Applications of the indirect sum in the design of several special classes of bent functions outside the completed $\mathcal{MM}$ class

Fengrong Zhang, Enes Pasalic, Amar Bapić, Baocang Wang

Abstract

Two main secondary constructions of bent functions are the direct and indirect sum methods. We show that the direct sum, under more relaxed conditions compared to those in [19], can generate bent functions provably outside the completed Maiorana-McFarland class ($\mathcal{MM}^{\#}$). We also show that the indirect sum method, though imposing certain conditions on the initial bent functions, can be employed in the design of bent functions outside $\mathcal{MM}^{\#}$. Furthermore, applying this method to suitably chosen bent functions we construct several generic classes of homogenous cubic bent functions (considered as a difficult problem) that might posses additional properties (namely without affine derivatives and/or outside $\mathcal{MM}^{\#}$). Our results significantly improve upon the best known instances of this type of bent functions given by Polujan and Pott [19], and additionally we solve an open problem in [19, Open Problem 5.1]. More precisely, we show that one class of our homogenous cubic bent functions is non-decomposable (inseparable) so that h under a non-singular transform B cannot be represented as $h(xB) = f(y) \oplus g(z)$. Finally, we provide a generic class of vectorial bent functions strongly outside $\mathcal{MM}^{\#}$ of relatively large output dimensions, which is generally considered as a difficult task.

Keywords: Bent functions, Direct and indirect sum, Completed classes, Homogenous bent functions, Strongly outside $\mathcal{MM}^{\#}$.

1 Introduction

The concept of bent functions was introduced by Rothaus [20] as a family of Boolean functions possessing several nice combinatorial properties, which allowed for their great range of applications such as in design theory, coding theory, sequences, cryptography to mention a few. An exhaustive survey on bent functions related to their design and properties can be found in [8] and in the recent textbook [16]. In general, the design methods of bent function can be divided into primary and secondary constructions. Whereas the two main primary classes (the partial spread [9] and Maiorana-McFarland class [14]) specify bent functions directly (without involving other bent functions), the known secondary constructions involve other bent functions either on the same or on smaller variable spaces. A non-exhaustive list of various secondary constructions can be found in the following works [4,5,7,11,15,26]. However, the question regarding the class inclusion of bent functions stemming from these secondary construction methods is commonly left open, apart from a few works [1,2,4,12,15,22,23,23,24]

where some explicit families of bent functions provably outside the completed $\mathcal{MM}$ class are given.

The best known secondary constructions are the direct and indirect sum method, where the latter approach was introduced by Carlet [5, 7]. However, the class inclusion of bent functions generated by these methods has not been addressed in the literature. Only recently, the direct sum method was analysed in this context by Polujan and Pott [19] and it was shown that $h(x, y) = f(x) \oplus g(y)$ can lie outside the completed $\mathcal{MM}^{\#}$ class, assuming that f and g are suitably selected. In addition, it was shown [19] that the direct sum method can be efficiently used in the design of homogenous cubic bent functions. In this article, we analyse the cryptographic properties of the indirect sum and show that this approach gives significant improvements over the direct sum employed in [19]. In the first place, we derive two generic families of bent functions that are provably outside $\mathcal{MM}^{\#}$. One of these methods is then employed for specifying infinite families of homogenous cubic bent functions outside $\mathcal{MM}^{\#}$ (on significantly smaller variable spaces), which may possess additional cryptographic properties such as the absence of affine derivatives and inseparability.

More precisely, we first demonstrate that the direct sum method $h(x, y) = f(x) \oplus g(y)$, under more relaxed conditions on f and g compared to those in [19], can generate bent functions provably outside $\mathcal{MM}^{\#}$. This also improves a recent result in [17], where g was a quadratic bent function of a special form but still violating the sufficient conditions in [17]. The analysis regarding the class exclusion from $\mathcal{MM}^{\#}$ of bent functions generated by means of the indirect sum (thus considering $h(x, y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y)$) is commonly tedious and we provide two explicit sets of conditions on f_i and g_i so that h is provably outside $\mathcal{MM}^{\#}$. We remark that, also supported by computer simulations, these conditions appear not to be necessary and there might be a possibility of relaxing these conditions further (see also Remark 3.3 and Open problem 2). In particular, the use of indirect sum in Theorem 4.1 provides an infinite family of homogenous cubic bent functions outside $\mathcal{MM}^{\#}$ which additionally are without affine derivatives. Most notably, employing our another method of specifying homogenous cubic bent functions outside $\mathcal{MM}^{\#}$ given in Theorem 4.2, we show that these bent functions are non-decomposable/inseparable (considered in general as a difficult problem) so that h under a non-singular transform B cannot be represented as $h(xB) = f(y) \oplus g(z)$. This also provides a solution to the open problem of Polujan and Pott [19, Open Problem 5.1]. Our results on homogenous cubic bent functions are summarized in Table 1, which illustrates significant improvements compared to the other approaches [13, 19]. Finally, we address another difficult task of specifying vectorial bent functions $\{F\}$ strongly outside $\mathcal{MM}^{\#}$, the concept introduced in [18] that refers the property that all the non-zero components of F are outside $\mathcal{MM}^{\#}$. We provide a generic construction method (based on the so-called companion matrices) of these objects having relatively large output dimension, which is a significant improvement compared to the results in [18] and [1].

The rest of this paper is organized as follows. In Section 2, we give some basic definitions related to Boolean functions. A set of sufficient conditions on the initial bent functions used, for the purpose of excluding them from the $\mathcal{MM}^{\#}$ class, is specified for both the direct and indirect sum method (for the latter approach two different sets of conditions are

given) in Section 3. In Section 4, we provide several methods (using the indirect sum) for constructing homogenous cubic bent functions outside $\mathcal{MM}^{\#}$ which additionally might not have affine derivatives. In particular, we show in Section 4.2 that certain subclasses of these homogenous cubic bent functions are also non-decomposable which positively answers the open problem in [19, Open Problem 5.1]. In Section 5, we provide a generic class of vectorial bent functions strongly outside $\mathcal{MM}^{\#}$ of relatively large output dimensions. Finally, some concluding remarks are given in Section 6.

2 Preliminaries

The vector space $\mathbb{F}_2^n$ is the space of all n-tuples $x = (x_1, \ldots, x_n)$, where $x_i \in \mathbb{F}_2$. For $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_2^n$, the usual scalar (or dot) product over $\mathbb{F}_2$ is defined as $x \cdot y = x_1 y_1 \oplus \cdots \oplus x_n y_n$. The Hamming weight of $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ is denoted and computed as $wt(x) = \sum_{i=1}^{n} x_i$. By "$\sum$" we denote the integer sum (without modulo evaluation), whereas "$\bigoplus$" denotes the sum evaluated modulo two. By 0_n we denote the all-zero vector with n coordinates, that is $(0, 0, \ldots, 0) \in \mathbb{F}_2^n$. By 1_n we denote the all-one vector with n coordinates, that is $(1, 1, \ldots, 1) \in \mathbb{F}_2^n$.

The set of all Boolean functions in n variables, which is the set of mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, is denoted by $\mathcal{B}_n$. Especially, the set of affine functions in n variables is given by $\mathcal{A}_n = \{a \cdot x \oplus b : a \in \mathbb{F}_2^n,\ b \in \{0, 1\}\}$, and similarly $\mathcal{L}_n = \{a \cdot x : a \in \mathbb{F}_2^n\} \subset \mathcal{A}_n$ denotes the set of linear functions. It is well-known that any $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented by its associated algebraic normal form (ANF) as follows:

$$f(x_1, \ldots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u \left(\prod_{i=1}^{n} {x_i}^{u_i} \right), \tag{1}$$

where $x_i, \lambda_u \in \mathbb{F}_2$ and $u = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$. The algebraic degree of f, denoted by $\deg(f)$, is equal to the maximum Hamming weight of $u \in \mathbb{F}_2^n$ for which $\lambda_u \neq 0$.

The first order derivative of a function f in the direction $a \in \mathbb{F}_2^n$ is given by $D_a f(x) = f(x) \oplus f(x \oplus a)$. The point $a \in \mathbb{F}_2^n$ is called a fast point of a function $f \in \mathcal{B}_n$ if it satisfies $\deg(D_a f) < \deg(f) - 1$, and a slow point if $\deg(D_a f) = \deg(f) - 1$. The set of fast points $\mathbb{FP}_f$ forms a vector subspace and its dimension is bounded by $\dim(\mathbb{FP}_f) \leq n - \deg(f)$, as it was shown in [10].

The *Walsh-Hadamard transform* (WHT) of $f \in \mathcal{B}_n$, and its inverse WHT, at any point $\omega \in \mathbb{F}_2^n$ are defined, respectively, by

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

and

$$(-1)^{f(x)} = 2^{-n} \sum_{\omega \in \mathbb{F}_2^n} W_f(\omega) (-1)^{\omega \cdot x}. \tag{2}$$

A function $f \in \mathcal{B}_n$, for even n, is called *bent* if $W_f(u) = 2^{\frac{n}{2}}(-1)^{f^*(u)}$ for a Boolean function $f^* \in \mathcal{B}_n$ which is also a bent function, called the *dual* of f.

The Maiorana-McFarland class $\mathcal{MM}$ is the set of n-variable (n is even) Boolean functions of the form

$$f(x, y) = x \cdot \pi(y) \oplus g(y), \text{ for all } x, y \in \mathbb{F}_2^{n/2}, \tag{3}$$

where π is a permutation on $\mathbb{F}_2^{n/2}$, and g is an arbitrary Boolean function on $\mathbb{F}_2^{n/2}$. We recall that the *completed* class is obtained by applying the so-called extended affine (EA) equivalence to the functions in a given class. More precisely, if we consider the class $\mathcal{MM}$, given an arbitrary $f \in \mathcal{MM}$ defined on $\mathbb{F}_2^n$, this affine equivalence class includes a set of functions $\{g\}$ obtained by

$$g(x) = f(Ax + b) \oplus c \cdot x \oplus d,$$

where $A \in GL(n, \mathbb{F}_2)$ (the group of invertible matrices under composition), $b, c \in \mathbb{F}_2^n$ and $d \in \mathbb{F}_2$. Thus, the completed class $\mathcal{MM}^\#$ can be defined as

$$\mathcal{MM}^\# = \{f(Ax \oplus b) \oplus c \cdot x \oplus d : f \in \mathcal{MM}, A \in GL(n, \mathbb{F}_2), b, c \in \mathbb{F}_2^n, d \in \mathbb{F}_2\}.$$

3 Direct and indirect sum method

The direct sum method is probably one of the best known design rationales when constructing new bent functions form the known ones. Namely, provided that both f and g are bent functions on $\mathbb{F}_2^n$ and on $\mathbb{F}_2^m$ (both n and m are even), respectively, the function $h(x, y) = f(x) \oplus g(y)$ is also bent on $\mathbb{F}_2^{n+m}$. A special case of this approach arises when g is a quadratic bent function given in a canonical form $g(y) = y_1y_2 \oplus \cdots \oplus y_{m-1}y_m$, which was recently considered in [17]. It was shown that in this particular case h is outside $\mathcal{MM}^\#$ if and only if f is outside $\mathcal{MM}^\#$. This motivates us to investigate other choices of g (not only quadratic canonical ones) in this context.

3.1 Specifying sufficient conditions for the direct sum method

In this section, we consider the conditions under which $h(x, y) = f(x) \oplus g(y)$ is outside $\mathcal{MM}^\#$. The following lemma, due to Dillon [9], is of crucial importance for the discussion on class inclusion.

Lemma 3.1. *[9, p. 102] A bent function f in n variables belongs to $\mathcal{MM}^\#$ if and only if there exists an $\frac{n}{2}$-dimensional linear subspace V of $\mathbb{F}_2^n$ such that the second order derivatives*

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

vanish for any $\alpha, \beta \in V$.

Notice that, as remarked recently in [17], we always have $f \in \mathcal{MM}^\#$ if and only if $f^* \in \mathcal{MM}^\#$. In addition, the following special cases of the direct sum constructions have been recently addressed in [17].

Theorem 3.1. *[17] Let n be even and f be a bent function in n variables. Set $h(x, y_1, y_2) = f(x) \oplus y_1 y_2$ for $y_i \in \mathbb{F}_2$, so that $h = f||f||f||f||1 \oplus f \in \mathcal{B}_{n+2}$. Then f is outside $\mathcal{MM}^{\#}$ if and only if h is outside $\mathcal{MM}^{\#}$.*

Corollary 1. *[17] Let n and m be even positive integers and h be a bent function in $\mathcal{B}_n$. Then, the function $f(x, y_1, \ldots, y_m) = h(x) \oplus y_1 y_2 \oplus \cdots \oplus y_{m-1} y_m$ is outside $\mathcal{MM}^{\#}$ if and only if h is outside $\mathcal{MM}^{\#}$.*

Before we provide a more general statement of the above result, we provide an important observation useful in the analysis of the direct and indirect sum methods.

