Explicit infinite families of bent functions outside $\mathcal{MM}^{\#}$

E. Pasalic, A. Bapić, F. Zhang, Y. Wei

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 [3] in terms of the second-order derivatives and later reformulated in [16] 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, 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 either 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 designing infinite families of bent functions outside $\mathcal{MM}^{\#}$, using the spectral domain design considered in [15, 16], are proposed.

Keywords: 4-decomposition, Class inclusion, 5-valued spectra functions, Bent functions, Dual functions, Plateaued functions, Walsh support.

1 Introduction

The concept of bent functions has been introduced by Rothaus [21], as a subclass of Boolean functions possessing several nice combinatorial properties which allowed for their great range of applications in design and coding theory, sequences, and cryptography. A nice survey on bent functions related to their design and properties can be found in [9], whereas their exhaustive treatment can be found in [20]. For a detailed survey on (cryptographic) Boolean functions, the reader is referred to the textbooks of Carlet [5] 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 [14] 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, 7, 8, 15, 19, 23, 28]. 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, 19, 24–26] 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. 59].

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 [16]. 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 [16] (see Theorem 2.1), 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 a 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 $\mathcal{MM}^{\#}$. 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 either f_1 or f_2 is 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 3.3, where a single dual bent function on $\mathbb{F}_2^8$ which is not in $\mathcal{MM}^{\#}$ gives rise to $\approx 2^{70}$ 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 $\mathcal{MM}^{\#}$ 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 Section 2, we give some basic definitions related to Boolean functions and discuss the concept of dual for some important classes of Boolean functions. The design of bent functions provably outside $\mathcal{MM}^{\#}$ is addressed in Section 3. More precisely, for each of the three possible cases (bent, semi-bent, or 5-valued spectra functions), we provide construction methods for specifying suitable quadruples of these functions so that the resulting bent functions are provably outside $\mathcal{MM}^{\#}$. In Section 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 Section 5.

2 Preliminaries

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

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

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

where $x_i, \lambda_{\mathbf{u}} \in \mathbb{F}_2$ and $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$.

For an arbitrary function $f \in \mathcal{B}_n$, the set of its values on $\mathbb{F}_2^n$ (*the truth table*) is defined as

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

The corresponding (± 1)-*sequence of* f is defined 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 $f, g \in \mathcal{B}_n$, we define 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 $\chi_f \cdot \chi_g = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus g(\mathbf{x})}$.

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

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

and

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

The *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

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

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

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

A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is said to have 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

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

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

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

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

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

The following lemma, due to Dillon [12], is of crucial importance for the discussion on class inclusion.

Lemma 2.1. *[12, p. 102] A bent function f in n variables belongs to $\mathcal{MM}^\#$ if and only if there exists an $\frac{n}{2}$-dimensional linear subspace V of $\mathbb{F}_2^n$ such that the second-order derivatives*

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

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

2.1 Bent and plateaued functions and their duals

Throughout this paper we use the following definitions related to bent and plateaued functions:

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

- Two functions f and g on $\mathbb{F}_2^n$ are said to be at *bent distance* if $d_H(f, g) = 2^{n-1} \pm 2^{n/2-1}$. Similarly, for a subset $B \subset \mathcal{B}_n$, a function f is said to be at bent distance to B if for all $g \in B$ it holds that $d_H(f, g) = 2^{n-1} \pm 2^{n/2-1}$.

- 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).

  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 $S_f = \{\omega \in \mathbb{F}_2^n \ : \ W_f(\omega) \neq 0\}$ and for an s-plateaued function its cardinality is $\#S_f = 2^{n-s}$ [3, Proposition 4].

- A *dual* function f^* of an s-plateaued $f \in \mathcal{B}_n$ is defined through $W_f(\omega) = 2^{\frac{n+s}{2}}(-1)^{f^*(\omega)}$, for $\omega \in S_f$. To specify the dual function as $f^* : \mathbb{F}_2^{n-s} \to \mathbb{F}_2$ 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 $\mathbf{e}_0 = \mathbf{0}_n$.

