Constructing new superclasses of bent functions from known ones

A. Bapić [*] E. Pasalic[†] F. Zhang[‡]

Abstract

Some recent research articles addressed the specification of indicators leading to two classes of bent functions, denoted $\mathcal{C}$ and $\mathcal{D}$, derived from the Maiorana-McFarland ($\mathcal{M}$) class by C. Carlet in 1994. Many of these explicitly specified 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 sets may provide us with further classes of bent functions which are provably outside the completed $\mathcal{M}$ class. In this article, we exactly specify new families of bent functions by adding together indicators well suited for the $\mathcal{C}$ and $\mathcal{D}$ class, thus essentially modifying bent functions in $\mathcal{M}$ on suitable sets instead of subspaces. Apart from the desirable property of being outside the completed $\mathcal{M}$ class, these bent functions can be potentially used for constructing vectorial bent functions whose components (possibly not all) share the same property, which is an interesting research challenge. It is also shown that certain instances of these bent functions are simultaneously outside the completed $\mathcal{M}$ and $\mathcal{PS}^+$ classes.

1 Introduction

The term bent function was introduced by Rothaus [5]. Bent functions have a wide range of applications in error correcting codes, sequences, symmetric design and cryptography. We introduce a new superclass of bent functions which modifies bent functions in the $\mathcal{M}$ class on a suitable rather than modifying it on affine subspaces. We show that the function defined as $f(x,y) = Tr_1^m(x\pi(y)) + a_0\mathbf{1}_{L^\perp}(x) + a_1\mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y)$, with $x, y \in \mathbb{F}_{2^m}$, are bent for any choice of the binary constants $a_0, a_1 \in \mathbb{F}_2$, for suitably selected subspaces L, E_1, E_2 and permutation π, in accordance to the standard condition related to the bentness of functions in $\mathcal{C}$ and $\mathcal{D}$.

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 $x_i \in \mathbb{F}_2$. With $\mathbb{F}_{2^n}$ we denote the finite field of order 2^n and with $\mathbb{F}_{2^n}^*$ its multiplicative cyclic group consisting of $2^n - 1$ elements. With "+" we denote the addition in the finite field $\mathbb{F}_{2^n}$, and with "$\oplus$" (bitwise XOR) we denote the addition in $\mathbb{F}_2^n$.

For $x \in \mathbb{F}_{2^n}$ the *trace* $Tr_k^n(x) : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$ of x over $\mathbb{F}_{2^k}$, 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.* The *Walsh-Hadamard transform* of a Boolean function f on $\mathbb{F}_{2^n}$ at a point $u \in \mathbb{F}_{2^n}$ is defined by

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

If $W_f(u) = \pm 2^{\frac{n}{2}}$ for all $u \in \mathbb{F}_{2^n}$, then f is a *bent function.* A function $f : \mathbb{F}_{2^{2m}} \to \mathbb{F}_2$ is called *normal* (*weakly normal*) if there exists a flat of dimension m such that f is constant (affine) on this flat.

The following theorem will be useful when considering the inclusion/exclusion of bent Boolean functions in the class $\mathcal{M}^\#$, where $\mathcal{M}^\#$ is the completed version of $\mathcal{M}$ (see Section 2.1 for the definition of $\mathcal{M}$) which is globally invariant under the addition of any affine function and the composition (on the right) with any nonsingular affine transformation. Throughout this article we use $\oplus$ to denote the addition of vectors in $\mathbb{F}_2^m$, whereas "+" denotes addition in a finite field.

Theorem 1. *[3] 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 $\mathbf{a}, \mathbf{b} \in V$.

[*] University of Primorska, FAMNIT & IAM, Koper, Slovenia, e-mail: amar.bapic@famnit.upr.si

[†] University of Primorska, FAMNIT & IAM, Koper, Slovenia, e-mail: enes.pasalic6@gmail.com

[‡] State Key Laboratory of Integrated Services Networks, Xidian University, Xian, 710071, P.R. China, and Mine Digitization Engineering Research Center of Ministry of Education, CUMT, Xuzhou, Jiangsu 221116, China, email:zhfl203@cumt.edu.cn

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

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

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 [1] derived the $\mathcal{C}$ class of bent functions that contains all functions of the form

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus \mathbf{1}_{L^\perp}(\mathbf{x}), \tag{2}$$

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 (ϕ, L) *has property* (C).

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

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus \mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y}) \tag{3}$$

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 [7]. For convenience of the reader, we specify the main results related to the set of conditions for $\mathcal{C}$ class which uses a hard assumption related to the (C) property.