Proposition 3.1. *Let n be an even positive integer, and let E be a vector subspace of $\mathbb{F}_2^n$ with $\dim(E) \geq n/2 + 1$. Then, for every bent function $f \in \mathcal{B}_n$ and for every $x_0 \in \mathbb{F}_2^n$ there are $a, b \in E$ such that*

$$D_a D_b f(x)|_{x=x_0} \neq 0.$$

Proof. Assume that there is a bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and $x_0 \in \mathbb{F}_2^n$ such that $D_a D_b f(x_0) = 0$, for every $a, b \in E$. We can assume that $x_0 = 0$ (otherwise we can take $f'(x) = f(x \oplus x_0)$), and that $f(0) = 0$ (otherwise we can take $f \oplus 1$). Then, from $D_a D_b f(0) = 0$ we have $f(0) \oplus f(a) = f(b) \oplus f(a \oplus b)$, i.e. $f(a \oplus b) = f(a) \oplus f(b)$ for every $a, b \in E$. This means that f is linear on E and so there is a linear function $L : \mathbb{F}_2^n \to \mathbb{F}_2$ that agrees with f on E. To see this, take a basis $e_1, \ldots, e_k$ of E, extend it to a basis $e_1, \ldots, e_n$ on $\mathbb{F}_2^n$, and define L as $L(\sum_{i=1}^n w_i e_i) = \sum_{i=1}^k w_i f(e_i)$, for every $w_1, \ldots, w_n \in \mathbb{F}_2$. Then, L is linear and agrees with f on E. Let $l \in \mathbb{F}_2^n$ be such that $L(x) = l \cdot x$, for every $x \in \mathbb{F}_2^n$. Then, $f(x) \oplus l \cdot x = 0$ for every $x \in E$. By the Poisson summation formula [6, Corollary 1] we have:

$$\sum_{u \in v \oplus E^{\perp}} (-1)^{w \cdot u} \widehat{\varphi}(u) = |E^{\perp}| (-1)^{w \cdot v} \sum_{x \in w \oplus E} (-1)^{v \cdot x} \varphi(x),$$

for any pseudo-Boolean function φ on $\mathbb{F}_2^n$ where $\widehat{\varphi}(u) = \sum_{x \in \mathbb{F}_2^n} \varphi(x)(-1)^{u \cdot x}$ denotes the Fourier transform of φ at point $u \in \mathbb{F}_2^n$. Setting $w = 0, v = l$, $\varphi = (-1)^f$, and denoting by f^* the dual of f, we get:

$$\frac{1}{|E^{\perp}|} \sum_{u \in l \oplus E^{\perp}} 2^{n/2} (-1)^{f^*(u)} = \sum_{x \in E} (-1)^{f(x) \oplus l \cdot x} = \sum_{x \in E} (-1)^0 = 2^{\dim(E)}.$$

But $\sum_{u \in l \oplus E^{\perp}} (-1)^{f^*(u)} \leq |E^{\perp}|$, so we have $2^{\dim(E)} \leq 2^{n/2}$, and this is a contradiction because $\dim(E) \geq n/2 + 1$. □

We also recall a useful concept of relaxed $\mathcal{MM}$-subspaces introduced by Polujan and Pott [19].

Definition 3.1. *[19] A vector subspace $U \subseteq \mathbb{F}_2^n$ is called a relaxed $\mathcal{MM}$-subspace of a Boolean function $f \in \mathcal{B}_n$, if for all $a, b \in U$ the second order derivatives $D_a D_b f$ are either constant zero or constant one functions. i.e., $D_a D_b f = 0$ or $D_a D_b f = 1$. We denote by*

$\mathcal{RMS}_r(f)$ the collection of all r-dimensional relaxed $\mathcal{MM}$-subspaces of a Boolean function f and by $\mathcal{RMS}(f)$ the collection

$$\mathcal{RMS}(f) := \bigcup_{r=1}^{n} \mathcal{RMS}_r(f).$$

Definition 3.2. *[19] For a Boolean function $f \in \mathcal{B}_n$ its relaxed linearity index r-ind(f) is defined by r-ind(f):=* $\max_{U \in \mathcal{RMS}(f)} \dim(U)$.

Notice that for a quadratic Boolean function $f \in \mathcal{B}_n$ its relaxed linearity index equals r-ind$(f)= n$.

Lemma 3.2. *[19, Corollary 4.6] Let f and g be two bent function on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. The function h, defined as $h(x, y) = f(x) \oplus g(y)$, is outside $\mathcal{MM}^{\#}$ if r-ind$(f) < n/2$ and r-ind$(g) \leqslant m/2$.*

The following result further refines the above claim by dropping the condition that r-ind$(g) \leqslant m/2$.

Theorem 3.2. *Let f and g be two bent function on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. The function h, defined as $h(x, y) = f(x) \oplus g(y)$, is outside $\mathcal{MM}^{\#}$ if r-ind$(f) < n/2$.*

Proof. Let $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ and $b^{(1)}, b^{(2)} \in \mathbb{F}_2^m$. We prove that h does not belong to $\mathcal{MM}^{\#}$, by using Lemma 3.1. We need to show that there does not exist an $(\frac{n+m}{2})$-dimensional subspace V such that

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

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

$$D_{(a^{(1)},b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x, y) = D_{a^{(1)}} D_{a^{(2)}} f(x) \oplus D_{b^{(1)}} D_{b^{(2)}} g(y). \tag{4}$$

Let V ba a $(\frac{n+m}{2})$-dimensional subspace of $\mathbb{F}_2^n \times \mathbb{F}_2^m$. There are two cases to be considered.

a. If $\dim(\{x|(x, y) \in V\}) \geqslant n/2$, we can select two $a^{(1)}, a^{(2)} \in \{x|(x, y) \in V\}$ such that

$$D_{a^{(1)}} D_{a^{(2)}} f(x) \neq constant$$

since r-ind$(f) < n/2$. Thus, we have

$$D_{(a^{(1)},b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x, y) \neq 0$$

for any $b^{(1)}, b^{(2)} \in \{y|(x, y) \in V\}$ since $D_{a^{(1)}} D_{a^{(2)}} f(x)$ only depends on variables x.

b. If $\dim(\{x|(x, y) \in V\}) < n/2$, then we must have

$$\dim(\{y|(0_n, y) \in V\}) > m/2$$

since $\dim(V) = (n+m)/2$ (that is, $||V|| = 2^{(n+m)/2}$). From Proposition 3.1, we can select two vectors $b^{(1)}, b^{(2)} \in \{y|(0_n, y) \in V\}$ such that

$$D_{b^{(1)}} D_{b^{(2)}} g(y) \neq 0.$$

Thus, we can select $(0_n, b^{(1)}), (0_n, b^{(2)}) \in V$ such that

$$D_{(0_n, b^{(1)})} D_{(0_n, b^{(2)})} h(x, y) = D_{b^{(1)}} D_{b^{(2)}} g(y) \neq 0.$$

□

Example 3.1. *Let $f \in \mathcal{B}_8$ be a bent function in $\mathcal{PS}^{\#}$ outside $\mathcal{MM}^{\#}$ whose truth table in hexadecimal form corresponds to*

$$T_f = 0x813dcc51a81752a59d810e0f1761c3c124a73361682b629908db9455710bfffe,$$

and let $g \in \mathcal{B}_4$ be defined by $g(x_0, \ldots, x_3) = x_0x_3 \oplus x_1x_2 \oplus x_1x_3$. The function $h \in \mathcal{B}_{12}$ defined as the direct sum of f and g is a bent function outside $\mathcal{MM}^{\#}$, which was checked using the Sage *implementation described in [17].*

Remark 3.1. *By Theorem 3.2, the function h in Example 3.1 is outside $\mathcal{MM}^{\#}$. However, since $r\text{-}ind(g) = m > m/2$, this does not follow from Lemma 3.2.*

In the other direction, it is necessary that either f or g is outside $\mathcal{MM}^{\#}$ so that $h = f \oplus g$ is outside $\mathcal{MM}^{\#}$.

Theorem 3.3. *Let f and g be two bent function on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. If the function h, defined as $h(x, y) = f(x) \oplus g(y)$, is outside $\mathcal{MM}^{\#}$, then either f or g is outside $\mathcal{MM}^{\#}$.*

Proof. Assuming that both f and g are in $\mathcal{MM}^{\#}$ implies the existence of two subspaces $\Delta^{(n)} \in \mathbb{F}_2^n$ and $\Delta^{(m)} \in \mathbb{F}_2^m$ with dimension $n/2$ and $m/2$, respectively, such that $D_{a^{(1)}} D_{a^{(2)}} f = 0$ and $D_{b^{(1)}} D_{b^{(2)}} g = 0$ for any $a^{(1)}, a^{(2)} \in \Delta^{(n)}, b^{(1)}, b^{(2)} \in \Delta^{(m)}$. Hence, we can set $\Delta = \Delta^{(n)} \times \Delta^{(m)}$. Further, we have

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

for any $(a^{(1)}, b^{(1)}), (a^{(2)}, b^{(2)}) \in \Delta$. From Lemma 3.1, h is in $\mathcal{MM}^{\#}$, which contradicts the fact that h is outside $\mathcal{MM}^{\#}$. □

Open Problem 1. *It is clear that $f \in \mathcal{B}_n$ is outside $\mathcal{MM}^{\#}$ implies that there exist two vectors $a, b \in V \subset \mathbb{F}_2^n$ such that $D_a D_b(f) \neq 0$, for some V with $\dim(V) \geqslant n/2$. From Lemma 3.1, we know $f \in \mathcal{B}_n$ is outside $\mathcal{MM}^{\#}$ if $r\text{-}ind(f) < n/2$. However, there might exist bent functions $\{f\}$ with $r\text{-}ind(f) = n/2$ outside $\mathcal{MM}^{\#}$ (that is, for which there exists a subspace V, with $\dim(V) = n/2$, so that $D_a D_b(f) = 0$ or $D_a D_b(f) = 1$). We leave the construction of such functions as an open problem.*

3.2 Indirect sum method giving rise to bent functions outside $\mathcal{MM}^{\#}$

The indirect sum method, introduced by Carlet [5, 7], is a secondary construction of bent functions that does not impose any additional conditions on the initial bent functions. In this section, we provide sufficient conditions on the bent functions f_i and g_i so that h defined by (5) is provably outside $\mathcal{MM}^{\#}$.

Corollary 2. *[5] Let f_1 and f_2 be bent functions on $\mathbb{F}_2^n$ (n even) and g_1 and g_2 be bent functions defined on $\mathbb{F}_2^m$. Then, $h : \mathbb{F}_2^n \times \mathbb{F}_2^m$ defined as*

$$h(x,y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y), \quad x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m, \tag{5}$$

is a bent function and its dual is obtained from f_1^*, f_2^*, g_1^* and g_2^* by the same formula as h is obtained from f_1, f_2, g_1 and g_2.

It is important to notice that f_i and g_i are arbitrary bent functions, but interestingly enough the condition that both $f_1 \oplus f_2$ and $g_1 \oplus g_2$ are bent implies that h defined by (5) is outside $\mathcal{MM}^{\#}$.

Theorem 3.4. *Let f_1 and f_2 be bent functions on $\mathbb{F}_2^n$ (n even). Let g_1 and g_2 be bent functions defined on $\mathbb{F}_2^m$ (m even). Let h be defined as in (5). If $f_1 \oplus f_2$ and $g_1 \oplus g_2$ are bent, then h is outside $\mathcal{MM}^{\#}$.*

Proof. Let $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ and $b^{(1)}, b^{(2)} \in \mathbb{F}_2^m$. We prove that h does not belong to $\mathcal{MM}^{\#}$ by using Lemma 3.1. We need to show that there does not exist an $(\frac{n+m}{2})$-dimensional subspace V such that

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

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

$$\begin{aligned} & D_{(a^{(1)},b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x,y) \\ = \; & D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (g_1 \oplus g_2)(y) D_{a^{(1)}} D_{a^{(2)}} (f_1 \oplus f_2)(x) \\ & \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \oplus D_{a^{(1)}} (f_1 \oplus f_2)(x) D_{b^{(1)}} (g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(2)}} (f_1 \oplus f_2)(x) D_{b^{(2)}} (g_1 \oplus g_2)(y) \oplus D_{a^{(1)} \oplus a^{(2)}} (f_1 \oplus f_2)(x) D_{b^{(1)} \oplus b^{(2)}} (g_1 \oplus g_2)(y) \end{aligned} \tag{6}$$

There are three cases to be considered.

(i) For $n = m$, there are two subcases.

