Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-023-01204-w

Explicit infinite families of bent functions outside the completed Maiorana–McFarland class

Enes Pasalic[1] · Amar Bapić[1] · Fengrong Zhang[2,3] · Yongzhuang Wei[4]

Received: 18 July 2022 / Revised: 31 January 2023 / Accepted: 20 February 2023

Abstract
During the last five decades, many different secondary constructions of bent functions were proposed in the literature. Nevertheless, apart from a few works, the question about the class inclusion of bent functions generated using these methods is rarely addressed. Especially, if such a "new" family belongs to the completed Maiorana–McFarland ($\mathcal{MM}^{\#}$) class then there is no proper contribution to the theory of bent functions. In this article, we provide some fundamental results related to the inclusion in $\mathcal{MM}^{\#}$ and eventually we obtain many infinite families of bent functions that are provably outside $\mathcal{MM}^{\#}$. The fact that a bent function f is in/outside $\mathcal{MM}^{\#}$ if and only if its dual is in/outside $\mathcal{MM}^{\#}$ is employed in the so-called 4-decomposition of a bent function on $\mathbb{F}_2^n$, which was originally considered by Canteaut and Charpin (IEEE Trans Inf Theory 49(8):2004–2019, 2003) in terms of the second-order derivatives and later reformulated in (Hodžić et al. in IEEE Trans Inf Theory 65(11):7554–7565, 2019) in terms of the duals of its restrictions to the cosets of an $(n-2)$-dimensional subspace V. For each of the three possible cases of this 4-decomposition of a bent function (all four restrictions being bent, semi-bent, or 5-valued spectra functions), we provide generic methods for designing bent functions provably outside $\mathcal{MM}^{\#}$. For instance,

Communicated by C. Carlet.

✉ Amar Bapić
amarbapic7@gmail.com

Enes Pasalic
enes.pasalic6@gmail.com

Fengrong Zhang
zhfl203@163.com

Yongzhuang Wei
walker_wyz@guet.edu.cn

[1] IAM & FAMNIT, University of Primorska, Koper 6000, Slovenia

[2] State Key Laboratory of Integrated Services Networks, Xidian University, Xian 710071, People's Republic of China

[3] School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, Jiangsu, People's Republic of China

[4] Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, People's Republic of China

Published online: 22 March 2023

for the elementary case of defining a bent function $h(\mathbf{x}, y_1, y_2) = f(\mathbf{x}) \oplus y_1 y_2$ on $\mathbb{F}_2^{n+2}$ using a bent function f on $\mathbb{F}_2^n$, we show that h is outside $\mathcal{MM}^\#$ if and only if f is outside $\mathcal{MM}^\#$. This approach is then generalized to the case when two bent functions are used. More precisely, the concatenation $f_1||f_1||f_2||(1 \oplus f_2)$ also gives bent functions outside $\mathcal{MM}^\#$ if f_1 or f_2 is outside $\mathcal{MM}^\#$. The cases when the four restrictions of a bent function are semi-bent or 5-valued spectra functions are also considered and several design methods of constructing infinite families of bent functions outside $\mathcal{MM}^\#$ are provided.

Keywords 4-Decomposition · Class inclusion · 5-Valued spectra functions · Bent functions · Dual functions · Plateaued functions · Walsh support

Mathematics Subject Classification 94C10 · 06E30

1 Introduction

Bent functions were introduced by Rothaus [23], as a particular class of Boolean functions that has many interesting connections to other combinatorial objects such as Hadamard matrices and difference sets. Their applications in cryptography come in the first place from their characterization as a class of Boolean functions achieving the highest nonlinearity possible (thus being at the largest distance to the set of affine functions). A survey article [8] describes the main properties and construction methods related to bent functions, whereas their detailed study is given in the book of Mesnager [21]. On the other hand, for the applications of Boolean functions in cryptography we refer to the textbooks of Carlet [7] and Cusick and Stanica [11].

Two known primary classes of bent functions are the Maiorana–McFarland ($\mathcal{MM}$) class and the Partial Spreads ($\mathcal{PS}$) class, which were introduced in the 1970s in [19] and [12], respectively. Since it is not a simple matter to construct elements of the $\mathcal{PS}$ class practically, an explicit subclass of $\mathcal{PS}$, denoted by $\mathcal{PS}_{ap}$, was specified by Dillon in [13]. It seems quite unrealistic that other primary classes are yet to be discovered and therefore many secondary constructions (using known bent functions to build possibly new ones) have been proposed in the literature. A non-exhaustive list of various secondary constructions can be found in the following works [4, 6, 9, 16, 20, 24, 30]. 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, 4, 18, 20, 26–28] where some explicit families of bent functions provably outside the completed $\mathcal{MM}$ class are given. The main purpose of this article is to address the class inclusion more properly and thus also to contribute to a classification of bent functions. Nevertheless, the problem of finding efficient indicators for the inclusion/exclusion in the completed $\mathcal{PS}$ class remains unanswered. This problem is equivalent to finding cliques in a graph which is known to be NP-hard, see also [10, p. 43].

In this article, we employ a fundamental result (though not stated explicitly in the literature) concerning the inclusion in the completed $\mathcal{MM}$ class (denoted $\mathcal{MM}^\#$), which involves the dual function of a given bent function. More precisely, it can be shown that a bent function f is in/outside $\mathcal{MM}^\#$ if and only if its bent dual is in/outside $\mathcal{MM}^\#$. This result also implies that given a single bent function outside $\mathcal{MM}^\#$ (or alternatively its dual) one essentially derives a whole equivalence class whose members are also outside $\mathcal{MM}^\#$. To verify these results practically, we also propose a rather simple algorithm for determining the inclusion in $\mathcal{MM}^\#$. The algorithm uses the graph-theoretic notion of a clique (complete subgraph) to implement the second-order derivative criterion of Dillon [12], commonly used when determining the

inclusion/exclusion in $\mathcal{MM}^{\#}$. Its performance is quite satisfactory, allowing us to test the class inclusion for up to 12 variables efficiently. The above mentioned fact regarding a bent function and its dual (with respect to the inclusion in $\mathcal{MM}^{\#}$) is then useful when the so-called 4-decomposition of bent functions (say on $\mathbb{F}_2^n$) is considered, which regards the decomposition into the cosets of an $(n-2)$-dimensional subspace V of $\mathbb{F}_2^n$. It was originally investigated by Canteaut and Charpin [3] in terms of the second-order derivatives of the dual function, whereas the similar properties were recently stated using duals of the cosets of V [14]. The main conclusion in [3] is that there are exactly three possible cases of this 4-decomposition of a bent function, namely, all four restrictions being bent, semi-bent, or 5-valued spectra functions. For each of the cases, using the necessary and sufficient conditions in [14] (see Theorem 2.2), we provide generic methods (at least one) for designing bent functions provably outside $\mathcal{MM}^{\#}$. For instance, in the elementary case of defining a bent function $h(\mathbf{x}, y_1, y_2) = f(\mathbf{x}) \oplus y_1 y_2$ on $\mathbb{F}_2^{n+2}$ using any bent function f on $\mathbb{F}_2^n$ (corresponding to a bent 4-decomposition since $h = f||f||f||(1 \oplus f)$), we show that h is outside $\mathcal{MM}^{\#}$ if and only if f is outside $\mathcal{MM}^{\#}$. In this context, we also refer to [2] where four different (specific) bent functions $f_1, \ldots, f_4$ were used for the same purpose. This approach is then generalized to the case when two bent functions are used. More precisely, the concatenation $f_1||f_1||f_2||(1 \oplus f_2)$ also gives bent functions outside $\mathcal{MM}^{\#}$ if f_1 or f_2 is a bent function outside $\mathcal{MM}^{\#}$. This also naturally leads to a recursive construction of bent functions outside $\mathcal{MM}^{\#}$ on larger ambient spaces.

The cases when the four restrictions of a bent function are semi-bent or 5-valued spectra functions are also considered and several design methods of designing infinite families of bent functions outside $\mathcal{MM}^{\#}$ are proposed. We remark that the cardinality of bent functions that are provably outside $\mathcal{MM}^{\#}$ is extremely large which is also emphasized for instance in Remark 3.4, where a single dual bent function on $\mathbb{F}_2^8$ which is not in $\mathcal{MM}^{\#}$ gives rise to the EA-equivalence class comprising $\approx 2^{70}$ bent functions on $\mathbb{F}_2^{12}$ that are not in $\mathcal{MM}^{\#}$ as well. This only concerns our design method of concatenating four suitable semi-bent functions (using a dual which is not in $\mathcal{MM}^{\#}$), however our other constructions are similar in this context. Most notably, it seems that the presence of linear structures in these semi-bent functions (being restrictions of a bent function) is of no relevance for the class inclusion. More precisely, the use of a dual bent function outside $\mathcal{MM}^{\#}$, whose relaxed linearity index (see Definition 3.1) is of certain order, for their specification is sufficient for ensuring that the resulting bent function is outside $\mathcal{MM}^{\#}$ as well. A similar conclusion is valid when a sophisticated notion of duals of 5-valued spectra functions is employed for the same purpose, see for instance Theorem 3.7. Again, having a bent dual outside $\mathcal{MM}^{\#}$ ensures that the concatenation of four suitably selected 5-valued spectra functions generates bent functions that do not belong to $\mathcal{MM}^{\#}$ (regardless of the presence of linear structures in these constituent functions).

The rest of this paper is organized as follows. In Sect. 2, we give some basic definitions related to Boolean functions and discuss the concept of dual functions for some important classes of Boolean functions.

The design of bent functions provably outside $\mathcal{MM}^{\#}$ is addressed in Sect. 3. More precisely, we provide construction methods for specifying suitable quadruples of bent, semi-bent and 5-valued spectra functions so that the resulting bent functions are provably outside $\mathcal{MM}^{\#}$. In Sect. 4, we consider the design of bent functions by selecting 5-valued spectra functions in the generalized Maiorana-McFarland class. However, it remains an open problem whether this approach can generate bent functions outside $\mathcal{MM}^{\#}$. Some concluding remarks are given in Sect. 5.

2 Preliminaries

We denote the Galois field of order 2^n by $\mathbb{F}_{2^n}$ and the corresponding vector space by $\mathbb{F}_2^n$ which contains binary n-tuples $\mathbf{x} = (x_1, \ldots, x_n)$, where $x_i \in \mathbb{F}_2$. A mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called an n-variable Boolean function and we use $\mathcal{B}_n$ to denote the set of all possible Boolean mappings on $\mathbb{F}_2^n$. Any Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be represented using the so-called *algebraic normal form* (ANF), so that

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

where $x_i, \lambda_{\mathbf{u}} \in \mathbb{F}_2$ and $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$ and we reserve the symbol "$\bigoplus$" to denote the addition modulo two. Then, the *algebraic degree* of f, denoted by $deg(f)$ or sometimes simply d, is the maximal value of the Hamming weight of $\mathbf{u}$ such that $\lambda_{\mathbf{u}} \neq 0$. Throughout this article we will use $\mathbf{0}_n$ to denote the all-zero vector with n coordinates, that is $(0, 0, \ldots, 0) \in \mathbb{F}_2^n$.

Another useful representation of $f \in \mathcal{B}_n$ is its evaluation on $\mathbb{F}_2^n$ (known as *the truth table*) and defined as

$$T_f = (f(0, \ldots, 0, 0), f(0, \ldots, 0, 1), \ldots, f(1, \ldots, 1, 1)),$$

whose corresponding (± 1)-*sequence of* f is given as

$$\chi_f = ((-1)^{f(0,\ldots,0,0)}, (-1)^{f(0,\ldots,0,1)}, \ldots, (-1)^{f(1,\ldots,1,1)}).$$

The *Hamming distance* d_H between two arbitrary Boolean functions, say $f, g \in \mathcal{B}_n$, is defined by

$$d_H(f, g) = \{\mathbf{x} \in \mathbb{F}_2^n : f(\mathbf{x}) \neq g(\mathbf{x})\} = 2^{n-1} - \frac{1}{2} \chi_f \cdot \chi_g,$$

where $\chi_f \cdot \chi_g = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x})}$. In general, the standard inner (dot) product of two vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ in $\mathbb{F}_2^n$ is defined as $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 \oplus \cdots \oplus x_n y_n$.

The *Walsh–Hadamard transform* (WHT) of $f \in \mathcal{B}_n$, at any point $\boldsymbol{\omega} \in \mathbb{F}_2^n$ is defined as

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

Given the Walsh spectrum of a function $f \in \mathcal{B}_n$, its truth table can be recovered using the inverse WHT given by

$$(-1)^{f(\mathbf{x})} = 2^{-n} \sum_{\boldsymbol{\omega} \in \mathbb{F}_2^n} W_f(\boldsymbol{\omega}) (-1)^{\boldsymbol{\omega} \cdot \mathbf{x}}. \tag{3}$$

A function $f \in \mathcal{B}_n$, for even n, is called *bent* if $W_f(\mathbf{u}) = \pm 2^{\frac{n}{2}}$. We further note that for a bent function $f \in \mathcal{B}_n$, we have $W_f(\mathbf{u}) = (-1)^{f^*(\mathbf{u})} 2^{\frac{n}{2}}$ for a Boolean function $f^* \in \mathcal{B}_n$. This function f^* is called the *dual* of f and is also a bent function.

The first-order *derivative* of $f \in \mathcal{B}_n$ at $\mathbf{a} \in \mathbb{F}_2^n$, denoted by $D_{\mathbf{a}} f$, is the Boolean function defined by

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

In particular, $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is said to admit a linear structure $\boldsymbol{\gamma} \in \mathbb{F}_2^{n*}$ if $D_{\boldsymbol{\gamma}} f(\mathbf{x}) = f(\mathbf{x} \oplus \boldsymbol{\gamma}) \oplus f(\mathbf{x}) = c$ for all $\mathbf{x} \in \mathbb{F}_2^n$, where $c \in \mathbb{F}_2$.

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

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus g(\mathbf{y}), \text{ for all } \mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{n/2}, \tag{4}$$

where π is a permutation on $\mathbb{F}_2^{n/2}$, and g is an arbitrary Boolean function on $\mathbb{F}_2^{n/2}$. In general, the *completed* class is obtained by applying the so-called extended affine (EA) equivalence to all the functions in a given class. Since we are mainly interested in the class $\mathcal{MM}$, its completed version $\mathcal{MM}^{\#}$ is defined as,

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

where $GL(n, \mathbb{F}_2)$ denotes the group of invertible matrices under composition. The following lemma, originally due to Dillon [12] and later extended by Carlet [7, Proposition 54, pp. 167] to (easily) cover the other direction, is of crucial importance for the discussion on class inclusion.

Lemma 2.1 [12, p. 102] [7, Proposition 54, pp. 167] *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, defined by*

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

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

2.1 Plateaued functions and their duals

A function $f \in \mathcal{B}_n$ is called *s-plateaued* if its Walsh spectra only takes three values 0 and $\pm 2^{\frac{n+s}{2}}$ (the value $2^{\frac{n+s}{2}}$ is called the *amplitude*), where $s \geq 1$ if n is odd and $s \geq 2$ if n is even (s and n always have the same parity). In particular, a class of 1-plateaued functions for n odd, or 2-plateaued for n even, corresponds to so-called *semi-bent* functions. The *Walsh support* of $f \in \mathcal{B}_n$ is defined as $S_f = \{\boldsymbol{\omega} \in \mathbb{F}_2^n : W_f(\boldsymbol{\omega}) \neq 0\}$ and for an s-plateaued function its cardinality is $\#S_f = 2^{n-s}$ [3, Proposition 4].

We define a *dual* function $f^* : S_f \to \mathbb{F}_2$ of an s-plateaued function $f \in \mathcal{B}_n$ using $W_f(\boldsymbol{\omega}) = 2^{\frac{n+s}{2}}(-1)^{f^*(\boldsymbol{\omega})}$, for $\boldsymbol{\omega} \in S_f \subset \mathbb{F}_2^n$. To specify the dual function as $\overline{f}^* : \mathbb{F}_2^{n-s} \to \mathbb{F}_2$, we use the concept of *lexicographic ordering*. That is, a subset $E = \{\mathbf{e}_0, \ldots, \mathbf{e}_{2^{n-s}-1}\} \subset \mathbb{F}_2^n$ is ordered lexicographically if $|\mathbf{e}_i| < |\mathbf{e}_{i+1}|$ for any $i \in [0, 2^{n-s} - 2]$, where $|\mathbf{e}_i| = \sum_{j=0}^{n-1} \mathbf{e}_{i,n-1-j} 2^j$ denotes the integer representation of $\mathbf{e}_i \in \mathbb{F}_2^n$. Since S_f is not ordered in general, *we will always represent it* as $S_f = \mathbf{v} \oplus E$, where E is lexicographically ordered for some fixed $\mathbf{v} \in S_f$ and $\mathbf{e}_0 = \mathbf{0}_n$, thus E is a linear subspace of dimension $n - s$.

A direct correspondence between $\mathbb{F}_2^{n-s}$ and $S_f = \{\boldsymbol{\omega}_0, \ldots, \boldsymbol{\omega}_{2^{n-s}-1}\}$ is achieved through E, so that for the lexicographically ordered $\mathbb{F}_2^{n-s} = \{\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{2^{n-s}-1}\}$ we have

$$\overline{f}^*(\mathbf{x}_i) = f^*(\mathbf{v} \oplus \mathbf{e}_i) = f^*(\boldsymbol{\omega}_i), \tag{5}$$

where $\mathbf{x}_i \in \mathbb{F}_2^{n-s}$, $\mathbf{e}_i \in E$, $i \in [0, 2^{n-s} - 1]$.

Remark 2.1 Throughout this article, from the design perspective, the dual of an s-plateaued function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ will be denoted by f^* and is considered as a function on S_f (that is $f^* : S_f \to \mathbb{F}_2$). However, as specified in (5), the notation $\overline{f}^*$ associates this dual to a function defined on $\mathbb{F}_2^{n-s}$, that is $\overline{f}^* : \mathbb{F}_2^{n-s} \to \mathbb{F}_2$.

The main reason for ordering the elements in E lexicographically is Theorem 3.3 (that essentially follows from Lemma 3.1 in [16]), given originally in [15] and recalled in Sect. 3.3.1, which from the design perspective gives the conditions on S_f so that the spectral values defined through f^* (or $\overline{f}^*$) indeed specify a valid Walsh spectrum of a Boolean function. Furthermore, it was noted in [17] that different orderings of S_f, both with respect to the choice of $\boldsymbol{v}$ so that $S_f = \boldsymbol{v} \oplus E$ as well as representing it differently so that $S_f = \boldsymbol{v}' \oplus E'$ (with $\boldsymbol{v} \neq \boldsymbol{v}'$ and $E \neq E'$), essentially give affine equivalent duals $\overline{f}^*$ and $\overline{f'}^*$, see Section 5 in [17] for further details. Nevertheless, all these results use the assumption that item (i) in Lemma 3.1 in [16] is satisfied. Namely, an m-dimensional linear subspace $E = \{\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{2^m-1}\}$ is "suitably" ordered to be used in Theorem 3.3 whenever for any fixed $i \in \{0, \ldots, m-1\}$ it holds that $\mathbf{e}_j = \mathbf{e}_{2^i} \oplus \mathbf{e}_{j-2^i}$, for all $2^i \leq j \leq 2^{i+1} - 1$. In the case of lexicographic ordering this recursion is satisfied.

