm{wt}(i) : a_i \neq 0,\ 0 \leq i < 2^n\},$$

where wt(i) is the Hamming weight of $i = (i_0, i_1, \ldots, i_{n-1})$ (the number of nonzero coefficients $i_j \in \mathbb{F}_2$, $j = 0, \ldots, n-1$).

For $x \in \mathbb{F}_{2^n}$ the *(relative) trace* $Tr_k^n(x) : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$ of x over $\mathbb{F}_{2^k}$, where k is a divisor of n, is defined by

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

If $k = 1$, then Tr_1^n is called the *absolute trace*. For an (n, m)-function $F = (f_1, \ldots, f_m)$, where $f_1, \ldots, f_m : \mathbb{F}_{2^n} \to \mathbb{F}_2$ are the *coordinate functions* of F, all the $2^m - 1$ nonzero linear combinations of the coordinates f_i are called *component functions* of F, i.e. the functions $F_\lambda(x) = Tr_1^m(\lambda F(x))$, $\lambda \in \mathbb{F}_{2^m}^*$. The function $W_F : \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}^* \to \mathbb{Z}$ defined by

$$W_F(\lambda, u) := W_{F_\lambda}(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\lambda F(x)) + Tr_1^n(ux)}, \ u \in \mathbb{F}_{2^n}, \ \lambda \in \mathbb{F}_{2^n}^*,$$

is called the (extended) *Walsh-Hadamard transform* of the function F. Specially, if $m = 1$, then $F := f$ is a Boolean function and we denote the Walsh-Hadamard transform of f with W_f. If $W_f(u) = \pm 2^{\frac{n}{2}}$ for all $u \in \mathbb{F}_{2^n}$, then f is a *bent function* and n is necessarily even. The set of all Boolean functions on $\mathbb{F}_2^n$ is denoted by $\mathcal{B}_n$.

When $f \in \mathcal{B}_n$ is bent, then the Boolean function f^*, defined through $W_f(u) = 2^{\frac{n}{2}}(-1)^{f^*(u)}$ for any $u \in \mathbb{F}_{2^n}$, is also bent and is called the *dual* of f. For a Boolean function $f \in \mathcal{B}_n$, the *inverse Walsh-Hadamard transform* of f at any point $u \in \mathbb{F}_{2^n}$ is defined by

$$(-1)^{\mathrm{f(u)}} = \sum_{\mathrm{x} \in \mathrm{F}_{2^n}} \mathrm{W_f(x)} (-1)^{\mathrm{Tr_1^n(ux)}}.$$

Two (n, m)-functions F and G are called *extended affine equivalent* (EA-equivalent) if there exist some affine permutation L_1 on $\mathbb{F}_{2^n}$, some affine permutation L_2 on $\mathbb{F}_{2^m}$ and some affine function $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ such that $F = L_2 \circ G \circ L_1 + A$. They are called *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) (introduced in [18] and later named CCZ-equivalence in [19]) if there exists some affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$, where $L_1 : \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^n}$ and $L_2 : \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ are affine functions, such that $y = G(x)$ if and only if $L_2(x, y) = F \circ L_1(x, y)$. It is well known that EA-equivalence is a special case of CCZ-equivalence [19]. In the Boolean case, the CCZ-equivalence coincides with EA-equivalence which is given as follows. Given an arbitrary Boolean function $f \in \mathcal{B}_n$, its affine equivalence class includes a set of functions $\{g\}$ obtained by

$$g(\mathbf{x}) = f(A\mathbf{x} \oplus \mathbf{b}) \oplus \mathbf{c} \cdot \mathbf{x} \oplus d,$$

where $A \in GL(n, \mathbb{F}_2)$ (the group of invertible matrices under composition), $\mathbf{b}, \mathbf{c} \in \mathbb{F}_2^n$ and $d \in \mathbb{F}_2$.

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 affine transformations 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.

The following theorem will be useful when considering the inclusion/exclusion of bent Boolean functions in the completed class $\mathcal{M}^\#$.

Theorem 1 [9] *An n-variable bent function f, $n = 2m$, belongs to $\mathcal{M}^\#$ if and only if there exists an m-dimensional linear subspace V of $\mathbb{F}_2^n$ such that the second order derivatives*

$$D_{\mathbf{a}}D_{\mathbf{b}}f(\mathbf{x}) = f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{a}) \oplus f(\mathbf{x} \oplus \mathbf{b}) \oplus f(\mathbf{x} \oplus \mathbf{a} \oplus \mathbf{b})$$

vanish for any $\mathbf{a}, \mathbf{b} \in V$.

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

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

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus g(\mathbf{y}), \text{ for all } \mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m, \qquad (\mathcal{M})$$

where π is a permutation on $\mathbb{F}_2^m$, and g is an arbitrary Boolean function on $\mathbb{F}_2^m$. From this class, Carlet [3] derived the $\mathcal{C}$ class of bent functions that contains all functions of the form

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus \mathbf{1}_{L^\perp}(\mathbf{x}), \qquad (\mathcal{C}), \tag{1}$$

where L is any linear subspace of $\mathbb{F}_2^m$, $\mathbf{1}_{L^\perp}$ is the indicator function of the space $L^\perp = \{\mathbf{x} \in \mathbb{F}_2^m : \mathbf{x} \cdot \mathbf{y} = 0, \ \forall \mathbf{y} \in L\}$, and π is any permutation on $\mathbb{F}_2^m$ such that:

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

The permutation ϕ and the subspace L are then said to satisfy the (C) property, or for short (π^{-1}, L) has property (C).

Another class introduced by Carlet [3], called $\mathcal{D}$, is defined similarly as

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus \mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y}), \qquad (\mathcal{D}), \tag{2}$$

where π is a permutation on $\mathbb{F}_2^m$ and E_1, E_2 two linear subspaces of $\mathbb{F}_2^m$ such that $\pi(E_2) = E_1^\perp$. Quite recently, a set of sufficient conditions for bent functions in $\mathcal{C}$ and $\mathcal{D}$ to lie outside the completed $\mathcal{M}$ class was derived in [1, 2]. These conditions involve the concept of linear structures which is defined below.

Definition 2 An n-variable Boolean function f is said to have a linear structure if there exists a nonzero $\mathbf{a} \in \mathbb{F}_2^n$ such that $f(\mathbf{x} \oplus \mathbf{a}) \oplus f(\mathbf{x})$ is a constant function.

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

(C1) $\dim(L) \geq 2$;
(C2) $\mathbf{u} \cdot \pi$ *has no nonzero linear structure for all* $\mathbf{u} \in \mathbb{F}_2^{m^*}$,

then f is a bent function in $\mathcal{C}$ outside $\mathcal{M}^\#$.

Similar conditions concerning class $\mathcal{D}$ were deduced in [2]:

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

(D1) $\dim(E_1) \geq 2$ *and* $\dim(E_2) \geq 2$;
(D2) $\mathbf{u} \cdot \pi$ *has no nonzero linear structure for all* $\mathbf{u} \in \mathbb{F}_2^{m^*}$;
(D3) $\deg(\pi) \leq m - \dim(E_2)$,

then f is a bent function in $\mathcal{D}$ outside $\mathcal{M}^{\#}$.

3 New classes of Boolean bent functions

In this section, we recall the definition of the class $\mathcal{SC}$ introduced in [15] and investigate the possibility of defining similar classes via suitable mixtures of indicators typical for $\mathcal{C}$ and $\mathcal{D}$. Nevertheless, any choice of these indicators must preserve the bent property of the resulting functions which consequently leads to only one new superclass of bent functions called $\mathcal{CD}$. We again emphasize that using the addition of two indicators (corresponding to subspaces) essentially implies a modification of bent functions in $\mathcal{M}$ on subsets rather than affine subspaces.

3.1 Bent functions in $\mathcal{SC}$

Let $g : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a bent Boolean function in $\mathcal{M}$ defined by $g(x, y) = Tr_1^m(x\pi(y))$, where π is a permutation on $\mathbb{F}_{2^m}$. Furthermore, let

$$\delta_0(x) = x^{2^m-1} + 1$$

be the Dirac symbol, that is, $\delta_0(x) = 1$ if $x = 0$ and 0 otherwise, which is essentially the indicator of the m-dimensional subspace $\{0\} \times \mathbb{F}_{2^m}$. Then, $(x, y) \mapsto g(x, y) + \delta_0(x)$ is a bent function in the class $\mathcal{D}_0$, which is outside $\mathcal{M}^{\#}$ provided that π is not affine on any hyperplane of $\mathbb{F}_{2^m}$ [Proposition 2] [3]. Notice that when L is a linear subspace of $\mathbb{F}_{2^m}$, then

$$\mathbf{1}_{L^{\perp}}(x) = \prod_{\omega \in \mathbf{b}(L)} (Tr_1^m(\omega x) + 1),$$

where $\mathbf{b}(L)$ is the basis of L, is the indicator function of $L^{\perp}$ in finite field notation.

In [15], the authors introduced a new superclass of bent functions constructed from the classes $\mathcal{C}$ and $\mathcal{D}_0$, and it is defined as follows.

Definition 3 [15] Let π be a permutation on $\mathbb{F}_{2^m}$ and let $L \subset \mathbb{F}_{2^m}$ be a linear subspace of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property. Then, the class of bent functions $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ containing all functions of the form

$$f(x, y) = Tr_1^m(x\pi(y)) + a_0 1_{L^{\perp}}(x) + a_1 \delta_0(x), \quad a_i \in \mathbb{F}_2, \qquad (\mathcal{SC}), \tag{3}$$

is called $\mathcal{SC}$ and is a superclass of $\mathcal{D}_0$ and $\mathcal{C}$.

Furthermore, it was shown that (under certain conditions) the functions in $\mathcal{SC}$ are outside the class $\mathcal{M}^{\#}$.

Theorem 4 [15] *Let π be a permutation on $\mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^m}$ be a linear subspace of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property, $\dim(L) \geq 2$ and $Tr_1^m(\mu\pi)$ has no non-zero linear structures for all $\mu \in \mathbb{F}_{2^m}^*$. Then, the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x, y) = Tr_1^m(x\pi(y)) + \mathbf{1}_S(x),\ x, y \in \mathbb{F}_{2^m},$$

where $\mathbf{1}_S(x) = \mathbf{1}_{L^\perp}(x) + \delta_0(x)$, is a bent function in $\mathcal{SC}$ outside $\mathcal{M}^{\#}$.

Motivated by this construction, we will consider the existence of other superclasses: $\mathcal{SD}$ (superclass of $\mathcal{D}$ and $\mathcal{D}_0$), $\mathcal{CD}$ (superclass of $\mathcal{C}$ and $\mathcal{D}$) and $\mathcal{SCD}$ (superclass of $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}_0$). It turns out that only the class $\mathcal{CD}$ contains bent functions, whereas the other classes do not.

3.2 Bentness of Boolean functions in the class $\mathcal{SD}$

As before, we consider $g : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined as $g(x, y) = Tr_1^m(x\pi(y))$, where π is a permutation on $\mathbb{F}_{2^m}$, which is a bent function in $\mathcal{M}$. We now show that if $E_1, E_2 \neq \{0\}$ are two linear subspaces of $\mathbb{F}_{2^m}$ such that $\pi(E_2) = E_1^\perp$ (we do not consider the possibilities $E_1 \times E_2 = \{0\} \times \mathbb{F}_{2^m}$ or $\mathbb{F}_{2^m} \times \{0\}$), then Boolean functions of the form, constituting the $\mathcal{SD}$ class,

$$f(x, y) = g(x, y) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) + \delta_0(x),\ x, y \in \mathbb{F}_{2^m}, \quad (\mathcal{SD}), \tag{4}$$

cannot be bent.

Theorem 5 *Let π be a permutation on $\mathbb{F}_{2^m}$ and $E_1, E_2 \subset \mathbb{F}_{2^m}$ be two linear subspace of $\mathbb{F}_{2^m}$ such that $\pi(E_2) = E_1^\perp$. Then, the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x, y) = Tr_1^m(x\pi(y)) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) + \delta_0(x)$$

is not bent.

Proof Let us first compute $W_f(0, 0)$ as:

$$\begin{aligned}
W_f(0,0) &= \sum_{x \in \mathbb{F}_{2^m}^*} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y)) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)} + \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathbf{1}_{E_2}(y)+1} \\
&= \sum_{x \in \mathbb{F}_{2^m}^*} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y)) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)} - \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathbf{1}_{E_2}(y)} \\
&= \sum_{x \in \mathbb{F}_{2^m}} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y)) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)} - 2 \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathbf{1}_{E_2}(y)} \\
&= W_g(0,0) - 2 \cdot (2^m - |E_2|).
\end{aligned}$$

Since $g(x, y) = Tr_1^m(x\pi(y)) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)$ is a bent function in $\mathcal{D}$, we have that either $W_g(0, 0) = 2^m$ or -2^m.

Assuming that $W_g(0, 0) = 2^m$, then

$$W_f(0,0) = 2^m - 2 \cdot 2^m + 2|E_2| = -2^m + 2|E_2|.$$

The requirement that $W_f(0,0) = \pm 2^m$ implies that $|E_2| = 0$ or 2^m. However, $E_2 \neq \emptyset$ and obviously $\dim E_2 < m$, thus this case is not possible.