(a) If $\dim(\{x|(x,y) \in V\}) = \dim(\{y|(x,y) \in V\}) = n$ (that is, $\{x|(x,y) \in V\} = \{y|(x,y) \in V\} = \mathbb{F}_2^n$), then there are two cases to be considered.

i. Assume that either $\deg(f_1 \oplus f_2) > 2$ or $\deg(g_1 \oplus g_2) > 2$. Without loss of generality, we suppose $\deg(f_1 \oplus f_2) > 2$. Then, we can find two vectors $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ such that

$$D_{a^{(1)}} D_{a^{(2)}} (f_1 \oplus f_2)(x) \neq constant. \tag{7}$$

Since the algebraic degree of $g_1 \oplus g_2$ is strictly greater than the algebraic degree of its derivatives, from (6) and (7), we obtain

$$D_{(a^{(1)},b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x,y) \neq 0.$$

ii. For $\deg(f_1 \oplus f_2) = 2$ and $\deg(g_1 \oplus g_2) = 2$, we can find two vectors $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ such that

$$D_{a^{(1)}} D_{a^{(2)}} (f_1 \oplus f_2)(x) = 1. \tag{8}$$

Since $g_1 \oplus g_2$ is bent and $\deg(g_1 \oplus g_2) = 2$, its derivatives are affine functions. We also know $D_{b^{(1)}} D_{b^{(2)}} g_1(y)$ has nonzero linear structures, since g_1 is a quadratic function. Hence, from (6) and (8), we get

$$D_{(a^{(1)},b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x,y) \neq 0.$$

(b) If $\dim(\{x|(x,y) \in V\}) < n$ or $\dim(\{y|(x,y) \in V\}) < n$, then we have $\{y|(0_n,y) \in V\} \neq \emptyset$ or $\{x|(x,0_n) \in V\} \neq \emptyset$. Without loss of generality, we suppose that $\{y|(0_n,y) \in V\} \neq \emptyset$. Hence, we can select $(0_n, b^{(1)}) \in V \cap (\{0_n\} \times \mathbb{F}_2^{n*})$ and $(a^{(2)}, b^{(2)}) \in V \cap (\mathbb{F}_2^{n*} \times \mathbb{F}_2^{n*})$. From (6), we have

$$\begin{aligned} & D_{(0_n,b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x,y) \\ = \; & D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(2)}} (f_1 \oplus f_2)(x) D_{b^{(1)}} (g_1 \oplus g_2)(y \oplus b^{(2)}) \\ \neq \; & 0, \end{aligned} \tag{9}$$

since $f_1 \oplus f_2$, $g_1 \oplus g_2$ are bent (that is, $D_{a^{(2)}}(f_1 \oplus f_2)(x) \neq$ *constant* and $D_{b^{(1)}}(g_1 \oplus g_2)(y \oplus b^{(2)}) \neq$ *constant*) and $\deg((f_1 \oplus f_2)(x)) > \deg(D_{a^{(2)}}(f_1 \oplus f_2)(x))$.

(ii) For $n \neq m$, there are also two cases to be considered.

(a) For $n > m$, we have $(n+m)/2 > m$. Thus, we can select two vectors $(a^{(1)}, 0_m) \in V \cap (\mathbb{F}_2^{n*} \times \{0_m\})$ and $(a^{(2)}, b^{(2)}) \in V \cap (\mathbb{F}_2^{n*} \times \mathbb{F}_2^{m*})$. From (6), we have

$$\begin{aligned} & D_{(a^{(1)},0_m)} D_{(a^{(2)},b^{(2)})} h(x,y) \\ = \; & D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus (g_1 \oplus g_2)(y) D_{a^{(1)}} D_{a^{(2)}} (f_1 \oplus f_2)(x) \\ & \oplus D_{a^{(1)}} (f_1 \oplus f_2)(x \oplus a^{(2)}) D_{b^{(2)}} (g_1 \oplus g_2)(y) \\ \neq \; & 0, \end{aligned} \tag{10}$$

since $f_1 \oplus f_2$, $g_1 \oplus g_2$ are bent (that is, $D_{a^{(1)}}(f_1 \oplus f_2)(x \oplus a^{(2)}) \neq$ *constant* and $D_{b^{(2)}}(g_1 \oplus g_2)(y) \neq$ *constant*) and $\deg((g_1 \oplus g_2)(y)) > \deg(D_{b^{(2)}}(g_1 \oplus g_2)(y))$.

(b) For $n < m$, we have $(n+m)/2 > n$. Now, we select $(0_n, b^{(1)}) \in V \cap (\{0_n\} \times \mathbb{F}_2^{m*})$ and $(a^{(2)}, b^{(2)}) \in V \cap (\mathbb{F}_2^{n*} \times \mathbb{F}_2^{m*})$ and from item $(i) - (b)$ we conclude that $D_{(0_n,b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x,y) \neq 0$. This concludes the proof.

□

It is tempting to relax the conditions on the initial functions as illustrated in the following example. The condition that either $\deg(f_1 \oplus f_2) > 2$ or $\deg(g_1 \oplus g_2) > 2$ seems to be sufficient at least for certain choices of the initial functions. However, proving this in general appears to be a difficult task since there exist certain $(n+m)/2$-dimensional subspaces of $\mathbb{F}_2^{(n+m)/2}$, say $\{V\}$, for which this condition is not enough to ensure the existence of $a, b \in V$ so that $D_a D_b h \neq 0$, for h defined by (5).

Example 3.2. *Let $f_1, f_2 \in \mathcal{B}_6$ and $g_1, g_2 \in \mathcal{B}_4$ be bent functions such that $\deg(f_1 \oplus f_2) > 2$. Then, $h \in \mathcal{B}_{10}$ defined by (5) is a bent function outside $\mathcal{MM}^{\#}$. For example, we may take*

$$\begin{aligned}
f_1(x_0,\ldots,x_5) &= x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1x_4 \oplus x_0x_2x_3 \oplus x_0x_2x_5 \oplus x_0x_3x_4 \oplus x_0x_3x_5 \\
&\quad \oplus x_0x_4x_5 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_2x_3x_4 \\
&\quad \oplus x_2x_3x_5 \oplus x_2x_4x_5 \\
f_2(x_0,\ldots,x_3) &= x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \\
g_1(x_0,\ldots,x_3) &= x_0x_1 \oplus x_0x_3 \oplus x_1x_2 \oplus x_0 \oplus x_1 \\
g_2(x_0,\ldots,x_3) &= x_0x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_1
\end{aligned}$$

The truth table in hexadecimal form of the function h obtained from (5) equals:

0x4874842e842eb78b842e7bd17bd14874842e48747bd17bd1b78b7bd17bd14874842e7bd148747bd17bd1b78bb78b842e7bd1b78bb78b842e4874842e842e842e842e7bd17bd17bd14874b78bb78b842e7bd1b78b842e842e7bd1842e842e842eb78b48747bd148747bd1842e842e842e7bd1842e842e842e4874842e842e842e

Using the Sage *implementation from [17], we have confirmed that $h \in \mathcal{B}_{10}$ is outside $\mathcal{MM}^{\#}$.*

Open Problem 2. *We leave as an open problem the specification of more relaxed sufficient conditions on the initial bent functions f_i and g_i used to define h in (5) so that h is provably outside $\mathcal{MM}^{\#}$.*

3.2.1 Outside $\mathcal{MM}^{\#}$ property from the class membership of the initial functions

We remark that the previous results do not impose any condition on the constituent bent functions in terms of their class membership. However, it turns out that the indirect sum behave quite similarly as the direct sum, though requiring additional constraints on the initial functions which ensure that h is outside $\mathcal{MM}^{\#}$. The following lemma is needed in the proof of our main result.

Lemma 3.3. *Let f_1 be a bent function on $\mathbb{F}_2^n$. If r-ind$(f_1) < n/2$, then there exist three vectors $a^{(1)}, a^{(2)}, a^{(3)} \in E$ such that $D_{a^{(1)}}D_{a^{(2)}}f_1(x) \neq$ constant, $D_{a^{(1)}}D_{a^{(3)}}f_1(x) \neq$ constant, and $D_{a^{(1)}}D_{a^{(2)}}f_1(x) \oplus D_{a^{(1)}}D_{a^{(3)}}f_1(x) \neq$ constant, where $E \subseteq \mathbb{F}_2^n$ is a subspace with $\dim(E) > n/2$.*

Proof. Since r-ind$(f_1) < n/2$, from Definitions 3.1 and 3.2, we know $\dim(\mathcal{RMS}(f_1)) < n/2$. Without loss of generality, set $\dim(\mathcal{RMS}(f_1)) = n/2 - 1$ and $\dim(E) = n/2 + 1$.

Let $U \subseteq E$ be a relaxed $\mathcal{MM}$-subspace of f_1 such that $U \cup \{\alpha \oplus U\}$ is not a relaxed $\mathcal{MM}$-subspace for all $\alpha \in E \setminus U$. Then, we have

$$\dim(E) - \dim(U) \geq \dim(E) - \dim(\mathcal{RMS}(f_1)) \geq 2. \tag{11}$$

Without loss of generality, we suppose $\dim(U) = n/2 - 1$. We set $\{\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n/2-1)}\}$ to be a basis of U and $\{\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n/2+1)}\}$ be a basis of E.

We set $U^{(\alpha)} = \{\gamma : D_\gamma D_\alpha f_1(x) = constant, \gamma \in E\}$, where $\alpha \in \{\alpha^{(n/2)}, \alpha^{(n/2+1)}, \alpha^{(n/2)} \oplus \alpha^{(n/2+1)}\}$. From r-ind$(f_1) < n/2$ and the definition of U, we have

$$U^{(\alpha^{(n/2)})} \subset E, \;\; U^{(\alpha^{(n/2+1)})} \subset E, \;\; U^{(\alpha^{(n/2)} \oplus \alpha^{(n/2+1)})} \subset E. \tag{12}$$

We also know $U^{(\alpha^{(n/2)})}$, $U^{(\alpha^{(n/2+1)})}$ and $U^{(\alpha^{(n/2)} \oplus \alpha^{(n/2+1)})}$ are subspaces of E. From (12), we have

$$\begin{aligned} \Delta := & \left(E \setminus U^{(\alpha^{(n/2)})}\right) \cap \left(E \setminus U^{(\alpha^{(n/2+1)})}\right) \cap \left(E \setminus U^{(\alpha^{(n/2)} \oplus \alpha^{(n/2+1)})}\right) \\ = & E \setminus \left(U^{(\alpha^{(n/2)})} \cup U^{(\alpha^{(n/2+1)})} \cup U^{(\alpha^{(n/2)} \oplus \alpha^{(n/2+1)})}\right) \neq \emptyset. \end{aligned} \tag{13}$$

Hence, we can select $a^{(1)} \in \Delta, a^{(2)} = \alpha^{(n/2)}, a^{(3)} = \alpha^{(n/2+1)}$. Further, we have $D_{a^{(1)}} D_{a^{(2)}} f_1(x) \neq constant$, $D_{a^{(1)}} D_{a^{(3)}} f_1(x) \neq constant$ and $D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus D_{a^{(1)}} D_{a^{(3)}} f_1(x) \neq constant$, since $D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus D_{a^{(1)}} D_{a^{(3)}} f_1(x) = D_{a^{(1)}} D_{a^{(2)} \oplus a^{(3)}} f_1(x)$. □

Theorem 3.5. *Let f_1 and f_2 be bent functions on $\mathbb{F}_2^n$ (n even). Let g_1 and g_2 be bent functions defined on $\mathbb{F}_2^m$ (m even) such that* $\deg(g_1 \oplus g_2) > 0$. *Let h be defined as in (5). If r-ind$(f_1) < n/2$ (hence $f_1 \notin \mathcal{MM}^\#$) and* $\deg(f_1 \oplus f_2) = 1$, *then h is outside $\mathcal{MM}^\#$.*

Proof. Let $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ and $b^{(1)}, b^{(2)} \in \mathbb{F}_2^m$. We prove that h does not belong to $\mathcal{MM}^\#$, by using Lemma 3.1. We need to show that there does not exist an $(\frac{n+m}{2})$-dimensional subspace V of $\mathbb{F}_2^{n+m}$ such that

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

for any $(a^{(1)}, b^{(1)})$, $(a^{(2)}, b^{(2)}) \in V$. Since $\deg(f_1 \oplus f_2) = 1$, we have

$$\begin{aligned} & D_{(a^{(1)}, b^{(1)})} D_{(a^{(2)}, b^{(2)})} h(x, y) \\ = \; & D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(1)}} (f_1 \oplus f_2)(x) D_{b^{(1)}} (g_1 \oplus g_2)(y) \oplus D_{a^{(2)}} (f_1 \oplus f_2)(x) D_{b^{(2)}} (g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(1)} \oplus a^{(2)}} (f_1 \oplus f_2)(x) D_{b^{(1)} \oplus b^{(2)}} (g_1 \oplus g_2)(y) \\ = \; & D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \\ & \oplus \varepsilon_{a^{(1)}} D_{b^{(1)}} (g_1 \oplus g_2)(y) \oplus \varepsilon_{a^{(2)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \oplus \varepsilon_{a^{(1)} \oplus a^{(2)}} D_{b^{(1)} \oplus b^{(2)}} (g_1 \oplus g_2)(y), \end{aligned} \tag{14}$$

where $\varepsilon_{a^{(1)}}, \varepsilon_{a^{(2)}}, \varepsilon_{a^{(1)} \oplus a^{(2)}} \in \mathbb{F}_2$. Since r-ind$(f_1) < n/2$, we know $\deg(f_1) \geq 3$.

There are three cases to be considered.

(i) For $\dim(\{x | (x, y) \in V\}) > n/2$, since r-ind$(f_1) < n/2$, from Definitions 3.1 and 3.2, we know $\dim(\mathcal{RMS}(f_1)) < n/2$. Without loss of generality, set $\dim(\mathcal{RMS}(f_1)) = n/2 - 1$.