In this context, we recall one essential result on the properties of the dual plateaued functions for different representations of S_f. We remark that an s-plateaued function on $\mathbb{F}_2^n$ is called trivial if its Walsh support is an affine subspace.

Theorem 2.1 [15] *Let $f, h : \mathbb{F}_2^n \to \mathbb{F}_2$ be two trivial s-plateaued functions whose Walsh supports are related as $S_h = \mathbf{c} \oplus S_f M$, for some matrix $M \in GL(n, \mathbb{F}_2)$ and $\mathbf{c} \in \mathbb{F}_2^n$. Representing $S_f = \mathbf{v} \oplus E = \{\boldsymbol{\omega}_i = \mathbf{v} \oplus \mathbf{e}_i : \mathbf{e}_i \in E\}$ for a lexicographically ordered linear space $E = \{\mathbf{e}_0, \ldots, \mathbf{e}_{2^{n-s}-1}\}$, let the functions $\overline{f}^*$ and $\overline{h}^*$ be defined as*

$$\overline{f}^*(\mathbf{x}_i) = f^*(\boldsymbol{\omega}_i) \quad \text{and} \quad \overline{h}^*(\mathbf{x}_i) = h^*(\mathbf{z}_i), \quad (i \in [0, 2^{n-s} - 1]),$$

where $\mathbf{z}_i = c \oplus \boldsymbol{\omega}_i M \in S_h$. Then, f and h are EA-equivalent if and only if their duals $\overline{f}^*, \overline{h}^* : \mathbb{F}_2^{n-s} \to \mathbb{F}_2$ are EA-equivalent bent functions.

2.2 Specifying 5-valued spectra functions through duals

We first recall certain notations, introduced in [14] and also used in [17], useful in handling a 5-valued spectra Boolean function which has two different non-zero absolute values.

Let the WHT spectrum of a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ contain the values $0, \pm c_1, \pm c_2$ ($c_1 \neq c_2$), where $c_1, c_2 \in \mathbb{N}$. Some of the results in [14] are stated in a more general context, but since the 4-decomposition of bent functions is our main objective we only consider the cases $c_1 = 2^{n/2}$ and $c_2 = 2^{(n+2)/2}$ above. For $i = 1, 2$, by $S_f^{[i]} \subset \mathbb{F}_2^n$ we denote the set $S_f^{[i]} = \{\mathbf{u} \in \mathbb{F}_2^n : |W_f(\mathbf{u})| = c_i\}$, and we can define the functions $f^*_{[i]} : S_f^{[i]} \to \mathbb{F}_2$ such that the following equality holds:

$$W_f(\mathbf{u}) = \begin{cases} 0, & \mathbf{u} \notin S_f^{[1]} \cup S_f^{[2]}, \\ c_i \cdot (-1)^{f^*_{[i]}(\mathbf{u})}, & \mathbf{u} \in S_f^{[i]}, \quad i \in \{1, 2\}. \end{cases} \tag{6}$$

For $i = 1, 2$, let $\mathbf{v}_i \in \mathbb{F}_2^n$ and $E_i = \{\mathbf{e}_0^{(i)}, \ldots, \mathbf{e}_{2^{\lambda_i}-1}^{(i)}\} \subset \mathbb{F}_2^n$ ($\mathbf{e}_0^{(i)} = \mathbf{0}_n$) be lexicographically ordered subsets of cardinality 2^{λ_i} such that $S_f^{[i]} = \{\boldsymbol{\omega}_0^{(i)}, \ldots, \boldsymbol{\omega}_{2^{\lambda_i}-1}^{(i)}\} = \mathbf{v}_i \oplus E_i$, where $\boldsymbol{\omega}_j^{(i)} = \mathbf{v}_i \oplus \mathbf{e}_j^{(i)}$, for $j \in [0, 2^{\lambda_i} - 1]$. Clearly, the lexicographically ordered set E_i imposes an ordering on $S_f^{[i]}$ with respect to the equality $\boldsymbol{\omega}_j^{(i)} = \mathbf{v}_i \oplus \mathbf{e}_j^{(i)}$. Using the representation of $S_f^{[i]} = \mathbf{v}_i \oplus E_i$ and the fact that the cardinality of $S_f^{[i]}$ is a power of two, the function $\overline{f}^*_{[i]}$, as a mapping from $\mathbb{F}_2^{\lambda_i}$ to $\mathbb{F}_2$, is defined as

$$\overline{f}^*_{[i]}(\mathbf{x}_j) = f^*_{[i]}(\mathbf{v}_i \oplus \mathbf{e}_j^{(i)}) = f^*_{[i]}(\boldsymbol{\omega}_j^{(i)}), \quad j \in [0, 2^{\lambda_i} - 1], \tag{7}$$

where $\mathbb{F}_2^{\lambda_i} = \{\mathbf{x}_0, \ldots, \mathbf{x}_{2^{\lambda_i}-1}\}$ is ordered lexicographically.

A more specific method for designing 5-valued spectra functions on $\mathbb{F}_2^n$ (thus $W_f(\mathbf{u}) \in \{0, \pm 2^{n/2}, \pm 2^{\frac{n+2}{2}}\}$), originally considered in [14], will be used in Sect. 3.4 for specifying suitable quadruples of such functions whose concatenation will give bent functions outside $\mathcal{MM}^{\#}$.

2.3 Decomposition of bent functions

In [3], Canteaut and Charpin considered the decomposition of bent functions on $\mathbb{F}_2^n$, $n \geq 4$ is even, with respect to affine subspaces $\mathbf{a} \oplus V$, for some k-dimensional linear subspace $V \subset \mathbb{F}_2^n$. In general, this decomposition of $\mathfrak{f} \in \mathcal{B}_n$ can be viewed as a collection of 2^{n-k} Boolean functions denoted by $\mathfrak{f}_{\mathbf{a}\oplus V}$ and defined on $\mathbb{F}_2^k \to \mathbb{F}_2$ using

$$\mathfrak{f}_{\mathbf{a}\oplus V}(\mathbf{x}_i) = \mathfrak{f}_{\mathbf{a}\oplus V}(\mathbf{a} \oplus \mathbf{v}_i), \quad i \in [0, 2^k - 1], \tag{8}$$

for lexicographically ordered $V = \{\mathbf{v}_0, \ldots, \mathbf{v}_{2^k-1}\}$ and $\mathbb{F}_2^k = \{\mathbf{x}_0, \ldots, \mathbf{x}_{2^k-1}\}$. This identification between V and $\mathbb{F}_2^k$, and thus the definition of $\mathfrak{f}_{\mathbf{a}\oplus V} : \mathbb{F}_2^k \to \mathbb{F}_2$, strongly depends on the ordering of V in a similar sense as mentioned in Sect. 2.

Since in this article we are mainly interested in the design methods of bent functions on $\mathbb{F}_2^n$ using a concatenation of four functions on $\mathbb{F}_2^{n-2}$, we will consider V to be an $(n-2)$-dimensional subspace of $\mathbb{F}_2^n$. Hence, the functions $f_1, \ldots, f_4 \in \mathcal{B}_{n-2}$ can be defined on the four cosets $\mathbf{0}_n \oplus V$, $\mathbf{a} \oplus V$, $\mathbf{b} \oplus V$, $(\mathbf{a} \oplus \mathbf{b}) \oplus V$ respectively, for an arbitrary linear subspace V of dimension $n-2$ so that $Q = \langle \mathbf{a}, \mathbf{b} \rangle$ and $Q \oplus V = \mathbb{F}_2^n$ (with $Q \cap V = \{\mathbf{0}_n\}$). We will denote such a decomposition as $\mathfrak{f} = (f_1, f_2, f_3, f_4)_V$, where $\mathfrak{f} \in \mathcal{B}_n$ and $f_i \in \mathcal{B}_{n-2}$. However, specifying $V = \mathbb{F}_2^{n-2} \times (0, 0)$ we have the canonical decomposition which we simply denote as $\mathfrak{f} = (f_1, f_2, f_3, f_4)$. Following the terminology in [3], this decomposition is said to be a *bent 4-decomposition* when all f_i ($i \in [1, 4]$), are bent; a *semi-bent 4-decomposition* when all f_i ($i \in [1, 4]$) are semi-bent; a *5-valued 4-decomposition* when all f_i ($i \in [1, 4]$) are 5-valued spectra functions so that $W_{f_i} \in \{0, \pm 2^{(n-2)/2}, \pm 2^{n/2}\}$.

The 4-decomposition was fully described in [3] in terms of the second-order derivatives (with respect to $\mathbf{a}$ and $\mathbf{b}$) of the dual $\mathfrak{f}^*$ of a bent function $\mathfrak{f}$. Alternatively, the approach that will be used in this article, this decomposition can be specified in terms of Walsh supports and duals of its restrictions $f_1, \ldots, f_4$ [14]. Note that functions f_i are considered as functions in $(n-2)$-variables in terms of Eq. (8) (that is when $\dim(V) = k = n-2$).

Theorem 2.2 [14] *Let $\mathfrak{f} \in \mathcal{B}_n$ be a bent function, for even $n \geq 4$. Let $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n \backslash \{\mathbf{0}_n\}$ ($\mathbf{a} \neq \mathbf{b}$) and V a linear subspace of $\mathbb{F}_2^n$ with $\dim(V) = n-2$ so that $\langle \mathbf{a}, \mathbf{b} \rangle \oplus V = \mathbb{F}_2^n$. If we denote by $(f_1, \ldots, f_4)$ the 4-decomposition of $\mathfrak{f}$ with respect to V, then $(f_1, \ldots, f_4)$ is:*

(i) *A bent 4-decomposition if and only if it holds that $f_1^* \oplus f_2^* \oplus f_3^* \oplus f_4^* = 1$.*

(ii) *A semi-bent 4-decomposition if and only if functions f_i ($i \in [1, 4]$) are pairwise disjoint spectra semi-bent functions.*[1]

(iii) *A five-valued 4-decomposition if and only if the following statements hold:*

  (a) *The sets $S_{f_i}^{[1]} = \{\boldsymbol{\vartheta} \in \mathbb{F}_2^{n-2} : |W_{f_i}(\boldsymbol{\vartheta})| = 2^{\frac{n}{2}}\}$ ($i \in [1, 4]$) are pairwise disjoint;*

  (b) *All $S_{f_i}^{[2]} = \{\boldsymbol{\vartheta} \in \mathbb{F}_2^{n-2} : |W_{f_i}(\boldsymbol{\vartheta})| = 2^{\frac{n-2}{2}}\}$ are equal ($i \in [1, 4]$), and for $f_{[2],i}^* : S_{f_i}^{[2]} \to \mathbb{F}_2$ it holds that $f_{[2],1}^* \oplus f_{[2],2}^* \oplus f_{[2],3}^* \oplus f_{[2],4}^* = 1$.*

[1] Two semi-bent functions f_1 and f_2 on $\mathbb{F}_2^{n-2}$, for even n, are said to be disjoint spectra functions if $W_{f_1}(u) = 0 \Rightarrow W_{f_2}(u) = \pm 2^{n/2}$, and vice versa.

In the rest of this article, we consider the canonical 4-decomposition so that $\mathbf{a} = (0, 0, \ldots, 0, 1)$, $\mathbf{b} = (0, 0, \ldots, 1, 0) \in \mathbb{F}_2^n$ and consequently $V = \mathbb{F}_2^{n-2} \times \{(0, 0)\}$ in Theorem 2.2. Then, the function $\mathfrak{f}$ is the concatenation of $f_i \in \mathcal{B}_{n-2}$ which we denote by $\mathfrak{f} = f_1||f_2||f_3||f_4$. Using the convention that $\mathfrak{f}(\mathbf{x}, 0, 0) = f_1(\mathbf{x})$, $\mathfrak{f}(\mathbf{x}, 0, 1) = f_2(\mathbf{x})$, $\mathfrak{f}(\mathbf{x}, 1, 0) = f_3(\mathbf{x})$ and $\mathfrak{f}(\mathbf{x}, 1, 1) = f_4(\mathbf{x})$, the ANF of $\mathfrak{f} = f_1||f_2||f_3||f_4$ is given by

$$\mathfrak{f}(\mathbf{x}, y_1, y_2) = f_1(\mathbf{x}) \oplus y_1(f_1 \oplus f_3)(\mathbf{x}) \oplus y_2(f_1 \oplus f_2)(\mathbf{x}) \oplus y_1 y_2(f_1 \oplus f_2 \oplus f_3 \oplus f_4)(\mathbf{x}). \tag{9}$$

3 Decomposing bent functions: design methods

From the design perspective, Theorem 2.2 allows us to specify (possibly new) bent functions by specifying suitable quadruples of bent, semi-bent, or 5-valued spectra functions. We develop these ideas below more precisely in the rest of this section, but before this we propose an efficient algorithm for testing the inclusion in $\mathcal{MM}^{\#}$. Throughout this article, due to the fact that all bent functions up to six variables are contained in $\mathcal{MM}^{\#}$, we will consider the design of bent functions on $\mathbb{F}_2^n$, where $n \geq 8$ is even.

3.1 An algorithm for determining whether $f \in \mathcal{MM}^{\#}$

We first describe an algorithmic approach to determine whether a bent function is outside $\mathcal{MM}^{\#}$. The algorithm is based on Lemma 2.1 and some graph-theoretical concepts.

Let $f \in \mathcal{B}_n$ be a bent function. Set $\Gamma = (V, E)$ to be a graph with edge set

$$E = \{\{\mathbf{a}, \mathbf{b}\} : \mathbf{a}, \mathbf{b} \in \mathbb{F}_2^{n*}; D_{\mathbf{a}} D_{\mathbf{b}} f \equiv 0\},$$

and vertex set $V \subset \mathbb{F}_2^{n*}$ consisting of all distinct vertices appearing in the edge set E. For simplicity, we do not add 0 to V as $D_0 D_{\mathbf{b}} f \equiv 0$ for all $\mathbf{b} \in \mathbb{F}_2^n$. With this approach, we reduce the size of the vertex set V as $D_{\boldsymbol{a}} D_{\boldsymbol{b}} f \not\equiv 0$, for some $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^{n*}$. In practice, for functions outside the completed Maiorana-McFarland class, the size of the vertex set becomes relatively small and for instance in dimension $n = 8$ we could verify that typical values for $|V|$ are 0 and 6. We also remark that we consider the graph Γ to be simple as there are no loops ($D_{\mathbf{a}} D_{\mathbf{a}} f \equiv 0$ holds for all $\mathbf{a} \in \mathbb{F}_2^n$); and it is not directed since $D_{\mathbf{a}} D_{\mathbf{b}} f = D_{\mathbf{b}} D_{\mathbf{a}} f$ for any $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$.

From Lemma 2.1, we know that we need to find an $(n/2)$-dimensional linear subspace V of $\mathbb{F}_{2^n}$ on which the second-order derivatives of f vanish. From the graph-theoretical perspective, this problem corresponds to finding a clique Λ (complete subgraph) of size $2^{n/2} - 1$ in the graph Γ and additionally checking whether $V(\Lambda) \cup \{0\}$ forms a linear subspace in $\mathbb{F}_2^n$. Finding a clique in a graph is known to be an NP-complete problem and, specifically, the time complexity of this search would be of size $\mathcal{O}(2^{n2^{n/2}})$. However, in practice, this number is much smaller because the number of vertices (namely $|V|$) of the graph Γ is almost negligible compared to 2^n. The full Sage implementation has been added to the appendix. It might be of interest to optimize further the performance of this algorithm so that larger input sizes can be efficiently tested.

We have considered 100 bent functions in dimension 8 and the average time needed to check whether one function is outside $\mathcal{MM}^{\#}$ was approximately 17 seconds. For $n = 10$,

the average time for checking the property of being in or outside $\mathcal{MM}^{\#}$ was 30 minutes. On the other hand, when $n = 12$, the time complexity is approximately 22 h on average. For the purpose of this article, the proposed algorithm is sufficiently efficient and is superior to a straightforward approach of checking all $n/2$-dimensional subspaces and verifying the vanishing property of the second-order derivatives. Most importantly, all the examples provided in this article (in certain cases the ANFs are also given) can be efficiently checked using the Sage algorithm given in the appendix. We also note the following interesting observation.

Remark 3.1 We remark that the dual of a bent function $f \in \mathcal{MM}$, given by $f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus h(\mathbf{y})$ for $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{n/2}$, where π is a permutation on $\mathbb{F}_2^{n/2}$ and h is arbitrary, is apparently in $\mathcal{MM}$ (see for instance [7] for the specification of f^*). The same is true when $f \in \mathcal{MM}^{\#}$ is considered since the class inclusion is invariant under the EA transform.

3.2 Defining suitable bent 4-decompositions

Recently, a quadruple of *distinct* bent functions, satisfying that $f_1^* \oplus f_2^* \oplus f_3^* \oplus f_4^* = 1$, was identified in [2]. It was additionally shown that their concatenation $f_1||f_2||f_3||f_4$ is provably outside the $\mathcal{MM}^{\#}$ class. More precisely, the authors considered a quadruple of bent functions (not all of them being in $\mathcal{MM}^{\#}$) that belong to the $\mathcal{C}$ and $\mathcal{D}$ class of Carlet [4] and their suitable "modifications" for this purpose. Nevertheless, the following results show that the same method can generate new bent functions outside $\mathcal{MM}^{\#}$ when a single bent function (alternatively a pair of bent functions considered in Theorem 3.2) outside $\mathcal{MM}^{\#}$ is used.

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

Proof It is well-known that $h = f||f||f||(1 \oplus f) \in \mathcal{B}_{n+2}$ is bent if f is bent, since $h(\mathbf{x}, y_1, y_2) = f(\mathbf{x}) \oplus y_1 y_2$ is the direct sum of two bent functions [12, 23]. Notice that 'f is outside $\mathcal{MM}^{\#}$ if and only if h is outside $\mathcal{MM}^{\#}$' is equivalent to 'f is in $\mathcal{MM}^{\#}$ if and only if h is in $\mathcal{MM}^{\#}$'.

Suppose first that h is outside $\mathcal{MM}^{\#}$, thus we want to show that f is outside $\mathcal{MM}^{\#}$. Assume on the contrary that f is in $\mathcal{MM}^{\#}$, thus there exists (at least) one linear subspace $V \subset \mathbb{F}_2^n$ with $\dim(V) = n/2$ such that $D_{\mathbf{a}'} D_{\mathbf{b}'} f \equiv 0$, for any $\mathbf{a}', \mathbf{b}' \in V$. Let $E = V \times \{(0, 0), (0, 1)\}$ which is a subspace of $\mathbb{F}_2^{n+2}$ of dimension $n/2 + 1$. We then have that

$$D_{(\mathbf{a}', a_1, a_2)} D_{(\mathbf{b}', b_1, b_2)} h \equiv 0,$$

for any $\mathbf{a}', \mathbf{b}' \in V$ and $(a_1, a_2), (b_1, b_2) \in \{(0, 0), (0, 1)\}$, thus the second-order derivatives of h vanish on E. Hence, h is in $\mathcal{MM}^{\#}$ which contradicts our assumption that h is outside $\mathcal{MM}^{\#}$.