  A direct correspondence between $\mathbb{F}_2^{n-s}$ and $S_f = \{\omega_0, \ldots, \omega_{2^{n-s}-1}\}$ 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

$$\overline{f}^*(\mathbf{x}_i) = f^*(\mathbf{v} \oplus \mathbf{e}_i) = f^*(\omega_i), \tag{4}$$

  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 (4), the notation $\overline{f}^*$ associates this dual to a function defined on $\mathbb{F}_2^{n-s}$, that is $\overline{f}^* : \mathbb{F}_2^{n-s} \to \mathbb{F}_2$.*

2.2 Specifying 5-valued spectra functions through duals

We first recall certain notations, introduced in [16], useful in handling the 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 [16] 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:

$$W_f(\mathbf{u}) = \begin{cases} 0, & \mathbf{u} \notin S_f^{[1]} \cup S_f^{[2]}, \\ c_i \cdot (-1)^{f^*_{[i]}(\mathbf{u})}, & \mathbf{u} \in S_f^{[i]}, \ \ i \in \{1, 2\}. \end{cases} \tag{5}$$

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 $S_f^{[i]} = \{\omega_0^{(i)}, \ldots, \omega_{2^{\lambda_i}-1}^{(i)}\} = \mathbf{v}_i \oplus E_i$, where $\omega_j^{(i)} = \mathbf{v}_i \oplus \mathbf{e}_j^{(i)}$, 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 $\omega_j^{(i)} = \mathbf{v}_i \oplus \mathbf{e}_j^{(i)}$. 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

$$\overline{f}^*_{[i]}(\mathbf{x}_j) = f^*_{[i]}(\mathbf{v}_i \oplus \mathbf{e}_j^{(i)}) = f^*_{[i]}(\omega_j^{(i)}), \ \ j \in [0, 2^{\lambda_i} - 1], \tag{6}$$

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 [16], will be used in Section 3.4 for specifying suitable quadruples of such functions whose concatenation will give bent functions outside $\mathcal{MM}^{\#}$.

2.3 Decomposition of bent functions

The decomposition of bent functions on $\mathbb{F}_2^n$, n is even, to affine subspaces $\mathbf{a} \oplus V$, for some k-dimensional linear subspace $V \subset \mathbb{F}_2^n$, was considered in [3]. For a bent function $\mathfrak{f} \in \mathcal{B}_n$, the restriction to $\mathbf{a} \oplus V$ is denoted by $\mathfrak{f}_{\mathbf{a}\oplus V}$ and it can be viewed as a function from $\mathbb{F}_2^k \to \mathbb{F}_2$ using

$$\mathfrak{f}_{\mathbf{a}\oplus V}(\mathbf{x}_i) = \mathfrak{f}_{\mathbf{a}\oplus V}(\mathbf{a} \oplus \mathbf{v}_i), \quad i \in [0, 2^k - 1], \tag{7}$$

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.

The 4-decomposition of a bent function $\mathfrak{f} \in \mathcal{B}_n$, as a special case considered in [3], then defines four subfunctions on the four cosets of some $(n-2)$-dimensional linear subspace. More precisely, for nonzero $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$ with $\mathbf{a} \neq \mathbf{b}$ this $(n-2)$-dimensional subspace is defined as $V = \langle \mathbf{a}, \mathbf{b} \rangle^{\perp}$, where the *dual* of a linear subspace, say $S \subset \mathbb{F}_2^n$, is defined as $S^{\perp} = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} \cdot \mathbf{y} = 0, \ \forall \mathbf{y} \in S\}$.

Let (f_1, f_2, f_3, f_4) be such a decomposition, that is, $f_1, \ldots, f_4 \in \mathcal{B}_{n-2}$ are 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, thus $Q = \langle \mathbf{a}, \mathbf{b} \rangle$ and $Q \oplus V = \mathbb{F}_2^n$ (with $Q \cap V = \{\mathbf{0}_n\}$). Such a decomposition is called a *bent 4-decomposition* when all f_i ($i \in [1,4]$), are bent; a *semi-bent 4-decomposition* when all f_i ($i \in [1,4]$) are semi-bent; a *5-valued 4-decomposition* when all f_i ($i \in [1,4]$) are 5-valued spectra functions so that $W_{f_i} \in \{0, \pm 2^{(n-2)/2}, \pm 2^{n/2}\}$ [3]. These are the only possibilities and we strictly have that all the restrictions have the same spectral profile, for instance the restrictions cannot be a mixture of bent and semi-bent functions.

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 $f_1, \ldots, f_4$ [16]. Note that functions f_i are considered as functions in $(n-2)$-variables in terms of relation (7) (that is when $\dim(V) = k = n-2$).

Theorem 2.1. *[16] Let $\mathfrak{f} \in \mathcal{B}_n$ be a bent function, for even $n \geq 4$. Let $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n \setminus \{\mathbf{0}_n\}$ ($\mathbf{a} \neq \mathbf{b}$) and $V = \langle \mathbf{a}, \mathbf{b} \rangle^{\perp}$. 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.