From Lemma 3.3, we know there exist $(a^{(1)}, b^{(1)}), (a^{(2)}, b^{(2)}), (a^{(3)}, b^{(3)}) \in V$ such that

$$\begin{aligned} D_{a^{(1)}} D_{a^{(2)}} f_1(x) &\neq constant, \\ D_{a^{(1)}} D_{a^{(3)}} f_1(x) &\neq constant, \\ D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus D_{a^{(1)}} D_{a^{(3)}} f_1(x) = D_{a^{(1)}} D_{a^{(2)} \oplus a^{(3)}} f_1(x) &\neq constant. \end{aligned} \tag{15}$$

Since $f_1 \oplus f_2$ is given, from (15), we get

$$D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus (f_1 \oplus f_2)(x) \neq constant \tag{16}$$

or

$$D_{a^{(1)}}D_{a^{(3)}}f_1(x)\oplus(f_1\oplus f_2)(x)\neq constant. \tag{17}$$

Without loss generality, we assume that (16) holds. There are three cases to be considered.

(a) If $D_{b^{(1)}}D_{b^{(2)}}(g_1\oplus g_2)(y)\neq constant$, from (14), we obtain

$$D_{(a^{(1)},b^{(1)})}D_{(a^{(2)},b^{(2)})}h(x,y)\neq constant.$$

(b) If $D_{b^{(1)}}D_{b^{(2)}}(g_1\oplus g_2)(y)=1$, we conclude

$$D_{b^{(1)}}(g_1\oplus g_2)(y)\neq constant,$$

$$D_{b^{(2)}}(g_1\oplus g_2)(y)\neq constant$$

and

$$D_{b^{(1)}\oplus b^{(2)}}(g_1\oplus g_2)(y)\neq constant.$$

If (15), (16) and (14), we deduce

$$D_{(a^{(1)},b^{(1)})}D_{(a^{(2)},b^{(2)})}h(x,y)\neq constant.$$

(c) Finally, when $D_{b^{(1)}}D_{b^{(2)}}(g_1\oplus g_2)(y)=0$, from (15) and (14), we get

$$D_{(a^{(1)},b^{(1)})}D_{(a^{(2)},b^{(2)})}h(x,y)\neq constant.$$

(ii) If $\dim(\{x|(x,y)\in V\})=n/2$, then there are three cases to be considered.

(a) If $\dim(\{y|(x,y)\in V\})=m/2$, then

$$V=\{x|(x,0_m)\in V\}\times\{y|(0_n,y)\in V\}$$

since $\dim(V)=(n+m)/2$. Using the assumption that $r\text{-ind}(f_1)<n/2$, there will exist $(a^{(1)},0_m),(a^{(2)},0_m)\in V$ such that

$$D_{a^{(1)}}D_{a^{(2)}}f_1(x)\neq constant.$$

Applying this to (14), we deduce that

$$D_{(a^{(1)},0_m)}D_{(a^{(2)},0_m)}h(x,y)\neq constant.$$

(b) Assume now that $m/2<\dim(\{y|(x,y)\in V\})<(n+m)/2$. Then, for arbitrary $a_1,a_2\in\{x|(x,y)\in V\}$, we always have $\{y|(a_1,y)\in V\}\cap\{y|(a_2,y)\in V\}\neq\emptyset$. Hence, we can select two vectors $(a^{(1)},b^{(1)}),(a^{(2)},b^{(2)})\in V$ such that $b^{(1)}=b^{(2)}$ and $D_{a^{(1)}}D_{a^{(2)}}f_1(x)\neq constant$. Again, using that $D_{a^{(1)}}D_{a^{(2)}}f_1(x)\neq constant$ in (14), we conclude

$$D_{(a^{(1)},b^{(1)})}D_{(a^{(2)},b^{(2)})}h(x,y)\neq constant.$$

(c) When $\dim(\{y|(x,y)\in V\}) = (n+m)/2$, we have $\{y|(a_1,y)\in V\}\cap\{y|(a_2,y)\in V\} = \emptyset$ for arbitrary $a_1, a_2 \in \{x|(x,y)\in V\}$ and $\dim(\{y|(0_n,y)\in V\}) = m/2$. Since $\dim(\{\alpha|D_\alpha(f_1\oplus f_2)=0\}) = n-1$ and $\dim(\{x|(x,y)\in V\}) = n/2$, we can select one nonzero vector $a\in\{x|(x,y)\in V\}$ such that $D_a(f_1\oplus f_2)=0$. Further,

$$\dim(\{(0_n,y)|(0_n,y)\in V\}\cup\{(a,y)|(a,y)\in V\}) = m/2+1.$$

Then, by Proposition 3.1, we can select two vectors $(a^{(1)},b^{(1)}),(a^{(2)},b^{(2)})\in\{(0_n,y)|(0_n,y)\in V\}\cup\{(a,y)|(a,y)\in V\}$ such that

$$D_{b^{(1)}}D_{b^{(2)}}g_1(y)\neq 0.$$

Setting this in (14), we obtain

$$\begin{aligned} & D_{(a^{(1)},b^{(1)})}D_{(a^{(2)},b^{(2)})}h(x,y) \\ = \; & D_{b^{(1)}}D_{b^{(2)}}g_1(y)\oplus(f_1\oplus f_2)(x)D_{b^{(1)}}D_{b^{(2)}}(g_1\oplus g_2)(y)\neq 0. \end{aligned} \tag{18}$$

(iii) If $\dim(\{x|(x,y)\in V\}) < n/2$, then we have $\dim(\{y|(x,y)\in V\})\geq m/2+1$. Further, we have $\dim(\{y|(0,y)\in V\})\geq m/2+1$ since $\dim(V) = (n+m)/2$. Hence, from Proposition 3.1, we can select two vectors $(0_n,b^{(1)}),(0_n,b^{(2)})\in V$ such that

$$D_{b^{(1)}}D_{b^{(2)}}g_1(y)\neq 0.$$

Again, putting this in (14), we have

$$\begin{aligned} & D_{(0_n,b^{(1)})}D_{(0_n,b^{(2)})}h(x,y) \\ = \; & D_{b^{(1)}}D_{b^{(2)}}g_1(y)\oplus(f_1\oplus f_2)(x)D_{b^{(1)}}D_{b^{(2)}}(g_1\oplus g_2)(y)\neq 0. \end{aligned} \tag{19}$$

□

Remark 3.2. *We note that the functions f_1 and f_2 as well as g_1 and g_2 in Example 3.2 are not affine related, that is, $\deg(f_1\oplus f_2), \deg(g_1\oplus g_2) > 1$. This leads us to believe that the condition $\deg(f_1\oplus f_2)=1$ in Theorem 3.5 seems to be only sufficient but not necessary.*

Remark 3.3. *The main reason for using the condition that $\deg(f_1\oplus f_2)=1$ in Theorem 3.5 is related to $n/2$-dimensional subspaces V of $\mathbb{F}_2^{n+m}$ with the property that $\dim(\{x|(x,y)\in V\})\geq n/2$ and $\dim(\{y|(x,y)\in V\})\geq m/2$. In this case, we cannot ensure that some of the following inequalities $D_{a^{(1)}}D_{a^{(2)}}f_1(x)\neq(f_1\oplus f_2)(x)$, $D_{a^{(1)}}D_{a^{(2)}}f_1(x)\neq D_{a^{(1)}}(f_1\oplus f_2)(x)$ and $D_{a^{(1)}}D_{a^{(2)}}f_1(x)\neq D_{a^{(2)}}(f_1\oplus f_2)(x)$ hold.*

Similarly to Theorem 3.5, we can prove even a stronger statement which excludes the possibility of having constant second order derivatives of h on any $(n+m)/2$-dimensional subspace. The proof of Theorem 3.6 can be found in Appendix.

Theorem 3.6. *Let f_1 and f_2 be bent functions on $\mathbb{F}_2^n$ (n even). Let g_1 and g_2 be bent functions defined on $\mathbb{F}_2^m$ (m even) such that $\deg(g_1\oplus g_2)>0$. Let h be defined as in (5). If r-ind$(f_1) < n/2$, $\deg(f_1\oplus f_2)=1$ and r-ind$(g_1) < m/2+1$, then h is outside $\mathcal{MM}^\#$ and r-ind$(h) < (n+m)/2$.*

4 Design methods for homogenous bent functions

The design methods for homogenous bent functions are very few and it appears that this subclass of bent functions is quite small. The main progress has been made recently in [19], where the authors efficiently specified new homogenous cubic bent functions using the direct sum and stated the following open problem: Construct homogeneous cubic bent functions without affine derivatives outside the $\mathcal{MM}^{\#}$ class without the use of the direct sum. In this section, we positively answer this problem by applying the indirect sum method to suitably selected initial bent functions. Moreover, we improve the results in [19] with respect to the dimension of input variable space, see Table 1.

4.1 Homogenous bent functions using the indirect sum

In what follows, we construct homogeneous cubic bent functions without affine derivatives outside the $\mathcal{MM}^{\#}$ by using the indirect sum and thereby partially solve the open problem in [19].

Theorem 4.1. *Let n and m be two positive even integers. Let f_1 and g_1 be two homogeneous cubic bent functions on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. Let $f_2(x) = f_1(x) \oplus c \cdot x$, where $c \in \mathbb{F}_2^n \setminus \{0_n\}$, and $g_2(y) = g_1(y) \oplus Q(y)$ be also bent, where Q is a homogeneous quadratic function. Then, the function $h \in \mathcal{B}_{n+m}$ defined by (5) is a homogeneous cubic bent function. Further, if r-ind$(f_1) < n/2$, then h is outside $\mathcal{MM}^{\#}$. If f_1 has no affine derivatives and $\mathbb{FP}_{g_1} \cap \mathbb{FP}_{g_1 \oplus g_2} = \{0_m\}$, then h has no affine derivatives.*

Proof. From Corollary 2, h is a bent function in $n+m$ variables. Since $\deg(f_1 \oplus f_2) = 1$ and Q is a homogeneous quadratic function in m variables, then h is a homogeneous cubic bent function.

From Theorem 3.5, since r-ind$(f_1) < n/2$ and $\deg(f_1 \oplus f_2) = 1$, h is outside $\mathcal{MM}^{\#}$. For $a^{(1)} \in \mathbb{F}_2^n$ and $b^{(1)} \in \mathbb{F}_2^m$, we have

$$\begin{aligned} D_{(a^{(1)},b^{(1)})}h(x,y) = \; & D_{a^{(1)}}f_1(x) \oplus D_{b^{(1)}}g_1(y) \\ & \oplus (g_1 \oplus g_2)(y) D_{a^{(1)}}(f_1 \oplus f_2)(x) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}}(g_1 \oplus g_2)(y). \end{aligned} \tag{20}$$

To show that h has no affine derivatives, we consider two cases:

a) If $a^{(1)} = 0_n$, then $b^{(1)} \neq 0_m$. From (20), we deduce

$$D_{(0_n,b^{(1)})}h(x,y) = D_{b^{(1)}}g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}}(g_1 \oplus g_2)(y).$$

Since g_1 is cubic and $\mathbb{FP}_{g_1} \cap \mathbb{FP}_{g_1 \oplus g_2} = \{0_m\}$, then $\deg(D_{b^{(1)}}g_1(y)) = 2$ or $\deg(D_{b^{(1)}}(g_1 \oplus g_2)(y)) = 1$. Hence, $\deg(D_{(0_n,b^{(1)})}h) = 2$.

b) If $a^{(1)} \neq 0_n$, then $\deg(D_{a^{(1)}}f_1) = 2$ due to the assumption on f_1. From (20), we have $\deg(D_{(a^{(1)},b^{(1)})}h) = 2$ since $f_1 \oplus f_2$ is a linear function.

□

Remark 4.1. *One can also set* $Q(y) := g_1(y) \oplus g_1(y \oplus a) \oplus A(y)$ *in Theorem 4.1, where* $a \in \mathbb{F}_2^n \setminus \mathbb{FP}_{g_1}$ *and* $A(y)$ *stands for the affine terms of* $g_1(y) \oplus g_1(y \oplus a)$.

Corollary 3. *Let* n, m *and* t *be three positive even integers such that* $t \leq m$. *Let* f_1 *and* g_1 *be two homogeneous cubic bent functions on* $\mathbb{F}_2^n$ *and* $\mathbb{F}_2^m$, *respectively. Let* $f_2(x) = f_1(x) \oplus c \cdot x$, *where* $c \in \mathbb{F}_2^n \setminus \{0_n\}$, *and* $g_2(y) = g_1(y \oplus e^{(t)})$, *where* $e^{(t)} = (e_1^{(t)}, e_2^{(t)}, \ldots, e_m^{(t)}) \in \mathbb{F}_2^m$, $e_i^{(t)} = 1$ *if* $i = t$, $e_i^{(t)} = 0$ *otherwise. Let* h *be defined as in (5). If* $r\text{-}ind(f_1) < n/2$, *then* h *is a homogeneous cubic bent functions on* $\mathbb{F}_2^{n+m}$ *outside* $\mathcal{MM}^{\#}$. *If* f_1 *has no affine derivatives and* $\mathbb{FP}_{g_1} \cap \mathbb{FP}_{g_1 \oplus g_2} = \{0_m\}$, *then* h *has no affine derivatives.*

Proof. Since g_1 is a homogeneous cubic bent function, $g_1(y) \oplus g_1(y \oplus e^{(t)})$ is a homogeneous quadratic function. From Theorem 4.1, identifying $Q(y) := g_1(y) \oplus g_1(y \oplus e^{(t)})$, we know that h is a homogeneous cubic bent function since $g_2(y) = g_1(y) \oplus \big(g_1(y) \oplus g_1(y \oplus e^{(t)})\big) = g_1(y) + Q(y)$ is a bent function. Furthermore, Theorem 4.1 implies that h has no affine derivatives if f_1 has no affine derivatives and $\mathbb{FP}_{g_1} \cap \mathbb{FP}_{g_1 \oplus g_2} = \{0_m\}$. □

Homogeneous cubic bent function without affine derivatives outside $\mathcal{MM}^{\#}$ were specified by Polujan and Pott [19, Theorem 4.9] with the number of variables $n \geq 50$. The following example demonstrates that such functions can be specified on much smaller variable spaces compared to [19] (namely for $n = 20$).