On the other hand, if $W_g(0,0) = -2^m$ then we necessarily have

$$W_f(0,0) = -2^m - 2 \cdot 2^m + 2|E_2| = -3 \cdot 2^m + 2|E_2|.$$

Requiring that $W_f(0,0) = \pm 2^m$, implies that $|E_2| = 2^{m+1}$ or 2^m, both of which are again not possible. Hence, $W_f(0,0) \neq \pm 2^m$, that is, f is not a bent function.

Remark 1 Similarly, using the ideas as in the proof of Theorem 5, one can show that functions of the form (constituting the $\mathcal{SCD}$ class)

$$f(x,y) = g(x,y) + \mathbf{1}_{L^\perp}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) + \delta_0(x) \qquad (\mathcal{SCD}),$$

cannot be bent.

3.3 Bentness of Boolean functions in the class $\mathcal{CD}$

In this section, we consider the remaining case which corresponds to the mixture of indicators stemming from $\mathcal{C}$ and $\mathcal{D}$. Let $g : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$, defined by $g(x,y) = Tr_1^m(x\pi(y)) \in \mathcal{M}$, be a bent Boolean function, where π is a permutation on $\mathbb{F}_{2^m}$. Let $L \subset \mathbb{F}_{2^m}$ be a linear subspace of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property, and let $E_1, E_2 \neq \{0\}$ be two linear subspaces of $\mathbb{F}_{2^m}$ such that $\pi(E_2) = E_1^\perp$. We consider the bentness of Boolean functions f in $2m$ variables, being members of the class $\mathcal{CD}$ (see Definition 4), of the form

$$f(x,y) = g(x,y) + \mathbf{1}_{L^\perp}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y),\ x,y \in \mathbb{F}_{2^m}. \tag{5}$$

Then, the primary task is to find conditions which ensure that the function f given by Eq. (5) is bent. Let us consider the Walsh coefficient $W_f(a,b)$ for arbitrary but fixed $(a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Furthermore, we denote with $C(x,y) := Tr_1^m(x\pi(y)) + \mathbf{1}_{L^\perp}(x)$ and $M(a,b) = C(x,y) + Tr_1^m(ax+by)$. Then,

$$\begin{aligned}
W_f(a,b) &= \sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)+\mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)} \\
&= \sum_{x\in E_1}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)+\mathbf{1}_{E_2}(y)} + \sum_{x\notin E_1}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)} \\
&= -\sum_{x\in E_1}\sum_{y\in E_2} (-1)^{M(a,b)} + \sum_{x\in E_1}\sum_{y\notin E_2} (-1)^{M(a,b)} + \sum_{x\notin E_1}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)} \\
&= -2\sum_{x\in E_1}\sum_{y\in E_2} (-1)^{M(a,b)} + \sum_{x\in E_1}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)} + \sum_{x\notin E_1}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)} \\
&= \sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)} - 2\sum_{x\in E_1}\sum_{y\in E_2} (-1)^{M(a,b)} = W_C(a,b) - 2\sum_{x\in E_1}\sum_{y\in E_2} (-1)^{M(a,b)} \\
&= W_C(a,b) - 2\sum_{x\in E_1}\sum_{y\in E_2} (-1)^{Tr_1^m(x\pi(y))+\mathbf{1}_{L^\perp}(x)+Tr_1^m(ax+by)}.
\end{aligned}$$

Since $E_1^\perp = \pi(E_2)$, we have that $Tr_1^m(x\pi(y)) = 0$ for $(x,y) \in E_1 \times E_2$. It follows now that

$$W_f(a,b) = W_C(a,b) - 2 \cdot \left(\sum_{x\in E_1} \sum_{y\in E_2} (-1)^{Tr_1^m(ax+by)} - 2 \sum_{x\in E_1\cap L^\perp} \sum_{y\in E_2} (-1)^{Tr(ax+by)} \right). \quad (6)$$

Furthermore, if we denote $K = E_1 \cap L^\perp$, it is easy to see that

$$\sum_{x\in E_1} \sum_{y\in E_2} (-1)^{Tr_1^m(ax+by)} = \begin{cases} 2^{\varepsilon_1+\varepsilon_2}, & (a,b) \in E_1^\perp \times E_2^\perp \\ 0, & \text{otherwise} \end{cases}, \quad (7)$$

$$\sum_{x\in K} \sum_{y\in E_2} (-1)^{Tr_1^m(ax+by)} = \begin{cases} 2^{\kappa+\varepsilon_2}, & (a,b) \in K^\perp \times E_2^\perp \\ 0, & \text{otherwise} \end{cases}, \quad (8)$$

where $\varepsilon_i = \dim(E_i)$ and $\kappa = \dim(K)$. Since $K \subset E_1$, it follows that $E_1^\perp \subset K^\perp$, and therefore $E_1^\perp \times E_2^\perp \subset K^\perp \times E_2^\perp$. Obviously, when $(a,b) \notin K^\perp \times E_2^\perp$, we have that $W_f(a,b) = W_C(a,b)$. Let us now consider the following cases:

Case 1: Suppose that $(a,b) \in E_1^\perp \times E_2^\perp$. Since we want that f is a bent function, we have the following situations:

(I) If $W_f(a,b) = W_C(a,b)$, then

$$W_C(a,b) = W_C(a,b) - 2^{\varepsilon_1+\varepsilon_2+1} + 2^{\kappa+\varepsilon_2+2} \Leftrightarrow 2^{\varepsilon_1+\varepsilon_2+1} = 2^{\kappa+\varepsilon_2+2} \Leftrightarrow \kappa = \varepsilon_1 - 1.$$

(II) If $W_f(a,b) = -W_C(a,b)$, then $-2W_C(a,b) = -2^{m+1} + 2^{\kappa+\varepsilon_2+2}$. Since $W_C(a,b) = \pm 2^m$, we have

$$-2^{m+1} = -2^{m+1} + 2^{\kappa+\varepsilon_2+2} \text{ or } 2^{m+1} = -2^{m+1} + 2^{\kappa+\varepsilon_2+2}.$$

The first case is not possible since a power of two is strictly larger than zero, and the second one leads to $\kappa = \varepsilon_1$.

Case 2: Suppose that $(a,b) \in (K^\perp \setminus E_1^\perp) \times E_2^\perp$. Again, requiring that f is bent leads to the following cases:

(I) If $W_f(a,b) = W_C(a,b)$, then

$$W_C(a,b) = W_C(a,b) + 2^{\kappa+\varepsilon_2+2} \Leftrightarrow 2^{\kappa+\varepsilon_2+2} = 0,$$

which is not possible.

(II) If $W_f(a,b) = -W_C(a,b)$, then $-2W_C(a,b) = 2^{\kappa+\varepsilon_2+2}$. Since the right-hand side of the equality is positive, so must be the left-hand side. Thus, we must have that $W_C(a,b) = -2^m$ and in this case $\kappa = \varepsilon - 1$.

From **Case** 1 and 2, we obtain bent Walsh coefficients only when $\kappa = \varepsilon_1$ or $\kappa = \varepsilon_1 - 1$. These observations are summarized below, where Theorem 6 corresponds to the case $\kappa = \varepsilon_1 - 1$ and Theorem 7 refers to the case $\kappa = \varepsilon_1$.

Theorem 6 *Let π be a permutation on $\mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^m}$ be a linear subspace of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property, and let $E_1, E_2 \neq \{0\}$ be two linear subspaces of $\mathbb{F}_{2^m}$ such that $\pi(E_2) = E_1^\perp$ and $\dim(E_1 \cap L^\perp) = \dim(E_1) - 1$. Then, the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x,y) = C(x,y) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y),$$

where $C(x,y) = Tr_1^m(x\pi(y)) + \mathbf{1}_{L^\perp}(x)$, *is bent. Moreover, it holds that*

$$W_f(a,b) = \begin{cases} -W_C(a,b), & (a,b) \in ((E_1 \cap L)^\perp \setminus E_1^\perp) \times E_2^\perp \\ W_C(a,b), & \text{otherwise} \end{cases}.$$

Proof Suppose that $(a,b) \notin (E_1 \cap L)^\perp \times E_2^\perp$. From Eqs. (6)-(8), it is easy to see that $W_f(a,b) = W_C(a,b)$. Suppose that $(a,b) \in E_1^\perp \times E_2^\perp$. Again, (6)-(8) implies that

$$W_f(a,b) = W_C(a,b) - 2 \cdot (2^{\epsilon_1+\epsilon_2} - 2 \cdot 2^{\epsilon_1-1+\epsilon_2}) = W_C(a,b).$$

Lastly, if $(a,b) \in ((E_1 \cap L)^\perp \setminus E_1^\perp) \times E_2^\perp$, the sum (7) is equal to zero, and thus from Eqs. (6) and (8) it follows that

$$W_f(a,b) = W_C(a,b) - 2 \cdot 2^{\epsilon_1+\epsilon_2} = W_C(a,b) - 2^{m+1}.$$

Using Parseval's equation, it is straightforward to show that $W_C(a,b) = 2^m$, for all $(a,b) \in (E_1 \cap L)^\perp \times E_2^\perp$. Thus,

$$W_f(a,b) = 2^m - 2^{m+1} = -2^m = -W_C(a,b).$$

In other words, the function f is bent.

Theorem 7 *Let* π *be a permutation on* $\mathbb{F}_{2^m}$, $E_1, E_2 \neq \{0\}$ *be two linear subspaces of* $\mathbb{F}_{2^m}$ *such that* $\pi(E_2) = E_1^\perp$ *and* $(\pi^{-1}, E_1^\perp)$ *satisfies the* (C) *property. Then the function* $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ *defined by*

$$f(x,y) = C(x,y) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y),$$

where $C(x,y) = Tr_1^m(x\pi(y)) + \mathbf{1}_{E_1}(x)$, *is bent. Moreover, it holds that*

$$W_f(a,b) = \begin{cases} -W_C(a,b), & (a,b) \in E_1^\perp \times E_2^\perp \\ W_C(a,b), & \text{otherwise} \end{cases}.$$

Proof We note that (6) becomes

$$W_f(a,b) = W_C(a,b) + 2\sum_{x \in E_1}\sum_{y \in E_2}(-1)^{Tr_1^m(ax+by)} = \begin{cases} W_C(a,b) + 2^{m+1}, & (a,b) \in E_1^\perp \times E_2^\perp \\ W_C(a,b), & \text{otherwise} \end{cases}.$$

Using Parseval's equation, it is straightforward to show that $W_C(a,b) = -2^m$ for all $(a,b) \in E_1^\perp \times E_2^\perp$. Thus,

$$W_f(a,b) = -2^m + 2^{m+1} = 2^m = -W_C(a,b).$$

In other words, the function f is bent.

Definition 4 Let π be a permutation on $\mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^m}$ be a linear subspace of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property, and let $E_1, E_2 \neq \{0\}$ be two linear subspaces of $\mathbb{F}_{2^m}$ such that $\pi(E_2) = E_1^\perp$. If $\dim(E_1 \cap L^\perp) = \dim(E_1) - 1$ or $E_1 = L^\perp$, then the class of bent functions $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ containing all functions of the form

$$f(x,y) = Tr_1^m(x\pi(y)) + a_0\mathbf{1}_{L^\perp}(x) + a_1\mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y), \;\; a_i \in \mathbb{F}_2, \quad (\mathcal{CD}), \tag{9}$$

is called $\mathcal{CD}$ and is a superclass of $\mathcal{C}$ and $\mathcal{D}$.

Remark 2 Let us consider the sum of the indicators $\mathbf{1}_{L^\perp}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)$ defined above. We note that

$$\begin{aligned}
&\mathbf{1}_{L^\perp}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) = 1\\
\Leftrightarrow &(x,y) \in (L^\perp \times \mathbb{F}_{2^m}) \setminus (E_1 \times E_2) \;\vee\; (x,y) \in (E_1 \times E_2) \setminus (L^\perp \times \mathbb{F}_{2^m})\\
\Leftrightarrow &(x,y) \in (L^\perp \times \mathbb{F}_{2^m}) \bigtriangleup (E_1 \times E_2) := S,
\end{aligned}$$

where Δ denotes the symmetric difference. Moreover, the cardinality of S is equal to

$$|S| = 2^{m+\lambda} + 2^{\epsilon_1+\epsilon_2} - 2^{\epsilon_2+1} \cdot |L^\perp \cap E_1|, \tag{10}$$

where $\dim(L^\perp) = \lambda$ and $\dim(E_i) = \epsilon_i$, $i = 1, 2$. It is easy to verify that S is neither a linear nor an affine subspace of $\mathbb{F}_{2^n}$, rather a set of elements in $\mathbb{F}_{2^n}$.

3.4 Modifying bent functions on subsets

For convenience of the reader, we know provide certain explanations related to the modification of bent functions in the Maiorana-McFarland class which appears to be highly suitable for specifying instances outside the completed class $\mathcal{M}^\#$. These modifications efficiently destroy the structure of bent functions in $\mathcal{M}$, which allows us to show that modified bent functions cannot be viewed as a concatenation of linear functions (up to EA-equivalence).