Now, we show that f is outside $\mathcal{MM}^{\#}$ implies that h is outside $\mathcal{MM}^{\#}$. Assuming $f \notin \mathcal{MM}^{\#}$, then for any subspace $V \subset \mathbb{F}_2^n$ with $\dim(V) = n/2$, we can always find two vectors $\mathbf{a}', \mathbf{b}'$ such that $D_{\mathbf{a}'} D_{\mathbf{b}'} f \not\equiv 0$. Let $E \subset \mathbb{F}_2^n \times \mathbb{F}_2^2$ be any subspace with $\dim(E) = n/2 + 1$. There are two cases to be considered.

a. If $\dim(E \cap (\mathbb{F}_2^n \times \{(0, 0)\})) \geq n/2$, then we can find two vectors $(\mathbf{a}', 0, 0)$, $(\mathbf{b}', 0, 0)$ and consequently

$$D_{(\mathbf{a}', 0, 0)} D_{(\mathbf{b}', 0, 0)} h = D_{\mathbf{a}'} D_{\mathbf{b}'} f \not\equiv 0.$$

b. If $\dim(E \cap (\mathbb{F}_2^n \times \{(0,0)\})) < n/2$, then we must have $E \cap (\{\mathbf{0}_n\} \times \mathbb{F}_2^2) = \{\mathbf{0}_n\} \times \mathbb{F}_2^2$ since $\dim(E) = n/2 + 1$ (using that $\dim(E \cap (\mathbb{F}_2^n \times \mathbb{F}_2^2)) = n/2 + 1$). Here, there are three cases to be considered.

(a) If $D_{\mathbf{a}'} D_{\mathbf{b}'} f \equiv 0$ for any two vectors $(\mathbf{a}', 0, 0), (\mathbf{b}', 0, 0) \in E \cap (\mathbb{F}_2^n \times \{(0,0)\})$, then we can specify $(a_1, a_2) = (1, 0), (b_1, b_2) = (1, 1)$ so that

$$D_{(a_1,a_2)} D_{(b_1,b_2)} (y_1 y_2) = 1.$$

Thus,

$$D_{(\mathbf{a}',a_1,a_2)} D_{(\mathbf{b}',b_1,b_2)} h = D_{\mathbf{a}'} D_{\mathbf{b}'} f \oplus D_{(a_1,a_2)} D_{(b_1,b_2)} (y_1 y_2) \equiv 1 \neq 0.$$

(b) If $D_{\mathbf{a}'} D_{\mathbf{b}'} f \equiv 1$ for any two nonzero vectors $(\mathbf{a}', \mathbf{0}_2), (\mathbf{b}', \mathbf{0}_2) \in E \cap (\mathbb{F}_2^n \times \{\mathbf{0}_2\})$, then we select $(a_1, a_2) = (1, 0), (b_1, b_2) = (0, 0)$ so that

$$D_{(a_1,a_2)} D_{(b_1,b_2)} y_1 y_2 \equiv 0.$$

Thus,

$$D_{(\mathbf{a}',a_1,a_2)} D_{(\mathbf{b}',b_1,b_2)} h = D_{\mathbf{a}'} D_{\mathbf{b}'} f \oplus D_{(a_1,a_2)} D_{(b_1,b_2)} (y_1 y_2) \equiv 1 \neq 0.$$

(c) If $D_{\mathbf{a}'} D_{\mathbf{b}'} f \neq const.$ for two nonzero vectors $(\mathbf{a}', \mathbf{0}_2), (\mathbf{b}', \mathbf{0}_2) \in E \cap (\mathbb{F}_2^n \times \{\mathbf{0}_2\})$, then

$$D_{(\mathbf{a}',a_1,a_2)} D_{(\mathbf{b}',b_1,b_2)} h = D_{\mathbf{a}'} D_{\mathbf{b}'} f \neq const.$$

This concludes the proof. □

Corollary 1 *Let n and m be even positive integers and h be a bent function in $\mathcal{B}_n$. Then, the function $f(\mathbf{x}, y_1, y_2, \ldots, y_m) = h(\mathbf{x}) \oplus y_1 y_2 \oplus y_3 y_4 \oplus \cdots \oplus y_{m-1} y_m$ is outside $\mathcal{MM}^{\#}$ if and only if h is outside $\mathcal{MM}^{\#}$.*

Now, we investigate another non-trivial selection of bent quadruples (different from $f = f_1||f_1||f_1||(1 \oplus f_1)$, which satisfies the necessary and sufficient condition $f_1^* \oplus f_2^* \oplus f_3^* \oplus f_4^* = 1$. It turns out that the basic concatenation method of using just two bent functions, where at least one of them is outside $\mathcal{MM}^{\#}$, also generates bent functions outside $\mathcal{MM}^{\#}$.

Theorem 3.2 *Let $n = 2m$ be even and $f_1, f_2 \in \mathcal{B}_n$ be two bent functions. Set $f = f_1||f_1||f_2||(f_2 \oplus 1)$, which by (9) gives*

$$f(\mathbf{x}, y_1, y_2) = (1 \oplus y_1) f_1(\mathbf{x}) \oplus y_1 f_2(\mathbf{x}) \oplus y_1 y_2, \ \mathbf{x} \in \mathbb{F}_2^n, y_1, y_2 \in \mathbb{F}_2. \tag{10}$$

If f_1 or f_2 is outside $\mathcal{MM}^{\#}$, then $f \in \mathcal{B}_{n+2}$ is bent and outside $\mathcal{MM}^{\#}$.

Proof Since $f_1^* \oplus f_1^* \oplus f_2^* \oplus (f_2 \oplus 1)^* = 1$, then f is bent.

For convenience, we denote $\mathbf{a} = (\mathbf{a}', a_2, a_3), \mathbf{b} = (\mathbf{b}', b_2, b_3) \in \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2$. Let V be an arbitrary $(m+1)$-dimensional subspace of $\mathbb{F}_2^{n+2}$. From Lemma 2.1, it is sufficient to show that for an arbitrary $(m+1)$-dimensional subspace V of $\mathbb{F}_2^{n+2}$ one can always find two vectors $\mathbf{a}, \mathbf{b} \in V$ such that $D_{(\mathbf{a}',a_2,a_3)} D_{(\mathbf{b}',b_2,b_3)} f(\mathbf{x}, y_1, y_2) \neq 0$ for some $(\mathbf{x}, y_1, y_2) \in \mathbb{F}_2^{n+2}$. We have

$$\begin{aligned} D_{(\mathbf{a}',a_2,a_3)} D_{(\mathbf{b}',b_2,b_3)} f(\mathbf{x}, y_1, y_2) = {} & (1 \oplus y_1) D_{\mathbf{a}'} D_{\mathbf{b}'} f_1(\mathbf{x}) \oplus y_1 D_{\mathbf{a}'} D_{\mathbf{b}'} f_2(\mathbf{x}) \\ & \oplus a_2 D_{\mathbf{b}'} (f_1 \oplus f_2)(\mathbf{x} \oplus \mathbf{a}') \oplus b_2 D_{\mathbf{a}'} (f_1 \oplus f_2)(\mathbf{x} \oplus \mathbf{b}') \\ & \oplus a_2 b_3 \oplus a_3 b_2. \end{aligned} \tag{11}$$

There are two cases to be considered.

a. Assuming that $\dim\left(V \cap (\mathbb{F}_2^n \times \{(0,0)\})\right) \geq m$ implies the existence of two vectors $\mathbf{a} = (\mathbf{a}', a_2, a_3), \mathbf{b} = (\mathbf{b}', b_2, b_3) \in V$ such that $\mathbf{a}' \neq \mathbf{b}'$, $a_2 = a_3 = b_2 = b_3 = 0$, for which $D_{\mathbf{a}'} D_{\mathbf{b}'} f_2 \not\equiv 0$ if we suppose that f_2 is outside $\mathcal{MM}^{\#}$.
From (11), for $y_1 = 1$, we obtain

$$D_{(\mathbf{a}', a_2, a_3)} D_{(\mathbf{b}', b_2, b_3)} f(\mathbf{x}, 1, y_2) = D_{\mathbf{a}'} D_{\mathbf{b}'} f_2(\mathbf{x}) \not\equiv 0.$$

Thus, we have found $\mathbf{a}, \mathbf{b} \in V$ such that $D_{\mathbf{a}} D_{\mathbf{b}} f(\mathbf{x}, 1, y_2) \neq 0$, which also implies that $D_{\mathbf{a}} D_{\mathbf{b}} f(\mathbf{x}, y_1, y_2) \neq 0$.
Now, assume that $f_1 \notin \mathcal{MM}^{\#}$. Similarly, there will exist two vectors $\mathbf{a} = (\mathbf{a}'', a_2, a_3), \mathbf{b} = (\mathbf{b}'', b_2, b_3) \in V$ such that $\mathbf{a}'' \neq \mathbf{b}''$, $a_2 = a_3 = b_2 = b_3 = 0$, for which $D_{\mathbf{a}''} D_{\mathbf{b}''} f_1 \not\equiv 0$. Setting $y_1 = 0$ in (11), we obtain

$$D_{(\mathbf{a}', a_2, a_3)} D_{(\mathbf{b}', b_2, b_3)} f(\mathbf{x}, 0, y_2) = D_{\mathbf{a}'} D_{\mathbf{b}'} f_1(\mathbf{x}) \not\equiv 0,$$

and again we conclude that $D_{\mathbf{a}} D_{\mathbf{b}} f(\mathbf{x}, y_1, y_2) \neq 0$.

b. When $\dim\left(V \cap (\mathbb{F}_2^n \times \{(0,0)\})\right) < m$, we have $V \cap (\{\mathbf{0}_n\} \times \mathbb{F}_2^2) = \{0_n\} \times \mathbb{F}_2^2$ since $\dim\left(V \cap (\mathbb{F}_2^n \times \mathbb{F}_2^2)\right) = m+1$. Furthermore, we can find two vectors $\mathbf{a} = (\mathbf{a}', a_2, a_3), \mathbf{b} = (\mathbf{b}', b_2, b_3) \in V$ such that $\mathbf{a}' = \mathbf{0}_n, \mathbf{b}' = \mathbf{0}_n, a_2 = 1, b_2 = 0$, and $a_3 = 0, b_3 = 1$. From (11), we have

$$D_{(\mathbf{0}_n, 1, 0)} D_{(\mathbf{0}_n, 0, 1)} f(\mathbf{x}, y_1, y_2) = 1 \neq 0. \tag{12}$$

Thus, there is no $(m+1)$-dimensional linear subspace of $\mathbb{F}_2^{n+2}$ on which the second-order derivatives of f vanish, i.e., f is outside $\mathcal{MM}^{\#}$. □

Example 3.1 Let $f_1, f_2 \in \mathcal{B}_8$ be defined by $f_1(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$ and $f_2(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi_2(\mathbf{y}) \oplus \delta_0(\mathbf{x})$, respectively, where $\pi_2 = (0, 1, 2, 3, 4, 5, 8, 10, 6, 12, 7, 15, 13, 11, 9, 14)$ is a permutation of $\mathbb{F}_2^4$ in integer form and $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^4$. Here, $\delta_0(\mathbf{x}) = \prod_{i=1}^4 (1 \oplus x_i)$ is the indicator of $\{\mathbf{0}_4\}$. We note that $f_1 \in \mathcal{MM}^{\#}$ and $f_2 \in \mathcal{D}_0 \backslash \mathcal{MM}^{\#}$, where $\mathcal{D}_0$ is the class of bent functions introduced by Carlet [4] whose members are of the same form as f_2 above. Let $\mathfrak{f}_1 = (f_1, f_1, f_2, f_2 \oplus 1)$ and $\mathfrak{f}_2 = (f_2, f_2, f_1, f_1 \oplus 1)$ be defined via (10). Using the algorithm in Sect. 3.1, we have confirmed that $\mathfrak{f}_1, \mathfrak{f}_2 \in \mathcal{B}_{10}$ are both bent functions outside $\mathcal{MM}^{\#}$.

An iterative design of bent functions outside $\mathcal{MM}^{\#}$ follows easily from Theorem 3.2.

Corollary 2 *Let $f_1, f_2 \in \mathcal{B}_n$ be two bent functions such that f_1 or f_2 is outside $\mathcal{MM}^{\#}$. Set $\mathfrak{f}_1^{(1)} = (f_1, f_1, f_2, f_2 \oplus 1)$ and $\mathfrak{f}_2^{(1)} = (f_2, f_2, f_1, f_1 \oplus 1)$. For $k \geq 2$ we define*

$$\mathfrak{f}_1^{(k)} = (\mathfrak{f}_1^{(k-1)}, \mathfrak{f}_1^{(k-1)}, \mathfrak{f}_2^{(k-1)}, \mathfrak{f}_2^{(k-1)} \oplus 1)$$

and

$$\mathfrak{f}_2^{(k)} = (\mathfrak{f}_2^{(k-1)}, \mathfrak{f}_2^{(k-1)}, \mathfrak{f}_1^{(k-1)}, \mathfrak{f}_1^{(k-1)} \oplus 1).$$

Then, $\mathfrak{f}_1^{(k)}$ and $\mathfrak{f}_2^{(k)}$ are bent functions in $n + 2k$ variables outside $\mathcal{MM}^{\#}$.

3.3 Semi-bent case of 4-decomposition

The construction of disjoint spectra semi-bent functions was treated in several articles, see [15] and references therein. In terms of the spectral design method in [15], constructing quadruples of semi-bent functions (f_1, f_2, f_3, f_4) on $\mathbb{F}_2^n$ (with n even), whose Walsh spectral values belong to $\{0, \pm 2^{\frac{n+2}{2}}\}$, with pairwise disjoint spectra (so that f_i and f_j are disjoint

spectra functions for $1 \leq i \neq j \leq 4$) can be easily achieved by specifying suitable Walsh supports. It has already been observed in [16, 29] that trivial plateaued functions, having an affine subspace as their Walsh support, essentially correspond to partially bent functions introduced by Carlet in [5] which admit linear structures. Nevertheless, the selection of these Walsh supports as affine subspaces or subsets will be shown to be irrelevant for the class inclusion of the resulting bent functions, which will be entirely governed by the bent duals.

3.3.1 Known results on the design methods of plateaued Boolean functions

Before proving the main results of this section, we will give a brief overview of some known useful results obtained in [15] regarding the construction and properties of s-plateaued Boolean functions. For simplicity, we adopt these results for semi-bent functions, thus $s = 2$, and employ only the parts relevant for our purposes.

Theorem 3.3 [15, Theorem 3.3 (with $s = 2$)] *Let $S_f = \mathbf{v} \oplus EM = \{\boldsymbol{\omega}_0, \ldots, \boldsymbol{\omega}_{2^{n-2}-1}\} \subset \mathbb{F}_2^n$, for some $\mathbf{v} \in \mathbb{F}_2^n$, $M \in GL(n, \mathbb{F}_2)$ and lexicographically ordered subset $E = \{\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{2^{n-2}-1}\} \subset \mathbb{F}_2^n$, where n is even. For a function $g : \mathbb{F}_2^{n-2} \to \mathbb{F}_2$ such that $wt(g) = 2^{n-3} + 2^{\frac{n-2}{2}-1}$ or $wt(g) = 2^{n-3} - 2^{\frac{n-2}{2}-1}$ (having bent weight), let the Walsh spectrum of f on $\mathbb{F}_2^n$ be defined (by identifying $\mathbf{x}_i \in \mathbb{F}_2^{n-2}$ and $\boldsymbol{\omega}_i \in S_f$ through $\mathbf{e}_i \in E$ using (5)) as*

$$W_f(\mathbf{u}) = \begin{cases} 2^{\frac{n+2}{2}}(-1)^{g(\mathbf{x}_i)}, & \text{for } \mathbf{u} = \mathbf{v} \oplus \mathbf{e}_i M \in S_f, \\ 0, & \mathbf{u} \notin S_f. \end{cases} \tag{13}$$

Then:

(i) *f is an 2-plateaued (semi-bent) function if and only if g is at bent distance to*

$$\Phi_f = \{\phi_{\mathbf{u}} : \mathbb{F}_2^{n-2} \to \mathbb{F}_2 : \chi_{\phi_{\mathbf{u}}} = ((-1)^{\mathbf{u}\cdot\omega_0}, (-1)^{\mathbf{u}\cdot\omega_1}, \ldots, (-1)^{\mathbf{u}\cdot\omega_{2^{n-2}-1}}),\ \omega_i \in S_f,\ \mathbf{u} \in \mathbb{F}_2^n\}, \tag{14}$$

where for a subset $B \subset \mathcal{B}_n$ a function g is said to be at bent distance to B if for all $f \in B$ it holds that $d_H(f, g) = 2^{n-1} \pm 2^{n/2-1}$.

(ii) *If $E \subset \mathbb{F}_2^n$ is a linear subspace, then f is semi-bent if and only if g is a bent function on $\mathbb{F}_2^{n-2}$.*

Remark 3.2 Since $|S_f| = 2^{n-2}$ and the absolute value of the Walsh coefficients in Theorem 3.3 is $2^{\frac{n+2}{2}}$, Parseval's identity $\sum_{\mathbf{u}\in\mathbb{F}_2^n} W_f(\mathbf{u})^2 = 2^{2n}$ is clearly satisfied. For ease of notation, we will consider $f \in \mathcal{B}_{n+2}$ and use a dual bent function $g \in \mathcal{B}_n$, which essentially corresponds to the dual function $\widetilde{f^*}$ discussed in Sect. 2.1 and specified in (5). The Walsh support $S_f \subset \mathbb{F}_2^{n+2}$ with $|S_f| = 2^n$, can be specified as a binary matrix of size $2^n \times (n+2)$ of the form $S_f = (\mathbf{c} \oplus \mathbb{F}_2^n M) \wr T_{\mu_1} \wr T_{\mu_2}$, $M \in GL(n, \mathbb{F}_2)$ and $\mathbf{c} \in \mathbb{F}_2^n$. Here, the part $\mathbf{c} \oplus \mathbb{F}_2^n M$ is an affine permutation of $\mathbb{F}_2^n$ and corresponds to the first n columns of S_f; whereas the last two columns $T_{\mu_1} \wr T_{\mu_2}$ of S_f are binary truth tables of $\mu_1, \mu_2 \in \mathcal{B}_n$.

To construct nontrivial semi-bent functions (whose Walsh supports are subsets), one can employ bent functions in the $\mathcal{MM}$ class defined by

$$g(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \psi(\mathbf{y}) \oplus t(\mathbf{y}); \quad \mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{n/2}, \tag{15}$$

where ψ is an arbitrary permutation on $\mathbb{F}_2^{n/2}$ and $t \in \mathcal{B}_{n/2}$ is arbitrary. We give below a slightly modified version of Theorem 4.2 in [15], since we are interested in semi-bent functions in

even dimensions. Therefore, we define the Walsh support as $S_f = (\mathbf{c} \oplus EM) \wr T_\mu \wr T_\mu$ rather than $S_f = (\mathbf{c} \oplus EM) \wr T_\mu$ as originally in [15]. Notice that the use of a nonlinear function $\mu : \mathbb{F}_2^n \to \mathbb{F}_2$ ensures that S_f is not an affine/linear subspace.