Theorem 2. *[7] 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 [7]:

Theorem 3. *[7] 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 $\mathbb{F}_2^n$ 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 Modifying bent functions in $\mathcal{M}$ on suitable sets

We first show that the addition of $\mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) + \delta_0(x)$ is not suitable for generating bent functions, where δ_0 denotes the Dirac symbol. That is, $\delta_0(x)$ equals 1 if $x = 0$, and 0 otherwise.

Theorem 4. *Let π be a permutation on $\mathbb{F}_{2^m}$ and let $E_1, E_2 \subset \mathbb{F}_{2^m}$ be two linear subspaces 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 consider $W_f(0, 0)$.

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

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. It is straightforward to show that in both cases $W_f(0, 0) \neq \pm 2^m$, thus f is not bent. □

Remark 1. *In the extended version of this abstract, we will also show that the addition of $\mathbf{1}_{L^\perp}(x) + \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) + \delta_0(x)$ is not suitable for generating new bent functions. Thus, when "combining" the classes $\mathcal{C}, \mathcal{D}$ and $\mathcal{D}_0$, only the superclasses $\mathcal{SC}$ ($\mathcal{C}$ and $\mathcal{D}_0$) and $\mathcal{CD}$ ($\mathcal{C}$ and $\mathcal{D}$) give bent functions.*

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

In this section, we consider 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 defined by

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

Then, the primary task is to find conditions which ensure that the function f 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 $M(a, b) = C(x, y) + Tr_1^m(ax + by)$.

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

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

$$W_f(a,b) = W_C(a,b) - 2\cdot\left(\sum_{x\in E_1}\sum_{y\in E_2}(-1)^{Tr_1^m(ax+by)} - 2\sum_{x\in E_1\cap L^\perp}\sum_{y\in E_2}(-1)^{Tr(ax+by)}\right). \tag{4}$$

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

$$\sum_{x\in E_1}\sum_{y\in E_2}(-1)^{Tr_1^m(ax+by)} = \begin{cases} 2^{\varepsilon_1+\varepsilon_2}, & (a,b)\in E_1^\perp\times E_2^\perp\\ 0, & \text{otherwise}\end{cases} \tag{5}$$

$$\sum_{x\in K}\sum_{y\in E_2}(-1)^{Tr_1^m(ax+by)} = \begin{cases} 2^{\kappa+\varepsilon_2}, & (a,b)\in K^\perp\times E_2^\perp\\ 0, & \text{otherwise}\end{cases}, \tag{6}$$

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 as such, $E_1^\perp \times E_2^\perp \subset K^\perp \times E_2^\perp$. 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 wish 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 $(a, b) \in (K^\perp \setminus E_1^\perp) \times E_2^\perp$. Since we wish that f is a bent function, we have the following situations:

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

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

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 for $\kappa = \varepsilon_1$ and $\kappa = \varepsilon_1 - 1$. Based on these observations, we give the following results. We note that Theorem 5 corresponds to the case $\kappa = \varepsilon_1 - 1$ and Theorem 6 corresponds to the case $\kappa = \varepsilon_1$.

Theorem 5. *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

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

Proof. Suppose that $(a,b) \notin (E_1 \cap L)^\perp \times E_2^\perp$. From (4) and (5)-(6), it is easy to see that $W_f(a,b) = W_C(a,b)$. Suppose that $(a,b) \in E_1^\perp \times E_2^\perp$. From (4) and (5)-(6), it follows that

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

Lastly, if $(a,b) \in ((E_1 \cap L)^\perp \setminus E_1^\perp) \times E_2^\perp$, the sum (5) is equal to zero, and thus from (4) and (6) it follows that

$$W_f(a,b) = W_C(a,b) - 2 \cdot 2^{\varepsilon_1+\varepsilon_2} = W_C(a,b) - 2^{m+1}.$$

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 6. *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

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

Proof. We note that (4) 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 1. *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 $\dim(E_1 \cap L^\perp) \in \{\dim(E_1), \dim(E_1) - 1\}$, 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*

$$f(x,y) = Tr_1^m(x\pi(y)) + a_0\mathbf{1}_{L^\perp}(x) + a_1\mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y), \ a_i \in \mathbb{F}_2, \tag{7}$$

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*

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

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

$$|S| = 2^{m+\lambda} + 2^{\epsilon_1+\epsilon_2} - 2^{\epsilon_2+1} \cdot |L^\perp \cap E_1|, \tag{8}$$

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 $\mathbb{F}_{2^n}$.