It is well-known that the $\mathcal{M}$ class can be viewed as a concatenation of affine functions when f is given as $f(\mathbf{x},\mathbf{y}) = \pi(\mathbf{y}) \cdot \mathbf{x} + g(\mathbf{y})$, for $\mathbf{x},\mathbf{y} \in \mathbb{F}_2^m$. In particular, when $f(\mathbf{x},\mathbf{y}) = \pi(\mathbf{y}) \cdot \mathbf{x}$ then f is a concatenation of all linear functions on $\mathbb{F}_2^m$ (there are exactly 2^m linear functions on $\mathbb{F}_2^m$). More specifically, for any fixed $\mathbf{y}^* \in \mathbb{F}_2^m$ the restriction of f to the affine subspace $\mathbb{F}_2^m \times \{\mathbf{y}^*\}$ becomes $\mathbf{a}^* \cdot \mathbf{x}$ where $\mathbf{a}^* = \pi(\mathbf{y}^*)$. This also implies that the weight of such bent functions is $2^{2m-1} - 2^{m-1}$ since the linear function $l(\mathbf{x}) = 0$ is used.

Now, let us consider the class $\mathcal{D}_0$ of Carlet [3] given by $f'(\mathbf{x},\mathbf{y}) = \pi(\mathbf{y}) \cdot \mathbf{x} + \delta_0(\mathbf{x})$, where $\delta_0(\mathbf{x})$ is the indicator of the m-dimensional subspace $\{\mathbf{0}_m\} \times \mathbb{F}_2^m$. It is obvious that the effect of adding $\delta_0(\mathbf{x})$ to $f(\mathbf{x},\mathbf{y}) = \pi(\mathbf{y}) \cdot \mathbf{x}$ is essentially a modification of any linear function l_i (representing f as a concatenation of linear functions so that $f = l_1||l_2||\cdots||l_{2^m}$) so that for f' instead of having $l_i(\mathbf{0}_m) = 0$ we have $l_i(\mathbf{0}_m) = 1$. Since this modification is performed on each linear function l_i, we conclude that the bent functions in $\mathcal{D}_0$ are of weight $2^{2m-1} + 2^{m-1}$ and can be viewed as a concatenation of these modified linear functions (at zero) which are now of algebraic degree m. This appears to be the main reason behind the fact that certain instances in $\mathcal{D}_0$ are provably outside the completed classes $\mathcal{M}^\#$ and $\mathcal{PS}^\#$ [3], for a suitably chosen permutation π over $\mathbb{F}_2^m$.

On the other hand, the class $\mathcal{SC}$ given as $f(\mathbf{x},\mathbf{y}) = \pi(\mathbf{y}) \cdot \mathbf{x} + \mathbf{1}_{L^\perp}(\mathbf{x}) + \delta_0(\mathbf{x})$ corresponds to the modification performed on $f(\mathbf{x},\mathbf{y}) = \pi(\mathbf{y}) \cdot \mathbf{x} + \delta_0(\mathbf{x}) \in \mathcal{D}_0$ through addition of the indicator $\mathbf{1}_{L^\perp}(\mathbf{x})$. In other words, we are now affecting already modified linear functions (as explained above) further. It can be easily verified, similarly to Remark 2, that $\mathbf{1}_{L^\perp}(\mathbf{x}) + \delta(\mathbf{x})$ forms a subset in $\mathbb{F}_2^m \times \mathbb{F}_2^m$ and cannot be an affine subspace. Assuming that $\dim(L^\perp) = d$,

the indicator $\mathbf{1}_{L^\perp}(x)$ further modifies the values (of already modified linear functions at zero) at exactly 2^d points. Since this modification is again performed at value $\mathbf{x} = \mathbf{0}_m$, the overall effect of having both indicators is essentially the modification of (original) linear functions at $2^d - 1$ points. As such a modification applies to all $\mathbf{y} \in \mathbb{F}_2^m$, we have performed a modification at exactly $2^m(2^d - 1)$ points. A similar reasoning applies to the class $\mathcal{CD}$ given in Definition 4, which will be shown to contain members outside $\mathcal{M}^\#$ in the next section.

Finally, we remark that the conditions in Theorems 2 and 3 (referring to the exclusion from $\mathcal{M}^\#$) are only sufficient and not necessary. In certain cases, even permutations whose components admit linear structures may give rise to bent functions outside $\mathcal{M}^\#$, see for instance [Theorem 12] [2]. It appears natural that the above described modifications efficiently destroy the concatenation structure of bent functions in $\mathcal{M}$ so that the resulting functions cannot belong to the completed $\mathcal{PS}$ class but this remains an open problem.

4 Sufficient conditions for functions in $\mathcal{CD}$ to be outside $\mathcal{M}^\#$

In this section, we present sufficient conditions for functions in the $\mathcal{CD}$ class to be provably outside $\mathcal{M}^\#$. We also partially address the normality of these functions and the main conclusion is that the choice of indicators must be further refined in order to possibly identify instances within $\mathcal{CD}$ class which are weakly non-normal. Consequently, this would imply that such functions lie outside the completed $\mathcal{PS}^+$ class.

The following proposition is proved useful for our main result.

Proposition 1 *Let V be a subspace of $\mathbb{F}_2^n$. Then, we have*

$$\deg(D_{\mathbf{a}}D_{\mathbf{b}}(\mathbf{1}_V(\mathbf{x}))) = \begin{cases} n - \dim(V) - 2, & \text{if } \mathbf{a}, \mathbf{b}, \mathbf{a} \oplus \mathbf{b} \notin V \\ 0, & \text{otherwise} \end{cases}.$$

Proof We know that $\deg(\mathbf{1}_V(\mathbf{x})) = n - \dim(V)$. Further, if $\mathbf{a}, \mathbf{b}, \mathbf{a} \oplus \mathbf{b} \notin V$, then

$$\begin{aligned} D_{\mathbf{a}}D_{\mathbf{b}}(\mathbf{1}_V(\mathbf{x}))) &= \mathbf{1}_V(\mathbf{x}) \oplus \mathbf{1}_V(\mathbf{x} \oplus \mathbf{a}) \\ &\quad \oplus \mathbf{1}_V(\mathbf{x} \oplus \mathbf{b}) \oplus \mathbf{1}_V(\mathbf{x} \oplus \mathbf{a} \oplus \mathbf{b}) \\ &= \mathbf{1}_{V \cup (V \oplus \mathbf{a}) \cup (V \oplus \mathbf{b}) \cup (V \oplus \mathbf{a} \oplus \mathbf{b})}(\mathbf{x}), \end{aligned}$$

that is, $\deg(D_{\mathbf{a}}D_{\mathbf{b}}(\mathbf{1}_V(\mathbf{x}))) = n - \dim(V) - 2$. If either $\mathbf{a} \in V$, $\mathbf{b} \in V$, or $\mathbf{a} \oplus \mathbf{b} \in V$ then

$$D_{\mathbf{a}}D_{\mathbf{b}}(\mathbf{1}_V(\mathbf{x}))) = 0.$$

We are now able to prove that, under certain conditions, functions in $\mathcal{CD}$ are provably outside $\mathcal{M}^\#$.

Theorem 8 *Let π be a permutation on $\mathbb{F}_2^m$, $L \subset \mathbb{F}_2^m$ be a linear subspace of $\mathbb{F}_2^m$ such that (π^{-1}, L) satisfies the (C) property, and let $E_1, E_2 \neq \{\mathbf{0}_m\}$ be two linear subspaces of $\mathbb{F}_2^m$ such that $\pi(E_2) = E_1^\perp$. Furthermore, we assume that either $\dim(E_1 \cap L^\perp) = \dim(E_1) - 1$ or $E_1 = L^\perp$. Let $f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ be defined by*

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus \mathbf{1}_{L^\perp}(\mathbf{x}) \oplus \mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y}).$$

If (π^{-1}, L) *and* (π, E_1, E_2) *satisfy the properties* $(C1)$ *and* $(D1)-(D3)$, *respectively*, *then* f *is a bent function in* $\mathcal{CD}$ *outside* $\mathcal{M}^{\#}$.

Proof From Theorems 6 and 7, it follows that f is bent. From Theorem 1, it suffices to show that there is no m-dimensional subspace V of $\mathbb{F}_2^m \times \mathbb{F}_2^m := \mathbb{F}_2^n$ on which the second-order derivative $D_{\mathbf{a}}D_{\mathbf{b}}(f)$ vanishes, for any nonzero $\mathbf{a}, \mathbf{b} \in V$.

The second-order derivative of f with respect to $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2)$ and $\mathbf{b} = (\mathbf{b}_1, \mathbf{b}_2)$ in $V \subset \mathbb{F}_2^m \times \mathbb{F}_2^m$, can be written as

$$\begin{aligned} D_{\mathbf{a}}D_{\mathbf{b}}f(\mathbf{x},\mathbf{y}) &= \mathbf{x} \cdot \left(D_{\mathbf{a}_2}D_{\mathbf{b}_2}\pi(\mathbf{y})\right) \oplus \mathbf{a}_1 \cdot D_{\mathbf{b}_2}\pi(\mathbf{y} \oplus \mathbf{a}_2) \\ &\quad \oplus \mathbf{b}_1 \cdot D_{\mathbf{a}_2}\pi(\mathbf{y} \oplus \mathbf{b}_2) \oplus D_{\mathbf{a}_1}D_{\mathbf{b}_1}\mathbf{1}_{L^{\perp}}(\mathbf{x}) \oplus D_{\mathbf{a}}D_{\mathbf{b}}\mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y}). \end{aligned} \tag{11}$$

We know that $E_1 \times E_2$ is a subspace of $\mathbb{F}_2^n$ and therefore $\mathbb{F}_2^n = \bigcup_{\mathbf{u}_i \in U} (E_1 \times E_2) \oplus \mathbf{u}_i$, where U is a set of (disjoint) coset representatives w.r.t. $E_1 \times E_2$ and consequently $\left(\mathbf{u}_i \oplus (E_1 \times E_2)\right) \cap \left(\mathbf{u}_j \oplus (E_1 \times E_2)\right) = \emptyset$ for any $\mathbf{u}_i \neq \mathbf{u}_j \in U$. Any $\mathbf{a} \in \mathbb{F}_2^n$ can then be written as $\mathbf{a} = \mathbf{a}^{[1]} \oplus \mathbf{a}^{[2]}$, where $\mathbf{a}^{[1]} \in E_1 \times E_2$ and $\mathbf{a}^{[2]} \in U$. Thus, we have

$$D_{\mathbf{a}}D_{\mathbf{b}}\mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y}) = D_{\mathbf{a}^{[2]}}D_{\mathbf{b}^{[2]}}\mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y}). \tag{12}$$

If $|\{\mathbf{a}^{[2]} \in U : (\mathbf{a}^{[1]} \oplus \mathbf{a}^{[2]}) \in V\}| > 2$, then we select two nonzero vectors $\mathbf{a}, \mathbf{b} \in V$ such that $\mathbf{a}^{[2]}, \mathbf{b}^{[2]} \in U$, where $\mathbf{a} = \mathbf{a}^{[1]} \oplus \mathbf{a}^{[2]}$ and $\mathbf{b} = \mathbf{b}^{[1]} \oplus \mathbf{b}^{[2]}$. Thus, we have $\mathbf{a}^{[2]} \oplus \mathbf{b}^{[2]} \in U$, that is, $\mathbf{a}^{[2]} \oplus \mathbf{b}^{[2]} \notin E_1 \times E_2$. From Proposition 1 and (12), we have that

$$\deg\left(D_{\mathbf{a}}D_{\mathbf{b}}\mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y})\right) = m - 2.$$

Since the properties $(D1)$ and $(D3)$ are satisfied, we have that $\deg\left(D_{\mathbf{a}}D_{\mathbf{b}}(\pi(\mathbf{y}) \cdot \mathbf{x})\right) < m - 2$ and $\deg\left(D_{\mathbf{a}_1}D_{\mathbf{b}_1}\mathbf{1}_{L^{\perp}}(\mathbf{x})\right) \leq \dim(L) - 2 < m - 2$. From Eq. (11), it follows that

$$D_{\mathbf{a}}D_{\mathbf{b}}\, f \not\equiv 0.$$

If $|\{\mathbf{a}^{[2]} \in U : (\mathbf{a}^{[1]} \oplus \mathbf{a}^{[2]}) \in V\}| \leq 2$, then $|V \cap (E_1 \times E_2)| \geq 2^{m-1}$ (since $|V| = 2^m$). From property $(D1)$ and $\pi(E_2) = E_1^{\perp}$, we have

$$|V \cap (E_1 \times E_2)| \geq 2^{m-1} > |E_1| \;\text{ and }\; |V \cap (E_1 \times E_2)| \geq 2^{m-1} > |E_2|.$$

Moreover, we have that

$$|V \cap (E_1 \times \mathbf{0}_m)| \geq 2 \;\text{ and }\; |V \cap (\mathbf{0}_m \times E_2)| \geq 2,$$

which can be justified as follows. For instance, assuming that $|V \cap (E_1 \times \mathbf{0}_m)| < 2$ then $|V \cap (E_1 \times E_2)| \leq |E_2|$, which is in contradiction with $|V \cap (E_1 \times E_2)| \geq 2^{m-1} > |E_2|$. Hence, we can select two nonzero vectors $\mathbf{a}, \mathbf{b} \in V \cap (E_1 \times E_2)$ such that $\mathbf{a} = (\mathbf{a}_1, \mathbf{0}_m), \mathbf{b} = (\mathbf{0}_m, \mathbf{b}_2)$.