Example 4.1. *Let* f_1 *be a homogenous cubic bent function without affine derivatives on* $\mathbb{F}_2^{10}$, *with* $r\text{-}ind(f_1) = 4$, *whose ANF is given as (see [19, Table 4])*
$f_1(x_0, \ldots, x_9) = x_0x_1x_5 \oplus x_0x_1x_6 \oplus x_0x_1x_7 \oplus x_0x_1x_9 \oplus x_0x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_2x_6 \oplus x_0x_2x_8 \oplus x_0x_2x_9 \oplus x_0x_3x_4 \oplus x_0x_3x_5 \oplus x_0x_3x_7 \oplus x_0x_3x_8 \oplus x_0x_3x_9 \oplus x_0x_4x_6 \oplus x_0x_5x_6 \oplus x_0x_5x_7 \oplus x_0x_5x_9 \oplus x_0x_6x_8 \oplus x_0x_6x_9 \oplus x_0x_8x_9 \oplus x_1x_2x_4 \oplus x_1x_2x_7 \oplus x_1x_2x_8 \oplus x_1x_2x_9 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_8 \oplus x_1x_5x_6 \oplus x_1x_5x_8 \oplus x_1x_5x_9 \oplus x_1x_6x_7 \oplus x_1x_6x_9 \oplus x_1x_7x_8 \oplus x_1x_7x_9 \oplus x_1x_8x_9 \oplus x_2x_3x_6 \oplus x_2x_3x_8 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_2x_4x_9 \oplus x_2x_5x_7 \oplus x_2x_5x_8 \oplus x_2x_6x_9 \oplus x_2x_7x_8 \oplus x_2x_7x_9 \oplus x_2x_8x_9 \oplus x_3x_4x_6 \oplus x_3x_4x_8 \oplus x_3x_4x_9 \oplus x_3x_5x_7 \oplus x_3x_5x_9 \oplus x_3x_6x_7 \oplus x_3x_6x_8 \oplus x_3x_6x_9 \oplus x_3x_7x_9 \oplus x_3x_8x_9 \oplus x_4x_5x_7 \oplus x_4x_5x_8 \oplus x_4x_5x_9 \oplus x_4x_6x_8 \oplus x_4x_6x_9 \oplus x_4x_7x_8 \oplus x_4x_7x_9 \oplus x_4x_8x_9 \oplus x_5x_6x_7 \oplus x_5x_7x_9 \oplus x_5x_8x_9 \oplus x_6x_7x_9$,
and let $g_1 = f_1$. *Then, from Corollary 3, the function* h *defined as in (5) via* f_1, f_2, g_1, g_2, *is a homogeneous cubic bent function without affine derivatives on* $\mathbb{F}_2^{20}$ *outside* $\mathcal{MM}^{\#}$.

Seberry, Xia and Pieprzyk in [21, Theorem 8] proved that one can construct homogeneous cubic bent functions for all even $m \neq 8$. Let $F : \mathbb{F}_2^m \to \mathbb{F}_2$ be defined as in [21, Theorem 8]

$$F(y) = \bigoplus_{i=1}^{m/2} y_i y_{i+m/2} \oplus C(y_{m/2+1}, y_{m/2+2}, \ldots, y_m),$$

where $C(y_{m/2+1}, y_{m/2+2}, \ldots, y_m)$ is a certain cubic function. Then, there exists a nonsingular matrix T such that $F(Ty)$ is a homogeneous cubic bent function [21]. Let ϕ be a linear permutation on $\mathbb{F}_2^{m/2}$ such that $\phi \oplus I$ is also a linear permutation, where I is the identity

permutation. Thus, $Q'(y) := \big(\phi(y_1, y_2, \ldots, y_{m/2})\big) \cdot (y_{m/2+1}, y_{m/2+2}, \ldots, y_m)$ is bent. Further, we have that

$$F(Ty) \oplus Q(y) \tag{21}$$

is a bent function, where $Q(y) = Q'(Ty) \oplus A(y)$ is a homogeneous quadratic function and $A(y)$ is affine.

In [19], the authors provided one 10-variable function, denoted by $h_4^{10} \in \mathcal{B}_{10}$, which is a homogeneous cubic bent function without affine derivatives and $r\text{-ind}(h_4^{10}) = 4 < 10/2$, thus $h_4^{10} \notin \mathcal{MM}^{\#}$.

Theorem 4.1, employing h_4^{10} and $F(Ty)$, implies the following result.

Theorem 4.2. *Let $n = 10$ and $m \geq 6$ be a positive even integer such that $m \neq 8$. Let $f_1 = h_4^{10}$, $g_1(y) = F(Ty)$ and $g_2(y) = g_1(y) \oplus Q(y)$, where $F(Ty)$ and $Q(y)$ are defined by (21). Let also $f_2(x) = f_1(x) \oplus c \cdot x$, where $c \in \mathbb{F}_2^{10} \setminus \{0_{10}\}$. Then, h defined by (5) is a homogeneous cubic bent function in $m + 10$ variables without affine derivatives outside $\mathcal{MM}^{\#}$.*

Proof. Since $r\text{-ind}(h_4^{10}) = 4 < 10/2$, from Theorem 4.1, we deduce that h is a homogeneous cubic bent functions in $m + 10$ variables outside the $\mathcal{MM}^{\#}$. Since Q is a quadratic bent function, we have $\mathbb{FP}_Q = \mathbb{FP}_{g_1 \oplus g_2} = \{0_m\}$. Theorem 4.1 implies that h has no affine derivatives. □

Theorem 4.3. *Let n, m be two positive even integers such that $n \geq 6, m \geq 6$. Let f_1 be a (homogeneous) cubic bent function with $\dim(\mathbb{FP}_{f_1}) = 1$ on $\mathbb{F}_2^n$. Without loss of generality, we set $\mathbb{FP}_{f_1} = \{0_n, \varepsilon\}$. Let $c \in \{\alpha | \alpha \in \mathbb{F}_2^n, \alpha \cdot \varepsilon = 1\}$ and define $f_2(x) = f_1(x) \oplus c \cdot x$. Let g_1 be a (homogeneous) cubic bent function without affine derivatives on $\mathbb{F}_2^m$ such that $r\text{-ind}(g_1) < m/2$. Define a bent function $g_2(y) = g_1(y) \oplus Q(y)$, where Q is a (homogeneous) quadratic function such that $\deg(D_b g_1(y) \oplus Q(y)) = 2$, for any $b \in \mathbb{FP}_Q \setminus \{0_m\}$. Then, h defined by (5) is a (homogeneous) cubic bent function without affine derivatives outside $\mathcal{MM}^{\#}$.*

Proof. From Theorem 4.1, we know that h is a (homogeneous) cubic bent function outside $\mathcal{MM}^{\#}$.

Now we prove h does not have affine derivatives. There are two cases to be considered. Let $a^{(1)} \in \mathbb{F}_2^n$ and $b^{(1)} \in \mathbb{F}_2^m$.

i) If $a^{(1)} \notin \mathbb{FP}_{f_1} = \{0_n, \varepsilon\}$, then $\deg(D_{a^{(1)}} f_1) = 2$. From (20), we have $\deg(D_{(a^{(1)}, b^{(1)})} h) = 2$ since $f_1 \oplus f_2$ is a linear function.

ii) If $a^{(1)} = \varepsilon$, from (20), we have

$$\begin{aligned} D_{(\varepsilon, b^{(1)})} h(x, y) = \; & D_\varepsilon f_1(x) \oplus D_{b^{(1)}} g_1(y) \\ & \oplus (g_1 \oplus g_2)(y) D_\varepsilon (c \cdot x) \oplus (c \cdot x) D_{b^{(1)}} (g_1 \oplus g_2)(y) \\ = \; & D_\varepsilon f_1(x) \oplus D_{b^{(1)}} g_1(y) \oplus Q(y) \oplus (c \cdot x) D_{b^{(1)}} Q(y). \end{aligned} \tag{22}$$

There are two cases to be considered.

(a) If $b^{(1)} \in \mathbb{FP}_Q \setminus \{0_m\}$, then $\deg(D_{b^{(1)}}g_1(y) \oplus Q(y)) = 2$. Hence, from (22), we have $\deg(D_{(\varepsilon,b^{(1)})}h(x,y)) = 2$.

(b) If $b^{(1)} \notin \mathbb{FP}_Q \setminus \{0_m\}$, from (22), we get $\deg(D_{(\varepsilon,b^{(1)})}h(x,y)) = 2$ since $\deg((c \cdot x)D_{b^{(1)}}Q(y)) = 2$ or $b^{(1)} = 0_m$.

□

Remark 4.2. *Let us consider the homogeneous quadratic function $Q(y) = D_{e^{(t)}}g_1(y)$ as defined in Corollary 3, where $e^{(t)} = (e_1^{(t)}, e_2^{(t)}, \ldots, e_m^{(t)}) \in \mathbb{F}_2^m$, $e_i^{(t)} = 1$ if $i = t$, $e_i^{(t)} = 0$ otherwise. The vector $e^{(t)}$ is obviously a fast point for the function Q (more precisely, it is a linear structure) because $D_{e^{(t)}}Q(y) = D_{e^{(t)}}D_{e^{(t)}}g_1 \equiv 0$. With respect to the above notation, we have that $D_{e^{(t)}}(g_1(y) \oplus Q(y)) = D_{e^{(t)}}g_1(y) \oplus D_{e^{(t)}}g_1(y) = 0$, thus Q does not satisfy Theorem 4.3. We also note that $D_{(\varepsilon,e^{(t)})}h(x,y) = D_\varepsilon f_1(x)$, which is an affine function. Using* Sage *we observed that ε is the only affine derivative of h.*

Based on the above remark, the following open problem is an interesting research challenge.

Open Problem 3. *Find instances of quadratic homogeneous bent functions Q which satisfy Theorem 4.3 and thus give rise to homogeneous cubic bent functions without affine derivatives outside $\mathcal{MM}^{\#}$.*

From Theorems 3.5 and 4.2, we note that [19, Theorem 4.9] (see Theorem 4.7) can be generalized as follows:

Theorem 4.4. *On $\mathbb{F}_2^n$ there exist homogeneous cubic bent functions (without affine derivatives) outside $\mathcal{MM}^{\#}$ for $n \geq 16$, $n \neq 18$.*

4.2 Non-decomposability of our bent functions

In this section, we solve an open problem on the decomposability of bent functions raised in [19, Open Problem 5.1]. We essentially show that the homogenous cubic bent functions constructed by means of Theorem 4.5 are non-decomposable in the sense of the definition below.

Definition 4.1. *[25] A function $f \in \mathcal{B}_n$ is said to be decomposable if there exists a nonsingular $n \times n$ matrix B over $\mathbb{F}_2$ and an integer l with $1 \leq l \leq n-1$ such that $f(xB) = g(y) \oplus h(z)$, where $x = (y,z), y \in \mathbb{F}_2^l, z \in \mathbb{F}_2^{n-l}, g \in \mathcal{B}_l$ and $h \in \mathcal{B}_{n-l}$. Otherwise, f is said to be non-decomposable.*

Lemma 4.1. *[25, Theorem 2] A function $f \in \mathcal{B}_n$ is decomposable if and only if there exists an integer p with $1 \leq p \leq n-1$, a p-dimensional linear subspace W of $\mathbb{F}_2^n$ and a complementary subspace U in $\mathbb{F}_2^n$ (thus $U + W = \mathbb{F}_2^n$) such that for every non-zero vector $\alpha \in W$ and every non-zero vector $\beta \in U$, we have*

$$f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \beta) \oplus f(x \oplus \alpha \oplus \beta) = 0.$$

The following result specifies some useful properties of the function h_4^{10} mentioned earlier.