Theorem 3.4 [15, Theorem 4.2] *Let $g(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \psi(\mathbf{y})$, $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{n/2}$, be a bent function, n is even. For an arbitrary matrix $M \in GL(n, \mathbb{F}_2)$ and vector $\mathbf{c} \in \mathbb{F}_2^n$, let $S_f = (\mathbf{c} \oplus EM) \wr T_\mu \wr T_\mu$, where $E = \mathbb{F}_2^n$ is ordered lexicographically and $\mu \in \mathcal{B}_n$. We have:*

(i) *Let E_1, E_2 be subspaces of $\mathbb{F}_2^{n/2}$ such that $\psi(E_2) = E_1^\perp$ and define $\mu(\mathbf{x}, \mathbf{y}) = \phi_{E_1}(\mathbf{x})\phi_{E_2}(\mathbf{y})$, where ϕ_{E_i} denotes the characteristic function of E_i. Then, $f : \mathbb{F}_2^{n+2} \to \mathbb{F}_2$, whose Walsh spectrum is specified by means of (13) in Theorem 3.3 (with dimension $n + 2$ instead of n), is a semi-bent function.*

(ii) *Let L be a subspace of $\mathbb{F}_2^n$ and define $\mu(\mathbf{x}, \mathbf{y}) = \phi_L(\mathbf{x})$. If $\psi^{-1}(\mathbf{v} + L^\perp)$ is an affine subspace for all $\mathbf{v} \in \mathbb{F}_2^n$, then $f : \mathbb{F}_2^{n+2} \to \mathbb{F}_2$, whose Walsh spectrum is specified by means of (13) in Theorem 3.3 (with dimension $n+2$ instead of n), is a semi-bent function.*

3.3.2 Bent functions outside $\mathcal{MM}^\#$ using semi-bent functions with suitable duals

By employing the above results, the authors in [15] also proposed a construction method of disjoint spectra plateaued functions, see Theorem 4.4 in [15], and additionally showed that these functions can be efficiently utilized for the construction of bent functions. For the particular case of specifying four semi-bent functions on $\mathbb{F}_2^{n+2}$, by using a bent dual $g \in \mathcal{B}_n$, it is convenient to express $\mathbb{F}_2^{n+2} = V \oplus Q$ where for simplicity $V = \mathbb{F}_2^n \times \{(0, 0)\}$ and $Q = \mathbf{0}_n \times \mathbb{F}_2^2$. Notice that the choice of V leads to the canonical concatenation/decomposition given by (9). The main idea is then to specify disjoint Walsh supports of semi-bent functions f_i on the cosets of V in $\mathbb{F}_2^{n+2}$. The reason for selecting $S_f(\mathbf{c} \oplus \mathbb{F}_2^n M) \wr T_{t_1} \wr T_{t_2}$ in Theorem 3.5 as a non-affine subspace is to demonstrate a somewhat harder design rationale that employs Theorem 3.3(i), which requires that the set Φ_f is at bent distance to the bent dual g. Again, the use of a suitable bent dual $g \in \mathcal{B}_n$ (taken outside $\mathcal{MM}^\#$) is decisive when the design of bent functions outside $\mathcal{MM}^\#$ is considered.

We note the following notion of the so-called relaxed linearity index introduced in [22].

Definition 3.1 [22] 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 $\mathbf{a}, \mathbf{b} \in U$ the second-order derivatives $D_\mathbf{a} D_\mathbf{b} f$ are either constant zero or constant one functions, that is, $D_\mathbf{a} D_\mathbf{b} f = 0$ or $D_\mathbf{a} D_\mathbf{b} f = 1$. 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

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

For a Boolean function $f \in \mathcal{B}_n$ its relaxed linearity index $r\text{-ind}(f)$ is defined by

$$r - \text{ind}(f) := \max_{U \in \mathcal{RMS}(f)} \dim(U).$$

Theorem 3.5 *Let $g \notin \mathcal{MM}^\#$ be a bent function in n variables, n even, with $r\text{-ind}(g) < n/2 - 2$. For an arbitrary matrix $M \in GL(n, \mathbb{F}_2)$ and vector $\mathbf{c} \in \mathbb{F}_2^n$, let $S_f = (\mathbf{c} \oplus \mathbb{F}_2^n M) \wr T_{t_1} \wr T_{t_2} \subset \mathbb{F}_2^{n+2}$, where $t_1, t_2 \in \mathcal{B}_n$ such that $g(\mathbf{x}, \mathbf{y}) \oplus v_1 t_1(\mathbf{x}, \mathbf{y}) \oplus v_2 t_2(\mathbf{x}, \mathbf{y})$ is bent for any $v_1, v_2 \in \mathbb{F}_2$, where $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{n/2}$. Let $Q = \{\mathbf{0}_n\} \times \mathbb{F}_2^2 = \{\mathbf{q}_{00}, \mathbf{q}_{01}, \mathbf{q}_{10}, \mathbf{q}_{11}\}$ and set*

$S_{f_\mathbf{a}} = \mathbf{q_a} \oplus S_f$, for $\mathbf{q_a} \in Q$ and $\mathbf{a} \in \mathbb{F}_2^2$. Then, the functions $f_\mathbf{a} \in \mathcal{B}_{n+2}$, constructed using Theorem 3.3 with $S_{f_\mathbf{a}}$ and g, are semi-bent functions on $\mathbb{F}_2^{n+2}$ with pairwise disjoint spectra. Moreover, the function $\mathfrak{f} \in \mathcal{B}_{n+4}$, whose canonical restrictions are $\mathfrak{f}|_{\mathbb{F}_2^{n+2} \times \{\mathbf{a}\}} := f_\mathbf{a}$, where $\mathbf{a} \in \mathbb{F}_2^2$ (thus $\mathfrak{f} = f_{00}||f_{01}||f_{10}||f_{11}$), is a bent function outside $\mathcal{MM}^\#$.

Proof Let $\mathbf{c} \in \mathbb{F}_2^n$ and $M \in GL(n, \mathbb{F}_2)$ be arbitrary. Let $S_f = (\mathbf{c} \oplus \mathbb{F}_2^n M) \wr T_{t_1} \wr T_{t_2}$, where $t_1, t_2 \in \mathcal{B}_n$. The columns of $\mathbf{c} \oplus \mathbb{F}_2^n M$ correspond to affine functions in n variables, say $l_1, \ldots, l_n \in \mathcal{A}_n$. Thus, by assumption on g, the function $g \oplus \mathbf{v} \cdot (l_1, \ldots, l_n, t_1, t_2)$ is bent for any $\mathbf{v} \in \mathbb{F}_2^{n+2}$. Hence, g is at bent distance to $\Phi_f = \{\phi_\mathbf{v} \in \mathcal{B}_n : T_{\phi_\mathbf{v}} = (\mathbf{v} \cdot \omega_0, \ldots, \mathbf{v} \cdot \omega_{2^n-1}),\ \omega_i \in S_f,\ \mathbf{v} \in \mathbb{F}_2^{n+2}\}$. Let $S_{f_\mathbf{a}} = \mathbf{q_a} \oplus S_f$, for $\mathbf{q_a} \in Q$. By Theorem 3.3(i), the functions $f_\mathbf{a} \in \mathcal{B}_{n+2}$, whose Walsh spectral values at $\mathbf{v} \in \mathbb{F}_2^{n+2}$ are defined by:

$$W_{f_\mathbf{a}}(\mathbf{v}) = \begin{cases} 2^{\frac{n+4}{2}}(-1)^{g(\mathbf{x}_i, \mathbf{y}_i)}, & \mathbf{v} = (\mathbf{c} \oplus (\mathbf{x}_i, \mathbf{y}_i) \cdot M, t_1(\mathbf{x}_i, \mathbf{y}_i), t_2(\mathbf{x}_i, \mathbf{y}_i)) \oplus \mathbf{q_a} \in S_{f_\mathbf{a}} \\ 0, & \mathbf{v} \notin S_{f_\mathbf{a}} \end{cases}, \tag{16}$$

are 2-plateaued (semi-bent) functions, for $\mathbf{a} \in \mathbb{F}_2^2$. Furthermore, we have $\cup_{\mathbf{q_a} \in Q}(\mathbf{q_a} \oplus S_f) = \mathbb{F}_2^{n+2}$ and the function $\mathfrak{f} = f_{00}||f_{01}||f_{10}||f_{11} \in \mathcal{B}_{n+4}$ is bent by Theorem 2.2(ii), since the restrictions $f_\mathbf{a}$ are pairwise disjoint spectra semi-bent functions.

It remains to show that $\mathfrak{f}$ is outside $\mathcal{MM}^\#$. For convenience, we write $\mathbf{u} = (\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\omega}) \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2} \times \mathbb{F}_2^2 \times \mathbb{F}_2^2$. Then, the Walsh-Hadamard transform of $\mathfrak{f}$ at $\mathbf{u} \in \mathbb{F}_2^{n+4}$ evaluates to:

$$\begin{aligned} W_\mathfrak{f}(\mathbf{u}) &= \sum_{(\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{w}) \in (\mathbb{F}_2^{n/2})^2 \times (\mathbb{F}_2^2)^2} (-1)^{\mathfrak{f}(\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{w}) \oplus (\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{w}) \cdot \mathbf{u}} \\ &= \sum_{\mathbf{w} \in \mathbb{F}_2^2} \sum_{(\mathbf{x},\mathbf{y},\mathbf{z}) \in (\mathbb{F}_2^{n/2})^2 \times \mathbb{F}_2^2} (-1)^{f_\mathbf{w}(\mathbf{x},\mathbf{y},\mathbf{z}) \oplus (\mathbf{x},\mathbf{y},\mathbf{z}) \cdot (\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}) \oplus \mathbf{w} \cdot \boldsymbol{\omega}} \\ &= \sum_{\mathbf{w} \in \mathbb{F}_2^2} (-1)^{\mathbf{w} \cdot \boldsymbol{\omega}} \sum_{(\mathbf{x},\mathbf{y},\mathbf{z}) \in (\mathbb{F}_2^{n/2})^2 \times \mathbb{F}_2^2} (-1)^{f_\mathbf{w}(\mathbf{x},\mathbf{y},\mathbf{z}) \oplus (\mathbf{x},\mathbf{y},\mathbf{z}) \cdot (\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma})} \\ &= \sum_{\mathbf{w} \in \mathbb{F}_2^2} (-1)^{\mathbf{w} \cdot \boldsymbol{\omega}} W_{f_\mathbf{w}}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}) = (*). \end{aligned}$$

As $\cup_{\mathbf{q} \in Q}(\mathbf{q} \oplus S_f) = \mathbb{F}_2^{n+2}$ and $\mathbf{q} \oplus S_f \cap \mathbf{q}' \oplus S_f = \emptyset$ for $\mathbf{q} \neq \mathbf{q}'$, we have that $(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma})$ is in exactly one support $S_{f_\mathbf{w}}$ for some $\mathbf{w} \in \mathbb{F}_2^2$. We note that $(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \mathbf{c} \oplus (\boldsymbol{\alpha}', \boldsymbol{\beta}') \cdot M$ for some $(\boldsymbol{\alpha}', \boldsymbol{\beta}') \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2}$ and $\boldsymbol{\gamma} = (t_1(\boldsymbol{\alpha}', \boldsymbol{\beta}'), t_2(\boldsymbol{\alpha}', \boldsymbol{\beta}')) \oplus \mathbf{a}_{\boldsymbol{\gamma}}$ for some $\mathbf{a}_{\boldsymbol{\gamma}} \in \mathbb{F}_2^2$, whose choice depends on the value of $\boldsymbol{\gamma}$. Hence,

$$(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}) = (\mathbf{c} \oplus (\boldsymbol{\alpha}', \boldsymbol{\beta}') \cdot M, t_1(\boldsymbol{\alpha}', \boldsymbol{\beta}'), t_2(\boldsymbol{\alpha}', \boldsymbol{\beta}')) \oplus \mathbf{q}_{\mathbf{a}_\gamma}.$$

Thus, we have that

$$\begin{aligned} (*) &= 2^{\frac{n+4}{2}} \cdot (-1)^{\mathbf{a}_\gamma \cdot \boldsymbol{\omega} \oplus g(\boldsymbol{\alpha}', \boldsymbol{\beta}')} \\ &= 2^{\frac{n+4}{2}} \cdot (-1)^{((t_1(((\boldsymbol{\alpha},\boldsymbol{\beta}) \oplus \mathbf{c}) \cdot M^{-1}), t_2(((\boldsymbol{\alpha},\boldsymbol{\beta}) \oplus \mathbf{c}) \cdot M^{-1})) \oplus \boldsymbol{\gamma}) \cdot \boldsymbol{\omega} \oplus g(((\boldsymbol{\alpha},\boldsymbol{\beta}) \oplus \mathbf{c}) \cdot M^{-1})} \end{aligned}$$

which implies that the dual $\mathfrak{f}^* \in \mathcal{B}_{n+4}$ of $\mathfrak{f}$ is defined by

$$\begin{aligned} \mathfrak{f}^*(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) &= ((t_1(((\mathbf{x}, \mathbf{y}) \oplus \mathbf{c}) \cdot M^{-1}), t_2(((\mathbf{x}, \mathbf{y}) \oplus \mathbf{c}) \cdot M^{-1})) \oplus \mathbf{z}) \\ &\cdot \mathbf{w} \oplus g(((\mathbf{x}, \mathbf{y}) \oplus \mathbf{c}) \cdot M^{-1}), \end{aligned}$$

for $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{n/2}$ and $\mathbf{z}, \mathbf{w} \in \mathbb{F}_2^2$. Without loss of generality, let us consider the function

$$\begin{aligned}\mathfrak{h}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) &= \mathfrak{f}^*((\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) \cdot M' \oplus (\mathbf{c}, \mathbf{0}_2, \mathbf{0}_2)) \\ &= ((t_1(\mathbf{x}, \mathbf{y}), t_2(\mathbf{x}, \mathbf{y})) \oplus \mathbf{z}) \cdot \mathbf{w} \oplus g(\mathbf{x}, \mathbf{y}) \\ &= g(\mathbf{x}, \mathbf{y}) \oplus \mathbf{z} \cdot \mathbf{w} \oplus (t_1(\mathbf{x}, \mathbf{y}), t_2(\mathbf{x}, \mathbf{y})) \cdot \mathbf{w},\end{aligned}$$

where

$$M' = \left(\begin{array}{c|c} M & O_4 \\ \hline O_4 & I_4 \end{array}\right).$$

We note that $\mathfrak{h}$ and $\mathfrak{f}^*$ are EA-equivalent functions and thus belong to the same completed class of bent functions.

Let us now consider the second-order derivative of $\mathfrak{h}$. Suppose that V is some $(n+4)/2$-dimensional subspace of $\mathbb{F}_2^{n+4} = \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2} \times \mathbb{F}_2^2 \times \mathbb{F}_2^2$ and let $\alpha = (\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}, \alpha^{(4)}), \beta = (\beta^{(1)}, \beta^{(2)}, \beta^{(3)}, \beta^{(4)}) \in V$, where $\alpha^{(1)}, \alpha^{(2)}, \beta^{(1)}, \beta^{(2)} \in \mathbb{F}_2^{n/2}, \alpha^{(3)}, \alpha^{(4)}, \beta^{(3)}, \beta^{(4)} \in \mathbb{F}_2^2$. For easier notation, we will denote with $\alpha_{12} = (\alpha^{(1)}, \alpha^{(2)})$ and $\beta_{12} = (\beta^{(1)}, \beta^{(2)})$. The second-order derivative of $\mathfrak{h}$ evaluates to

$$\begin{aligned}D_\alpha D_\beta \mathfrak{h}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) = {} & D_{\alpha_{12}} D_{\beta_{12}} g(\mathbf{x}, \mathbf{y}) \oplus \mathbf{w} \cdot (D_{\alpha_{12}} D_{\beta_{12}} t_1(\mathbf{x}, \mathbf{y}), D_{\alpha_{12}} D_{\beta_{12}} t_2(\mathbf{x}, \mathbf{y})) \\ & \oplus \alpha^{(4)} \cdot (D_{\beta_{12}} t_1((\mathbf{x}, \mathbf{y}) \oplus \alpha_{12}), D_{\beta_{12}} t_2((\mathbf{x}, \mathbf{y}) \oplus \alpha_{12})) \\ & \oplus \beta^{(4)} \cdot (D_{\alpha_{12}} t_1((\mathbf{x}, \mathbf{y}) \oplus \beta_{12}), D_{\alpha_{12}} t_2((\mathbf{x}, \mathbf{y}) \oplus \beta_{12})) \\ & \oplus \alpha^{(3)} \cdot \beta^{(3)} \oplus \alpha^{(4)} \cdot \beta^{(4)}. \end{aligned} \tag{17}$$

First, we note that there are no bent functions outside $\mathcal{MM}^\#$ for $n \leq 6$, i.e., we must have $n \geq 8$. Hence, the smallest possible dimension we can consider is $8 + 4 = 12$ for which the vanishing subspace V has dimension 6. Since $\dim(V) = n/2 + 2$, we have

$$\dim(\{(\mathbf{x}, \mathbf{y}, \mathbf{z}, 0_2) \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2} \times \mathbb{F}_2^2 \colon (\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) \in V\}) \geq n/2.$$

Hence, without loss of generality, we can take $\alpha = (\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}, 0, 0)$ and $\beta = (\beta^{(1)}, \beta^{(2)}, \beta^{(3)}, 0, 0)$ for some distinct nonzero α_{12}, β_{12}. From (17), for $\mathbf{w} = 0_2$ and $\alpha^{(4)} = \beta^{(4)} = (0, 0)$, we have that

$$D_\alpha D_\beta \mathfrak{h}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w})\Big|_{\mathbf{w}=0_2} = D_{\alpha_{12}} D_{\beta_{12}} g(\mathbf{x}, \mathbf{y}) \oplus \alpha^{(3)} \cdot \beta^{(3)}.$$

Furthermore, since $\dim(\{(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2} \colon (\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) \in V\}) \geq n/2 - 2$ and r-$\mathrm{ind}(g) < n/2 - 2$ we have that

$$D_\alpha D_\beta \mathfrak{h}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w})|_{\mathbf{w}=0_2} \neq 0.$$

Thus $\mathfrak{h} \notin \mathcal{MM}^\#$, which implies that $\mathfrak{f}^* \notin \mathcal{MM}^\#$. By Remark 3.1, it means that $\mathfrak{f}$ is outside $\mathcal{MM}^\#$. □

Remark 3.3 The condition that r-$\mathrm{ind}(g) < n/2-2$ is quite strict and can be relaxed in certain cases. For instance, taking that $t_1 = t_2 = 0$ in Theorem 3.5, the function $\mathfrak{h}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) = g(\mathbf{x}, \mathbf{y}) \oplus \mathbf{z} \cdot \mathbf{w} \oplus (t_1(\mathbf{x}, \mathbf{y}), t_2(\mathbf{x}, \mathbf{y})) \cdot \mathbf{w}$ becomes $\mathfrak{h}(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) = g(\mathbf{x}, \mathbf{y}) \oplus \mathbf{z} \cdot \mathbf{w}$, which by Corollary 1 is outside $\mathcal{MM}^\#$ if and only if g is outside $\mathcal{MM}^\#$. This also indicates that the choice of a non-affine Walsh support is not decisive for the class inclusion since the support S_f in Theorem 3.5 is affine when $t_1 = t_2 = 0$.