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

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

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

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 2.1. Then, the function $\mathfrak{f}$ is the concatenation of $f_i \in \mathcal{B}_{n-2}$ which we denote by $\mathfrak{f} = f_1 || f_2 || f_3 || f_4$.

3 Decomposing bent functions - design methods

From the design perspective, Theorem 2.1 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 $\mathcal{MM}^{\#}$.

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

$$E = \{\{a, b\} : a, b \in \mathbb{F}_{2^n}^*; D_a D_b f \equiv 0\},$$

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 $D_0 D_b f \equiv 0$ for all $b \in \mathbb{F}_{2^n}$. With this approach, we reduce the size of the vertex set V as $D_a D_b f \not\equiv 0$, for some $a, b \in \mathbb{F}_{2^n}^*$. In practice, 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 ($D_a D_a f \equiv 0$ holds for all $a \in \mathbb{F}_{2^n}$); and it is not directed since $D_a D_b f = D_b D_a f$ for any $a, b \in \mathbb{F}_{2^n}$.

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 (a 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 approx. 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 hours 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 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 [5] 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) 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 $h = f||f||f||f||(1 \oplus f) \in \mathcal{B}_{n+2}$ is also bent. Then, f is outside $\mathcal{MM}^\#$ if and only if h is outside $\mathcal{MM}^\#$.*

Proof. It is well-known that $h = f||f||f||f||(1 \oplus f) \in \mathcal{B}_{n+2}$ is bent if f is bent. 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 derivative 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

$$D_{(a_1,a_2)}D_{(b_1,b_2)}y_1y_2 \equiv 0.$$

Thus,

$$D_{(\mathbf{a}',a_1,a_2)}D_{(\mathbf{b}',b_1,b_2)}h = D_{\mathbf{a}'}D_{\mathbf{b}'}f \oplus D_{(a_1,a_2)}D_{(b_1,b_2)}(y_1y_2) \equiv 1 \neq 0.$$

(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 $f(\mathbf{x}, y_1, y_2, \ldots, y_m) = h(\mathbf{x}) \oplus y_1y_2 \oplus \cdots \oplus y_{m-1}y_m$ 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 satisfy 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 $\mathcal{MM}^{\#}$.

Using the convention that $f(\mathbf{x}, 0, 0) = f_1(\mathbf{x}), f(\mathbf{x}, 0, 1) = f_2(\mathbf{x}), f(\mathbf{x}, 1, 0) = f_3(\mathbf{x})$ and $f(\mathbf{x}, 1, 1) = f_4(\mathbf{x})$, the ANF of $f = f_1||f_2||f_3||f_4$ is given by

$$f(\mathbf{x}, y_1, y_2) = f_1(\mathbf{x}) \oplus y_1(f_1 \oplus f_3)(\mathbf{x}) \oplus y_2(f_1 \oplus f_2)(\mathbf{x}) \oplus y_1y_2(f_1 \oplus f_2 \oplus f_3 \oplus f_4)(\mathbf{x}). \quad (8)$$

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 (8) gives*

$$f(\mathbf{x}, y_1, y_2) = (1 \oplus y_1)f_1(\mathbf{x}) \oplus y_1f_2(\mathbf{x}) \oplus y_1y_2, \ \mathbf{x} \in \mathbb{F}_2^n, y_1, y_2 \in \mathbb{F}_2. \quad (9)$$

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

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

$$\begin{aligned} D_{(\mathbf{a}',a_2,a_3)}D_{(\mathbf{b}',b_2,b_3)}f(\mathbf{x}, y_1, y_2) = \ & (1 \oplus y_1)D_{\mathbf{a}'}D_{\mathbf{b}'}f_1(\mathbf{x}) \oplus y_1D_{\mathbf{a}'}D_{\mathbf{b}'}f_2(\mathbf{x}) \\ & \oplus a_2D_{\mathbf{b}'}\left(f_1 \oplus f_2\right)(\mathbf{x} \oplus \mathbf{a}') \oplus b_2D_{\mathbf{a}'}\left(f_1 \oplus f_2\right)(\mathbf{x} \oplus \mathbf{b}') \\ & \oplus a_2b_3 \oplus a_3b_2. \end{aligned} \quad (10)$$

There are two cases to be considered.