Lemma 4.2. *Let $A := (a^{(1)}, a^{(2)}, \ldots, a^{(10)})$ be a basis of $\mathbb{F}_2^{10}$. Then, $||\{\varepsilon \in A \mid D_{a^{(i)}} D_\varepsilon h_4^{10} \neq 0\}|| \geq 3$, for any $a^{(i)} \in A$. Moreover, for disjoint non-empty subsets $S, T \subset A$ that partition A, $S \cup T = A$, there exist two vectors $\alpha^{(1)} \in S$ and $\alpha^{(2)} \in T$ such that $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_4^{10} \neq 0$.*

Proof. From Theorem 4.2, we know that h given by (5), defined using h_4^{10}, is a homogeneous cubic bent function in $m+10$ variables without affine derivatives (with m even). In particular, $\deg(D_{a^{(i)}} h_4^{10}) = 2$, for any $i = 1, \ldots, 10$. Without loss of generality, we set $i = 1$. We also know $\dim(\mathbb{FP}_{D_{a^{(1)}} h_4^{10}}) \leq n - \deg(D_{a^{(1)}} h_4^{10})$. Hence,

$$\dim(\mathbb{FP}_{D_{a^{(1)}} h_4^{10}}) = \dim(\{\varepsilon \mid D_{a^{(1)}} D_\varepsilon h_4^{10} = constant\}) \leq n - 2. \tag{23}$$

Since h_4^{10} is bent, $D_{a^{(1)}} h_4^{10}$ is a quadratic balanced function, that is, there exists at least one vector β such that $D_{a^{(1)}} D_\beta h_4^{10} = 1$ (due to the existence of linear terms in the ANF of $D_{a^{(1)}} h_4^{10}$). Furthermore, using (23), we have

$$\dim(\{\varepsilon \in \mathbb{F}_2^{10} \mid D_{a^{(1)}} D_\varepsilon h_4^{10} = 0\}) \leq n - 3, \tag{24}$$

which implies that

$$\dim(\langle\{\varepsilon \in \mathbb{F}_2^{10} \mid D_{a^{(i)}} D_\varepsilon h_4^{10} \neq 0, \varepsilon \in A\}\rangle) \geq 3, \ \forall a^{(i)} \in A, \tag{25}$$

where $\langle\cdot\rangle$ denotes the span of a set.

Now we prove $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_4^{10} \neq 0$. There are two cases to be considered.

a. For $||S|| \leq 3$ or $||T|| \leq 3$, from (25), we must two vectors $\alpha^{(1)} \in S$ and $\alpha^{(2)} \in T$ such that $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_4^{10} \neq 0$ since $D_\alpha D_\alpha h_4^{10} = 0$ for any $\alpha \in \mathbb{F}_2^{10}$.

b. Let $||S|| = 4$ (resp. 5) and $||T|| = 6$ (resp. 5). There are also two cases to be considered. Since $r\text{-ind}(h_4^{10}) = 4$, without loss of generality, let U be a 4-dimensional subspace of $\mathbb{F}_2^{10}$ such that $D_{a^{(1)}} D_{a^{(2)}} h_4^{10} = constant$, for any $a^{(1)}, a^{(2)} \in U$. From Definitions 3.1, and 3.2, there exist $a^{(1)}, a^{(2)} \in U \cup (\alpha^{(2)} \oplus U)$ for any $\alpha^{(2)} \in \mathbb{F}_2^{10} \setminus U$ such that $D_{a^{(1)}} D_{a^{(2)}} h_4^{10} \neq constant$.

   (a) When either $U \subseteq \langle S\rangle$ or $U \subseteq \langle T\rangle$, using Definitions 3.1 and 3.2, we can find two vectors $\alpha^{(1)} \in S$ and $\alpha^{(2)} \in T$ such that $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_{10} \neq 0$.
   In fact, for any $\alpha^{(2)} \in \mathbb{F}_2^{10} \setminus U$, there must exist one vector $\alpha^{(1)} \in U$ such that $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_{10} \neq 0$ since

$$D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_4^{10} = D_{\alpha^{(1)}} D_{\alpha^{(1)} \oplus \alpha^{(2)}} h_4^{10} = D_{\alpha^{(2)}} D_{\alpha^{(1)} \oplus \alpha^{(2)}} h_4^{10}.$$

   (b) When $U \nsubseteq \langle S\rangle$ and $U \nsubseteq \langle T\rangle$, we know $||S|| = 4$ (resp. 5) and $||T|| = 6$ (resp. 5). Further, $||U \cup \langle S\rangle|| < 2^4$ and $||U \cup \langle T\rangle|| < 2^4$. Hence, we can find two vectors $\alpha^{(1)} \in S$ and $\alpha^{(2)} \in T$ such that $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_4^{10} \neq 0$.

□

Theorem 4.5. *For $n = 10$, and even $m \geq 6$ such that $m \neq 8$, let h be defined as in Theorem 4.2. Then, h is a homogeneous non-decomposable cubic bent function in $m + 10$ variables without affine derivatives outside $\mathcal{MM}^{\#}$.*

Proof. From Theorem 4.2, $h \in \mathcal{B}_{m+10}$ is a homogeneous cubic bent function without affine derivatives outside $\mathcal{MM}^{\#}$.

It remains to prove that h is non-decomposable. From Lemma 4.1, we need to show that for arbitrary integer p with $1 \leq p \leq m + 10 - 1$, any p-dimensional linear subspace W of $\mathbb{F}_2^{n+m}$ and its arbitrary complementary subspace U in $\mathbb{F}_2^{n+m}$, there always exists two vectors $(a^{(w)}, b^{(w)}) \in W$ and $(a^{(u)}, b^{(u)}) \in U$, such that

$$D_{(a^{(w)},b^{(w)})} D_{(a^{(u)},b^{(u)})} h \neq 0,$$

where $a^{(w)}, a^{(u)} \in \mathbb{F}_2^n$ and $b^{(w)}, b^{(u)} \in \mathbb{F}_2^m$. Similarly to (14), we have

$$\begin{array}{ll} & D_{(a^{(w)},b^{(w)})} D_{(a^{(u)},b^{(u)})} h(x,y) \\ = & D_{a^{(w)}} D_{a^{(u)}} f_1(x) \oplus D_{b^{(w)}} D_{b^{(u)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(w)}} D_{b^{(u)}} (g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(w)}} (f_1 \oplus f_2)(x) D_{b^{(w)}} (g_1 \oplus g_2)(y) \oplus D_{a^{(u)}} (f_1 \oplus f_2)(x) D_{b^{(u)}} (g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(w)} \oplus a^{(u)}} (f_1 \oplus f_2)(x) D_{b^{(w)} \oplus b^{(u)}} (g_1 \oplus g_2)(y). \end{array} \tag{26}$$

Since W is a p-dimensional linear subspace of $\mathbb{F}_2^{m+10}$ and U is the complementary subspace of W in $\mathbb{F}_2^{m+10}$, we have

$$\begin{array}{l} \langle \{x \mid (x,y) \in W\} \cup \{x \mid (x,y) \in U\} \rangle = \mathbb{F}_2^n, \\ \langle \{y \mid (x,y) \in W\} \cup \{y \mid (x,y) \in U\} \rangle = \mathbb{F}_2^m. \end{array} \tag{27}$$

Further, for any vector $(a, b) \in \mathbb{F}_2^{n+m}$, we have $(a^{(w)}, b^{(w)}) \in W$ and $(a^{(u)}, b^{(u)}) \in U$ such that $(a, b) = (a^{(w)}, b^{(w)}) \oplus (a^{(u)}, b^{(u)})$.

There are two cases to be considered:

a) For $\{x \mid (x, y) \in W\} = \{0_n\}$, from (27), we have $\{x \mid (x, y) \in U\} = \mathbb{F}_2^n$ and $W \subseteq \{0_n\} \times \mathbb{F}_2^m$. Further, we can select $(0_n, b^{(w)}) \in W, (a^{(u)}, b^{(u)}) \in U$ such that $D_{a^{(u)}}(f_1 \oplus f_2) = 1$ (since $\deg(f_1 \oplus f_2) = 1$) and

$$D_{b^{(w)}} D_{b^{(u)}} g_1(y) \oplus D_{b^{(w)}} (g_1 \oplus g_2)(y \oplus b^{(u)}) \neq constant, \tag{28}$$

since $g_1 \oplus g_2$ is a bent function (that is, $D_{\beta^{(1)}}(g_1 \oplus g_2)(y) \oplus D_{\beta^{(2)}}(g_1 \oplus g_2)(y) = D_{\beta^{(1)} \oplus \beta^{(2)}}(g_1 \oplus g_2)(y \oplus \beta^{(1)}) \neq constant$ if $\beta^{(1)} \neq \beta^{(2)}$) and $\{x \mid (x, y) \in U\} = \mathbb{F}_2^n$. From (26), we have

$$\begin{array}{ll} & D_{(a^{(w)},b^{(w)})} D_{(a^{(u)},b^{(u)})} h(x,y) \\ = & D_{b^{(w)}} D_{b^{(u)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(w)}} D_{b^{(u)}} (g_1 \oplus g_2)(y) \\ & \oplus D_{b^{(w)}} (g_1 \oplus g_2)(y \oplus b^{(u)}) \neq 0. \end{array} \tag{29}$$

b) For $\{x \mid (x,y) \in U\} = \{0_n\}$, from (27), we have $\{x \mid (x,y) \in W\} = \mathbb{F}_2^n$ and $U \subseteq \{0_n\} \times \mathbb{F}_2^m$. Similarly to a), we deduce $D_{(a^{(w)},b^{(w)})}D_{(a^{(u)},b^{(u)})}h(x,y) \neq 0$.

c) When both $\{x|(x,y) \in W\} \neq \{0_n\}$ and $\{x \mid (x,y) \in U\} \neq \{0_n\}$, from Lemma 4.2, there exist two vectors $a^{(w)} \in \{x \mid (x,y) \in W\}$ and $a^{(u)} \in \{x \mid (x,y) \in U\}$ such that $D_{a^{(w)}}D_{a^{(u)}}f_1 \neq 0$. Then, there must exist $(a^{(w)}, b^{(w)}) \in W$ and $(a^{(u)}, b^{(u)}) \in U$ such that $b^{(w)} = b^{(u)}$, since $(a^{(w)} \oplus a^{(u)}, 0_m) \in \mathbb{F}_2^{n+m}$. From (26), we have

$$\begin{aligned} & D_{(a^{(w)},b^{(w)})}D_{(a^{(u)},b^{(w)})}h(x,y) \\ = \; & D_{a^{(w)}}D_{a^{(u)}}f_1(x) \oplus D_{b^{(w)}}D_{b^{(w)}}g_1(y) \oplus (f_1 \oplus f_2)(x)D_{b^{(w)}}D_{b^{(w)}}(g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(w)}}(f_1 \oplus f_2)(x)D_{b^{(w)}}(g_1 \oplus g_2)(y) \oplus D_{a^{(u)}}(f_1 \oplus f_2)(x)D_{b^{(w)}}(g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(w)} \oplus a^{(u)}}(f_1 \oplus f_2)(x)D_{b^{(w)} \oplus b^{(w)}}(g_1 \oplus g_2)(y) \\ = \; & D_{a^{(w)}}D_{a^{(u)}}f_1(x) \oplus D_{a^{(w)} \oplus a^{(u)}}(f_1 \oplus f_2)(x)D_{b^{(w)}}(g_1 \oplus g_2)(y). \end{aligned} \tag{30}$$

There are two cases to be considered:

i) If $D_{a^{(w)} \oplus a^{(u)}}(f_1 \oplus f_2) = 0$, then $D_{(a^{(w)},b^{(w)})}D_{(a^{(u)},b^{(w)})}h(x,y) = D_{a^{(w)}}D_{a^{(u)}}f_1(x) \neq 0$.

ii) If $D_{a^{(w)} \oplus a^{(u)}}(f_1 \oplus f_2) = 1$, then $D_{(a^{(w)},b^{(w)})}D_{(a^{(u)},b^{(w)})}h(x,y) = D_{a^{(w)}}D_{a^{(u)}}f_1(x) \oplus D_{b^{(w)}}(g_1 \oplus g_2)(y) \neq 0$ since $g_1 \oplus g_2$ is a bent function.

□

Open Problem 4. *[19, Open Problem 5.1] Construct homogeneous cubic bent functions without affine derivatives outside the class $\mathcal{MM}^{\#}$ without the use of the direct sum.*

Apparently, if h is obtained by using the direct sum of two functions, then h is decomposable. Thus, if h is non-decomposable, then h is a bent function which cannot be represented as a direct sum of two functions on disjoint variable spaces (under an invertible linear transform). The functions constructed by Theorem 4.5 are homogeneous cubic bent functions without affine derivatives outside the class $\mathcal{MM}^{\#}$ and does not fall into the framework of the direct sum. Hence, we answer positively the open problem above.

4.3 Another method of specifying (non-decomposable) cubic bent functions

We now utilize a method of specifying cubic bent functions without affine derivatives specified in [3], suitable to be used in the indirect sum. Before we proceed, recall that the absolute trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$ is defined as $Tr_1^k(x) = x + x^{2^1} + \cdots + x^{2^{k-1}}$.

Lemma 4.3. *[3] Let $m = 2t$ be an even integer $m \geq 6, m \neq 8$, and let j be an integer such that $1 \leq j < t$ and $\gcd(2^j + 1, 2^t - 1) = 1$. The cubic bent function g on $\mathbb{F}_2^m$ defined by $g(z,w) = Tr_1^t(zw^{2^j+1})$ has no affine derivatives.*

This approach can be embedded in the indirect sum method so that the resulting bent functions are without affine derivatives and additionally do not belong to $\mathcal{MM}^{\#}$.