Since $g \in \mathcal{B}_n$ is supposed to be a bent function outside $\mathcal{MM}^\#$ (with additional restriction that $r\text{-ind}(g) < n/2 - 2$), we can employ the class $\mathcal{D}_0$ of Carlet [4] or certain families of bent functions in $\mathcal{C}$ and $\mathcal{D}$ that are provably outside $\mathcal{MM}^\#$ [18, 26, 28]. Alternatively g can be taken from the recent classes $\mathcal{SC}$ and $\mathcal{CD}$ [1, 2], which are specified in Corollary 3 below. Notice that the subspaces L, E_1, E_2 used to define g in Corollary 3 below, satisfy certain conditions with respect to the permutation π, see [4, 26, 28]. However, there exist efficient design methods for specifying bent functions in the above classes that are provably outside $\mathcal{MM}^\#$ [1, 2, 18, 26, 28]. On the other hand, for $t_1, t_2 \in \mathcal{B}_n$ we use certain indicators that preserve the bentness of $g(\mathbf{x}, \mathbf{y}) \oplus v_1 t_1(\mathbf{x}, \mathbf{y}) \oplus v_2 t_2(\mathbf{x}, \mathbf{y})$. The results are summarised in the following corollary, where we denote $\delta_0(\mathbf{x}) = \prod_{i=1}^{n/2}(x_i \oplus 1)$ which is the indicator function of $\{0_{n/2}\} \times \mathbb{F}_2^{n/2}$. Notice again that taking $t_1 = t_2 = 0$ in Corollary 3, it is sufficient to take any bent function g outside $\mathcal{MM}^\#$.

Corollary 3 *With the same notation as in Theorem 3.5, if a bent function $g \in \mathcal{B}_n$ satisfies $r\text{-ind}(g) < n/2 - 2$ and $t_1, t_2 \in \mathcal{B}_n$ are defined by:*

(i) $g(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus \delta_0(\mathbf{x}) \in \mathcal{D}_0 \setminus \mathcal{MM}^\#$, $t_1(\mathbf{x}, \mathbf{y}) = t_2(\mathbf{x}, \mathbf{y}) = \delta_0(\mathbf{x})$, $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{n/2}$,

(ii) $g(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus \mathbf{1}_{L^\perp}(\mathbf{x}) \in \mathcal{C} \setminus \mathcal{MM}^\#$, t_1, t_2 *correspond to* $\mathbf{1}_{L^\perp}(\mathbf{x})$ *or* $\delta_0(\mathbf{x})$, $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{n/2}$,

(iii) $g(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus \mathbf{1}_{L^\perp}(\mathbf{x}) \oplus \delta_0(\mathbf{x}) \in \mathcal{SC} \setminus \mathcal{MM}^\#$, t_1, t_2 *correspond to* $\mathbf{1}_{L^\perp}(\mathbf{x})$ *or* $\delta_0(\mathbf{x})$, $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{n/2}$, *or*

(iv) $g(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus \mathbf{1}_{L^\perp}(\mathbf{x}) \oplus \mathbf{1}_{E_1}(\mathbf{x})\mathbf{1}_{E_2}(\mathbf{y}) \in \mathcal{CD} \setminus \mathcal{MM}^\#$, $t_1(\mathbf{x}, \mathbf{y}) = t_2(\mathbf{x}, \mathbf{y}) = \mathbf{1}_{L^\perp}(\mathbf{x})$, $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{n/2}$,

then $\mathfrak{f} \in \mathcal{B}_{n+4}$ is a bent function outside $\mathcal{MM}^\#$.

In the following example, we take $g \in \mathcal{D}_0 \setminus \mathcal{MM}^\#$ in 8 variables (satisfying the condition $r\text{-ind}(g) < 8/2 - 2 = 2$) to construct a bent function in 12 variables outside $\mathcal{MM}^\#$ by means of Theorem 3.5. The result was also confirmed using our algorithm in Sect. 3.1.

Example 3.2 Let $g(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi(\mathbf{y}) \oplus \delta_0(\mathbf{x})$, $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^4$, be a bent function in $\mathcal{D}_0$ (outside $\mathcal{MM}^\#$), where $\pi = (0, 1, 11, 13, 9, 14, 6, 7, 12, 5, 8, 3, 15, 2, 4, 10)$ is a permutation of $\mathbb{F}_2^4$ represented in integer form. Using Sage, it was confirmed that $r\text{-ind}(g) = 1$. Let $\mathbf{c} \in \mathbb{F}_2^8$ and $M \in GL(8, \mathbb{F}_2)$ be arbitrary, say,

$$\mathbf{c} = (0, 0, 1, 0, 1, 1, 1, 1), \quad M = \begin{pmatrix} 0\,0\,0\,1\,0\,0\,1\,1 \\ 1\,1\,1\,1\,1\,1\,0\,1 \\ 0\,1\,1\,1\,0\,1\,0\,1 \\ 1\,1\,0\,1\,1\,1\,1\,1 \\ 0\,0\,1\,0\,0\,1\,1\,1 \\ 1\,1\,0\,0\,0\,0\,0\,1 \\ 0\,1\,0\,0\,0\,0\,1\,1 \\ 1\,1\,0\,1\,1\,1\,0\,0 \end{pmatrix}.$$

Let $S_f = (\mathbf{c} \oplus \mathbb{F}_2^8 \cdot M) \wr T_{\delta_0} \wr T_{\delta_0} \subset \mathbb{F}_2^{10}$, where T_{δ_0} is the truth table of the function $\delta_0(\mathbf{x})$ viewed as a function on $\mathbb{F}_2^8$. That is, $\delta_0(\mathbf{x}, \mathbf{y}) = \delta_0(\mathbf{x}) \in \mathcal{B}_8$. Then, $f_i \in \mathcal{B}_{10}$ defined via S_{f_i} and g, using Theorem 3.3, are pairwise disjoint spectra functions, where $S_{f_\mathbf{a}} = S_f \oplus \mathbf{q_a}$ and $\mathbf{q_a} \in Q = \{\mathbf{0}_8\} \times \mathbb{F}_2^2$ for $\mathbf{a} \in \mathbb{F}_2^2$. In other words, $\mathfrak{f} = (f_{00}, f_{01}, f_{10}, f_{11}) \in \mathcal{B}_{12}$ is a bent function and can be viewed as a concatenation of four semi-bent functions. Furthermore, using our algorithm in Sect. 3.1, we have confirmed that $\mathfrak{f}$ lies outside $\mathcal{MM}^\#$. The ANF of $\mathfrak{f}$ is given by (24) in the appendix.

The following remarks are important with respect to the cardinality of bent functions outside $\mathcal{MM}^{\#}$ or the presence of linear structures of the constituent semi-bent functions.

Remark 3.4 Notice that the number of possibilities of selecting for S_f (which is a binary matrix of size $2^n \times (n+2)$) is quite large. We have 2^n possible choices for $\mathbf{c} \in \mathbb{F}_2^n$ and $\prod_{k=0}^{n}(2^n - 2^k)$ choices for $M \in GL(n, \mathbb{F}_2)$. Thus, for fixed Boolean functions $t_1, t_2 \in \mathcal{B}_n$, we have $2^n \prod_{k=0}^{n}(2^n - 2^k)$ choices for S_f. For example, for $n = 8$ this number equals $\approx 2^{70.2}$.

Remark 3.5 The existence of linear structures in the semi-bent functions f_i, used in Theorem 3.5 to specify $\mathfrak{f}$, is of no importance when determining whether $\mathfrak{f} \notin \mathcal{MM}^{\#}$. We have confirmed this, using our algorithm from Sect. 3.1, by verifying that the resulting bent functions are always outside $\mathcal{MM}^{\#}$ provided that the bent function g used to define the dual of f_i (by means of (16)) is outside $\mathcal{MM}^{\#}$. It is completely irrelevant whether these semi-bent functions possess linear structures (having affine supports S_{f_i}) or not. This is also evident from Remark 3.3 since taking $t_1 = t_2 = 0$ the Walsh supports of the restrictions $f_{\mathbf{a}}$ are affine.

3.4 Four bent decomposition in terms of 5-valued spectra functions

To specify 5-valued spectra Boolean functions, the authors in [14] provided a sufficient and necessary condition that the Walsh spectra of f_i (corresponding to two different amplitudes) must satisfy, see Sect. 2.2. The notion of totally disjoint spectra functions was also introduced in [14], which can be regarded as a sufficient condition so that the Walsh spectrum specified by (6) is a valid spectrum of a Boolean function.

Definition 3.2 [14, *Definition 4.1*] For two disjoint sets $S_f^{[1]}, S_f^{[2]} \subset \mathbb{F}_2^n$, with $\#S_f^{[1]} + \#S_f^{[2]} = 2^{\lambda_1} + 2^{\lambda_2} < 2^n$, we say that the dual functions $f^*_{[1]} : S_f^{[1]} \to \mathbb{F}_2$ and $f^*_{[2]} : S_f^{[2]} \to \mathbb{F}_2$ (in terms of (6)) are *totally disjoint spectra functions* if it holds that

$$X_1(\mathbf{u})X_2(\mathbf{u}) = 0 \quad \text{and} \quad |X_1(\mathbf{u})| + |X_2(\mathbf{u})| > 0,$$

for all $\mathbf{u} \in \mathbb{F}_2^n$, where $X_i(\mathbf{u}) = \sum_{\omega \in S_f^{[i]}} (-1)^{f^*_{[i]}(\omega) \oplus \mathbf{u}\cdot\omega}$, for $i = 1, 2$.

Remark 3.6 Note that the second condition implies the nonexistence of a vector $\mathbf{u} \in \mathbb{F}_2^n$ for which $X_1(\mathbf{u}) = X_2(\mathbf{u}) = 0$. Without this condition, the notion of totally disjoint spectra coincides with non-overlap disjoint spectra functions in [25].

Furthermore, a generic method of specifying totally disjoint spectra functions was also given in [14].

Construction 1 [14] *Let n, m and k be even with $n = m + k$. Let $h \in \mathcal{B}_m$ and $g \in \mathcal{B}_k$ be two bent functions. Let H be any subspace of $\mathbb{F}_2^m$ of co-dimension 1, and let $\overline{H} = \mathbb{F}_2^m \backslash H$. Let also $E_1 = \mathbb{F}_2^k \times H$ and $E_2 = \{\mathbf{0}_k\} \times \overline{H}$. The Walsh spectrum of $f \in \mathcal{B}_n$, with $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{F}_2^k \times \mathbb{F}_2^m$, can be constructed as follows:*

$$W_f(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \begin{cases} (-1)^{g(\boldsymbol{\alpha}) \oplus h(\boldsymbol{\beta})} \cdot 2^{n/2}, & (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_1 \\ (-1)^{h(\boldsymbol{\beta})} \cdot 2^{m/2+k}, & (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_2 \\ 0, & otherwise. \end{cases} \tag{18}$$

Then, W_f is a valid spectrum of a Boolean function $f \in \mathcal{B}_n$. Let now

$$f_1(\boldsymbol{\alpha}, \boldsymbol{\beta}) = g(\boldsymbol{\alpha}) \oplus h(\boldsymbol{\beta}), \quad (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_1$$

$$f_2(\boldsymbol{\alpha}, \boldsymbol{\beta}) = h(\boldsymbol{\beta}), \quad (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_2.$$

Then, $f_1 : E_1 \to \mathbb{F}_2$ and $f_2 : E_2 \to \mathbb{F}_2$ are totally disjoint spectra functions.

Remark 3.7 Notice that the sets E_1 and E_2 in Construction 1 can be defined similarly using any element $\mathbf{v} \in \mathbb{F}_2^k$ instead of $\mathbf{0}_k$, so that $E_2 = \{\mathbf{v}\} \times \overline{H}$ and $E_1 = \mathbb{F}_2^k \times H$ remains the same. Then, E_1 and E_2 are clearly disjoint.

Now, we need to specify a quadruple of 5-valued spectra functions in $\mathcal{B}_{n-2}$ by means of Construction 1, which additionally satisfies the condition given by item (iii) of Theorem 2.2. More precisely:

(a) The sets $S_{f_i}^{[1]} = \{\boldsymbol{\vartheta} \in \mathbb{F}_2^{n-2} : |W_{f_i}(\boldsymbol{\vartheta})| = 2^{\frac{n}{2}}\}$ ($i \in [1, 4]$) are pairwise disjoint;

(b) All $S_{f_i}^{[2]} = \{\boldsymbol{\vartheta} \in \mathbb{F}_2^{n-2} : |W_{f_i}(\boldsymbol{\vartheta})| = 2^{\frac{n-2}{2}}\}$ are equal ($i \in [1, 4]$), and for $f_{[2],i}^* : S_{f_i}^{[2]} \to \mathbb{F}_2$ it holds that $f_{[2],1}^* \oplus f_{[2],2}^* \oplus f_{[2],3}^* \oplus f_{[2],4}^* = 1$.

When $k = 2$, Construction 1 can generate suitable quadruples of 5-valued spectra functions (which are individually totally disjoint spectra functions) as shown below. Notice that the subspaces $S_{f_i}^{[1]}$ will correspond to $E_2^{(i)}$ and $S_{f_i}^{[2]}$ to $E_1^{(i)}$ in Theorem 3.6.

Theorem 3.6 *Let $n = m + 2$ be even so that m is also even. Let $h \in \mathcal{B}_m$ and $g \in \mathcal{B}_k = \mathcal{B}_2$ be two bent functions. Let H be any subspace of $\mathbb{F}_2^m$ of co-dimension 1, and let $\overline{H} = \mathbb{F}_2^m \backslash H$. Let also $E_1^{(i)} = \mathbb{F}_2^2 \times H$ and $E_2^{(i)} = \{\mathbf{c}^{(i)}\} \times \overline{H}$, for $i = 1, \ldots, 4$, where $\mathbf{c}^{(i)} \in \mathbb{F}_2^2$ are ordered lexicographically so that $\mathbf{c}^{(i)} \neq \mathbf{c}^{(j)}$ for $1 \leq i \neq j \leq 4$. We specify the spectra of $f_i \in \mathcal{B}_n$ as follows:*

$$W_{f_i}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \begin{cases} (-1)^{g(\boldsymbol{\alpha}) \oplus h(\boldsymbol{\beta}) \oplus d} \cdot 2^{n/2}, & (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_1^{(i)} \\ (-1)^{h(\boldsymbol{\beta})} \cdot 2^{\frac{n-2}{2}+2}, & (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_2^{(i)} \\ 0, & otherwise, \end{cases} \tag{19}$$

where $d = 1$ if $i = 4$, otherwise $d = 0$. Then, the function $f \in \mathcal{B}_{n+2}$ given as the concatenation $f = f_1||f_2||f_3||f_4$ is a bent function.

Proof The functions $f_i \in \mathcal{B}_n$, specified by (19), are clearly 5-valued spectra functions. We need to verify that their spectra corresponds to Boolean functions. By Construction 1, corresponding to the definition of $E_1^{(1)}$ and $E_2^{(1)}$ using $\mathbf{c}^{(1)} = (0, 0)$, this is true for f_1. Due to the definition of $E_1^{(i)}$ and $E_2^{(i)}$ and Remark 3.7, the same is true for any f_i which are all Boolean 5-valued spectra functions. For instance, using $\mathbf{c}^{(2)} = (0, 1)$ to define f_2, the condition that $E_1^{(1)} = E_1^{(2)}$ is clearly true and furthermore $(0, 0) \times \overline{H} \cap (0, 1) \times \overline{H} = \emptyset$, that is $E_2^{(1)} \cap E_2^{(2)} = \emptyset$.

Now, the condition for a valid 4-decomposition into 5-valued spectra functions is given by (iii) in Theorem 2.2. The supports $E_2^{(i)}$ are clearly disjoint by their definition, whereas $E_1^{(i)}$ are defined on the same subspace of $\mathbb{F}_2^n$. The last condition that the bent duals defined on $E_1^{(i)}$ satisfy $f_{[2],1}^* \oplus f_{[2],2}^* \oplus f_{[2],3}^* \oplus f_{[2],4}^* = 1$ follows from the specification of the spectra on $E_1^{(i)}$, using the fact that $d = 1$ only when $i = 4$. □

Remark 3.8 Since $d = 1$ when $i = 4$, the complement of the dual is used for the fourth constituent function f_4. This ensures that the bent duals satisfy $f_{[2],1}^* \oplus f_{[2],2}^* \oplus f_{[2],3}^* \oplus f_{[2],4}^* = 1$. Nevertheless, this is not the only choice and the bent duals can be specified in other ways (through the complement operation) as long as their sum equals 1.

The following examples illustrate the details of this construction and the possibility of getting bent functions outside $\mathcal{MM}^{\#}$. Notice that the dual h used to specify f is not necessarily in $\mathcal{MM}^{\#}$.

Example 3.3 Let $n = 8$ and let $h \in \mathcal{B}_6$, $g \in \mathcal{B}_2$ be defined by $h(x_0, \ldots, x_5) = x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \in \mathcal{MM}$ and $g(x_0, x_1) = x_0x_1$. Let $H = \langle (1, 0, 0, 0, 0, 0) \rangle^{\perp} \subset \mathbb{F}_2^6$ be a subspace of codimension 1. Using the mathematical software Sage, we constructed the functions $f^{(i)} \in \mathcal{B}_8$ for $i = 1, \ldots, 4$ defined by (19) and their ANF's are given as follows:

$$
\begin{aligned}
f_1(x_0, \ldots, x_7) &= x_0x_1x_3 \oplus x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_6x_7,\\
f_2(x_0, \ldots, x_7) &= x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_2x_3 \oplus x_4x_5 \oplus x_6x_7,\\
f_3(x_0, \ldots, x_7) &= x_0x_1x_3 \oplus x_0x_1 \oplus x_1x_3 \oplus x_2x_3 \oplus x_4x_5 \oplus x_6x_7,\\
f_4(x_0, \ldots, x_7) &= x_0x_1x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3 \oplus x_4x_5 \oplus x_6x_7 \oplus 1
\end{aligned}
$$

Then, the function $f \in \mathcal{B}_{10}$ given as the concatenation $f = f_1||f_2||f_3||f_4$ is a cubic bent function defined by

$$f(x_0, \ldots, x_9) = x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3x_8 \oplus x_2x_3x_9 \oplus x2x_3 \oplus x_3x_8x_9 \oplus x_4x_5 \oplus x_6x_7 \oplus x_8x_9.$$

Using our algorithm in Sect. 3.1, we could verify that $f \in \mathcal{MM}^{\#}$.

On the other hand, the following two examples illustrate that selecting the dual h to be outside $\mathcal{MM}^{\#}$, the resulting bent functions (constructed using Theorem 3.6) are outside $\mathcal{MM}^{\#}$.

Example 3.4 Let $h \in \mathcal{B}_8$ defined by $h(x, y) = Tr_1^4(xy^7) + \delta_0(x)$, $x, y \in \mathbb{F}_{2^4}$, be a bent function in the class $\mathcal{D}_0 \setminus \mathcal{MM}^{\#}$ [4, 28], and let $g \in \mathcal{B}_2$ be defined by $g(x_0, x_1) = x_0x_1$. Let us define $H = \langle (1, 0, 0, 0, 0, 0, 0, 0) \rangle^{\perp} \subset \mathbb{F}_2^8$ to be a subspace of codimension 1. Using Sage we constructed the functions $f_i \in \mathcal{B}_{10}$ for $i = 1, \ldots, 4$ defined by (19). Then, the function $f \in \mathcal{B}_{12}$ given as $f = f_1||f_2||f_3||f_4$ is a bent function of algebraic degree 5. This time the function f, whose ANF is given by (22) in the appendix, is outside $\mathcal{MM}^{\#}$.