4 Conditions for $\mathcal{CD}$ to be outside $\mathcal{M}^{\#}$

In this section, we present sufficient conditions for functions in the $\mathcal{CD}$ class to be provably outside $\mathcal{M}^{\#}$. Furthermore, we believe that these functions, for $a_0 = a_1 = 1$ in (1), are also outside $\mathcal{C}^{\#}$ and $\mathcal{D}^{\#}$ (apparently they are outside $\mathcal{C}$ and $\mathcal{D}$), because the support of the indicator function used in the definition is not a subspace, as required by the definition of the $\mathcal{C}$ and $\mathcal{D}$ classes. A more rigorous treatment on this difficult task is left for the extended version of this abstract. 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*

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

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

$$D_{\mathbf{a}}(\mathbf{1}_V(\mathbf{x}))) = \mathbf{1}_V(\mathbf{x}) \oplus \mathbf{1}_V(\mathbf{x} \oplus \mathbf{a}) = \mathbf{1}_{V \cup (V + \mathbf{a})}(\mathbf{x}),$$

that is, $\deg(D_{\mathbf{a}}(\mathbf{1}_V(\mathbf{x}))) = n - \dim(V) - 1$.

If $\mathbf{a} \in V$, then

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

□

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

Theorem 7. *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 $\pi(E_2) = E_1^{\perp}$ and $\dim(E_1 \cap L^{\perp}) \in \{\dim(E_1), \dim(E_1) - 1\}$. 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 $(C1)-(C2)$ and $(D1)-(D3)$, respectively, then f is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$.

Proof. From Theorem 6 and Definition 1, it follows that f is bent. From Theorem 1, it suffices to show that there is no m-dimensional subspace $V = V_1 \times V_2$ of $\mathbb{F}_2^m \times \mathbb{F}_2^m$ on which the second-order derivative $D_{\mathbf{a}}D_{\mathbf{b}}(f)$ vanishes, for some $\mathbf{a}, \mathbf{b} \in V$.

The second derivative of f with respect to $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2)$ and $\mathbf{b} = (\mathbf{b}_1, \mathbf{b}_2)$, $\mathbf{a}_i, \mathbf{b}_i \in V_i$ for $i = 1, 2$, can be written as

$$\begin{aligned} D_{\mathbf{a}}D_{\mathbf{b}}f(\mathbf{x}, \mathbf{y}) &= \mathbf{x} \cdot (D_{\mathbf{a}_2}D_{\mathbf{b}_2}\pi(\mathbf{y})) \oplus \mathbf{a}_1 \cdot D_{\mathbf{b}_2}\pi(\mathbf{y} \oplus \mathbf{a}_2) \\ &\oplus \mathbf{b}_1 \cdot D_{\mathbf{a}_2}\pi(\mathbf{y} \oplus \mathbf{b}_2) \oplus D_{\mathbf{a}_1}D_{\mathbf{b}_1}\mathbf{1}_{L^{\perp}}(\mathbf{x}) \oplus D_{\mathbf{a}}D_{\mathbf{b}}\mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y}). \end{aligned} \tag{9}$$

For any $\mathbf{a} \in \mathbb{F}_2^n$, we have $\mathbf{a} = \mathbf{a}^{[1]} \oplus \mathbf{a}^{[2]}$, where $\mathbf{a}^{[1]} \in E_1 \times E_2, \mathbf{a}^{[2]} \in (E_1 \times E_2)^{\perp}$. Thus, we have

$$D_{\mathbf{a}}D_{\mathbf{b}}\mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y}) = D_{\mathbf{a}^{[2]}}D_{\mathbf{b}^{[2]}}\mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y}). \tag{10}$$

If $|\{\mathbf{a}^{[2]} : (\mathbf{a}^{[1]} \oplus \mathbf{a}^{[2]}) \in V\}| > 2$, then we select two nonzero vectors $\mathbf{a}, \mathbf{b} \in V$ such that $\mathbf{a}^{[2]}, \mathbf{b}^{[2]} \in (E_1 \times E_2)^{\perp} \setminus \{\mathbf{0}_m\}$. From Proposition 1 and (10), 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 (9), it follows that

$$D_{\mathbf{a}}D_{\mathbf{b}}f(\mathbf{x}, \mathbf{y}) \neq 0.$$

If $|\{\mathbf{a}^{[2]} : (\mathbf{a}^{[1]} \oplus \mathbf{a}^{[2]}) \in V\}| \leq 2$, 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