Theorem 4.6. *Let $n, m = 2t$ be two even integers $n \geq 10, m \geq 6$ and $m \neq 8$ (due to Lemma 4.3). Let $1 \leq j < t$ such that $\gcd(2^j + 1, 2^t - 1) = 1$. Let f be a cubic function on $\mathbb{F}_2^n$ without affine derivatives such that $r\text{-ind}(f) < n/2$. Define a cubic function g on $\mathbb{F}_2^m$ as $g(z, w) = Tr_1^t(zw^{2^j+1})$ and let the function h on $\mathbb{F}_2^{n+m}$ be given as*

$$h(x, z, w) = f(x) + g(z, w) + Tr_1^n(ax)\left(Tr_1^t(zw^{2^j+1}) + Tr_1^t((z + c)w^{2^j+1})\right),$$

where $x \in \mathbb{F}_{2^n}, z, w \in \mathbb{F}_{2^t}$ and $c \in \mathbb{F}_{2^t} \setminus \{0\}$. Then, h is a cubic bent function without affine derivatives outside $\mathcal{MM}^{\#}$.

Proof. From Lemma 4.3, we know that g is a bent function in m variables. Set $f'(x) = f(x) + Tr_1^n(ax)$ and $g'(z, w) = g(z, w) + (g(z, w) + g(z + c, w)) = g(z + c, w)$. Then, f' and g' are bent. Corollary 2 implies that h is a cubic bent function.

By Lemma 4.3, g has no affine derivatives. Similarly to the proof of Theorem 4.1, one can show that h has no affine derivatives.

Furthermore, $r\text{-ind}(f) < n/2$ and $\deg(f + f') = 1$. By Theorem 4.1, using the fact that $r\text{-ind}(f) < n/2$, h is outside $\mathcal{MM}^{\#}$. □

Remark 4.3. *Theorem 4.6 provides a generic construction of cubic bent functions on $\mathbb{F}_2^k$ (with $k = n+m$) without affine derivatives and outside $\mathcal{MM}^{\#}$, for even $k \geq 16$ with $k \neq 18$. However, these bent functions are not necessarily homogeneous. A similar approach, based on Lemma 4.3 above, was considered by Mandal* et al. *in [13] but without the condition that resulting bent functions are outside $\mathcal{MM}^{\#}$.*

Nevertheless, referring to the above remark, by selecting $f = h_4^{10}$ the function h in Theorem 4.6 is a non-decomposable cubic bent function without affine derivatives outside $\mathcal{MM}^{\#}$, see also Section 4.2.

In [19], the series of existence results about cubic bent functions with nice cryptographic properties were presented.

Theorem 4.7. *[19, Theorem 4.9] On $\mathbb{F}_2^n$ there exist:*

1. *Cubic bent functions outside $\mathcal{MM}^{\#}$ for all $n \geq 10$.*
2. *Cubic bent functions without affine derivatives outside $\mathcal{MM}^{\#}$ for all $n \geq 26$.*
3. *Homogeneous cubic bent functions outside $\mathcal{MM}^{\#}$ for all $n \geq 26$.*
4. *Homogeneous cubic bent functions without affine derivatives outside $\mathcal{MM}^{\#}$ for all $n \geq 50$.*

According to Corollary 3 and Theorem 4.6, we substantially improve the above results in terms of decreased variable spaces by provide new instances of (homogenous) cubic bent functions having additional properties (not having affine derivatives and being outside $\mathcal{MM}^{\#}$).

Theorem 4.8. *On $\mathbb{F}_2^n$ there exist:*

1. *Cubic bent functions outside $\mathcal{MM}^{\#}$ for all $n \geq 10$.*

2. *(Non-decomposable) cubic bent functions without affine derivatives outside $\mathcal{MM}^{\#}$ for all $n \geq 20$.*

3. *Homogeneous non-decomposable cubic bent functions outside $\mathcal{MM}^{\#}$ for all $n \geq 20$.*

4. *Homogeneous non-decomposable cubic bent functions without affine derivatives outside $\mathcal{MM}^{\#}$ for all $n \geq 20$.*

Proof. We know that h_4^{10} is a homogeneous cubic bent function without affine derivatives outside $\mathcal{MM}^{\#}$. From Theorem 3.2, we know cubic bent functions outside $\mathcal{MM}^{\#}$ in n variables can be obtained for $n \geq 10$, thus Case 1 holds. Theorems 4.5 and 4.6 support Case 2., whereas Theorem 4.5 implies that Cases 3 and 4 hold. □

Let "(H)CBF" denote "(homogeneous) cubic bent functions"' and "wAD" denote "without affine derivatives". To give a better overview and comparison of the results in this paper with those in [19], we present the following table:

Function	[19] $n \geq$	Missing n	$n \geq$	Missing n
CBF outside $\mathcal{MM}^{\#}$	10	-	10	-
CBFwAD outside $\mathcal{MM}^{\#}$	26	14, 18* , 24	20	14, 18
HCBF outside $\mathcal{MM}^{\#}$	26	12, 14, 18, 24	20	12, 14, 18
HCBFwAD outside $\mathcal{MM}^{\#}$	50	12, 14, 16, 18, 24, 26, 28, 38, 48	20	12, 14, 18

Table 1: Comparison of bounds for the dimension n obtained in [19] and this article. The entry denoted 18^* is the correct value instead of 16 stated in [19].

5 Vectorial bent functions strongly outside $\mathcal{MM}^{\#}$

Constructing vectorial bent functions whose all nonzero component functions are outside $\mathcal{MM}^{\#}$, named strongly outside $\mathcal{MM}^{\#}$ in [18], is considered to be a difficult problem.

Below we use the indirect sum in connection to Theorem 3.4 to show the existence of these objects for relatively large output dimensions.

Theorem 5.1. *Let $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ and $G : \mathbb{F}_2^{2m} \to \mathbb{F}_2^m$ be two vectorial bent functions, with $n < m$, whose coordinate representations are $F = (f_0, \ldots, f_{n-1})$ and $G = (g_0, \ldots, g_n, \ldots, g_{m-1})$, respectively. We set*

$$h_i(x, y) = f_i(x) \oplus g_i(y) \oplus (f_i \oplus f_{(i+1) \mod n})(x) g_n(y), \tag{31}$$

where $i = 0, 1, \ldots, n-1$. Then, $H = (h_0, h_1, \ldots, h_{n-1})$ is a bent $(2(n+m), n)$-function, i.e. $H : \mathbb{F}_2^{2(n+m)} \to \mathbb{F}_2^n$ is vectorial bent. Furthermore, the $(2(n+m), n-1)$-function $H' = (h_0, h_1, \ldots, h_{n-2})$ is strongly outside $\mathcal{MM}^{\#}$.

Proof. We first prove any h_i is a bent function in $n+m$ variables. We know that $f_i, f_{(i+1) \bmod n}$ are bent. From Corollary 2, h_i is bent if g_i and $g_i \oplus g_n$ are bent. Note, that $g_n = g_i \oplus (g_i \oplus g_n)$. Since G is vectorial bent, it follows that h_i is bent.

Let $0 \neq c \in \mathbb{F}_2^{n+m}$ be arbitrary and let us consider the bentness of the component $c \cdot H$. We have:

$$\begin{aligned} c \cdot H = & \; c \cdot (h_0, h_1, \ldots, h_{n-1})(x, y) \\ = & \; (c_0 h_0 \oplus c_1 h_1 \oplus \cdots \oplus c_{n-1} h_{n-1})(x, y) \\ = & \; (c_0 f_0 \oplus c_1 f_1 \oplus \cdots \oplus c_{n-1} f_{n-1})(x) \oplus (c_0 g_0 \oplus c_1 g_1 \oplus \cdots \oplus c_{n-1} g_{n-1})(y) \\ & \oplus (c_0(f_0 \oplus f_1) \oplus c_1(f_1 \oplus f_2) \oplus \cdots \oplus c_{n-1}(f_{n-1} \oplus f_0))(x) g_n(y) \\ = & \; (c \cdot F)(x) \oplus (c \cdot G')(y) \oplus (c \cdot F \oplus c \cdot F')(x) g_n(y) \\ = & \; (c \cdot F)(x) \oplus (c \cdot G')(y) \oplus (c \cdot F \oplus c \cdot F')(x)(c \cdot G' \oplus (c \cdot G' \oplus g_n))(y), \end{aligned} \tag{32}$$

where $G' = (g_0, \ldots, g_{n-1})$ and $F' = (f_1, \ldots, f_{n-1}, f_0)$. We know that $c \cdot F$, $c \cdot F'$, $c \cdot G'$ and $c \cdot G' \oplus g_n$ are bent, as F and G are vectorial bent. Thus, from Corollary 2, it follows that $c \cdot H'$ is also bent, for all $0 \neq c \in \mathbb{F}_2^{n+m}$. In other words, H is a bent $(2(n+m), n)$-function.

If $c \notin \{0_n, 1_n\}$, then the function $c \cdot F \oplus c \cdot F'$ is bent. We also know that g_n is bent. Hence, from Theorem 3.4, the function $c \cdot (h_0, h_1, \ldots, h_{n-1})$ is outside $\mathcal{MM}^{\#}$ for $c \in \mathbb{F}_2^n \backslash \{0_n, 1_n\}$ and consequently, $H' = (h_0, h_1, \ldots, h_{n-2})$ is a bent $(2(n+m), n-1)$-function strongly outside $\mathcal{MM}^{\#}$. □

Remark 5.1. *Since G is vectorial bent, the function g_n in (31) can be replaced by $d \cdot (g_n, g_{n+1}, \ldots, g_{m-1})$, where $d \in \mathbb{F}_2^{m-n} \backslash \{0_{m-n}\}$.*

For $n = m$, from Theorem 5.1, we have the following corollary.

Corollary 4. *Let $F, G : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ be two vectorial bent functions, whose coordinate representations are $F = (f_0, \ldots, f_{n-1})$ and $G = (g_0, \ldots, g_{n-1})$, respectively. We set*

$$h_i(x, y) = f_i(x) \oplus g_i(y) \oplus (f_i \oplus f_{i+1})(x) g_{n-1}(y), \; x, y \in \mathbb{F}_2^{2n}, \tag{33}$$

where $i = 0, 1, \ldots, n-2$. Then, $H' = (h_0, h_1, \ldots, h_{n-2})$ is a vectorial bent function, where $H' : \mathbb{F}_2^{4n} \to \mathbb{F}_2^{n-1}$, and it is strongly outside $\mathcal{MM}^{\#}$.

Example 5.1. *Let us consider the functions $F(x, y) = xy$ and $G(x, y) = xy^5$, where $x, y \in \mathbb{F}_{2^3}$. From Corollary 4, the function $H = (h_0, h_1)$, where h_i is defined with (33), is a bent $(12, 2)$-function strongly outside $\mathcal{MM}^{\#}$. The `base64` representations of h_0 and h_1 are (35) and (36), which can be found in the appendix. Additionally, the bentness of H and its exclusion from $\mathcal{MM}^{\#}$ have been confirmed using* Sage.

5.1 A generic construction using companion matrices

We now employ the indirect sum and primitive polynomials in the design of vectorial bent functions strongly outside $\mathcal{MM}^{\#}$. It is well-known that if $p(z) = z^m + a_{m-1} z^{m-1} + \ldots + a_1 z +$

1, $a_i \in \mathbb{F}_2$ is a primitive polynomial over the field $\mathbb{F}_2$ (which implies that $wt((a_1, \ldots, a_{m-1}))$ is odd), then its order is equal to $2^m - 1$. The companion matrix $\mathbf{A}$ of $p(z)$ is

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_{m-1} \end{bmatrix}.$$

Thus, we have $\mathbf{A}^i \neq \mathbf{A}^j$ for $0 \leq i < j \leq 2^m - 2$. Theorem 5.1 then induces the following generic construction of vectorial bent functions that are strongly outside $\mathcal{MM}^{\#}$.

Theorem 5.2. *Let n, m be two positive integers such that $n < m$. Let π and ϕ be two arbitrary permutations in n and m variables, respectively. Let*

$$f_i(x^{(1)}, x^{(2)}) = \mathbf{A}^i \pi(x^{(2)}) \cdot x^{(1)}, \quad g_j(y^{(1)}, y^{(2)}) = \mathbf{B}^j \phi(y^{(2)}) \cdot y^{(1)}, \quad x^{(1)}, x^{(2)} \in \mathbb{F}_2^n, y^{(1)}, y^{(2)} \in \mathbb{F}_2^m, \tag{34}$$

where $i = 0, 1, \ldots, n-1, j = 0, 1, \ldots m-1$, and $\mathbf{A}, \mathbf{B}$ be companion matrices of the corresponding primitive polynomials over $\mathbb{F}_2$ of degree n and m, respectively. Let $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ and $G : \mathbb{F}_2^{2m} \to \mathbb{F}_2^m$ be two vectorial bent functions, whose coordinate representations are $F = (f_0, \ldots, f_{n-1})$ and $G = (g_0, \ldots, g_n, \ldots, g_{m-1})$, respectively. Let h_i be defined by (31). Then, $H = (h_0, h_1, \ldots, h_{n-1})$ is a bent $(2(n+m), n)$-function. Further, the $(2(n+m), n-1)$-function $H' = (h_0, h_1, \ldots, h_{n-2})$ is strongly outside $\mathcal{MM}^{\#}$.