Example 3.5 Let $n = 10$ and $h \in \mathcal{B}_8$, $g \in \mathcal{B}_2$ be bent functions, where $g(x_0, x_1) = x_0x_1$. The function $h \in \mathcal{B}_8$, whose ANF is given by (21) in Appendix, lies in $\mathcal{PS}^{\#}$ and is outside $\mathcal{MM}^{\#}$. Using Sage, we constructed the functions $f_i \in \mathcal{B}_{10}$ for $i = 1, \ldots, 4$ defined by (19). Then, the function $f \in \mathcal{B}_{12}$ given as $f = f_1||f_2||f_3||f_4$ is a bent function of algebraic degree 5. Again, it could be confirmed that f is outside $\mathcal{MM}^{\#}$ (its ANF is given by (23) in the appendix).

The above examples indicate that the conclusions (related to the dual) given in Sect. 3.2 seem to be applicable in this case as well. More precisely, the class belongingness of f in Theorem 3.6 is strongly related to the choice of the dual bent functions.

Theorem 3.7 *Let $f \in \mathcal{B}_{n+2}$ be constructed by means of Theorem 3.6, thus $f = f_1||f_2||f_3||f_4$ where $f_i \in \mathcal{B}_n$. If the dual bent function $h \in \mathcal{B}_{n-2}$ in Theorem 3.6 is outside $\mathcal{MM}^{\#}$, then f is outside $\mathcal{MM}^{\#}$.*

Proof By Remark 3.1, f is outside $\mathcal{MM}^{\#}$ if and only if its dual f^* is outside $\mathcal{MM}^{\#}$. Hence, it is enough to show that f^* is outside $\mathcal{MM}^{\#}$. The "duals" of the restrictions f_i are actually given by (19). By the definition of f^*, we have that $(-1)^{f^*(\mathbf{u})} = 2^{-\frac{n+2}{2}} W_f(\mathbf{u})$ for any $\mathbf{u} \in \mathbb{F}_2^{n+2}$, since $f \in \mathcal{B}_{n+2}$. For convenience, we write $\mathbf{u} = (\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}) \in \mathbb{F}_2^2 \times \mathbb{F}_2^m \times \mathbb{F}_2^2$ with

$n = m+2$ as used in Theorem 3.6. We notice that in general, using that $\mathbf{x} = (\mathbf{x}', x_{n+1}, x_{n+2}) \in \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2$, we have

$$\begin{aligned} W_f(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}) &= \sum_{\mathbf{x} \in \mathbb{F}_2^n \times \mathbb{F}_2^2} (-1)^{f(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}} \\ &= \sum_{\mathbf{x} \in \mathbb{F}_2^n \times (0,0)} (-1)^{f(\mathbf{x}', 0, 0) + (\boldsymbol{\alpha}, \boldsymbol{\beta}) \cdot \mathbf{x}'} + \sum_{\mathbf{x} \in \mathbb{F}_2^n \times (0,1)} (-1)^{f(\mathbf{x}', 0, 1) + (\boldsymbol{\alpha}, \boldsymbol{\beta}) \cdot \mathbf{x}' + \gamma_2} \\ &\quad + \sum_{\mathbf{x} \in \mathbb{F}_2^n \times (1,0)} (-1)^{f(\mathbf{x}', 1, 0) + (\boldsymbol{\alpha}, \boldsymbol{\beta}) \cdot \mathbf{x}' + \gamma_1} \\ &\quad + \sum_{\mathbf{x} \in \mathbb{F}_2^n \times (1,1)} (-1)^{f(\mathbf{x}', 1, 1) + (\boldsymbol{\alpha}, \boldsymbol{\beta}) \cdot \mathbf{x}' + \gamma_1 + \gamma_2} \\ &= W_{f_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}) + (-1)^{\gamma_2} W_{f_2}(\boldsymbol{\alpha}, \boldsymbol{\beta}) \\ &\quad + (-1)^{\gamma_1} W_{f_3}(\boldsymbol{\alpha}, \boldsymbol{\beta}) + (-1)^{\gamma_1 + \gamma_2} W_{f_4}(\boldsymbol{\alpha}, \boldsymbol{\beta}). \end{aligned} \tag{20}$$

Hence, for any fixed $\gamma \in \mathbb{F}_2^2$, we can compute the value of $W_f(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma})$ by using the Walsh spectra of the constituent functions f_i.

We first notice that $W_{f_i}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = (-1)^{h(\boldsymbol{\beta})} \cdot 2^{\frac{n-2}{2}+2}$ when $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_2^{(i)}$, and furthermore by construction the sets $E_2^{(i)}$ are mutually disjoint for $i = 1, \ldots, 4$. Hence, if for instance $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_2^{(1)}$ then $W_{f_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = (-1)^{h(\boldsymbol{\beta})} \cdot 2^{\frac{n-2}{2}+2}$ and $W_{f_i}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 0$ for $2 \leq i \leq 4$, which implies that $W_f(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}) = (-1)^{h(\boldsymbol{\beta})} \cdot 2^{\frac{n}{2}+1}$ when $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_2^{(1)}$. The other cases when $(\alpha, \beta) \in E_2^{(i)}$ for $i \neq 1$ are similar.

Now, considering the case $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_1^{(i)}$, we first notice that $E_1 := E_1^{(1)} = \cdots = E_1^{(4)}$ (by construction), where $E_1 = \mathbb{F}_2^2 \times H$ as in Theorem 3.6. In addition, $W_{f_i}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = (-1)^{g(\boldsymbol{\alpha}) \oplus h(\boldsymbol{\beta}) + d} \cdot 2^{n/2}$, where $d = 1$ when $i = 4$ only. This also implies that $W_{f_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = W_{f_2}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = W_{f_3}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = -W_{f_4}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ when $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_1$. Therefore, using (20), we have

$$\begin{aligned} W_f(\boldsymbol{\alpha}, \boldsymbol{\beta}, 0, 0) &= W_{f_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}) + W_{f_2}(\boldsymbol{\alpha}, \boldsymbol{\beta}) + W_{f_3}(\boldsymbol{\alpha}, \boldsymbol{\beta}) - W_{f_4}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 2W_{f_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}) \\ W_f(\boldsymbol{\alpha}, \boldsymbol{\beta}, 0, 1) &= W_{f_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}) - W_{f_2}(\boldsymbol{\alpha}, \boldsymbol{\beta}) + W_{f_3}(\boldsymbol{\alpha}, \boldsymbol{\beta}) + W_{f_4}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 2W_{f_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}) \\ W_f(\boldsymbol{\alpha}, \boldsymbol{\beta}, 1, 0) &= W_{f_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}) + W_{f_2}(\boldsymbol{\alpha}, \boldsymbol{\beta}) - W_{f_3}(\boldsymbol{\alpha}, \boldsymbol{\beta}) + W_{f_4}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 2W_{f_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}) \\ W_f(\boldsymbol{\alpha}, \boldsymbol{\beta}, 1, 1) &= W_{f_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}) - W_{f_2}(\boldsymbol{\alpha}, \boldsymbol{\beta}) - W_{f_3}(\boldsymbol{\alpha}, \boldsymbol{\beta}) - W_{f_4}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = -2W_{f_1}(\boldsymbol{\alpha}, \boldsymbol{\beta}). \end{aligned}$$

Hence, $W_f(\boldsymbol{\alpha}, \boldsymbol{\beta}, \gamma_1, \gamma_2) = 2 \cdot 2^{n/2}(-1)^{g(\boldsymbol{\alpha}) \oplus h(\boldsymbol{\beta}) \oplus \gamma_1 \gamma_2}$ when $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_1$, where $g(\boldsymbol{\alpha}) \oplus h(\boldsymbol{\beta}) \oplus \gamma_1 \gamma_2$ falls into the framework of Theorem 3.1 and additionally Remark 3.1 applies. Notice that the case $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \notin E_1$ and at the same time having $W_{f_i}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 0$ is already covered above since then $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in E_2^{(j)}$ for some $j \neq i$. This is a consequence of the fact that $E_1 \cup (\cup_{i=1}^4 E_2^{(i)}) = \mathbb{F}_2^n$.

To summarize, the dual f^* is equal to $g(\boldsymbol{\alpha}) \oplus h(\boldsymbol{\beta}) \oplus \gamma_1 \gamma_2$ when f^* is restricted to the subspace $(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}) \in E_1 \times \mathbb{F}_2^2$ and to $h(\boldsymbol{\beta})$ when f^* is restricted to the complement of $E_1 \times \mathbb{F}_2^2$. Notice that g is a 2-variable quadratic bent function, thus $g(\alpha_1, \alpha_2) = \alpha_1 \alpha_2$. Therefore, using the assumption that $h \notin \mathcal{MM}^\#$, Remark 3.1 and Corollary 1 imply that $f^* \notin \mathcal{MM}^\#$ and hence $f \notin \mathcal{MM}^\#$. □

Remark 3.9 The condition on the dual bent function $h \in \mathcal{B}_{n-2}$ to be outside $\mathcal{MM}^\#$ is strictly sufficient and not necessary. There exist bent functions $\{f\}$ in eight variables, represented as $f = f_1 || f_2 || f_3 || f_4$ where f_i are 5-valued spectra functions, that are outside $\mathcal{MM}^\#$. Since in this case the dual bent function h is defined on $\mathbb{F}_2^4$ it apparently belongs to $\mathcal{MM}$.

4 5-valued spectra functions from the generalized MM class

Another method of specifying 5-valued spectra functions, also given in [14], uses the generalized Maiorana-McFarland class (GMM) of Boolean functions. For convenience and ease of notation, we use the variable set $x_0, \ldots, x_{n-1}$ instead of $x_1, \ldots, x_n$ for functions on $\mathbb{F}_2^n$.

Theorem 4.1 [14] *Let $E_0 \subset \mathbb{F}_2^s$ with $1 \le s \le \lfloor n/2 \rfloor$. Let $E_1 = \overline{E_0} \times \mathbb{F}_2^t$, where $\overline{E_0} = \mathbb{F}_2^s \backslash E_0$ and $0 \le t \le \lfloor n/2 \rfloor$. Let ϕ_0 be an injective mapping from E_0 to $\mathbb{F}_2^{n-s}$, and ϕ_1 be an injective mapping from E_1 to $\mathbb{F}_2^{n-s-t}$. Let $X = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n$ and $X_{(i,j)} = (x_i, \ldots, x_j) \in \mathbb{F}_2^{j-i+1}$. Let $f \in \mathcal{B}_n$ be defined as follows:*

$$f(X) = \begin{cases} \phi_0(X_{(0,s-1)}) \cdot X_{(s,n-1)}, & if\ X_{(0,s-1)} \in E_0 \\ \phi_1(X_{(0,s+t-1)}) \cdot X_{(s+t,n-1)}, & if\ X_{(0,s+t-1)} \in E_1. \end{cases}$$

Let

$$T_0 = \{\phi_0(\boldsymbol{\eta}) \mid \boldsymbol{\eta} \in E_0\},$$

and

$$T_1 = \{\phi_1(\boldsymbol{\theta}) \mid \boldsymbol{\theta} \in E_1\}.$$

Then, we have

(a) $W_f(\boldsymbol{\omega}) \in \{0, \pm 2^{n-s}, \pm 2^{n-s-t}\}$ *if* $t \ne 0$ *and* $T_0 \subset \mathbb{F}_2^t \times \overline{T_1}$, *where* $\overline{T_1} = \mathbb{F}_2^{n-s-t} \backslash T_1$;
(b) $W_f(\boldsymbol{\omega}) \in \{0, \pm 2^{n-s}, \pm 2^{n-s+1}\}$ *if* $t = 0$, $T_0 \cap T_1 \ne \emptyset$ *and* $T_0 \ne T_1$.

Example 4.1 Let $n = 8, s = 3$ and $t = 1$. Now, we employ Theorem 4.1 to construct 5-valued spectra functions $f^{(1)}, \ldots, f^{(4)}$ that satisfy Theorem 2.2. The resulting function $f = f^{(1)}||f^{(2)}||f^{(3)}||f^{(4)} \in \mathcal{B}_{10}$ is then bent. Let $\mathbb{F}_2^r = \{\mathbf{v}_0^{(r)}, \ldots, \mathbf{v}_{2^r-1}^{(r)}\}$ denote the lexicographically ordered r-dimensional vector space over $\mathbb{F}_2$.

Furthermore, we note that all sets defined below are also lexicographically ordered. We define $E_0 = \{\mathbf{e}_0^{(0)}, \mathbf{e}_1^{(0)}, \mathbf{e}_2^{(0)}\}$, where $\mathbf{e}_i^{(0)} = \mathbf{v}_i^{(3)} \in \mathbb{F}_2^3$ for $i = 0, 1, 2$ (hence $\mathbf{e}_0^{(0)} = (0, 0, 0), \mathbf{e}_1^{(0)} = (0, 0, 1), \mathbf{e}_2^{(0)} = (0, 1, 0)$),

and $E_1 = \overline{E_0} \times \mathbb{F}_2 = \{\mathbf{e}_0^{(1)}, \mathbf{e}_1^{(1)}, \ldots, \mathbf{e}_9^{(1)}\} \subset \mathbb{F}_2^4$, where $\overline{E_0} = \mathbb{F}_2^3 \backslash E_0$. Let $\phi_1 : E_1 \to \mathbb{F}_2^4$ be defined by

$$\phi_1(\mathbf{e}_i^{(1)}) = \mathbf{v}_i^{(4)},$$

for $i = 0, \ldots, 9$ Let $T_1 = \{\phi_1(\boldsymbol{\theta}) : \boldsymbol{\theta} \in E_1\}$ and $\overline{T_1} = \mathbb{F}_2^4 \setminus T_1$, where clearly $|\overline{T_1}| = 6$. Let $\Gamma = \mathbb{F}_2 \times \overline{T_1} = \{\boldsymbol{\gamma}_0, \ldots, \boldsymbol{\gamma}_{11}\} \subset \mathbb{F}_2 \times \mathbb{F}_2^4 = \mathbb{F}_2^5$ and let $\phi_0^{(j)} : E_0 \to \mathbb{F}_2^5$ be defined by

$$\phi_0^{(j)}(\mathbf{e}_i^{(0)}) = \boldsymbol{\gamma}_{i+3j},\ \mathbf{e}_i^{(0)} \in E_0,$$

for $j = 1, \ldots, 4$.

If $T_0^{(j)} = \{\phi_0^{(j)}(\boldsymbol{\eta}) : \boldsymbol{\eta} \in E_0\}$, then $T_0^{(j)} \subset \mathbb{F}_2 \times \overline{T_1}$ (as required in Theorem 4.1-(a)), for $j = 1, \ldots, 4$. Now let $X = (x_0, \ldots, x_7) \in \mathbb{F}_2^8$ and $X_{(i,j)} = (x_i, \ldots, x_j) \in \mathbb{F}_2^{j-i+1}$. For $j = 1, 2, 3, 4$, $f^{(j)} \in \mathcal{B}_8$ is defined as follows:

$$f^{(j)}(X) = \begin{cases} \phi_0^{(j)}(X_{(0,2)}) \cdot X_{(3,7)} + \delta_1(j), & if\ X_{(0,2)} \in E_0 \\ \phi_1(X_{(0,3)}) \cdot X_{(4,7)} + \delta_1(j), & if\ X_{(0,3)} \in E_1, \end{cases}$$

where $\delta_1(j) = 1$ for $j = 1$ and 0 otherwise. Let $S_1^{(j)} = \{\mathbf{x} \in \mathbb{F}_2^8 : |W_{f^{(j)}}(\mathbf{x})| = 2^5\}$ and $S_2^{(j)} = \{\mathbf{x} \in \mathbb{F}_2^8 : |W_{f^{(j)}}(\mathbf{x})| = 2^4\}$. Using Sage we could verify that all $S_1^{(j)}$ are pairwise disjoint and all $S_2^{(j)}$ are equal. Furthermore, by the construction, $f^*_{[2],1} \oplus \cdots \oplus f^*_{[2],4} = 1$. Hence, by Theorem 2.2, the function $f = f^{(1)}||f^{(2)}||f^{(3)}||f^{(4)} \in \mathcal{B}_{10}$ of algebraic degree 5 is bent, and its ANF is defined by:

$$
\begin{aligned}
f(x_0,\ldots,x_9) &= x_0x_1x_2x_3x_4 \oplus x_0x_1x_2x_3x_9 \oplus x_0x_1x_2x_4x_8 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_6\\
&\oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_9 \oplus x_0x_1x_4x_8 \oplus x_0x_1x_4 \oplus x_0x_1x_6 \oplus x_0x_1x_7\\
&\oplus x_0x_2x_4 \oplus x_0x_2x_5x_8 \oplus x_0x_2x_5 \oplus x_0x_2x_6 \oplus x_0x_4 \oplus x_0x_5x_8 \oplus x_1x_2x_5 \oplus x_1x_2x_6x_8 \oplus x_1x_5\\
&\oplus x_1x_6x_8 \oplus x_1x_6 \oplus x_2x_3x_4 \oplus x_2x_3x_9 \oplus x_2x_4x_8 \oplus x_2x_5x_8 \oplus x_2x_6x_8\\
&\oplus x_2x_7 \oplus x_3x_9 \oplus x_4x_8 \oplus x_5x_8 \oplus x_5 \oplus x_6x_8 \oplus x_7 \oplus x_8x_9 \oplus x_8 \oplus x_9 \oplus 1.
\end{aligned}
$$

Nevertheless, using our algorithm in Sect. 3.1 implemented in Sage, we could confirm that $f \in \mathcal{MM}^{\#}$.

As a generalization of the previous example, we give the following result.

Remark 4.1 We assume that all sets defined in Theorem 4.2 are ordered lexicographically, and with $\mathbb{F}_2^k = \{\mathbf{v}_0^{(k)}, \mathbf{v}_1^{(k)}, \ldots, \mathbf{v}_{2^k-1}^{(k)}\}$ (for suitable k) we will denote the elements of the lexicographically ordered k-dimensional vector space over $\mathbb{F}_2$.