a. Assuming that $\dim(V \cap (\mathbb{F}_2^n \times \{(0,0)\})) \geq m$ 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 $\mathbf{a}' \neq \mathbf{b}'$, $a_2 = a_3 = b_2 = b_3 = 0$. Firstly, suppose that f_2 is outside $\mathcal{MM}^{\#}$. Thus:

$$D_{\mathbf{a}'} D_{\mathbf{b}'} f_2 \not\equiv 0.$$

From (10), 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 (10), 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 $\dim(V \cap (\mathbb{F}_2^n \times \{(0,0)\})) < m$, we have $V \cap (\{\mathbf{0}_n\} \times \mathbb{F}_2^2) = \mathbb{F}_2^2$ 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 (10), we have

$$D_{(\mathbf{0}_n, 1, 0)} D_{(\mathbf{0}_n, 0, 1)} f(\mathbf{x}, y_1, y_2) = 1 \neq 0. \tag{11}$$

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 $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^4$. We note that $f_1 \in \mathcal{MM}^{\#}$ and $f_2 \in \mathcal{D}_0 \setminus \mathcal{MM}^{\#}$. 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 (9). Using the algorithm in Section 3.1, we have confirmed that $\mathfrak{f}_1, \mathfrak{f}_2 \in \mathcal{B}_{10}$ are both bent function 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 either 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 [17] and references therein. In terms of the spectral design method in [17], constructing quadruples of semi-bent functions on $\mathbb{F}_2^n$ (with n even), whose spectra belong to $\{0, \pm 2^{\frac{n+2}{2}}\}$, with pairwise disjoint spectra can be easily achieved by specifying suitable Walsh supports. It has already been observed in [15, 27] that trivial plateaued functions, having an affine subspace as their Walsh support, essentially correspond to partially bent functions introduced by Carlet in [6] 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 [17] 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. *[17, Theorem 3.3 (with $s = 2$)] Let $S_f = \mathbf{v} \oplus EM = \{\omega_0, \ldots, \omega_{2^{n-2}-1}\} \subset \mathbb{F}_2^n$, for some $\mathbf{v} \in \mathbb{F}_2^n$, $M \in GL(n, \mathbb{F}_2)$ and 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 $\omega_i \in S_f$ through $\mathbf{e}_i \in E$ using (4)) as*

$$W_f(\mathbf{u}) = \begin{cases} 2^{\frac{n+2}{2}}(-1)^{g(\mathbf{x}_i)}, & \text{for } \mathbf{u} = \mathbf{v} \oplus \mathbf{e}_i M \in S_f, \\ 0, & \mathbf{u} \notin S_f. \end{cases} \tag{12}$$

Then:

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

$$\Phi_f = \{\phi_{\mathbf{u}} : \mathbb{F}_2^{n-2} \to \mathbb{F}_2 \ : \ \chi_{\phi_{\mathbf{u}}} = ((-1)^{\mathbf{u}\cdot\omega_0}, (-1)^{\mathbf{u}\cdot\omega_1}, \ldots, (-1)^{\mathbf{u}\cdot\omega_{2^{n-2}-1}}),\ \omega_i \in S_f,\ \mathbf{u} \in \mathbb{F}_2^n\}. \tag{13}$$

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 $g \in \mathcal{B}_n$. 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

$$g(\mathbf{x},\mathbf{y}) = \mathbf{x}\cdot\psi(\mathbf{y}) \oplus t(\mathbf{y}); \quad \mathbf{x},\mathbf{y} \in \mathbb{F}_2^{n/2}, \tag{14}$$

where ψ is an arbitrary permutation on $\mathbb{F}_2^{n/2}$ and $t \in \mathcal{B}_{n/2}$ is arbitrary.

Theorem 3.4. *[17, 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, $f : \mathbb{F}_2^{n+2} \to \mathbb{F}_2$ specified using S_f and the dual g as in Theorem 3.3, 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 $f : \mathbb{F}_2^{n+2} \to \mathbb{F}_2$, specified using S_f and the dual g as in Theorem 3.3, 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 [17] also proposed a construction method of disjoint spectra plateaued functions, see Theorem 4.4 in [17], 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 $Q = \mathbf{0}_n \times \mathbb{F}_2^2$. The main idea is then to specify disjoint Walsh supports of semi-bent functions f_i on the cosets of V in $\mathbb{F}_2^{n+2}$. 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.