Proof. Since $\mathbf{A}, \mathbf{B}$ are companion matrices of the corresponding primitive polynomials over $\mathbb{F}_2$ of degree n and m, respectively, we conclude that $\bigoplus_{i=0}^{n-1} \lambda_i \mathbf{A}^i \pi(x^{(2)})$ and $\bigoplus_{j=0}^{m-1} \lambda_j \mathbf{B}^j \phi(y^{(2)})$ are also permutations in n and m variables, respectively. Hence, F and G are two vectorial bent functions. From Theorem 5.1, H is a bent $(2(n+m), n)$-function and the $(2(n+m), n-1)$-function $H' = (h_0, \ldots, h_{n-2})$ is strongly outside $\mathcal{MM}^{\#}$. □

In difference to [18], where the output dimension of this class of vectorial bent functions was only two, the value $n - 1$ is a significant improvement. It can be easily verified that $(2(n+m), n-1)$ functions provide a larger output dimension compared to $(n, n/6)$ functions (also strongly outside $\mathcal{MM}^{\#}$) recently specified in [1]. Notice, however, that the maximal output dimension of a vectorial bent function in $2(n+m)$ variables is $n+m$. Therefore, our approach still does not provide vectorial bent functions strongly outside $\mathcal{MM}^{\#}$ with maximal output dimension. The existence of these objects still remains unknown.

6 Conclusions

We have shown that the indirect sum method, under certain conditions on its initial bent functions, can generate bent functions that are provably outside the completed Maiorana-McFarland class. Most notably, this method also give rise to homogenous cubic bent functions outside $\mathcal{MM}^{\#}$ which are characterized by some interesting cryptographic properties such as the absence of affine derivatives and inseparability. Moreover, vectorial bent functions

strongly outside $\mathcal{MM}^{\#}$ with the largest output space dimension currently known can be designed using this technique. An interesting research problem is to further relax the sufficient conditions on the initial bent functions for the purpose of enlarging the class of bent functions lying outside $\mathcal{MM}^{\#}$.

References

[1] A. Bapić, and E. Pasalic, "Constructions of (vectorial) bent functions outside the completed Maiorana-McFarland class," *Discret. Appl. Math.*, vol. 314, pp. 197–212, 2022.

[2] A. Bapić, E. Pasalic, F. Zhang and S. Hodžić, "Constructing new superclasses of bent functions from known ones," *Cryptogr. Commun.*, (2022). https://doi.org/10.1007/s12095-022-00566-7.

[3] A. Canteaut and P. Charpin, "Decomposing bent functions," *IEEE Trans. Inf. Theory*, vol. 49, no. 8, pp. 2004–2019, Aug. 2003.

[4] C. Carlet, "Two new classes of bent functions," in *Proc. EUROCRYPT '93,* in Lecture Notes in Computer Science, vol.e 765, 1993, pp. 77–101.

[5] C. Carlet,"On the secondary constructions of resilient and bent functions," in *Proc. Coding, Cryptograph. Combinat.*, published by Birkhäuser Verlag, vol. 23, 2004, pp. 3–28.

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

[7] C. Carlet, F. Zhang, and Y. Hu, "Secondary constructions of bent functions and their enforcement," *Adv. Math. Commun.*, vol. 6, pp. 305–314, 2012.

[8] C. Carlet, and S. Mesnager, "Four decades of research on bent functions," *Designs, Codes and Cryptogr.*, vol. 78, no. 1, pp. 5–50, 2016.

[9] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation. University of Maryland, College Park, Md, USA, 1974.

[10] M. Duan, X. Lai, M. Yang, X. Sun, and B. Zhu, "Distinguishing properties of higher order derivatives of Boolean functions," Cryptology ePrint Archive, Report 2010/417 (2010). Available: https://eprint.iacr.org/2010/417.pdf.

[11] S. Hodžić, E. Pasalic, and Y. Wei, "A general framework for secondary constructions of bent and plateaued functions," *Designs, Codes and Cryptogr.*, vol. 88, no. 10, pp. 2007–2035, 2020.

[12] S. Kudin, E. Pasalic, N. Cepak, and F. Zhang, "Permutations without linear structures inducing bent functions outside the completed Maiorana-McFarland class," *Cryptogr. Commun.*, vol. 14, pp.101–116, 2022.

[13] B. Mandal, S. Gangopadhyay, and P. Stanica, "Cubic Maiorana-McFarland bent functions with no affine derivative," *Int. J. Comput. Math. Comput. Syst. Theory,* vol. 2, no. 1, pp. 14–27, 2017.

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

[15] S. Mesnager, " Several new infinite families of bent functions and their duals," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 4397–4407, 2014.

[16] S. Mesnager, "Bent functions - Fundamentals and Results". Springer, 2016, ISBN 978-3-319-32593-4.

[17] E. Pasalic, A, Bapić, F. Zhang, and Y. Wei, "Explicit infinite families of bent functions outside $\mathcal{MM}^{\#}$," Cryptology ePrint Archive, Report (2022). Available at https://eprint.iacr.org/2022/1126

[18] E. Pasalic, F. Zhang, S. Kudin, Y. Wei, "Vectorial bent functions weakly/strongly outside the completed Maiorana-McFarland class," *Discret. Appl. Math.*, vol. 294, pp. 138–151, 2021.

[19] A. A. Polujan, and A. Pott, "Cubic bent functions outside the completed Maiorana-McFarland class," *Des. Codes Cryptogr.*, vol. 88, pp. 1701–1722, 2020.

[20] O. S. Rothaus, "On 'bent' functions," *J. Combinatorial Theory, Ser. A*, vol. 20, no. 3, pp. 300–305, 1976.

[21] J. Seberry, T. Xia, and J. Pieprzyk, "Construction of cubic homogeneous Boolean bent functions," *Australasian Journal of Combinatorics,* vol. 22, pp. 233-245, 2000.

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

[23] F. Zhang, N. Cepak, E. Pasalic, and Y. Wei, " Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^{\#}$," *Discret. Appl. Math.*, vol. 285, no. 1, pp. 458–472, 2020.

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

[25] Y. Zheng, and X. M. Zhang, "Non-Separable Cryptographic Functions," in *Proc. 2000 IEEE International Symposium on Information Theory and its Application (ISITA 2000)*, Hawaii, pp. 51–58, 2000 .

[26] L. Zheng, J. Peng, H. Kan, and Y. Li, "Several new infinite families of bent functions via second order derivatives," *Cryptogr. Commun.*, vol. 12, pp. 1143–1160, 2020.

Appendix

The `base64` representations of h_0 and h_1 in Example 5.1:

AE0eU3Q5aicATR5TdDlqJwBNHlN0OWonAE0eU3Q5aicATR5TdDlqJwBNHlN0OWonAE0eU3Q5
aicATR5TdDlqJwBNHlN0OWon/6yVxtiLsuEAU2o5J3RNHv+y4ayLxpXYAE0eU3Q5aif/rJXG2Iuy
4QBTajkndE0e/7LhrIvGldgATR5TdDlqJwBTajkndE0eAE0eU3Q5aicAU2o5J3RNHv+y4ayLxpXY
/6yVxtiLsuH/suGsi8aV2P+slcbYi7LhAE0eU3Q5aif/suGsi8aV2ABTajkndE0e/6yVxtiLsuH/suGsi8a
V2ABNHlN0OWon/6yVxtiLsuEAU2o5J3RNHgBNHlN0OWonAE0eU3Q5aif/suGsi8aV2P+y4ayLxp
XYAFNqOSd0TR4AU2o5J3RNHv+slcbYi7Lh/6yVxtiLsuEATR5TdDlqJ/+slcbYi7Lh/6yVxtiLsuE
ATR5TdDlqJwBTajkndE0e/7LhrIvGldj/suGsi8aV2ABTajkndE0eAE0eU3Q5aicAU2o5J3RNHv+y4
ayLxpXY/6yVxtiLsuH/rJXG2Iuy4f+y4ayLxpXYAFNqOSd0TR4ATR5TdDlqJwBNHlN0OWon/7L
hrIvGldj/rJXG2Iuy4QBTajkndE0e/6yVxtiLsuEAU2o5J3RNHgBNHlN0OWon/7LhrIvGldg=

(35)

ACc5Hk1qdFMAJzkeTWp0UwAnOR5NanRTACc5Hk1qdFMAJzkeTWp0UwAnOR5NanRTACc5H
k1qdFMAJzkeTWp0UwAnOR5NanRTACc5Hk1qdFP/xrKL4dislf/Gsovh2KyVADlNdB4nU2oAOU
10HidTav/YxuGylYus/9jG4bKVi6wAJzkeTWp0U//Gsovh2KyVADlNdB4nU2r/2MbhspWLrP/Gso
vh2KyVACc5Hk1qdFP/2MbhspWLrAA5TXQeJ1NqACc5Hk1qdFP/xrKL4dislf/YxuGylYusADlNd
B4nU2r/2MbhspWLrAA5TXQeJ1NqACc5Hk1qdFP/xrKL4dislQAnOR5NanRTADlNdB4nU2r/xrK
L4dislf/YxuGylYus/9jG4bKVi6z/xrKL4dislQA5TXQeJ1NqACc5Hk1qdFMAJzkeTWp0UwA5TXQ
eJ1NqACc5Hk1qdFMAOU10HidTav/Gsovh2KyV/9jG4bKVi6z/xrKL4dislf/YxuGylYusACc5Hk1qd
FP/2MbhspWLrP/YxuGylYusACc5Hk1qdFMAOU10HidTav/Gsovh2KyV/8ayi+HYrJUAOU10Hid
TagAnOR5NanRT/9jG4bKVi6wAOU10HidTav/Gsovh2KyVACc5Hk1qdFP/2MbhspWLrAA5TXQ
eJ1Nq/8ayi+HYrJU=

(36)

Proof. (of Theorem 3.6) Let $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ and $b^{(1)}, b^{(2)} \in \mathbb{F}_2^m$. We prove that $r\text{-ind}(h) < (n+m)/2$, by using Definitions 3.1 and 3.2. We need to show that there does not exist an $(\frac{n+m}{2})$-dimensional subspace V of $\mathbb{F}_2^{n+m}$ such that

$$D_{(a^{(1)},b^{(1)})}D_{(a^{(2)},b^{(2)})}h = constant,$$

for any $(a^{(1)}, b^{(1)})$, $(a^{(2)}, b^{(2)}) \in V$. There are three cases to be considered.

(i) For $\dim(\{x|(x,y) \in V\}) > n/2$, the proof is same with the proof of Theorem 3.5.

(ii) If $\dim(\{x|(x,y) \in V\}) = n/2$, then there are three cases to be considered.

(a) For $\dim(\{y|(x,y)\in V\}) = m/2$, the proof is same with the proof of Theorem 3.5.

(b) For $m/2 < \dim(\{y|(x,y)\in V\}) < (n+m)/2$, the proof is same with the proof of Theorem 3.5.

(c) For $\dim(\{y|(x,y)\in V\}) = (n+m)/2$, we have $\{y|(a_1,y)\in V\}\cap\{y|(a_2,y)\in V\} = \emptyset$ for arbitrary $a_1, a_2 \in \{x|(x,y)\in V\}, a_1 \neq a_2$ and $\dim(\{y|(0_n,y)\in V\}) = m/2$. Since $\dim(\{\alpha|D_\alpha(f_1\oplus f_2) = 0\}) = n-1$ and $\dim(\{x|(x,y)\in V\}) = n/2$, we can select one nonzero vector $\mathbf{a}\in\{x|(x,y)\in V\}$ such that $D_{\mathbf{a}}(f_1\oplus f_2) = 0$. Further,

$$\dim(\{(0_n,y)|(0_n,y)\in V\}\cup\{(\mathbf{a},y)|(\mathbf{a},y)\in V\}) = m/2+1.$$

Thus, from r-ind$(g_1) < m/2+1$, we can select two vectors $(a^{(1)},b^{(1)}),(a^{(2)},b^{(2)}) \in \{(0_n,y)|(0_n,y)\in V\}\cup\{(\mathbf{a},y)|(\mathbf{a},y)\in V\}$ such that

$$D_{b^{(1)}}D_{b^{(2)}}g_1(y) \neq constant.$$

From (14), we have

$$\begin{aligned} & D_{(a^{(1)},b^{(1)})}D_{(a^{(2)},b^{(2)})}h(x,y) \\ = \; & D_{b^{(1)}}D_{b^{(2)}}g_1(y)\oplus(f_1\oplus f_2)(x)D_{b^{(1)}}D_{b^{(2)}}(g_1\oplus g_2)(y) \neq constant. \end{aligned} \tag{37}$$

(iii) If $\dim(\{x|(x,y)\in V\}) < n/2$, then we have $\dim(\{y|(x,y)\in V\}) \geq m/2+1$. Further, we have $\dim(\{y|(0,y)\in V\}) \geq m/2+1$ since $\dim(V) = (n+m)/2$. Hence, from r-ind$(g_1) < m/2+1$, we can select two vectors $(0_n,b^{(1)}),(0_n,b^{(2)})\in V$ such that

$$D_{b^{(1)}}D_{b^{(2)}}g_1(y) \neq constant.$$

From (14), we have

$$\begin{aligned} & D_{(0_n,b^{(1)})}D_{(0_n,b^{(2)})}h(x,y) \\ = \; & D_{b^{(1)}}D_{b^{(2)}}g_1(y)\oplus(f_1\oplus f_2)(x)D_{b^{(1)}}D_{b^{(2)}}(g_1\oplus g_2)(y) \neq constant. \end{aligned} \tag{38}$$

□