Theorem 4.2 *Let $n = 2m \geq 8$, $s = m-1$, and $E_0 = \{\mathbf{v}_0^{(m-1)}, \ldots, \mathbf{v}_{\tau-1}^{(m-1)}\} \subset \mathbb{F}_2^{m-1}$ where $\tau < 2^s - 1$ and $4\tau \leq 2^{m+1}$. Define $E_1 = \overline{E_0} \times \mathbb{F}_2 = \{\mathbf{e}_0^{(1)}, \ldots, \mathbf{e}_\lambda^{(1)}\} \subset \mathbb{F}_2^m$, where $\lambda = 2 \cdot (2^{m-1} - \tau) - 1$ and $\overline{E_0} = \mathbb{F}_2^{m-1} \backslash E_0$. Let $\phi_1 : E_1 \to \mathbb{F}_2^m$ be an injective mapping defined by*

$$\phi_1(\mathbf{e}_i^{(1)}) = \mathbf{v}_i^{(m)},\ \mathbf{e}_i^{(1)} \in E_1,$$

for $i = 0, 1, \ldots, \lambda$, whose image set is denoted by $T_1 = \{\phi_1(\boldsymbol{\theta}) : \boldsymbol{\theta} \in E_1\}$. Now, denoting $\Gamma = \mathbb{F}_2 \times (\mathbb{F}_2^m \backslash T_1) = \{\boldsymbol{\gamma}_0, \boldsymbol{\gamma}_1, \ldots, \boldsymbol{\gamma}_{4\tau-1}\}$, let $\phi_0^{(j)} : E_0 \to \Gamma \subset \mathbb{F}_2^{m+1}$, for $j = 1, \ldots, 4$, be injective mappings defined by

$$\phi_0^{(j)}(\mathbf{e}_i^{(0)}) = \boldsymbol{\gamma}_{i+\tau(j-1)},\ \mathbf{e}_i^{(0)} \in E_0.$$

Let $X = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n$ and $X_{(i,j)} = (x_i, \ldots, x_j) \in \mathbb{F}_2^{j-i+1}$. For $j = 1, \ldots, 4$, $f^{(j)} \in \mathcal{B}_n$ is defined as follows:

$$f^{(j)}(X) = \begin{cases} \phi_0^{(j)}(X_{(0,m-2)}) \cdot X_{(m-1,n-1)} + \delta_1(j), & if\ X_{(0,m-2)} \in E_0 \\ \phi_1(X_{(0,m-1)}) \cdot X_{(m,n-1)} + \delta_1(j), & if\ X_{(0,m-1)} \in E_1, \end{cases}$$

where $\delta_1(j) = 1$ for $j = 1$ and 0 otherwise. Then, the function $f \in \mathcal{B}_{n+2}$ given as the concatenation $f = f^{(1)}||f^{(2)}||f^{(3)}||f^{(4)}$ is a bent function.

Proof Firstly, we note that $W_{f^{(j)}}(\mathbf{x}) \in \{0, \pm 2^m, \pm 2^{m+1}\}$ by Theorem 4.1, for $j = 1, \ldots, 4$ (with $s = m-1$ and $t = 1$). It remains to show that these functions satisfy the conditions of Theorem 2.2 *iii*).

Let $S^{[1]}_{f^{(j)}} = \{\mathbf{x} \in \mathbb{F}_2^n : |W_{f^{(j)}}(\mathbf{x})| = 2^{m+1}$ and $S^{[2]}_{f^{(j)}} = \{\mathbf{x} \in \mathbb{F}_2^n : |W_{f^{(j)}}(\mathbf{x})| = 2^m$, for $j = 1, \ldots, 4$. The cardinality of Γ can be computed as

$$|\Gamma| = 2 \cdot |\mathbb{F}_2^m \setminus T_1| = 2(2^m - |E_1|) = 2 \cdot (2^m - 2(2^{m-1} - \tau)) = 2^{m+1} - 2^{m+1} + 4\tau = 4\tau.$$

Because $|\Gamma| = 4\tau \leq 2^{m+1}$ and $|\phi_0^{(j)}(E_0)| = \tau$, it is easy to see that $\phi_0^{(j)}$ splits Γ into 4 disjoint subsets, that is, $\Gamma = \bigcup_{j=1}^{4} \phi_0^{(j)}(E_0)$ and $\phi_0^{(j)}(E_0) \cap \phi_0^{(j')}(E_0) = \emptyset$ for $j \neq j'$.

Consequently, the sets $S^{[1]}_{f^{(j)}}$ are pairwise disjoint for $j = 1, \ldots, 4$. As the function ϕ_1 is the same for all $f^{(j)}$, it follows that all sets $S^{[2]}_{f^{(j)}}$ are equal. The condition that the bent duals defined on $S^{[2]}_{f^{(j)}}$ satisfy $f^*_{[2],1} \oplus f^*_{[2],2} \oplus f^*_{[2],3} \oplus f^*_{[2],4} = 1$, follows from the fact that $\delta_1(j) = 1$ only for $j = 1$. This follows from the fact that $|W_f(\mathbf{x})| = 2^m$ is determined by the value of $\phi_1(X_{(0,m-1)}) \cdot X_{(m,n-1)}$ (cf. proof of [14, Theorem V.6]) and consequently the values of $f^*_{[2],j}$ are the same except for $j = 1$, where we additionally add the constant 1.

Thus, the conditions given in item $iii)$ of Theorem 2.2 are satisfied and $f = f^{(1)}||f^{(2)}||f^{(3)}||f^{(4)} \in \mathcal{B}_{n+2}$ is a bent function. □

Remark 4.2 The above statement also holds if E_0 is a collection of arbitrary τ elements in $\mathbb{F}_2^{m-1}$. However, (partial) computer simulations indicate that this approach only generates bent functions inside the $\mathcal{MM}^{\#}$ class, regardless of the choice of E_0.

Open Problem 1 *Prove or disprove that the bent functions constructed using Theorem 4.2 always belong to $\mathcal{MM}^{\#}$ regardless of the choice of E_0.*

5 Conclusions

This article significantly provides several infinite families of bent functions provably outside the completed Maiorana-McFarland class. In the context of enumeration of bent functions, it would be of interest to investigate whether the obtained families, that belong to different cases of 4-decomposition, are fully/partially non-intersecting. Another important question that remains unanswered, due to the lack of indicators for the partial spread class, is whether these families intersect with the $\mathcal{PS}$ class.

Acknowledgements Enes Pasalic is partly supported by the Slovenian Research Agency (research program P1-0404 and research Projects J1-9108, J1-1694, N1-1059), and the European Commission for funding the InnoRenew CoE project (Grant Agreement No. 739574) under the Horizon2020 Widespread-Teaming program and the Republic of Slovenia (Investment funding of the Republic of Slovenia and the European Union of the European Regional Development Fund). Amar Bapić is supported in part by the Slovenian Research Agency (research program P1-0404 and Young Researchers Grant). Fengrong Zhang is supported in part by the Natural Science Foundation of China (No. 61972400), in part by the Fundamental Research Funds for the Central Universities (XJS221503). Y. Wei is supported in part by the Natural Science Foundation of China (No. 61872103), in part by the Guangxi Natural Science Foundation (2019GXNSFGA245004).

Appendix

Sage implementation of Lemma 2.1

```
def is_in_MM(f,n):
    s=[];
    for a in [1..2^n-1]:
        for b in [a+1..2^n-1]:
            if set(ttab(f.derivative(a).
            derivative(b)))=={0}:
                s.append([a,b]);
    G=Graph();
    G.add_edges(s);
    cl=list(sage.graphs.cliquer.all_cliques
     (G,2^(n/2)-1,2^(n/2)-1));
    V=VectorSpace(GF(2),n);
    V1=sorted(V);
    b1=[V.subspace([V1[0]]+[V1[i] for i in s])
      for s in cl];
    for K in b1:
        if len(K)==2^(n/2):
            return True;
    return False;
```

ANF representations of certain bent functions

$$
\begin{aligned}
&x_0x_1x_2x_4 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3x_7\\
&\oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_7 \oplus x_0x_1x_6x_7\\
&\oplus x_0x_2x_3x_6 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_5x_6 \oplus x_0x_2x_5x_7 \oplus x_0x_2x_5\\
&\oplus x_0x_2x_6x_7 \oplus x_0x_3x_4x_6 \oplus x_0x_3x_4x_7 \oplus x_0x_3x_4 \oplus x_0x_3x_5x_7 \oplus x_0x_3x_6x_7\\
&\oplus x_0x_3x_6 \oplus x_0x_3x_7 \oplus x_0x_4x_5x_6 \oplus x_0x_4x_5 \oplus x_0x_4x_6 \oplus x_0x_5x_6x_7\\
&\oplus x_0x_5x_6 \oplus x_0x_5x_7 \oplus x_0x_7 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_6\\
&\oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_4 \oplus x_1x_2x_5x_6 \oplus x_1x_2x_5\\
&\oplus x_1x_2x_6x_7 \oplus x_1x_2x_7 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_5x_6 \oplus x_1x_3x_5\\
&\oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_4x_6x_7 \oplus x_1x_4x_7 \oplus x_1x_4\\
&\oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_1x_6 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4x_7\\
&\oplus x_2x_3x_4 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_5x_7 \oplus x_2x_3x_5 \oplus x_2x_4x_5x_6\\
&\oplus x_2x_4x_5x_7 \oplus x_2x_4x_5 \oplus x_2x_4x_7 \oplus x_2x_4 \oplus x_2x_6x_7\\
&\oplus x_2x_7 \oplus x_3x_4x_5x_7 \oplus x_3x_4x_6x_7 \oplus x_3x_5x_6 \oplus x_3x_5 \oplus x_3x_6x_7 \oplus x_3x_6 \qquad (21)\\
&x_0x_1x_3x_4x_5 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4\\
&\oplus x_0x_1x_5 \oplus x_0x_1x_6x_7x_9 \oplus x_0x_1x_6x_7 \oplus x_0x_1x_6x_8 \oplus x_0x_1x_6x_9\\
&\oplus x_0x_1x_7x_8x_9 \oplus x_0x_1x_7x_8 \oplus x_0x_1x_8x_9 \oplus x_0x_1x_8 \oplus x_0x_1x_9 \oplus x_0x_3x_4x_5x_10\\
&\oplus x_0x_3x_4x_10 \oplus x_0x_3x_5x_10 \oplus x_0x_3x_10 \oplus x_0x_4x_5x_10 \oplus x_0x_4x_10
\end{aligned}
$$

$$\oplus x_0x_5x_1 0 \oplus x_0x_6x_7x_9x_1 0 \oplus x_0x_6x_7x_1 0 \oplus x_0x_6x_8x_1 0 \oplus x_0x_6x_9x_1 0$$
$$\oplus x_0x_7x_8x_9x_1 0 \oplus x_0x_7x_8x_1 0 \oplus x_0x_8x_9x_1 0 \oplus x_0x_8x_1 0 \oplus x_0x_9x_1 0$$
$$\oplus x_0x_1 0 \oplus x_1x_3x_4x_5x_1 1 \oplus x_1x_3x_4x_1 1 \oplus x_1x_3x_5x_1 1 \oplus x_1x_3x_1 1$$
$$\oplus x_1x_4x_5x_1 1 \oplus x_1x_4x_1 1 \oplus x_1x_5x_1 1 \oplus x_1x_6x_7x_9x_1 1 \oplus x_1x_6x_7x_1 1$$
$$\oplus x_1x_6x_8x_1 1 \oplus x_1x_6x_9x_1 1 \oplus x_1x_7x_8x_9x_1 1 \oplus x_1x_7x_8x_1 1 \oplus x_1x_8x_9x_1 1$$
$$\oplus x_1x_8x_1 1 \oplus x_1x_9x_1 1 \oplus x_1x_1 1 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4$$
$$\oplus x_2x_3x_5 \oplus x_2x_3 \oplus x_2x_4x_5 \oplus x_2x_4 \oplus x_2x_5$$
$$\oplus x_2x_6x_7x_9 \oplus x_2x_6x_7 \oplus x_2x_6x_8 \oplus x_2x_6x_9 \oplus x_2x_7x_8x_9$$
$$\oplus x_2x_7x_8 \oplus x_2x_8x_9 \oplus x_2x_8 \oplus x_2x_9 \oplus x_2$$
$$\oplus x_3x_4x_5x_1 0x_1 1 \oplus x_3x_4x_5 \oplus x_3x_4x_1 0x_1 1 \oplus x_3x_4 \oplus x_3x_5x_1 0x_1 1$$
$$\oplus x_3x_5 \oplus x_3x_6x_7x_9 \oplus x_3x_6x_8 \oplus x_3x_6x_9 \oplus x_3x_7x_9$$
$$\oplus x_3x_7 \oplus x_3x_8x_9 \oplus x_3x_1 0x_1 1 \oplus x_3 \oplus x_4x_5x_1 0x_1 1 \oplus x_4x_5$$
$$\oplus x_4x_6x_7x_8 \oplus x_4x_6x_8x_9 \oplus x_4x_6x_9 \oplus x_4x_6 \oplus x_4x_7x_8$$
$$\oplus x_4x_7x_9 \oplus x_4x_7 \oplus x_4x_8x_9 \oplus x_4x_8 \oplus x_4x_1 0x_1 1$$
$$\oplus x_4 \oplus x_5x_6x_7x_8 \oplus x_5x_6x_7 \oplus x_5x_6x_8 \oplus x_5x_6x_9$$
$$\oplus x_5x_7 \oplus x_5x_8 \oplus x_5x_1 0x_1 1 \oplus x_5 \oplus x_6x_7x_9x_1 0x_1 1$$
$$\oplus x_6x_7x_1 0x_1 1 \oplus x_6x_8x_1 0x_1 1 \oplus x_6x_9x_1 0x_1 1 \oplus x_7x_8x_9x_1 0x_1 1$$
$$\oplus x_7x_8x_1 0x_1 1 \oplus x_8x_9x_1 0x_1 1 \oplus x_8x_1 0x_1 1 \oplus x_9x_1 0x_1 1 \oplus 1 \tag{22}$$
$$x_0x_1x_2x_5 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_3x_6 \oplus x_0x_1x_3x_7 \oplus x_0x_1x_3x_8x_9 \oplus x_0x_1x_3x_8x_{10}$$
$$\oplus x_0x_1x_3x_9x_{11} \oplus x_0x_1x_3x_{10}x_{11} \oplus x_0x_1x_4x_6 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4x_8x_9 \oplus x_0x_1x_4x_8x_{10}$$
$$\oplus x_0x_1x_4x_9x_{11} \oplus x_0x_1x_4x_{10}x_{11} \oplus x_0x_1x_4 \oplus x_0x_1x_5x_6 \oplus x_0x_1x_6x_7$$
$$\oplus x_0x_1x_6x_8x_9 \oplus x_0x_1x_6x_8x_{10} \oplus x_0x_1x_6x_9x_{11} \oplus x_0x_1x_6x_{10}x_{11} \oplus x_0x_1x_6$$
$$\oplus x_0x_2x_3x_5 \oplus x_0x_2x_4x_7 \oplus x_0x_2x_4x_8x_9 \oplus x_0x_2x_4x_8x_{10} \oplus x_0x_2x_4x_9x_{11}$$
$$\oplus x_0x_2x_4x_{10}x_{11} \oplus x_0x_2x_5x_6 \oplus x_0x_2x_5 \oplus x_0x_2x_6 \oplus x_0x_2x_7$$
$$\oplus x_0x_2x_8x_9 \oplus x_0x_2x_8x_{10} \oplus x_0x_2x_9x_{11} \oplus x_0x_2x_{10}x_{11} \oplus x_0x_3x_4x_5$$
$$\oplus x_0x_3x_4x_7 \oplus x_0x_3x_4x_8x_9 \oplus x_0x_3x_4x_8x_{10} \oplus x_0x_3x_4x_9x_{11} \oplus x_0x_3x_4x_{10}x_{11}$$
$$\oplus x_0x_3x_4 \oplus x_0x_3x_5x_7 \oplus x_0x_3x_5x_8x_9 \oplus x_0x_3x_5x_8x_{10} \oplus x_0x_3x_5x_9x_{11}$$
$$\oplus x_0x_3x_5x_{10}x_{11} \oplus x_0x_3x_6x_7 \oplus x_0x_3x_6x_8x_9 \oplus x_0x_3x_6x_8x_{10} \oplus x_0x_3x_6x_9x_{11}$$
$$\oplus x_0x_3x_6x_{10}x_{11} \oplus x_0x_4x_5x_7 \oplus x_0x_4x_5x_8x_9 \oplus x_0x_4x_5x_8x_{10} \oplus x_0x_4x_5x_9x_{11} \oplus x_0x_4x_5x_{10}x_{11}$$
$$\oplus x_0x_4x_6x_7 \oplus x_0x_4x_6x_8x_9 \oplus x_0x_4x_6x_8x_{10} \oplus x_0x_4x_6x_9x_{11} \oplus x_0x_4x_6x_{10}x_{11}$$
$$\oplus x_0x_4x_6 \oplus x_0x_4x_7 \oplus x_0x_4x_8x_9 \oplus x_0x_4x_8x_{10} \oplus x_0x_4x_9x_{11}$$
$$\oplus x_0x_4x_{10}x_{11} \oplus x_0x_5x_7 \oplus x_0x_5x_8x_9 \oplus x_0x_5x_8x_{10} \oplus x_0x_5x_9x_{11}$$
$$\oplus x_0x_5x_{10}x_{11} \oplus x_0x_5 \oplus x_0x_6x_7 \oplus x_0x_6x_8x_9 \oplus x_0x_6x_8x_{10}$$
$$\oplus x_0x_6x_9x_{11} \oplus x_0x_6x_{10}x_{11} \oplus x_0x_7 \oplus x_0x_8x_9 \oplus x_0x_8x_{10}$$
$$\oplus x_0x_9x_{11} \oplus x_0x_{10}x_{11} \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_7 \oplus$$
$$x_1x_2x_3x_8x_9 \oplus x_1x_2x_3x_8x_{10} \oplus x_1x_2x_3x_9x_{11} \oplus x_1x_2x_3x_{10}x_{11} \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_6$$
$$\oplus x_1x_2x_4 \oplus x_1x_2x_5x_6 \oplus x_1x_2x_5x_7 \oplus x_1x_2x_5x_8x_9 \oplus x_1x_2x_5x_8x_{10}$$
$$\oplus x_1x_2x_5x_9x_{11} \oplus x_1x_2x_5x_{10}x_{11} \oplus x_1x_2x_5 \oplus x_1x_2x_7 \oplus x_1x_2x_8x_9$$
$$\oplus x_1x_2x_8x_{10} \oplus x_1x_2x_9x_{11} \oplus x_1x_2x_{10}x_{11} \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4x_6$$
$$\oplus x_1x_3x_4x_7 \oplus x_1x_3x_4x_8x_9 \oplus x_1x_3x_4x_8x_{10} \oplus x_1x_3x_4x_9x_{11} \oplus x_1x_3x_4x_{10}x_{11}$$
$$\oplus x_1x_3x_5 \oplus x_1x_3x_6x_7 \oplus x_1x_3x_6x_8x_9 \oplus x_1x_3x_6x_8x_{10} \oplus x_1x_3x_6x_9x_{11}$$