From Eq. (11), we have that

$$\begin{aligned} D_{\mathbf{a}}D_{\mathbf{b}}\, f(\mathbf{x},\mathbf{y}) &= \mathbf{a}_1 \cdot D_{\mathbf{b}_2}\pi(\mathbf{y}) \oplus D_{\mathbf{a}}D_{\mathbf{b}}\mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y}) \\ &= \mathbf{a}_1 \cdot D_{\mathbf{b}_2}\pi(\mathbf{y}), \end{aligned}$$

since $\mathbf{a}, \mathbf{b} \in V \cap (E_1 \times E_2)$ and therefore $D_{\mathbf{a}}D_{\mathbf{b}}\mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2} \equiv 0$. As the property $(D2)$ is satisfied, it holds that $\mathbf{a}_1 \cdot D_{\mathbf{b}_2}\pi \not\equiv const$. Thus, for any m-dimensional subspace V of $\mathbb{F}_2^m \times \mathbb{F}_2^m$ we can find nonzero $\mathbf{a}, \mathbf{b} \in V$ such that $D_{\mathbf{a}}D_{\mathbf{b}}\, f \not\equiv 0$.

Proposition 2 *Let $n = 2m$, m even, and s be a positive divisor of m such that m/s is odd. Let $\pi(y) = y^d$ be a permutation on $\mathbb{F}_{2^m}$ such that $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $\mathrm{wt}(d) \geq 3$. Let $L = \langle 1, \alpha, \ldots, \alpha^{s-1} \rangle$, where α is a primitive element of $\mathbb{F}_{2^s}$, $E_2 = \langle \alpha^{\frac{2^s-1}{3}}, \alpha^{\frac{2(2^s-1)}{3}} \rangle$ and $E_1 = E_2^{\perp}$. Then, the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x,y) = Tr_1^m(xy^d) + \mathbf{1}_{L^{\perp}}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y),\ x,y \in \mathbb{F}_{2^m},$$

is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$.

Proof From [Theorem 9] [2] we know that (π^{-1}, L) satisfies the (C) property. Since m is even and m/s is odd, we must have that s is even. Thus, $2^2 - 1 = 3 | 2^s - 1$ and furthermore E_2 is not only a vector space but also corresponds to a subfield $\{0, 1, \alpha^{\frac{2^s-1}{3}}, \alpha^{\frac{2(2^s-1)}{3}}\}$ of $\mathbb{F}_{2^s}$. Since π is a monomial permutation, it must map every subfield to itself, thus $\pi(E_2) = E_2 = E_1^{\perp}$. Since $\mathrm{wt}(d) \geq 3$, from [Proposition 5] [2], we have that $Tr_1^m(u\pi(y))$ admits no linear structures, for any $u \in \mathbb{F}_{2^m}^*$. Since $\dim(E_2) = 2$, we have that $\dim(E_1) = m - 2$. Hence, the conditions $(C1)$ and $(D1) - (D3)$ of Theorems 2 and 3, respectively, are satisfied. From Theorem 8, it follows that f is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$.

Example 1 Let $m = 6, s = 2$ and $d = 38$. One can easily verify that $d(2^s+1) \equiv 1 \ (mod\ 2^m - 1)$. With respect to the notation in Proposition 2, we have that for $E_2 = \mathbb{F}_{2^2}$ and $E_1 = E_2^{\perp}$ the function $f : \mathbb{F}_{2^6} \times \mathbb{F}_{2^6} \to \mathbb{F}_2$ defined by

$$f(x,y) = Tr_1^6(xy^{38}) + \mathbf{1}_{E_1}(x)(1 + \mathbf{1}_{E_2}(y)),\ x,y \in \mathbb{F}_{2^6},$$

is a bent function in $\mathcal{CD}$ and is outside $\mathcal{M}^{\#}$.

Remark 3 Especially, for $m = 6$, we inspected all possible choices for L, E_1 and E_2 such that either $\dim(L) = \dim(E_2) = 2$ or 3, (π^{-1}, L) satisfies the (C) property and $\pi(E_2) = E_1^{\perp}$, where $\pi(y) = y^{38}$ is a fixed permutation on $\mathbb{F}_{2^6}$. Using the mathematical software Sage, we were able to construct 500 functions $f \in \mathcal{CD}$ of the form (9) for the fixed permutation π given above. Furthermore, all of them are outside $\mathcal{M}^{\#}$. With the same notation as in the example above, we could also confirm that the function f is pairwise EA-inequivalent to the functions $f_1(x,y) = Tr_1^6(xy^{38}) + \mathbf{1}_{E_1}(x) \in \mathcal{C}$ and $f_2(x,y) = Tr_1^6(xy^{38}) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2} \in \mathcal{D}$. The question whether (some of) these functions induce distinct EA-equivalent classes is left open.

We now provide one more example of bent functions in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$, for larger n.

Example 2 Let $m = 9$ and $d = 284$. We note that $d(2^3+1) \mod (2^9-1) = 1$, $\mathrm{wt}(d) = 4$ and $d \mod (2^3-1) = 4$. Let $L = \langle 1, \alpha, \alpha^2 \rangle$ and $E_2 = \langle \alpha, \alpha^2 \rangle$, where α is a primitive element of $\mathbb{F}_{2^3}$ such that $\alpha^3 + \alpha + 1 = 0$. From [Theorem 9] [2], we know that (π^{-1}, L) satisfies the (C) property. We further observe that E_2 is a 2-dimensional subspace of $\mathbb{F}_{2^6}$. Let us show that $\pi(E_2) = E_2$. From $\alpha^3 = \alpha + 1$ we have that $\alpha^4 = \alpha + \alpha^2$. Because α is an element in the small field $\mathbb{F}_{2^3}$, we consider its exponent modulo $2^3 - 1$. Thus, we have that:

$$\begin{aligned} 0^d &= 0, \\ \alpha^d &= \alpha^4 = \alpha + \alpha^2, \\ (\alpha^2)^d &= (\alpha^2)^4 = \alpha^8 = \alpha, \\ (\alpha + \alpha^2)^d &= (\alpha^4)^d = \alpha^{16} = (\alpha^8)^2 = \alpha^2. \end{aligned}$$

In other words, $\pi(E_2) = E_2 = E_1^{\perp}$. Since $\mathrm{wt}(d) \geq 3$, from [Proposition 5] [2], we have that $Tr_1^m(u\pi)$ does not admit linear structures, for any $u \in \mathbb{F}_{2^m}^*$. Since $\dim(E_2) = 2$, we have that $\dim(E_1) = m - 2$. Hence the conditions $(C1)$ and $(D1) - (D3)$ of Theorems 2 and 3, respectively, are satisfied. From Theorem 8, it follows that the function $f : \mathbb{F}_{2^9} \times \mathbb{F}_{2^9} \to \mathbb{F}_2$ defined by

$$f(x, y) = Tr_1^9(xy^d) + \mathbf{1}_S(x, y),\ x, y \in \mathbb{F}_{2^9},$$

is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$, where $\mathbf{1}_S(x, y) = 1$ if and only if $(x, y) \in S$ and $S = (L^{\perp} \times \mathbb{F}_{2^m}) \bigtriangleup (E_1 \times E_2)$ (see Remark 2), and equals 0 otherwise. From Eq. (10), it is clear that $\mathbf{1}_S$ modifies the truth table of $g(x, y)$ at $2^{9+6} = 2^{15}$ positions. Furthermore, S is neither a linear nor an affine subspace.

With the same notation as in Example 2, Table 1 illustrates the bentness and algebraic degree of the Boolean function $f : \mathbb{F}_{2^9} \times \mathbb{F}_{2^9} \to \mathbb{F}_2$ defined as

$$f(x, y) = Tr_1^9(xy^d) + a_0\mathbf{1}_{L^{\perp}}(x) + a_1\mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) + a_2\delta_0(x), \tag{13}$$

for all possible values $a_0, a_1, a_2 \in \mathbb{F}_2$.

Proposition 3 *Let $n = 2m$, $m = 3l$ is odd and r be a positive integer such that $\gcd(r, 3l) = 3$ and $d(2^r + 1) \equiv 1 \pmod{2^m - 1}$ with $wt(d) \geq 3$. Let $L = \langle 1, \alpha, \alpha^2 \rangle$ and $E_2 = \langle \alpha, \alpha^2 \rangle$ and $E_1 = E_2^{\perp}$, where α is a primitive element of $\mathbb{F}_{2^3}$ such that $\alpha^3 + \alpha + 1 = 0$. Then the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x, y) = Tr_1^m(xy^d) + \mathbf{1}_{L^{\perp}}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y),\ x, y \in \mathbb{F}_{2^m},$$

is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$.

Proof Because $\gcd(r, 3l) = 3$ and $m/3 = l$ is odd, by [Theorem 9] [2], we have that (ϕ, L) satisfies the (C) property, where $\phi(x) = x^{2^r+1}$ is a permutation of $\mathbb{F}_{2^m}$ and $L = \langle 1, \alpha, \alpha^2 \rangle$. Furthermore, since $\pi(x) = x^d$ is the inverse of ϕ and $wt(d) \geq 3$, we know that $Tr_1^m(u\pi)$ has no nonzero linear structures for any $u \in \mathbb{F}_{2^m}^*$. Now, we prove that $d \mod (2^3 - 1) = 4$. It is well-known that $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$. Thus, $\gcd(2^{3l} - 1, 2^3 - 1) = 2^3 - 1$. Furthermore, if $a \equiv b \pmod{N}$ and $M|N$, then $a \equiv b \pmod{M}$. Hence, we have that $d(2^r + 1) \equiv 1 \pmod{2^3 - 1}$. Since $(2^3 - 1)|(2^r - 1) = (2^r + 1 - 2)$, we have that $2^r + 1 \equiv 2 \pmod{2^3 - 1}$. From the last two congruences, we conclude that $2d \equiv 1 \pmod 7$ and it is easy to compute that $d \equiv 4 \pmod 7$. From $\alpha^3 = \alpha + 1$ we have that $\alpha^4 = \alpha + \alpha^2$.

Table 1 Class inclusion in $\mathcal{M}^{\#}$ of the Boolean function f defined by Eq. (13)

$(a_0, a_1, a_2) \in \mathbb{F}_2^3$	Algebraic degree	Bent	Class
(0, 0, 0)	5	yes	$\mathcal{M}$
(0, 0, 1)	9	yes	$\mathcal{D}_0 \setminus \mathcal{M}^{\#}$
(0, 1, 0)	9	yes	$\mathcal{D} \setminus \mathcal{M}^{\#}$
(0, 1, 1)	9	no	-
(1, 0, 0)	5	yes	$\mathcal{C} \setminus \mathcal{M}^{\#}$
(1, 0, 1)	9	yes	$\mathcal{SC} \setminus \mathcal{M}^{\#}$
(1, 1, 0)	9	yes	$\mathcal{CD} \setminus \mathcal{M}^{\#}$
(1, 1, 1)	9	no	-

Because α is an element in the small field $\mathbb{F}_{2^3}$, we consider its exponent modulo $2^3 - 1$. Thus, we have that:

$$\begin{aligned} 0^d &= 0, \\ \alpha^d &= \alpha^4 = \alpha + \alpha^2, \\ (\alpha^2)^d &= (\alpha^2)^4 = \alpha^8 = \alpha, \\ (\alpha + \alpha^2)^d &= (\alpha^4)^d = \alpha^{16} = (\alpha^8)^2 = \alpha^2. \end{aligned}$$

In other words, $\pi(E_2) = E_2 = E_1^{\perp}$. Since $\dim(E_2) = 2$, we have that $\dim(E_1) = m - 2$. Hence, the conditions $(C1)$ and $(D1) - (D3)$ of Theorems 2 and 3, respectively, are satisfied. From Theorem 8, it follows that the function $f : \mathbb{F}_{2^9} \times \mathbb{F}_{2^9} \to \mathbb{F}_2$ defined by

$$f(x, y) = Tr_1^m(xy^d) + \mathbf{1}_{L^{\perp}}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y),\ x, y \in \mathbb{F}_{2^m},$$

is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$.

Using the software `Wolfram Mathematica`, we could confirm this result, and additionally some suitable values of r and d for different m are listed below.

m	r	d
9	3	284
9	6	228
15	3	18204
15	6	18652
15	9	14116
15	12	14564
21	3	1165084
21	6	935652
21	9	1197788
21	12	899364
21	15	1161500
21	18	932068

4.1 Addressing the normality of functions in $\mathcal{CD}$

In [20], it has been shown that if a Boolean function f in $2m$ variables is in the completed $\mathcal{PS}^+$ class, then it is weakly normal. In other words, if a function is weakly non-normal then it lies outside the completed $\mathcal{PS}^+$ class. Recall that a function $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$ is called *normal* (*weakly normal*) if there exists a flat of dimension m in $\mathbb{F}_2^{2m}$ such that f is constant (affine) on this flat. In this section, we discuss the weak normality of the functions in $\mathcal{CD}$ and propose an interesting research problem regarding them.