Theorem 3.5. *Let $g \notin \mathcal{MM}^\#$ be a bent function in n variables. 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 $Q = \{\mathbf{0}_n\} \times \mathbb{F}_2^2 = \{\mathbf{q}_0, \mathbf{q}_1, \mathbf{q}_2, \mathbf{q}_3\}$ and set $S_{f_i} = \mathbf{q}_i \oplus S_f$, for $i = 0, \ldots, 3$. Then, the functions $f_i \in \mathcal{B}_{n+2}$, constructed using Theorem 3.3 with S_{f_i} 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 restrictions are $\mathfrak{f}|_{\mathbf{a}_i \oplus \mathbb{F}_2^{n+4}} = f_i$ (thus $\mathfrak{f} = f_1||f_2||f_3||f_4$), where $\mathbf{a}_i \in \{\mathbf{0}_{n+2}\} \times \mathbb{F}_2^2$, 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, 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 $\Phi_f = \{\phi_\mathbf{u} \in \mathcal{B}_n : T_{\phi_\mathbf{u}} = (\mathbf{u}\cdot\omega_0, \ldots, \mathbf{u}\cdot\omega_{2^n-1}),\ \omega_i \in S_f,\ \mathbf{u} \in \mathbb{F}_2^{n+2}\}$.

Let $S_{f_i} = S_f \oplus \mathbf{q}_i$ and $\mathbf{q}_i \in Q = \{\mathbf{0}_n\} \times \mathbb{F}_2^2$. By Theorem 3.3, the functions $f_i \in \mathcal{B}_{n+2}$, whose Walsh spectral values at $\mathbf{u} \in \mathbb{F}_2^{n+2}$ are defined by:

$$W_{f_i}(\mathbf{u}) = \begin{cases} 2^{\frac{n+4}{2}}(-1)^{g(\mathbf{x}_i,\mathbf{y}_i)}, & \mathbf{u} = (\mathbf{c} \oplus (\mathbf{x}_i,\mathbf{y}_i) \cdot M, t_1(\mathbf{x}_i,\mathbf{y}_i), t_2(\mathbf{x}_i,\mathbf{y}_i)) \oplus \mathbf{q}_i \in S_{f_i} \\ 0, & \mathbf{u} \notin S_{f_i} \end{cases}, \tag{15}$$

are 2-plateaued (semi-bent) functions, for $i = 0, \ldots, 3$.

By [17, Theorem 4.4] mentioned above, the functions $f_i \in \mathcal{B}_{n+2}$ are pairwise disjoint spectra functions (this is also obvious from the definition of S_{f_i}). Furthermore, we have $\cup_{\mathbf{q}\in Q}(\mathbf{q} \oplus S_f) = \mathbb{F}_2^{n+2}$ and the function $\mathfrak{f} \in \mathcal{B}_{n+4}$ is bent by Theorem 2.1 *ii*). For convenience, we write $\mathbf{u} = (\alpha, \beta, \gamma, \omega_i) \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2} \times \mathbb{F}_2^2 \times \mathbb{F}_2^2$. Let $\Delta = (t_1(\alpha,\beta), t_2(\alpha,\beta))$. We know that for some $\mathbf{q}_j \in Q$ we have that $(\alpha, \beta, \gamma) = (\alpha, \beta, \Delta) \oplus \mathbf{q}_j$. Then, the Walsh-Hadamard transform of $\mathfrak{f}$ at $\mathbf{u} \in \mathbb{F}_2^{n+2}$ evaluates to:

$$\begin{aligned}
W_{\mathfrak{f}}(\mathbf{u}) &= \sum_{(\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{t})\in(\mathbb{F}_2^{n/2})^2\times(\mathbb{F}_2^2)^2} (-1)^{\mathfrak{f}(\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{t})\oplus(\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{t})\cdot\mathbf{u}} \\
&= \sum_{i=0}^{3} \sum_{(\mathbf{x},\mathbf{y},z)\in(\mathbb{F}_2^{n/2})^2\times\mathbb{F}_2^2} (-1)^{\mathfrak{f}((\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{0}_2)\oplus\mathbf{a}_i)\oplus((\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{0}_2)\oplus\mathbf{a}_i)\cdot\mathbf{u}} \\
&= \sum_{i=0}^{3} (-1)^{\mathbf{a}_i\cdot\mathbf{u}} \sum_{(\mathbf{x},\mathbf{y},\mathbf{z})\in(\mathbb{F}_2^{n/2})^2\times\mathbb{F}_2^2} (-1)^{f_i(\mathbf{x},\mathbf{y},\mathbf{z})\oplus(\mathbf{x},\mathbf{y},\mathbf{z})\cdot(\alpha,\beta,\gamma)} \\
&= \sum_{i=0}^{3} (-1)^{\mathbf{a}_i\cdot\mathbf{u}} W_{f_i}(\alpha,\beta,\gamma) = \sum_{i=0}^{3} (-1)^{\mathbf{a}_i\cdot\mathbf{u}} W_{f_i}((\alpha,\beta,\Delta)\oplus\mathbf{q}_j) \\
&= (-1)^{\mathbf{a}_j\cdot\mathbf{u}} W_{f_j}(\alpha,\beta,\Delta) = (-1)^{\mathbf{a}_j\cdot\mathbf{u}} 2^{\frac{n+4}{2}} (-1)^{g(\alpha,\beta)} \\
&= 2^{\frac{n+4}{2}} (-1)^{g(\alpha,\beta)\oplus\mathbf{a}_j\cdot\mathbf{u}}.
\end{aligned}$$