$$
\begin{aligned}
&\oplus x_1x_3x_6x_{10}x_{11} \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_3x_8x_9 \oplus x_1x_3x_8x_{10}\\
&\oplus x_1x_3x_9x_{11} \oplus x_1x_3x_{10}x_{11} \oplus x_1x_4x_5x_6 \oplus x_1x_4x_5x_7 \oplus x_1x_4x_5x_8x_9\\
&\oplus x_1x_4x_5x_8x_{10} \oplus x_1x_4x_5x_9x_{11} \oplus x_1x_4x_5x_{10}x_{11} \oplus x_1x_5x_6 \oplus x_1x_6 \oplus x_1x_7 \oplus\\
&x_1x_8x_9 \oplus x_1x_8x_{10} \oplus x_1x_9x_{11} \oplus x_1x_{10}x_{11} \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4x_6 \oplus x_2x_3x_5x_6\\
&\oplus x_2x_3x_6x_7 \oplus x_2x_3x_6x_8x_9 \oplus x_2x_3x_6x_8x_{10} \oplus x_2x_3x_6x_9x_{11} \oplus x_2x_3x_6x_{10}x_{11}\\
&\oplus x_2x_3x_6 \oplus x_2x_3x_7 \oplus x_2x_3x_8x_9 \oplus x_2x_3x_8x_{10} \oplus x_2x_3x_9x_{11}\\
&\oplus x_2x_3x_{10}x_{11} \oplus x_2x_4x_5x_6 \oplus x_2x_4x_6x_7 \oplus x_2x_4x_6x_8x_9 \oplus x_2x_4x_6x_8x_{10}\\
&\oplus x_2x_4x_6x_9x_{11} \oplus x_2x_4x_6x_{10}x_{11} \oplus x_2x_4x_6 \oplus x_2x_4 \oplus x_2x_5x_6x_7\\
&\oplus x_2x_5x_6x_8x_9 \oplus x_2x_5x_6x_8x_{10} \oplus x_2x_5x_6x_9x_{11} \oplus x_2x_5x_6x_{10}x_{11} \oplus x_2x_5x_7\\
&\oplus x_2x_5x_8x_9 \oplus x_2x_5x_8x_{10} \oplus x_2x_5x_9x_{11} \oplus x_2x_5x_{10}x_{11} \oplus x_2x_7 \oplus x_2x_8x_9\\
&\oplus x_2x_8x_{10} \oplus x_2x_9x_{11} \oplus x_2x_{10}x_{11} \oplus x_3x_4x_5x_7 \oplus x_3x_4x_5x_8x_9\\
&\oplus x_3x_4x_5x_8x_{10} \oplus x_3x_4x_5x_9x_{11} \oplus x_3x_4x_5x_{10}x_{11} \oplus x_3x_4x_6 \oplus x_3x_5x_6x_7\\
&\oplus x_3x_5x_6x_8x_9 \oplus x_3x_5x_6x_8x_{10} \oplus x_3x_5x_6x_9x_{11} \oplus x_3x_5x_6x_{10}x_{11} \oplus x_3x_5x_6\\
&\oplus x_3x_5 \oplus x_3x_6x_7 \oplus x_3x_6x_8x_9 \oplus x_3x_6x_8x_{10} \oplus x_3x_6x_9\\
&x_{11} \oplus x_3x_6x_{10}x_{11} \oplus x_3x_6 \oplus x_8x_9 \oplus x_{10}x_{11}
\end{aligned}
\tag{23}
$$

$$
\begin{aligned}
\mathfrak{f}(x_0,\ldots,x_{11}) &= x_0x_1x_2x_3x_8 \oplus x_0x_1x_2x_3x_9 \oplus x_0x_1x_2x_4x_8\\
&\oplus x_0x_1x_2x_4x_9 \oplus x_0x_1x_2x_5x_8 \oplus x_0x_1x_2x_5x_9\\
&\oplus x_0x_1x_2x_5 \oplus x_0x_1x_2x_6x_8 \oplus x_0x_1x_2x_6x_9 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_2x_7x_8 \oplus x_0x_1x_2x_7x_9\\
&\oplus x_0x_1x_2x_7 \oplus x_0x_1x_2x_8 \oplus x_0x_1x_2x_9 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_6x_8\\
&\oplus x_0x_1x_3x_6x_9 \oplus x_0x_1x_3x_6 \oplus x_0x_1x_3x_8 \oplus x_0x_1x_3x_9 \oplus x_0x_1x_4x_5\\
&\oplus x_0x_1x_4x_6x_8 \oplus x_0x_1x_4x_6x_9 \oplus x_0x_1x_4x_6 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4x_8\\
&\oplus x_0x_1x_4x_9 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_6x_8 \oplus x_0x_1x_5x_6x_9 \oplus x_0x_1x_5x_6\\
&\oplus x_0x_1x_5x_8 \oplus x_0x_1x_5x_9 \oplus x_0x_1x_6x_7x_8 \oplus x_0x_1x_6x_7x_9 \oplus x_0x_1x_6x_7\\
&\oplus x_0x_1x_6x_8 \oplus x_0x_1x_6x_9 \oplus x_0x_1x_6 \oplus x_0x_1x_7x_8 \oplus x_0x_1x_7x_9 \oplus x_0x_1x_7\\
&\oplus x_0x_1x_8 \oplus x_0x_1x_9 \oplus x_0x_2x_3x_4x_8 \oplus x_0x_2x_3x_4x_9 \oplus x_0x_2x_3x_5\\
&\oplus x_0x_2x_3x_6x_8 \oplus x_0x_2x_3x_6x_9 \oplus x_0x_2x_3x_6 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_3x_8\\
&\oplus x_0x_2x_3x_9 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5x_8 \oplus x_0x_2x_4x_5x_9 \oplus x_0x_2x_4x_7x_8\\
&\oplus x_0x_2x_4x_7x_9 \oplus x_0x_2x_4x_8 \oplus x_0x_2x_4x_9 \oplus x_0x_2x_4 \oplus x_0x_2x_5x_6x_8\\
&\oplus x_0x_2x_5x_6x_9 \oplus x_0x_2x_5x_6 \oplus x_0x_2x_5x_7 \oplus x_0x_2x_5x_8 \oplus x_0x_2x_5x_9\\
&\oplus x_0x_2x_6x_7x_8 \oplus x_0x_2x_6x_7x_9 \oplus x_0x_2x_6x_7 \oplus x_0x_2x_6x_8 \oplus x_0x_2x_6x_9\\
&\oplus x_0x_2x_6 \oplus x_0x_2x_7x_8 \oplus x_0x_2x_7x_9 \oplus x_0x_2x_8 \oplus x_0x_2x_9\\
&\oplus x_0x_2 \oplus x_0x_3x_4x_6x_8 \oplus x_0x_3x_4x_6x_9 \oplus x_0x_3x_4x_6 \oplus x_0x_3x_4x_7\\
&\oplus x_0x_3x_4x_8 \oplus x_0x_3x_4x_9 \oplus x_0x_3x_6x_8 \oplus x_0x_3x_6x_9 \oplus x_0x_3x_7\\
&\oplus x_0x_3x_8 \oplus x_0x_3x_9 \oplus x_0x_3 \oplus x_0x_4x_5x_6x_8 \oplus x_0x_4x_5x_6x_9\\
&\oplus x_0x_4x_5x_6 \oplus x_0x_4x_5x_8 \oplus x_0x_4x_5x_9 \oplus x_0x_4x_6x_7x_8 \oplus x_0x_4x_6x_7x_9\\
&\oplus x_0x_4x_6x_7 \oplus x_0x_4x_6x_8 \oplus x_0x_4x_6x_9 \oplus x_0x_4x_7x_8 \oplus x_0x_4x_7x_9\\
&\oplus x_0x_4x_7 \oplus x_0x_4x_8 \oplus x_0x_4x_9 \oplus x_0x_4 \oplus x_0x_5x_6x_8\\
&\oplus x_0x_5x_6x_9 \oplus x_0x_5x_8 \oplus x_0x_5x_9 \oplus x_0x_5 \oplus x_0x_6x_7x_8\\
&\oplus x_0x_6x_7x_9 \oplus x_0x_6x_8 \oplus x_0x_6x_9 \oplus x_0x_6 \oplus x_0x_7x_8\\
&\oplus x_0x_7x_9 \oplus x_0x_7 \oplus x_0x_8 \oplus x_0x_9 \oplus x_1x_2x_3x_4\\
&\oplus x_1x_2x_3x_5x_8 \oplus x_1x_2x_3x_5x_9 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_6x_8 \oplus x_1x_2x_3x_6x_9
\end{aligned}
$$

$$
\begin{aligned}
&\oplus x_1x_2x_3x_6 \oplus x_1x_2x_3x_8 \oplus x_1x_2x_3x_9 \oplus x_1x_2x_4x_5x_8 \oplus x_1x_2x_4x_5x_9\\
&\oplus x_1x_2x_4x_6x_8 \oplus x_1x_2x_4x_6x_9 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_4x_7 \oplus x_1x_2x_4x_8\\
&\oplus x_1x_2x_4x_9 \oplus x_1x_2x_5x_6 \oplus x_1x_2x_5x_7x_8 \oplus x_1x_2x_5x_7x_9 \oplus x_1x_2x_5x_7\\
&\oplus x_1x_2x_5x_8 \oplus x_1x_2x_5x_9 \oplus x_1x_2x_5 \oplus x_1x_2x_6x_7x_8 \oplus x_1x_2x_6x_7x_9\\
&\oplus x_1x_2x_6x_8 \oplus x_1x_2x_6x_9 \oplus x_1x_2x_6 \oplus x_1x_2x_7x_8 \oplus x_1x_2x_7x_9\\
&\oplus x_1x_2x_7 \oplus x_1x_2x_8 \oplus x_1x_2x_9 \oplus x_1x_2 \oplus x_1x_3x_4x_5\\
&\oplus x_1x_3x_4x_6 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_5x_6x_8 \oplus x_1x_3x_5x_6x_9 \oplus x_1x_3x_5x_6\\
&\oplus x_1x_3x_5x_8 \oplus x_1x_3x_5x_9 \oplus x_1x_3x_6x_8 \oplus x_1x_3x_6x_9 \oplus x_1x_3x_7 \oplus x_1x_3x_8\\
&\oplus x_1x_3x_9 \oplus x_1x_4x_5x_6x_8 \oplus x_1x_4x_5x_6x_9 \oplus x_1x_4x_5x_6 \oplus x_1x_4x_5x_8 \oplus x_1x_4x_5x_9\\
&\oplus x_1x_4x_6x_8 \oplus x_1x_4x_6x_9 \oplus x_1x_4x_7 \oplus x_1x_4x_8 \oplus x_1x_4x_9\\
&\oplus x_1x_5x_6x_7x_8 \oplus x_1x_5x_6x_7x_9 \oplus x_1x_5x_6x_7 \oplus x_1x_5x_6x_8 \oplus x_1x_5x_6x_9\\
&\oplus x_1x_5x_7x_8 \oplus x_1x_5x_7x_9 \oplus x_1x_5x_8 \oplus x_1x_5x_9 \oplus x_1x_5\\
&\oplus x_1x_6x_7x_8 \oplus x_1x_6x_7x_9 \oplus x_1x_6x_7 \oplus x_1x_6x_8 \oplus x_1x_6x_9\\
&\oplus x_1x_6 \oplus x_1x_7x_8 \oplus x_1x_7x_9 \oplus x_1x_8 \oplus x_1x_9\\
&\oplus x_2x_3x_4x_5x_8 \oplus x_2x_3x_4x_5x_9 \oplus x_2x_3x_4x_6x_8 \oplus x_2x_3x_4x_6x_9 \oplus x_2x_3x_4x_6 \oplus x_2x_3x_4x_8\\
&\oplus x_2x_3x_4x_9 \oplus x_2x_3x_5x_6x_8 \oplus x_2x_3x_5x_6x_9 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_5x_7\\
&\oplus x_2x_3x_5x_8 \oplus x_2x_3x_5x_9 \oplus x_2x_3x_5 \oplus x_2x_3x_6x_7 \oplus x_2x_3x_6x_8\\
&\oplus x_2x_3x_6x_9 \oplus x_2x_3x_6 \oplus x_2x_3x_8 \oplus x_2x_3x_9 \oplus x_2x_3 \oplus x_2x_4x_5x_6x_8\\
&\oplus x_2x_4x_5x_6x_9 \oplus x_2x_4x_5x_7x_8 \oplus x_2x_4x_5x_7x_9 \oplus x_2x_4x_5x_7 \oplus x_2x_4x_5x_8\\
&\oplus x_2x_4x_5x_9 \oplus x_2x_4x_5 \oplus x_2x_4x_6x_7x_8 \oplus x_2x_4x_6x_7x_9 \oplus x_2x_4x_6x_7\\
&\oplus x_2x_4x_6x_8 \oplus x_2x_4x_6x_9 \oplus x_2x_4x_7x_8 \oplus x_2x_4x_7x_9 \oplus x_2x_4x_8\\
&\oplus x_2x_4x_9 \oplus x_2x_5x_6x_7x_8 \oplus x_2x_5x_6x_7x_9 \oplus x_2x_5x_6x_7 \oplus x_2x_5x_6x_8 \oplus x_2x_5x_6x_9\\
&\oplus x_2x_5x_6 \oplus x_2x_5x_7x_8 \oplus x_2x_5x_7x_9 \oplus x_2x_5x_7 \oplus x_2x_5x_8\\
&\oplus x_2x_5x_9 \oplus x_2x_5 \oplus x_2x_6x_7x_8 \oplus x_2x_6x_7x_9 \oplus x_2x_6x_8\\
&\oplus x_2x_6x_9 \oplus x_2x_7x_8 \oplus x_2x_7x_9 \oplus x_2x_8 \oplus x_2x_9\\
&\oplus x_2 \oplus x_3x_4x_5x_6x_8 \oplus x_3x_4x_5x_6x_9 \oplus x_3x_4x_5x_8 \oplus x_3x_4x_5x_9\\
&\oplus x_3x_4x_5 \oplus x_3x_4x_6x_7 \oplus x_3x_4x_6x_8 \oplus x_3x_4x_6x_9 \oplus x_3x_4x_6\\
&\oplus x_3x_4x_8 \oplus x_3x_4x_9 \oplus x_3x_5x_6x_8 \oplus x_3x_5x_6x_9 \oplus x_3x_5x_7\\
&\oplus x_3x_5x_8 \oplus x_3x_5x_9 \oplus x_3x_6x_8 \oplus x_3x_6x_9 \oplus x_3x_7\\
&\oplus x_3x_8 \oplus x_3x_9 \oplus x_4x_5x_6x_7x_8 \oplus x_4x_5x_6x_7x_9 \oplus x_4x_5x_6x_8\\
&\oplus x_4x_5x_6x_9 \oplus x_4x_5x_7x_8 \oplus x_4x_5x_7x_9 \oplus x_4x_5x_8 \oplus x_4x_5x_9\\
&\oplus x_4x_5 \oplus x_4x_6x_7x_8 \oplus x_4x_6x_7x_9 \oplus x_4x_6x_7 \oplus x_4x_6x_8\\
&\oplus x_4x_6x_9 \oplus x_4x_6 \oplus x_4x_7x_8 \oplus x_4x_7x_9 \oplus x_4x_8\\
&\oplus x_4x_9 \oplus x_4 \oplus x_5x_6x_7x_8 \oplus x_5x_6x_7x_9 \oplus x_5x_6x_7 \oplus x_5x_6x_8\\
&\oplus x_5x_6x_9 \oplus x_5x_7x_8 \oplus x_5x_7x_9 \oplus x_5x_7 \oplus x_5x_8\\
&\oplus x_5x_9 \oplus x_5 \oplus x_6x_7x_8 \oplus x_6x_7x_9 \oplus x_6x_7\\
&\oplus x_6x_8 \oplus x_6x_9 \oplus x_6 \oplus x_7x_8 \oplus x_7x_9 \oplus x_8x_{11} \oplus x_8 \oplus x_9x_{10} \oplus x_9 \oplus 1
\end{aligned}
\tag{24}
$$

References

1. Bapić A., Pasalic E.: Constructions of (vectorial) bent functions outside the completed Maiorana–McFarland class. Discret. Appl. Math. **314**, 197–212 (2022).
2. Bapić A., Pasalic E., Zhang F., Hodžić S.: Constructing new superclasses of bent functions from known ones. Cryptogr. Commun. **4**, 1–28 (2022).
3. Canteaut A., Charpin P.: Decomposing bent functions. IEEE Trans. Inf. Theory **49**(8), 2004–2019 (2003).
4. Carlet C.: Two new classes of bent functions. Lect. Not. Comput. Sci. **765**, 77–101 (1993).
5. Carlet C.: Partially bent functions. Des. Codes Cryptogr. **3**(2), 135–145 (1993).
6. Carlet C.: On the secondary constructions of resilient and bent functions. Proc. Coding Cryptogr. Comb. **23**, 3–28 (2004).
7. Carlet C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2021).
8. Carlet C., Mesnager S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5–50 (2016).
9. Carlet C., Zhang F., Hu Y.: Secondary constructions of bent functions and their enforcement. Adv. Math. Commun. **6**, 305–314 (2012).
10. Cepak N.: On bent functions lying outside the completed Maiorana–McFarland class and permutations via translators'. PhD thesis, University of Primorska, Faculty of mathematics, natural sciences and information technologies (2018). https://www.famnit.upr.si/sl/studij/zakljucna_dela/view/711.
11. Cusick T.W., Stănică P.: Cryptographic Boolean Functions and Applications. Elsevier-Academic Press, London (2009).
12. Dillon J.F.: Elementary Hadamard difference sets. Ph.D. dissertation. University of Maryland, College Park (1974).
13. Dillon J.F.: Elementary Hadamard difference sets. In: Proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, pp. 237–249 (1975).
14. Hodžić S., Pasalic E., Zhang W.G.: Generic constructions of five-valued spectra Boolean functions. IEEE Trans. Inf. Theory **65**(11), 7554–7565 (2019).
15. Hodžić S., Pasalic E., Wei Y., Zhang F.: Designing plateaued Boolean functions in spectral domain and their classification. IEEE Trans. Inf. Theory **65**(9), 5865–5879 (2019).
16. Hodžić S., Pasalic E., Wei Y.: A general framework for secondary constructions of bent and plateaued functions. Des. Codes Cryptogr. **88**(10), 2007–2035 (2020).
17. Hodžić S., Horak P., Pasalic E.: Characterization of basic 5-value spectrum functions through Walsh–Hadamard transform. IEEE Trans. Inf. Theory **67**(2), 1038–1053 (2021).
18. Kudin S., Pasalic E., Cepak N., Zhang F.: Permutations without linear structures inducing bent functions outside the completed Maiorana–McFarland class. Cryptogr. Commun. (2021). https://doi.org/10.1007/s12095-021-00523-w.
19. McFarland R.L.: A family of noncyclic difference sets. J. Comb. Theory A **15**, 1–10 (1973).
20. Mesnager S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inf. Theory **60**(7), 4397–4407 (2014).
21. Mesnager S.: Bent Functions: Fundamentals and Results. Springer, New York (2016).
22. Polujan A.A., Pott A.: Cubic bent functions outside the completed Maiorana–McFarland class. Des. Codes Cryptogr. **88**(9), 1701–1722 (2020).
23. Rothaus O.S.: On 'bent' functions. J. Comb. Theory Ser. A **20**(3), 300–305 (1976).
24. Wang L., Wu B., Liu Z., Lin D.: Three new infinite families of bent functions. Sci. China Inf. Sci. **61**, 032104 (2018). https://doi.org/10.1007/s11432-016-0624-x.
25. Wei Y., Pasalic E., Zhang F., Wu W., Wang C.-X.: New constructions of resilient functions with strictly almost optimal nonlinearity via non-overlap spectra functions. Inform. Sci. **415–416**, 377–396 (2017).
26. Zhang F., Pasalic E., Cepak N., Wei Y.: Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana–McFarland class. In: Codes, Cryptology and Information Security, C2SI, LNCS 10194, Springer, New York, pp. 298–313 (2017).
27. Zhang F., Pasalic E., Wei Y., Cepak N.: Constructing bent functions outside the Maiorana–McFarland class using a general form of Rothaus. IEEE Trans. Inf. Theory **63**(8), 5336–5349 (2017).
28. Zhang F., Cepak N., Pasalic E., Wei Y.: Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^{\#}$. Discret. Appl. Math. **285**(1), 458–472 (2020).
29. Zheng Y., Zhang X.M.: On plateaued functions. IEEE Trans. Inf. Theory **47**(3), 1215–1223 (2001).
30. Zheng L., Peng J., Kan H., Li Y.: Several new infinite families of bent functions via second-order derivatives. Cryptogr. Commun. **12**, 1143–1160 (2020).