Remark 4 Depending on the choice of L, E_1 and E_2, the functions in $\mathcal{CD}$ are weakly normal in the majority of cases when $\pi(E_2) = E_2 = E_1^{\perp}$.

If $\dim(E_1 \cap L^\perp) = \dim(E_1) - 1$ or $E_1 = L^\perp$, we can have four possible situations $E_1 = L^\perp, L^\perp \subset E_1, E_1 \subset L^\perp$ and $\dim(E_1) = \dim(L^\perp) \wedge \dim(E_1 \cap L^\perp) = \dim(E_1) - 1$. We will consider these cases depending if $\pi(E_2) = E_2$ or $\pi(E_2) \neq E_2$.

1. Suppose that $\pi(E_2) = E_2 = E_1^\perp$.

   (a) $L^\perp = E_1$. If we consider an m-dimensional subspace $E_1 \times E_2$ of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, we have that $1 + \mathbf{1}_{E_2}(y) = 0$ for all $y \in E_2$. Thus, $\mathbf{1}_{E_1}(x)(1 + \mathbf{1}_{E_2}(y))$ is always equal to 0. On the other hand, because of the choice of E_1 and E_2, we have that $Tr_1^m(x\pi(y)) = 0$ because $x \in E_1$ and $\pi(E_2) = E_1^\perp$. Thus, $f|_{E_1 \times E_2} \equiv 0$.

   (b) $L^\perp \subset E_1$. If we take $\alpha \in \mathbb{F}_{2^m} \setminus E_1$, we have that $\mathbf{1}_{L^\perp}(x) = \mathbf{1}_{E_1}(x) = 0$ for all $x \in \alpha + E_1$. Thus, $\mathbf{1}_{L^\perp}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)$ vanishes on the m-dimensional flat $(\alpha + E_1) \times E_2$. Furthermore, for $(x, y) \in (\alpha + E_1) \times E_2$ (w.l.o.g. say $x = \alpha + e_1$) we have:

   $$Tr_1^m(x\pi(y)) = Tr_1^m((\alpha + e_1)\pi(y)) = Tr_1^m(\alpha\pi(y)) + \underbrace{Tr_1^m(e_1\pi(y))}_{=0 \text{ (same as in 1.)}} = Tr_1^m(\alpha\pi(y)).$$

   Since $\pi(E_2) = E_2$ we have that $\{Tr_1^m(\alpha\pi(y)) : y \in E_2\} = \{Tr_1^m(\alpha y) : y \in E_2\}$, which is obviously the truth table of an affine function. Thus, $f|_{(\alpha+E_1)\times E_2}$ is affine.

   (c) $E_1 \subset L^\perp$. If we take $\lambda \in L^\perp \setminus E_1$, we have that $\mathbf{1}_{L^\perp}(x) = 1$ and $\mathbf{1}_{E_1}(x) = 0$ for all $x \in \lambda + E_1$. Thus, $\mathbf{1}_{L^\perp}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) = 1$ on the m-dimensional flat $(\lambda + E_1) \times E_2$. Similarly as in 2., $Tr_1^m(x\pi(y))$ is affine on this flat. Thus, $f|_{(\lambda+E_1)\times E_2}$ is affine.

   (d) $\dim(E_1) = \dim(L^\perp) = m - \mu$, $\dim(E_1 \cap L^\perp) = m - \mu - 1$. Let $U = E_1 + L^\perp$ be the direct sum of E_1 and $L^\perp$. It holds that $\dim(U) = \dim(E_1) + \dim(L^\perp) - \dim(E_1 \cap L^\perp) = m - \mu + 1$. On the other hand, $\dim(E_2) = \mu$.

      i If $\mu = 2$ (all of the known constructions of functions in $\mathcal{D}$ outside $\mathcal{M}^\#$ have $\dim(E_2) = 2$), then $\dim(U) = m - 1$. Let $\alpha \in \mathbb{F}_{2^m} \setminus U$. If we consider the flat $A = (\alpha + U) \times \{0, \beta\}$, where $\beta \in E_2$, we have that $\mathbf{1}_{L^\perp}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) = 0$ and $Tr_1^m(x\pi(y))$ is affine for all $(x, y) \in A$. Thus, $f|_A$ is affine.

      ii Suppose $\mu > 2$. Again, we have that $\dim(U) = m - \mu + 1$ and $\dim(E_2) = \mu$. Let W be any $(\mu - 1)$-dimensional subspace of E_2. Then, $\mathbf{1}_{L^\perp}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)$ vanishes on $A = (\alpha, 0) + (U \times W)$, where $\alpha \notin U$. Let us consider the function $Tr_1^m(x\pi(y))$. If $x \in \alpha + U$, then w.l.o.g. $x = \alpha + x_u$ for some $x_u \in U$. We have that:

      $$Tr_1^m((\alpha + x_u)\pi(y))) = Tr_1^m(\alpha\pi(y)) + Tr_1^m(x_u\pi(y)).$$

      We note that if $x_u \in U \setminus E_1$, then $Tr_1^m(x_u\pi(y))$ is not necessarily an affine function and thus we cannot be certain if f is affine on A.

   To summarize, we have that f is weakly normal for the situations (a)-(d-i). In the case (d-ii), the question whether f is weakly normal remains open.

The case when $\pi(E_2) \neq E_2$, seems to be more difficult to analyse which leads to the following open problem.

Open problem With the same notation as in Definition 4, suppose that either $\pi(E_2) \neq E_2$ or $\pi(E_2) = E_2$ with $\dim(E_1) = \dim(L^{\perp}) = m - \mu$, $\mu > 2$. Is the function f defined by Eq. (9) weakly normal?

Remark 5 Apart from the exclusion from the $\mathcal{PS}$ class, it would be of interest to investigate whether bent functions in $\mathcal{CD}$ may also lie outside the completed classes $\mathcal{C}^{\#}$ and $\mathcal{D}^{\#}$. Apparently, by the definition of $\mathcal{CD}$, the members of $\mathcal{CD}$ cannot lie in $\mathcal{C}$ or $\mathcal{D}$ but due to the lack of indicators for the membership in their completed versions there is no rigorous conclusion concerning this question. Most likely, only certain instances of functions in $\mathcal{CD}$ are outside $\mathcal{C}^{\#}$ and $\mathcal{D}^{\#}$. This however remains to be shown and appears to be a difficult task.

5 Bent duals of functions in $\mathcal{SC}$ and $\mathcal{CD}$ and their application

In 1993, Carlet determined the bent duals of functions in $\mathcal{D}_0$ [Corollary 1] [3] and $\mathcal{D}$ [Proposition 1] [3]. In this section, we determine explicitly the bent duals of certain instances of functions in $\mathcal{C}$ not covered by Carlet's result. We also present another approach to determine the duals of certain functions in $\mathcal{D}$ and show that these can be constructed from the $\mathcal{C}$ and $\mathcal{M}$ class. The duals of certain functions in $\mathcal{SC}$ and $\mathcal{CD}$ are also specified and it is shown that these can be used to construct bent functions in $\mathcal{B}_{n+2}$ by concatenating four suitable bent functions in $\mathcal{B}_n$ that stem from these classes. Moreover, we show that the resulting bent functions are outside the $\mathcal{M}^{\#}$ class.

We recall that, by [Corollary 1] [3], the following result gives us the bent duals of functions in $\mathcal{D}_0$.

Proposition 4 [3] *Let $n = 2m$ and π be a permutation on $\mathbb{F}_{2^m}$. Let $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a bent function in the $\mathcal{D}_0$ class defined by*

$$f(x, y) = x\pi(y) + \delta_0(x), \ x, y \in \mathbb{F}_{2^m}. \tag{14}$$

Then, its dual f^* is also a bent function in $2m$ variables defined by $f^*(x, y) = y\pi^{-1}(x) + \delta_0(y)$.

Throughout this section we will be using the notion of (P_U) property, which is defined as follows [21].

Definition 5 Let $g \in \mathcal{B}_n$ be any Boolean function. We say that g satisfies the property (P_U) with the defining set $U = \{u_1, \ldots, u_t\} \subseteq \mathbb{F}_{2^n}$ if there exists $g_1, \ldots, g_t \in \mathcal{B}_n$ such that $g\left(x + \sum_{i=1}^{t} w_i u_i\right) = g(x) + \sum_{i=1}^{t} w_i g_i(x)$ for any $\mathbf{w} = (w_1, \ldots, w_t) \in \mathbb{F}_2^t$. Equivalently, g is said to satisfy the property (P_U) with the defining set $U = \{u_1, \ldots, u_t\} \subseteq \mathbb{F}_{2^n}$ if $D_{u_i} D_{u_j} g \equiv 0$ for any $1 \leq i < j \leq t$.

5.1 Bent duals of certain functions in $\mathcal{C}$ and $\mathcal{D}$.

In what follows, we determine the bent duals of certain instances of bent functions in $\mathcal{C}$ and $\mathcal{D}$.

Proposition 5 ($\mathcal{C}$ instance) *Let $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a bent function defined by*

$$f(x,y) = Tr_1^m(xy^d) + \prod_{i\in I}(Tr_1^m(\alpha^i x) + 1),\ x,y \in \mathbb{F}_{2^m}, \tag{15}$$

where α is a primitive element of $\mathbb{F}_{2^s}$, $I \subset \{0,\dots,s-1\}$, s is a positive divisor of m such that m/s is odd, $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $\mathrm{wt}(d) \geq 3$. Then, the dual $f^* : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ of f is defined by

$$f^*(x,y) = Tr_1^m(x^{2^s+1}y) + \prod_{i\in I}(Tr_1^m(y(\alpha^i x + \alpha^i x^{2^s} + \alpha^{2i})) + 1),\ x,y \in \mathbb{F}_{2^m}.$$

Proof By [Lemma 4.15] [21], it holds that the function $(x,y) \mapsto Tr_1^m(x^{2^s+1}y)$ satisfies the (P_U) property with the defining set $U = \{(\alpha^i, 0) : i = 0,\dots,s-1\}$ (we note that the general condition is that for all $(u_1,u_2),(v_1,v_2) \in U \subset \mathbb{F}_{2^s} \times \mathbb{F}_{2^s}$ it holds that $u_1v_2 + u_2v_1 = 0$ and $Tr_1^m(u_1^2v_2 + v_1^2u_2) = 0$). Thus, by [Theorem 4.17] [21], its dual is defined by

$$f^*(x,y) = Tr_1^m(x^{2^s+1}y) + \prod_{i\in I}(Tr_1^m(y(\alpha^i x + \alpha^i x^{2^s} + \alpha^{2i})) + 1),\ x,y \in \mathbb{F}_{2^m}.$$

Notice that $\prod_{i\in I}(Tr_1^m(\alpha^i x) + 1)$ corresponds to the indicator function $\mathbb{F}_{2^m} \ni x \mapsto \mathbf{1}_{L^\perp}(x)$ where $L = \langle \alpha^i : i \in I\rangle$. Furthermore, by [Theorem 5.8-(ii)] [22], we can take $L = \langle c_1,\dots,c_l\rangle$ where $c_i \in \mathbb{F}_{2^s}^*$ for $i = 1,\dots,l$, so that (π^{-1}, L) satisfies the (C) property, where π is defined as above.

To determine the duals of functions in the $\mathcal{D}$ class, we will use a secondary construction of bent functions in bivariate form introduced in [21]:

Construction 1 [21] Let $U = \{\mathbf{u}_i = (u_{1,i}, u_{2,i}) : 1 \leq i \leq t\} \subseteq \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, where $1 \leq t \leq m$. Let $g : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ be any bent function function whose dual g^* satisfies the (P_U) property with the defining set U. Let $F(X_1,\dots,X_t)$ be any reduced polynomial in $\mathbb{F}_2[X_1,\dots,X_t]$. Then the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by

$$f(x,y) = g(x,y) + F(Tr_1^m(u_{1,1}x + u_{1,2}y),\dots,Tr_1^m(u_{t,1}x + u_{t,2}y))$$

is bent and its dual (by [Theorem 2.3] [23]) is defined by

$$f^*(x,y) = g^*(x,y) + F(D_{\mathbf{u}_1}g^*(x,y),\dots,D_{\mathbf{u}_t}g^*(x,y)). \tag{16}$$

Let $\pi(y) = y^d$ and E_2 be a vector subspace corresponding to a subfield in $\mathbb{F}_{2^s}$, where s is a positive divisor of m such that m/s is odd, $d(2^s+1) \equiv 1$ (*mod* 2^m-1) and $\mathrm{wt}(d) \geq 3$. The following lemma shows that the duals g^* of bent functions g in $2m$ variables, defined by $g(x,y) = Tr_1^m(xy^d) + \mathbf{1}_{E_2}(y)$, $x,y \in \mathbb{F}_{2^m}$, satisfy the (P_U) property with the defining set $U = \{0\} \times \mathbf{b}(E_2)$, where $\mathbf{b}(E_2)$ is a basis of E_2.