Hence, $\mathfrak{f}^*$ is defined via g which is outside $\mathcal{MM}^\#$ and it follows that $\mathfrak{f}^*$ is outside $\mathcal{MM}^\#$. By Remark 3.1, it means that $\mathfrak{f}$ is outside $\mathcal{MM}^\#$. □

Since $g \in \mathcal{B}_n$ is supposed to be a bent function outside $\mathcal{MM}^\#$, 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 $\mathcal{MM}^\#$ [18,24,25]. 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 [4,24,25]. However, there exist efficient design methods for specifying bent functions in the above classes that are provably outside $\mathcal{MM}^\#$ [1,2,18,24,25]. 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 the subspace $\mathbf{0}_{n/2} \times \mathbb{F}_2^{n/2}$.

Corollary 3. *With the same notation as in Theorem 3.5, if a bent function $g \in \mathcal{B}_n$ 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 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 Section 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. 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 $S_f = (\mathbf{c} \oplus \mathbb{F}_2^8 \cdot M) \wr T_{\delta_0} \wr T_{\delta_0}$, *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* $S_{f_i} = S_f \oplus \mathbf{q}_i$ *and* $\mathbf{q}_i \in Q = \{\mathbf{0}_8\} \times \mathbb{F}_2^2$. *In other words,* $\mathfrak{f} = (f_0, f_1, f_2, f_3) \in \mathcal{B}_{12}$ *is a bent function and can be viewed as a concatenation of four semi-bent functions. Furthermore, using our algorithm in Section 3.1, we have confirmed that* $\mathfrak{f}$ *lies outside* $\mathcal{MM}^{\#}$. *The ANF of* $\mathfrak{f}$ *is given by (22) in Appendix.*

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

Remark 3.3. *Notice that the number of possibilities of selecting* S_{f_i} *(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 3.4. *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 Section 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 (15)) is outside $\mathcal{MM}^{\#}$. It is completely irrelevant whether these semi-bent functions possess linear structures (having affine supports S_{f_i}) or not.*

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

To specify 5-valued spectra Boolean functions, the authors in [16] provided a sufficient and necessary condition that the Walsh spectra of f_i (corresponding to two different amplitudes) must satisfy, see Section 2.2. The notion of totally disjoint spectra functions was also introduced in [16], which can be regarded as a sufficient condition so that the Walsh spectrum specified by (5) is a valid spectrum of a Boolean function.

Definition 3.1. *[16, 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 functions $f_{[1]}^* : S_f^{[1]} \to \mathbb{F}_2$ and $f_{[2]}^* : S_f^{[2]} \to \mathbb{F}_2$ are* totally disjoint spectra functions *if it holds that*

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

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 3.5. *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 [22].*

Furthermore, a generic method of specifying totally disjoint spectra functions was also given in [16].

Construction 1. *[16] 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 $(\alpha, \beta) \in \mathbb{F}_2^k \times \mathbb{F}_2^m$, can be constructed as follows:*

$$W_f(\alpha, \beta) = \begin{cases} (-1)^{g(\alpha) \oplus h(\beta)} \cdot 2^{n/2}, & (\alpha, \beta) \in E_1 \\ (-1)^{h(\beta)} \cdot 2^{m/2+k}, & (\alpha, \beta) \in E_2 \\ 0, & \textit{otherwise.} \end{cases} \tag{16}$$

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

$$\begin{aligned} f_1(\alpha, \beta) &= g(\alpha) \oplus h(\beta), \quad (\alpha, \beta) \in E_1 \\ f_2(\alpha, \beta) &= h(\beta), \quad (\alpha, \beta) \in E_2. \end{aligned}$$

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

Now, we need to specify a quadruple of 5-valued spectra functions which are all of this kind and, additionally satisfying the condition given by item *iii*) of Theorem 2.1. More precisely:

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

b) All $S_{f_i}^{[2]} = \{\vartheta \in \mathbb{F}_2^{n-2} : |W_{f_i}(\vartheta)| = 2^{\frac{n-2}{2}}\}$ 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.