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

W.l.o.g., if we assume $|V \cap (E_1 \times \mathbf{0}_m)| < 2$, then $|V \cap (E_1 \times E_2)| < |E_2|$, 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 $\mathbf{a} = (\mathbf{a}_1, \mathbf{0}_m), \mathbf{b} = (\mathbf{0}_m, \mathbf{b}_2)$. Combining Proposition 1, (9) and property $(D2)$, we have

$$D_{\mathbf{a}}D_{\mathbf{b}}f(\mathbf{x}, \mathbf{y}) = \mathbf{a}_1 \cdot D_{\mathbf{b}_2}\pi(\mathbf{y}) \neq 0.$$

□

As an immediate consequence of the previous result, we present the following explicit family of bent functions in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$. We will define it using a finite field notation.

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 $wt(d) \geq 3$. 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 [7, Theorem 9] 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 [7, Proposition 5], we have that $Tr(u\pi(y))$ 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 $(C1) - (C2)$ and $(D1) - (D3)$ of Theorems 2 and 3, respectively, are satisfied. From Theorem 7, 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 $d(2^s + 1) \equiv 1 \pmod{2^m - 1}$. 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*

$$f(x,y) = Tr_1^6(xy^{38}) + \mathbf{1}_{E_1}(x)(1 + \mathbf{1}_{E_2}(y)),\ x, y \in \mathbb{F}_{2^{16}}$$

is a bent function in 12 variables lying in $\mathcal{CD}$ 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 `Sage` we were able to construct 500 functions $f \in \mathcal{CD}$ of the form (1) for the fixed permutation π given above. Furthermore, all of them are outside $\mathcal{M}^{\#}$. 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. We leave the discussion about their generalization for the extended version of this abstract.

Example 2. *Let $m = 9$ and $d = 284$. We note that $d(2^3+1) \mod (2^9-1) = 1$, $wt(d) = 4$ 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 [7, Theorem 9] 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 $wt(d) \geq 3$, from [7, Proposition 5], we have that $Tr(u\pi)$ 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 $(C1) - (C2)$ and $(D1) - (D3)$ of Theorems 2 and 3, respectively, are satisfied. From Theorem 7 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 $S = (L^{\perp} \times \mathbb{F}_{2^m}) \triangle (E_1 \times E_2)$ (see Remark 2), and equals 0 otherwise. From (8) we see 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.

4.1 Exclusion from the $\mathcal{PS}^+$ class

In [2] 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 nonnormal it lies outside the completed $\mathcal{PS}^+$ class. In this section we discuss the weakly 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 $\dim(E_1 \cap L^\perp) \in \{\dim(E_1), \dim(E_1) - 1\}$, 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:

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

   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 $\pi(E_2) \neq E_2$, that is, the permutation π is not affine on E_2 seems to be more difficult to analyze (due to the lack of assumption that f is affine on E_2) which leads to the following open problem.

Open problem: With the same notation as in Definition 1, 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 (1) weakly normal ?

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

$$f(x, y) = Tr_1^9(xy^d) + a_0\mathbf{1}_{L^\perp}(x) + a_1\mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) + a_2\delta_0(x), \tag{11}$$

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

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 7). Furthermore, we strongly believe that these functions are also outside $\mathcal{C}^\#$ and $\mathcal{D}^\#$, because the modification of a bent function in the Maiorana-McFarland class is performed on a set rather than on a linear/affine subspace. 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. 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.

$(a_0, a_1, a_2) \in \mathbb{F}_2^3$	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	-

Table 1: Class inclusion of the Boolean function f defined by (11)

References

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

[2] A. Canteaut, M. Daum, H. Dobbertin and G. Leander. Finding nonnormal bent functions. *Discrete Applied Mathematics*, 154(2): 202–218, 2006.

[3] Dillon, J.F.: Elementary Hadamard difference sets. Ph.D. thesis, University of Maryland (1974).

[4] E. Pasalic, F. Zhang, S. Kudin and Y. Wei. Vectorial bent functions weakly/strongly outside the completed Maiorana-McFarland class. *Discrete Applied Mathematics*, 294(1): 138–151, 2021.

[5] O. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3): 300 – 305, 1976.

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

[7] F. Zhang, E. Pasalic, N. Cepak, Y. Wei. Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^\#$. *Discrete Applied Mathematics*, vol. 285, pp. 458–472, 2020.