Lemma 1 *Let E_2 be a vector space in $\mathbb{F}_{2^m}$ which corresponds to a subfield in $\mathbb{F}_{2^s}$, where s is a positive divisor of m such that m/s is odd, $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $\mathrm{wt}(d) \geq 3$. Let $g : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a bent function defined by*

$$g(x,y) = Tr_1^m(xy^d) + \mathbf{1}_{E_2}(y),\ x,y \in \mathbb{F}_{2^m}.$$

Then, its dual is defined by

$$g^*(x,y) = Tr_1^m(x^{2^s+1}y) + \mathbf{1}_{E_2}(x^{2^s+1}),$$

and furthermore $D_aD_bg^* \equiv 0$ *for all* $a,b \in U = \{0\} \times \mathbf{b}(E_2)$ *or* $\mathbf{b}(E_2) \times \{0\}$.

Proof Obviously, the function g is a Maiorana-McFarland function of the form $g(x,y) = Tr_1^m(x\pi(y)) + h(y)$ with $\pi(y) = y^d$ and $h(y) = \mathbf{1}_{E_2}(y)$. Thus, its dual is of the form

$$g^*(x,y) = Tr_1^m(y\pi^{-1}(x)) + h(\pi^{-1}(x)) = Tr_1^m(x^{2^s+1}y) + \mathbf{1}_{E_2}(x^{2^s+1}),\ x,y \in \mathbb{F}_{2^m}.$$

Let $a,b \in U$ and $x,y \in \mathbb{F}_{2^m}$ be arbitrary. Clearly,

$$D_aD_bg^*(x,y) = D_aD_bTr_1^m(yx^{2^s+1}) + D_aD_b\mathbf{1}_{E_2}(x^{2^s+1}).$$

By [Lemma 4.15] [21], it holds that $D_aD_bTr_1^m(yx^{2^s+1}) = 0$. On the other hand, because $\mathbf{1}_{E_2}(x^{2^s+1})$ depends only on x, it is easy to note that $D_aD_b\mathbf{1}_{E_2}(x^{2^s+1}) = 0$ for all $x \in \mathbb{F}_{2^m}$ if $a,b \in \{0\} \times E_2$. Hence, g^* satisfies the (P_U) property with the defining set $U = \{0\} \times \mathbf{b}(E_2)$. On the other hand, if $U = \mathbf{b}(E_2) \times \{0\}$, then

$$D_aD_b\mathbf{1}_{E_2}(x^{2^s+1}) = \mathbf{1}_{E_2}(x^{2^s+1}) + \mathbf{1}_{E_2}((x+a)^{2^s+1}) + \mathbf{1}_{E_2}((x+b)^{2^s+1}) + \mathbf{1}_{E_2}((x+a+b)^{2^s+1}).$$

Now if $x \in E_2$, then $x^{2^s+1}, (x+a)^{2^s+1}, (x+b)^{2^s+1}, (x+a+b)^{2^s+1} \in E_2$ for all $a,b \in \mathbf{b}(E_2)$ and thus $D_aD_b\mathbf{1}_{E_2}(x^{2^s+1}) = 0$. If $x \notin E_2$, as E_2 is a field and $x \mapsto x^{2^s+1}$ is a monomial permutation, the elements of E_2 are mapped to itself and thus $x^{2^s+1} \notin E_2$. Furthermore, since $a \in \mathbf{b}(E_2)$, it must hold that $x+a \notin E_2$ and similarly as before $(x+a)^{2^s+1} \notin E_2$. The same argument holds for $(x+b)^{2^s+1}$ and $(x+a+b)^{2^s+1}$. Thus, $D_aD_b\mathbf{1}_{E_2}(x^{2^s+1}) = 0$ for all $x \in \mathbb{F}_{2^m}$.

Now, as a direct consequence of Construction 1 and Lemma 1, we have the following result which is used to provide the dual of certain instances of bent functions in $\mathcal{D}$, namely in Theorem 10.

Proposition 6 *With the same notation as in Lemma 1, let* $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ *be defined by*

$$f(x,y) = g(x,y) + \mathbf{1}_{E_1}(x),\ x,y \in \mathbb{F}_{2^m},$$

where $g(x,y) = Tr_1^m(xy^d) + \mathbf{1}_{E_2}(y)$ *and* $E_1 = E_2^\perp$. *Then,* f *is bent and its dual is defined by*

$$f^*(x,y) = g^*(x,y) + \prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(y(\omega x^{2^s} + \omega x + \omega^2)) + 1),\ x,y \in \mathbb{F}_{2^m}.$$

Proof By Lemma 1, g^* satisfies the property (P_U) with the defining set $\mathbf{b}(E_2) \times \{0\}$. Thus, by Construction 1, the function f defined by

$$f(x,y) = g(x,y) + \prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(\omega x) + 1) = g(x,y) + \mathbf{1}_{E_1}(x)$$

is bent. Let us compute the first order derivative of g^* in $(\omega, 0)$ for $\omega \in \mathbf{b}(E_2)$.

$$\begin{aligned} D_{(\omega,0)}g^*(x,y) &= g^*(x,y) + g^*(x+\omega,y) \\ &= Tr_1^m(x^{2^s+1}y) + \mathbf{1}_{E_2}(x^{2^s+1}) + Tr_1^m((x+\omega)^{2^s+1}y) + \mathbf{1}_{E_2}((x+\omega)^{2^s+1}) \\ &= Tr_1^m(y(\omega x^{2^s} + \omega x + \omega^2). \end{aligned}$$

Thus, by Construction 1, the dual f^* of f is defined by

$$f^*(x,y) = g^*(x,y) + \prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(y(\omega x^{2^s} + \omega x + \omega^2)) + 1),\ x,y \in \mathbb{F}_{2^m}.$$

In [24] the author determines the duals for functions obtained by the following secondary construction of bent functions.

Theorem 9 [*Theorem* 4] [24] *Let n be any positive even integer. Let f_1,f_2 and f_3 be three bent functions on $\mathbb{F}_2^n$. Denote by f_4 the function $f_1+f_2+f_3$ and by σ the function $f_1f_2+f_1f_3+f_2f_3$. Now, if f_4 is bent and if $f_4^* = f_1^* + f_2^* + f_3^*$, then σ is bent and $\sigma^* = f_1^*f_2^* + f_1^*f_3^* + f_2^*f_3^*$.*

We will now prove that certain functions in $\mathcal{D}$ can be expressed in terms of Theorem 9 and as a direct consequence we will be able to determine the duals of the corresponding functions in $\mathcal{SC}$ and $\mathcal{CD}$.

Theorem 10 ($\mathcal{D}$ instances) *With the same notation as in Theorem 9, let $n = 2m$, s be a positive divisor of m such that m/s is odd, and d a positive integer such that $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $\mathrm{wt}(d) \geq 3$. Let E_2 be a subfield of $\mathbb{F}_{2^s}$ and $E_1 = E_2^{\perp}$. Let $f_i : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$, $i = 1,2,3,4$, be defined by:*

$$\begin{aligned} f_1(x,y) &= Tr_1^m(xy^d), \\ f_2(x,y) &= Tr_1^m(xy^d) + \mathbf{1}_{E_1}(x), \\ f_3(x,y) &= Tr_1^m(xy^d) + \mathbf{1}_{E_2}(y), \\ f_4(x,y) &= f_1(x,y) + f_2(x,y) + f_3(x,y). \end{aligned}$$

Then, using $\sigma = f_1f_2 + f_1f_3 + f_2f_3$, the function $\sigma(x,y) = Tr_1^m(xy^d) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)$ is bent and its dual is defined by

$$\sigma^*(x,y) = Tr_1^m(x^{2^s+1}y) + \prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(\omega x^{2^s+1}) + 1)(Tr_1^m(y(\omega x + \omega x^{2^s} + \omega^2)) + 1). \tag{17}$$

Proof Firstly, by Proposition 6, we have that f_4 is bent and its dual f_4^* is defined by

$$f_4^* = Tr_1^m(x^{2^s+1}y) + \underbrace{\prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(\omega x^{2^s+1}) + 1)}_{\psi_1(x)} + \underbrace{\prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(y(\omega x + \omega x^{2^s} + \omega^2)) + 1)}_{\psi_2(x,y)}. \tag{18}$$

From Proposition 5 and Lemma 1, it is easy to compute that $f_1^* + f_2^* + f_3^* = f_4^*$. Thus, by Theorem 9, the function σ is bent. Furthermore,

$$\begin{aligned}\sigma(x,y) &= f_1(x,y)f_2(x,y) + f_1(x,y)f_3(x,y) + f_2(x,y)f_3(x,y)\\ &= Tr_1^m(xy^d) + Tr_1^m(xy^d)\mathbf{1}_{E_1}(x) + Tr_1^m(xy^d) + Tr_1^m(xy^d)\mathbf{1}_{E_2}(y) +\\ &+ Tr_1^m(xy^d) + Tr_1^m(xy^d)\mathbf{1}_{E_2}(y) + Tr_1^m(xy^d)\mathbf{1}_{E_1}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)\\ &= Tr_1^m(xy^d) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y),\end{aligned}$$

that is $\sigma \in \mathcal{D}$, and its dual is defined by:

$$\begin{aligned}\sigma^*(x,y) &= f_1^*(x,y)f_2^*(x,y) + f_1^*(x,y)f_3^*(x,y) + f_2^*f_3^*(x,y)\\ &= Tr_1^m(x^{2^s+1}y) + \psi_1(x)\psi_2(x,y)\\ &= Tr_1^m(x^{2^s+1}y) + \prod_{\omega\in\mathbf{b}(E_2)} (Tr_1^m(\omega x^{2^s+1}) + 1)(Tr_1^m(y(\omega x + \omega x^{2^s} + \omega^2)) + 1).\end{aligned}$$

The above results are used in the next section for specifying the duals of bent functions in $\mathcal{SC}$ and $\mathcal{CD}$.

5.2 Duals of bent functions in $\mathcal{SC}$ and $\mathcal{CD}$

Using a similar approach as in Proposition 6, we will show that certain functions ("parts" of functions in $\mathcal{SC}$ and $\mathcal{CD}$) satisfy the (P_U) property with some defining set, and consequently we will be able to determine the duals of the corresponding functions in $\mathcal{SC}$ and $\mathcal{CD}$.

Proposition 7 ($\mathcal{SC}$ case) *Let $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a bent function defined by*

$$f(x,y) = Tr_1^m(xy^d) + \prod_{i\in I} \left(Tr_1^m(\alpha^i x) + 1\right) + \delta_0(x),\ x,y \in \mathbb{F}_{2^m}, \tag{19}$$

where α is a primitive element of $\mathbb{F}_{2^s}$, $I \subset \{0,1,\ldots,s-1\}$, s is a positive divisor of m such that m/s is odd, $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $\mathrm{wt}(d) \geq 3$. Then, the dual $f^* : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ of f is defined by

$$f^*(x,y) = Tr_1^m(x^{2^s+1}y) + \prod_{i\in I} \left(Tr_1^m(y(\alpha^i x + \alpha^i x^{2^s} + \alpha^{2i})) + 1\right) + \delta_0(y),\ x,y \in \mathbb{F}_{2^m}.$$

Proof Let $g(x,y) = Tr_1^m(xy^d) + \delta_0(x)$. Then, by Proposition 4, we have that $g^*(x,y) = Tr_1^m(yx^{2^s+1}) + \delta_0(y)$. We will prove that g^* satisfies the (P_U) property with the defining set $U = \{\alpha^i : i \in I\} \times \{0\}$. Let $a, b \in U$ and $x, y \in \mathbb{F}_{2^m}$ be arbitrary. Then,

$$D_aD_bg^*(x,y) = D_aD_b(Tr_1^m(x^{2^s+1}y)) + D_aD_b(\delta_0(y)) = 0,$$

because the first summand is equal to zero by [Lemma 4.15] [21] and the second summand is equal to zero since the y-coordinate of a and b is equal to zero. Thus, by [Theorem 4.17] [21], the function f is indeed bent and its dual is defined by

$$f^*(x,y) = Tr_1^m(x^{2^s+1}y) + \prod_{i\in I} \left(Tr_1^m(y(\alpha^i x + \alpha^i x^{2^s} + \alpha^{2i})) + 1\right) + \delta_0(y),\ x,y \in \mathbb{F}_{2^m}.$$

Using a similar method, we determine the duals of bent functions in $\mathcal{CD}$.

Theorem 11 ($\mathcal{CD}$ case) *With the same notation as in Theorem 10, let $\sigma : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be defined by $\sigma(x,y) = Tr_1^m(xy^d) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)$, $x,y \in \mathbb{F}_{2^m}$. Let $L \subset E_2$ be any subspace of $\mathbb{F}_{2^m}$ of dimension at least 2. Then, the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x,y) = \sigma(x,y) + \prod_{\omega \in \mathbf{b}(L)} (Tr_1^m(\omega x) + 1),\ x,y \in \mathbb{F}_{2^m},$$

is bent and its dual is defined by

$$f^*(x,y) = \sigma^*(x,y) + \prod_{\omega \in \mathbf{b}(L)} (Tr_1^m(y(\omega x + \omega x^{2^s} + \omega^2)) + 1),\ x,y \in \mathbb{F}_{2^m}, \tag{20}$$

where $\mathbf{b}(L)$ is the basis of L.