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 $\mathbf{c}^{(i)} \in \mathbb{F}_2^2$ and $\mathbf{c}^{(i)} \neq \mathbf{c}^{(j)}$ for $1 \leq i \neq j \leq 4$. We specify the spectra of $f_i \in \mathcal{B}_n$ as follows:*

$$W_{f_i}(\alpha, \beta) = \begin{cases} (-1)^{g(\alpha) \oplus h(\beta) + d} \cdot 2^{n/2}, & (\alpha, \beta) \in E_1^{(i)} \\ (-1)^{h(\beta)} \cdot 2^{\frac{n-2}{2}+2}, & (\alpha, \beta) \in E_2^{(i)} \\ 0, & \textit{otherwise}, \end{cases} \tag{17}$$

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 (17), are clearly 5-valued spectra functions. We need to verify that their spectra corresponds to Boolean functions. By Construction 1, this is true for f_1. Due to the definition of $E_1^{(i)}$ and $E_2^{(i)}$, the same is true for any f_i which are all Boolean 5-valued spectra functions. Now, the condition for a valid 4-decomposition into 5-valued spectra functions is given by *iii*) in Theorem 2.1. 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 $E_1^{(i)}$ satisfies $f_{[2],1}^* \oplus f_{[2],2}^* \oplus f_{[2],3}^* \oplus f_{[2],4}^* = 1$ follows from the specification of the spectra on $E_1^{(i)}$, using the fact that $d = 1$ only when $i = 4$. □

Remark 3.6. *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 $g(x_0, x_1) = x_0x_1$. Using the mathematical software* Sage*, we constructed the functions $f^{(i)} \in \mathcal{B}_8$ for $i = 1, \ldots, 4$ defined by (17) and their ANF's are given as follows:*

$$f_1(x_0, \ldots, x_7) = x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_4x_6x_7 \oplus x_6x_7,$$

$$f_2(x_0,\ldots,x_7) = x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_4x_6x_7 \oplus x_4x_6 \oplus x_6x_7,$$
$$f_3(x_0,\ldots,x_7) = x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_4x_6x_7 \oplus x_4x_7 \oplus x_6x_7,$$
$$f_4(x_0,\ldots,x_7) = x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_4x_6x_7 \oplus x_4x_6 \oplus x_4x_7 \oplus x_4 \oplus x_6x_7 \oplus 1$$

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

$$f(x_0,\ldots,x_9) = x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_4x_6x_7 \oplus x_4x_6x_8 \oplus x_4x_7x_9 \oplus x_4x_8x_9 \oplus x_6x_7 \oplus x_8x_9.$$

Using our algorithm in Section 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, 24], and let $g \in \mathcal{B}_2$ be defined by $g(x_0,x_1) = x_0x_1$. Using* Sage *we constructed the functions $f_i \in \mathcal{B}_{10}$ for $i = 1,\ldots,4$ defined by (17). 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 (20) in 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 (19) in Appendix, lies in $\mathcal{PS}^{\#}$ and is outside $\mathcal{M}^{\#}$. Using* Sage*, we constructed the functions $f_i \in \mathcal{B}_{10}$ for $i = 1,\ldots,4$ defined by (17). 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 (21) in Appendix).*

The above examples indicate that the conclusions (related to the dual) given in Section 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 $f_i \in \mathcal{B}_n$. Then, f is outside $\mathcal{MM}^{\#}$ if and only if the dual bent function $h \in \mathcal{B}_{n-2}$ in Theorem 3.6 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 (17). 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 $\mathbf{u} = (\alpha,\beta,\gamma) \in \mathbb{F}_2^2 \times \mathbb{F}_2^m \times \mathbb{F}_2^2$ with $n = m+2$ as used in Theorem 3.6. We notice that in general, using that $\mathbf{x} = (\mathbf{x}', x_{n+1}, x_{n+2})$, we have

$$\begin{aligned} W_f(\alpha,\beta,\gamma) &= \sum_{\mathbf{x} \in \mathbb{F}_2^n \times \mathbb{F}_2^2} (-1)^{f(\mathbf{x}) + \mathbf{u}\cdot\mathbf{x}} \\ &= \sum_{\mathbf{x} \in \mathbb{F}_2^n \times (0,0)} (-1)^{f(\mathbf{x}',0,0) + (\alpha,\beta)\cdot\mathbf{x}'} + \sum_{\mathbf{x} \in \mathbb{F}_2^n \times (0,1)} (-1)^{f(\mathbf{x}',0,1) + (\alpha,\beta)\cdot\mathbf{x}' + \gamma_2} \end{aligned}$$