Proof Let $a,b \in \mathbf{b}(L) \times \{0\}$ and $x,y \in \mathbb{F}_{2^m}$ be arbitrary. From Theorem 10, we have that $D_aD_b\sigma^*(x,y) = D_aD_bTr_1^m(x^{2^s+1}y) + D_aD_b\psi_1(x)\psi_2(x,y)$, where ψ_1,ψ_2 are defined by Eq. (18). By [Lemma 4.15] [21], we have that $D_aD_bTr_1^m(x^{2^s+1}y) = 0$. Let $\lambda \in \mathbf{b}(L) \subset E_2$ be arbitrary. Then,

$$\psi_2(x+\lambda,y) = \prod_{\omega \in \mathbf{b}(E_2)} (Tr1^m(y(\omega x^{2^s} + \omega\lambda + \omega x + \omega\lambda + \omega^2)) + 1) = \psi_2(x,y)$$

and thus $\psi_2(x) = \psi_2(x+a) = \psi_2(x+b) = \psi_2(x+a+b)$. Hence,

$$\begin{aligned} D_aD_b\psi_1(x)\psi_2(x,y) &= \psi_1(x)\psi_2(x,y) + \psi_1(x+a)\psi_2(x+a,y) \\ &\quad + \psi_1(x+b)\psi_2(x+b,y) + \psi_1(x+a+b)\psi_2(x+a+b,y)) \\ &= \psi_2(x,y)(\psi_1(x) + \psi_1(x+a) + \psi_1(x+b) + \psi_1(x+a+b) \\ &= \psi_2(x,y)(\mathbf{1}_{E_2}(x^{2^s+1}) + \mathbf{1}_{E_2}((x+a)^{2^s+1}) + \\ &\quad \mathbf{1}_{E_2}((x+b)^{2^s+1}) + \mathbf{1}_{E_2}((x+a+b)^{2^s+1})). \end{aligned}$$

Because $x \mapsto x^{2^s+1}$ is a monomial permutation and E_2 is a field, it holds that $(x+\lambda)^{2^s+1} \in E_2$ if and only if $x+\lambda \in E_2$, and for $\lambda \in E_2$, it is equivalent to the fact that $x \in E_2$. Thus, as $a,b \in \mathbf{b}(L) \subset E_2$, we have that

$$D_aD_b\psi_1(x)\psi_2(x,y) = \psi_2(x,y)(\mathbf{1}_{E_2}(x^{2^s+1}) + \mathbf{1}_{E_2}(x^{2^s+1}) + \mathbf{1}_{E_2}(x^{2^s+1}) + \mathbf{1}_{E_2}(x^{2^s+1})) = 0,$$

for all $x,y \in \mathbb{F}_{2^m}$. Hence, σ^* satisfies the (P_U) property with the defining set $\mathbf{b}(L) \times \{0\}$. Consequently, by Construction 1, the function f is bent and its dual is defined by Eq. (20).

5.3 Two bent 4-decompositions

In [16], the authors completely describe the 4-decomposition (f_1,f_2,f_3,f_4), where $f_i \in \mathcal{B}_{n-2}$, of a bent function $f \in \mathcal{B}_n$ in terms of the second order derivatives. More precisely, the notation (f_1,f_2,f_3,f_4) means that $f_1,\ldots,f_4 \in \mathcal{B}_{n-2}$ are defined on the four cosets of $V = \langle \mathbf{a},\mathbf{b} \rangle^\perp$, thus f_i are defined on $\mathbf{0}_n \oplus V, \mathbf{a} \oplus V, \mathbf{b} \oplus V, (\mathbf{a} \oplus \mathbf{b}) \oplus V$, respectively. Such a decomposition is called a *bent 4-decomposition* when all f_i ($i \in [1,4]$), are bent; a *semi-bent 4-decomposition* when all f_i ($i \in [1,4]$) are semi-bent; a *5-valued 4-decomposition* when all f_i ($i \in [1,4]$) are 5-valued spectra functions so that $W_{f_i} \in \{0, \pm 2^{(n-2)/2}, \pm 2^{n/2}\}$

[16]. These are the only possibilities and we strictly have that all the restrictions f_i have the same spectral profile.

For our purpose, we are only interested in bent 4-decomposition and its characterization in terms of the duals of f_i. Notice that the canonical decomposition of f corresponds to the choice of $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$ given by $\mathbf{a} = (0, 0, \ldots, 0, 0, 1)$ and $\mathbf{b} = (0, 0, \ldots, 0, 1, 0)$ in which case the restrictions f_i are given as: $f_1(\mathbf{x}) = f(\mathbf{x}, 0, 0), \cdots, f_4(\mathbf{x}) = f(\mathbf{x}, 1, 1)$, where $\mathbf{x} \in \mathbb{F}_2^{n-2}$. In this case, we use a shorthand notation $f = f_1 || f_2 || f_3 || f_4$ to denote this canonical decomposition of f.

Theorem 12 [17] *Let $f \in \mathcal{B}_n$ be a bent function, for even $n \geq 4$. Let $\alpha, \beta \in \mathbb{F}_{2^n}^*$ be two distinct elements and $V = \langle \alpha, \beta \rangle^{\perp}$. If we denote by $(f_1, \ldots, f_4)$ the 4-decomposition of f with respect to V, then $(f_1, \ldots, f_4)$ is a bent 4-decomposition if and only if $f_1^* + f_2^* + f_3^* + f_4^* = 1$.*

Using this result, we show that bent functions stemming from $\mathcal{M}, \mathcal{C}, \mathcal{D}_0$ and $\mathcal{SC}$ form a bent 4-decomposition. To satisfy the conditions of Theorem 1, we note that f_1 is defined by $f_1(x, y) = Tr_1^m(xy^d) + 1$ instead of $Tr_1^m(xy^d)$, so that the sum $f_1^* + f_2^* + f_3^* + f_4^*$ equals 1 (otherwise it would be 0).

Theorem 13 *Let $n = 2m$, s be a positive divisor of m such that m/s is odd, and d a positive integer such that $d(2^s + 1) \equiv 1 \pmod{2^m - 1}$ and $\mathrm{wt}(d) \geq 3$. Let $f_1 : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be defined by $f_1(x, y) = Tr_1^m(xy^d) + 1$, and f_2, f_3 and f_4 be defined by Eqs. (14), (15) and (19), respectively. Then, $f = (f_1, \ldots, f_4)$ is a bent function in $n + 2$ variables.*

Proof Firstly, we note that $f_1^*(x, y) = Tr_1^m(x^{2^s+1}y) + 1$, $x, y \in \mathbb{F}_{2^m}$. From Propositions 5, 4 and 7 it is easy to compute that $f_1^*(x, y) + f_2^*(x, y) + f_3^*(x, y) + f_4^*(x, y) = 1$ for all $x, y \in \mathbb{F}_{2^m}$. Thus, by Theorem 1 it holds that $f = (f_1, \ldots, f_4)$ is a bent 4-decomposition, i.e., it follows that f is a bent function in $n + 2$ variables.

Remark 6 Explicitly, let $f = (f_1, f_2, f_3, f_4)$ be defined as in Theorem 1, then by [Corollary 1] [25], we can write $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^2} \to \mathbb{F}_2$ as

$$f(x, y, z_1, z_2) = f_1(x, y) + z_1(f_1 + f_3)(x, y) + z_2(f_1 + f_2)(x, y),\ x, y \in \mathbb{F}_{2^m}, z_1, z_2 \in \mathbb{F}_2, \tag{21}$$

which corresponds to the concatenation $f = f_1 || f_2 || f_3 || f_4$. Let f_1, f_2, f_3, f_4 and f be defined as in Theorem 13, then Eq. (21) evaluates to:

$$f(x, y, z_1, z_2) = Tr_1^m(xy^d) + z_1 \mathbf{1}_{L^{\perp}}(x) + z_2 \delta_0(x) + z_1 + z_2 + 1,\ x, y \in \mathbb{F}_{2^m}, z_1, z_2 \in \mathbb{F}_2.$$

Moreover, it turns out that bent functions described in Theorem 13 do not belong to the completed $\mathcal{M}$ class. For convenience, we use the vector space representation below.

Theorem 14 *Let $n = 2m$ be even and $f \in \mathcal{B}_n$ be given as in Theorem 13 so that*

$$f(\mathbf{x}, \mathbf{y}, z_1, z_2) = \phi(\mathbf{y}) \cdot \mathbf{x} \oplus z_1 \mathbf{1}_{L^{\perp}}(\mathbf{x}) \oplus z_2 \delta_0(\mathbf{x}) \oplus z_1 \oplus z_2 \oplus 1,\ \mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m, z_1, z_2 \in \mathbb{F}_2. \tag{22}$$

If $\mathbf{c} \cdot \phi$ has no nonzero linear structures for any $\mathbf{c} \in \mathbb{F}_2^m \setminus \{\mathbf{0}_m\}$, then f is outside $\mathcal{M}^{\#}$.

Proof For convenience, we denote $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, a_3, a_4), \mathbf{b} = (\mathbf{b}_1, \mathbf{b}_2, b_3, b_4) \in \mathbb{F}_2^m \times \mathbb{F}_2^m \times \mathbb{F}_2 \times \mathbb{F}_2$. Let V be an arbitrary $(m + 1)$-dimensional subspace of $\mathbb{F}_2^{n+2}$.

It is sufficient to show that for an arbitrary $(m+1)$-dimensional subspace V of $\mathbb{F}_2^{n+2}$ one can always find two vectors $\mathbf{a}, \mathbf{b} \in V$ such that $D_{(\mathbf{a}_1,\mathbf{a}_2,a_3,a_4)}D_{(\mathbf{b}_1,\mathbf{b}_2,b_3,b_4)}f(\mathbf{x},\mathbf{y},z_1,z_2) \neq 0$ for some $(\mathbf{x},\mathbf{y},z_1,z_2) \in \mathbb{F}_2^{n+2}$.

We have

$$\begin{aligned} D_{(\mathbf{a}_1,\mathbf{a}_2,a_3,a_4)}D_{(\mathbf{b}_1,\mathbf{b}_2,b_3,b_4)}f(\mathbf{x},\mathbf{y},z_1,z_2) = {} & D_{\mathbf{a}_2}D_{\mathbf{b}_2}(\phi(\mathbf{y}))\cdot\mathbf{x} \\ & \oplus D_{\mathbf{b}_2}(\phi(\mathbf{y}\oplus\mathbf{a}_2))\cdot\mathbf{a}_1 \oplus D_{\mathbf{a}_2}(\phi(\mathbf{y}\oplus\mathbf{b}_2))\cdot\mathbf{b}_1 \\ & \oplus z_2 D_{\mathbf{a}_1}D_{\mathbf{b}_1}\delta_0(\mathbf{x}) \oplus z_1 D_{\mathbf{a}_1}D_{\mathbf{b}_1}\mathbf{1}_{L^\perp}(\mathbf{x}) \oplus T(\mathbf{x}), \end{aligned} \tag{23}$$

where

$T(\mathbf{x}) = a_3 D_{\mathbf{b}_1}\mathbf{1}_{L^\perp}(\mathbf{x}\oplus\mathbf{a}_1) \oplus b_3 D_{\mathbf{a}_1}\mathbf{1}_{L^\perp}(\mathbf{x}\oplus\mathbf{b}_1) \oplus a_4 D_{\mathbf{b}_1}\delta_0(\mathbf{x}\oplus\mathbf{a}_1) \oplus b_4 D_{\mathbf{a}_1}\delta_0(\mathbf{x}\oplus\mathbf{b}_1)$.

There are three cases to be considered.

1. Let $|\{\mathbf{x}\in\mathbb{F}_2^m : (\mathbf{x},\mathbf{y},z_1,z_2)\in V\}| > 2$. We can select two vectors $\mathbf{a},\mathbf{b}\in V$ such that $\mathbf{a}_1 \neq \mathbf{0}_m$, $\mathbf{b}_1 \neq \mathbf{0}_m$ and $\mathbf{a}_1 \neq \mathbf{b}_1$. From Eq. (23), we have

   $$D_{(\mathbf{a}_1,\mathbf{a}_2,a_3,a_4)}D_{(\mathbf{b}_1,\mathbf{b}_2,b_3,b_4)}f(\mathbf{x},\mathbf{y},z_1,z_2) = z_2 D_{\mathbf{a}_1}D_{\mathbf{b}_1}\delta_0(\mathbf{x}) \oplus M(x,y,z_1),$$

   where
   $M(x,y,z_1) = D_{\mathbf{a}_2}D_{\mathbf{b}_2}(\phi(\mathbf{y}))\cdot\mathbf{x} \oplus D_{\mathbf{b}_2}(\phi(\mathbf{y}\oplus\mathbf{a}_2))\cdot\mathbf{a}_1 \oplus D_{\mathbf{a}_2}(\phi(\mathbf{y}\oplus\mathbf{b}_2))\cdot\mathbf{b}_1 \oplus z_1 D_{\mathbf{a}_1}D_{\mathbf{b}_1}\mathbf{1}_{L^\perp}(\mathbf{x}) \oplus T(\mathbf{x})$.
   As $D_{\mathbf{a}_1}D_{\mathbf{b}_1}\delta_0 \not\equiv 0$, it must hold that $D_{\mathbf{a}}D_{\mathbf{b}}f \not\equiv 0$.
2. Let $|\{\mathbf{x}\in\mathbb{F}_2^m : (\mathbf{x},\mathbf{y},z_1,z_2)\in V\}| = 2$. We select $\mathbf{a} = (\mathbf{a}_1,\mathbf{a}_2,a_3,a_4) \in V$ such that $\mathbf{a}_1 \neq \mathbf{0}_m$. Since $|V| = 2^{m+1}$, we can select $\mathbf{b} = (\mathbf{b}_1,\mathbf{b}_2,b_3,b_4) \in V$ such that $\mathbf{b}_1 = \mathbf{0}_m$ and $\mathbf{b}_2 \neq \mathbf{0}_m$. Notice that $\mathbf{b}_1 = \mathbf{0}_m$ implies that $D_{\mathbf{a}_2}(\phi(\mathbf{y}\oplus\mathbf{b}_2))\cdot\mathbf{b}_1 = 0$. From Eq. (23), we deduce that

   $$D_{(\mathbf{a}_1,\mathbf{0}_m,0,0)}D_{(\mathbf{0}_m,\mathbf{b}_2,0,0)}f(\mathbf{x},\mathbf{y},z_1,z_2)\Big|_{\mathbf{x}=\mathbf{0}_m,z_1=z_2=0} = D_{\mathbf{b}_2}(\phi(\mathbf{y}))\cdot\mathbf{a}_1.$$

   As $\mathbf{c}\cdot\phi$ has no nonzero linear structures for any $\mathbf{c}\in\mathbb{F}_2^m\setminus\{\mathbf{0}_m\}$, then $D_{\mathbf{b}_2}\phi(\mathbf{y})\cdot\mathbf{a}_1$ is not a constant function. Thus, we have found two elements $\mathbf{a},\mathbf{b}\in V$ such that $D_{\mathbf{a}}D_{\mathbf{b}}f \not\equiv 0$.
3. Let $|\{\mathbf{x}\in\mathbb{F}_2^m : (\mathbf{x},\mathbf{y},z_1,z_2)\in V\}| = 1$. We have $|\{\mathbf{y}\in\mathbb{F}_2^m : (\mathbf{x},\mathbf{y},z_1,z_2)\in V\}| \geq 2^{m-1}$. For any $\mathbf{a} = (\mathbf{0}_m,\mathbf{a}_2,a_3,a_4)\in V$ such that $\mathbf{a}_2 \neq \mathbf{0}_m$, we have $D_{\mathbf{a}_2}\phi_i \not\equiv const.$, $D_{\mathbf{a}_2}\phi_j \not\equiv const.$ and $D_{\mathbf{a}_2}(\phi_i\oplus\phi_j) \not\equiv const.$, where $1\leq i\neq j\leq m$ and $\phi = (\phi_1,\ldots,\phi_m)$, since $\mathbf{c}\cdot\phi$ has no nonzero linear structure for any $\mathbf{c}\in\mathbb{F}_2^m\setminus\{\mathbf{0}_m\}$. Furthermore,

   $$|\{\mathbf{b}_2\in\mathbb{F}_2^m : D_{\mathbf{b}_2}D_{\mathbf{a}_2}\phi_i = D_{\mathbf{b}_2}D_{\mathbf{a}_2}\phi_j \equiv \mathbf{0}_m\}| < 2^{m-1},$$

   since the maximum cardinality

   $$|\{\mathbf{b}_2\in\mathbb{F}_2^m : D_{\mathbf{b}_2}D_{\mathbf{a}_2}\phi_i = D_{\mathbf{b}_2}D_{\mathbf{a}_2}\phi_j \equiv \mathbf{0}_m\}| = 2^{m-2}$$

   is attained if both $D_{\mathbf{a}_2}\phi_i$ and $D_{\mathbf{a}_2}\phi_j$ are affine. Hence, we can select two vectors $\mathbf{a},\mathbf{b}\in V$ such that $D_{\mathbf{a}_2}D_{\mathbf{b}_2}\phi \not\equiv \mathbf{0}_m$. Since

   $$D_{(\mathbf{0}_m,\mathbf{a}_2,a_3,a_4)}D_{(\mathbf{0}_m,\mathbf{b}_2,b_3,b_4)}f(\mathbf{x},\mathbf{y},z_1,z_2) = D_{\mathbf{a}_2}D_{\mathbf{b}_2}(\phi(\mathbf{y}))\cdot\mathbf{x},$$

   we conclude that $D_{(\mathbf{a}_1,\mathbf{a}_2,a_3,a_4)}D_{(\mathbf{b}_1,\mathbf{b}_2,b_3,b_4)}f \not\equiv 0$.

Similarly as in Theorem 13, we will show that certain functions from $\mathcal{M},\mathcal{C},\mathcal{D}$ and $\mathcal{CD}$ can form a bent 4-decomposition.

Theorem 15 *Let $n = 2m$, s be a positive divisor of m such that m/s is odd, and d a positive integer such that $d(2^s + 1) \equiv 1 \pmod{2^m - 1}$ and $\mathrm{wt}(d) \geq 3$. Let $E_2 = \mathbb{F}_{2^s}$, $L \subset E_2$ be a subspace of $\mathbb{F}_{2^m}$ and $E_1 = E_2^{\perp}$. Let $f_1 : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be defined by $f_1(x, y) = Tr_1^m(xy^d) + 1$, and f_2,f_3 and f_4 be defined by*:

$$f_2(x, y) = Tr_1^m(xy^d) + \mathbf{1}_{L^{\perp}}(x),$$
$$f_3(x, y) = Tr_1^m(xy^d) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y),$$
$$f_4(x, y) = Tr_1^m(xy^d) + \mathbf{1}_{L^{\perp}}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y).$$

Then, $f = (f_1, \ldots, f_4)$ is a bent function in $n + 2$ variables.

Proof From Proposition 5, Theorems 10 and 11, it is easy to compute that $f_1^*(x, y) + f_2^*(x, y) + f_3^*(x, y) + f_4^*(x, y) = 1$ for all $x, y \in \mathbb{F}_{2^m}$. Thus, by Theorem 1, it holds that $f = (f_1, \ldots, f_4)$ is a bent 4-decomposition, i.e., it follows that f is a bent function in $n + 2$ variables.

Remark 7 Let f_1,f_2,f_3,f_4 and f be defined as in Theorem 15, then Eq. (21) evaluates to

$$f(x, y, z_1, z_2) = Tr_1^m(xy^d) + z_1\mathbf{1}_{L^{\perp}}(x) + z_2\mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) + z_1 + z_2 + 1,\ x, y \in \mathbb{F}_{2^m}, z_1, z_2 \in \mathbb{F}_2.$$

6 Concluding remarks

We have introduced a new superclass of bent functions obtained from $\mathcal{C}$ and $\mathcal{D}$ which is shown to be provably outside $\mathcal{M}^{\#}$ under certain conditions (see Theorem 8). Furthermore, we strongly believe that these functions may also lie outside $\mathcal{C}^{\#}$ and $\mathcal{D}^{\#}$ (due to the modification performed on subsets), but due to the lack of suitable indicators this question appears to be difficult to answer. We have provided an explicit class of bent functions in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$ (see Proposition 2) and two examples which can (possibly) be generalized. The question whether these bent functions can be simultaneously outside the completed $\mathcal{M}$ and $\mathcal{PS}^{+}$ classes is partially addressed. Furthermore, it is shown that one can employ different families of n-variable bent functions (whose duals are explicitly determined) in the so-called 4-bent concatenation for the purpose of generating new bent functions in $n + 2$ variables. Most notably, the resulting bent functions in $n + 2$ variables can also lie outside $\mathcal{M}^{\#}$ class. Construction methods of vectorial bent functions, based on this $\mathcal{CD}$ class, whose components (possibly not all) are outside $\mathcal{M}^{\#}$ are also of interest.

Acknowledgements Amar Bapić is supported in part by the Slovenian Research Agency (research program P1-0404 and Young Researchers Grant). Enes Pasalic is supported in part by the Slovenian Research Agency (research program P1-0404 and research projects J1-9108, J1-1694, N1-0159, J1-2451). Fengrong Zhang is supported in part by the Natural Science Foundation of China (No. 61972400). Samir Hodžić is supported by the Slovenian Research Agency (research program P1-0404 and research projects J1-1694 and N1-1059).

References

1. Zhang, F., Cepak, N., Pasalic, E., Wei, Y.: Bent functions in C and D stemming from Maiorana-McFarland class. In Codes, Cryptology and Information Security. C2SI 2017. Lecture Notes in Computer Science, **10194**, 298–313. (2017)
2. Zhang, F., Cepak, N., Pasalic, E., Wei, Y.: Further analysis of bent functions from C and D which are provably outside or inside $M^{\#}$. Discret. Appl. Math. **285**(1), 458–472 (2020)
3. Carlet, C.: Two new classes of bent functions. In Lecture Notes in Computer Science **765**, 77–101 (1993)
4. Rothaus, O.: On bent functions. J. Comb. Theory, Ser. A, **20**(3), 300-305. (1976)
5. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press (2021)
6. Mesnager, S.: Bent functions - Fundamentals and Results. Springer. (2016)
7. Tokareva, N.: Bent Functions: Results and Applications to Cryptography. Academic Press (2015)
8. Carlet, C., Mesnager, S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5–50 (2016)
9. Dillon, J.: Elementary Hadamard Difference Sets. PhD thesis, University of Maryland. (1974)
10. McFarland, R.L.: A family of difference sets in non-cyclic groups. J. Comb. Theory, Ser. A, **15**(1): 1–10. (1973)
11. Dobbertin, H.: Construction of bent functions and balanced Boolean functions with high nonlinearity. In B. Preneel, editor, Fast Software Encryption, pages 61–74, Berlin, Heidelberg. Springer Berlin Heidelberg. (1995)
12. Langevin, P., Leander, G.: Counting all bent functions in dimension eight 99270589265934370305785 861242880. Des. Codes Cryptogr. **59**(1), 193–205 (2011)
13. Kudin, S., Pasalic, E., Cepak, N., Zhang, F.: Permutations without linear structures inducing bent functions outside the completed Maiorana-McFarland class. Cryptogr. Commun. (2021)
14. Pasalic, E., Zhang, F., Kudin, S., Wei, Y.: Vectorial bent functions weakly/strongly outside the completed Maiorana-McFarland class. Discret. Appl. Math. **294**(8), 138–151 (2021)
15. Bapić, A., Pasalic, E.: Constructions of (vectorial) bent functions outside the completed Maiorana-McFarland class. Submitted to Discret. Appl. Math. (2021)
16. Canteaut, A., Charpin, P.: Decomposing bent functions. IEEE Trans. Inf. Theory **49**(8), 2004–2019 (2003)
17. Hodžić, S., Pasalic, E., Zhang, W.: Generic constructions of five-valued spectra Boolean functions. IEEE Trans. Inf. Theory **65**(11), 7554–7565 (2019)
18. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**(2), 125–156 (1998)
19. Budaghyan, L., Carlet, C., Pott, A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inf. Theory **52**(3), 1141–1152 (2006)
20. Canteaut, A., Daum, M., Dobbertin, H., Leander, G.: Finding nonnormal bent functions. Discret. Appl. Math. **154**(2), 202–218 (2006)
21. Tang, C., Zhou, Z., Qi, Y., Zhang, X., Fan, C., Helleseth, T.: Generic construction of bent functions and bent idempotents with any possible algebraic degrees. IEEE Trans. Inf. Theory **63**(10), 6149–6157 (2017)
22. Mandal, B., Stănică, P., Gangopadhyay, S., Pasalic, E.: An analysis of the C class of bent functions. Fundam. Inform. **146**(3), 271–292 (2016)
23. Zheng, L., Kan, H., Peng, J., Tang, D.: Constructing vectorial bent functions via second-order derivatives. Discrete Math. **344**(8), 112473 (2021)
24. Mesnager, S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inf. Theory **60**(7), 4397–4407 (2014)
25. Hodžić, S., Pasalic, E., Wei, Y.: A general framework for secondary constructions of bent and plateaued functions. Des. Codes Cryptogr. **88**(1), 2007–2035 (2020)

Authors and Affiliations

Amar Bapić[1,2] · Enes Pasalic[1,2] · Fengrong Zhang[3,4] · Samir Hodžić[1]

Enes Pasalic
enes.pasalic6@gmail.com

Fengrong Zhang
zhfl203@163.com

Samir Hodžić
samir.hodzic@famnit.upr.si

[1] Faculty of Mathematics, Natural Sciences and Informatics, University of Primorska, Glagoljaška ulica 8, Koper 6000, Slovenia

[2] Andrej Marušič Institute, University of Primorska, Muzejski trg 2, Koper 6000, Slovenia

[3] State Key Laboratory of Integrated Services Networks, Xidian University, Xian 710071, P.R. China

[4] Mine Digitization Engineering Research Center of Ministry of Education, China University of Mining and Technology, Xuzhou, Jiangsu 221116, China