$$
\begin{aligned}
&+ \sum_{\mathbf{x}\in\mathbb{F}_2^n\times(1,0)} (-1)^{f(\mathbf{x}',1,0)+(\alpha,\beta)\cdot\mathbf{x}'+\gamma_1} + \sum_{\mathbf{x}\in\mathbb{F}_2^n\times(1,1)} (-1)^{f(\mathbf{x}',1,1)+(\alpha,\beta)\cdot\mathbf{x}'+\gamma_1+\gamma_2} \\
&= W_{f_1}(\alpha,\beta) + (-1)^{\gamma_2} W_{f_2}(\alpha,\beta) + (-1)^{\gamma_1} W_{f_3}(\alpha,\beta) \\
&+ (-1)^{\gamma_1+\gamma_2} W_{f_4}(\alpha,\beta). \qquad (18)
\end{aligned}
$$

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

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

Now, considering the case $(\alpha,\beta) \in E_1^{(i)}$, 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, $W_{f_i}(\alpha,\beta) = (-1)^{g(\alpha)\oplus h(\beta)+d} \cdot 2^{n/2}$, where $d = 1$ when $i = 4$ only. This also implies that $W_{f_1}(\alpha,\beta) = W_{f_2}(\alpha,\beta) = W_{f_3}(\alpha,\beta) = -W_{f_4}(\alpha,\beta)$ when $(\alpha,\beta) \in E_1$. Therefore, using (18), we have

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

Hence, $W_f(\alpha,\beta,\gamma_1,\gamma_2) = 2\cdot 2^{n/2}(-1)^{g(\alpha)\oplus h(\beta)+\gamma_1\gamma_2}$ when $(\alpha,\beta) \in E_1$, where $g(\alpha)\oplus h(\beta)+\gamma_1\gamma_2$ falls into the framework of Theorem 3.1 and additionally Remark 3.1 applies. Notice that the case $(\alpha,\beta) \notin E_1$ and at the same time having $W_{f_i}(\alpha,\beta) = 0$ is already covered above since then $(\alpha,\beta) \in E_2^{(j)}$ 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 $g(\alpha) \oplus h(\beta) + \gamma_1\gamma_2$ when f^* is restricted to the subspace $(\alpha,\beta,\gamma) \in E_1 \times \mathbb{F}_2^2$ and to $h(\beta)$ 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 $f \notin \mathcal{MM}^\#$.

□

4 5-valued spectra functions from the generalized MM class

Another method of specifying 5-valued spectra functions, also given in [16], uses the generalized Maiorana-McFarland class (GMM).

Theorem 4.1. *[16] 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 $X = (x_1,\ldots,x_n) \in \mathbb{F}_2^n$ and $X_{(i,j)} = (x_i,\ldots,x_j) \in \mathbb{F}_2^{j-i+1}$.*

$f \in \mathcal{B}_n$ is defined as follows:

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

Let

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

and

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

Then, we have

a) $W_f(\omega) \in \{0, \pm 2^{n-s}, \pm 2^{n-s-t}\}$ *if* $t \neq 0$ *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) $W_f(\omega) \in \{0, \pm 2^{n-s}, \pm 2^{n-s+1}\}$ *if* $t = 0$, $T_0 \cap T_1 \neq \emptyset$ *and* $T_0 \neq T_1$.

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 2.1. The resulting function* $f = f^{(1)}||f^{(2)}||f^{(3)}||f^{(4)} \in \mathcal{B}_{10}$ *is then bent. Let* $\mathbb{F}_2^n = \{\mathbf{v}_0, \ldots, \mathbf{v}_{2^n-1}\}$ *be ordered lexicographically. 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* $\mathbf{e}_i^{(0)} = \mathbf{v}_i \in \mathbb{F}_2^3$, *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* $\overline{E_0} = \mathbb{F}_2^3 \setminus E_0$. *Let* $\phi_1 : E_1 \to \mathbb{F}_2^4$ *be defined by*

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

Let $T_1 = \{\phi_1(\theta) : \theta \in E_1\}$ *and* $\overline{T_1} = \mathbb{F}_2^4 \setminus T_1$. *Let* $\Gamma = \mathbb{F}_2 \times \overline{T_1} \subset \mathbb{F}_2^4 = \{\gamma_0, \ldots, \gamma_{11}\} \subset \mathbb{F}_2^5$ *and let* $\phi_0^{(j)} : E_0 \to \mathbb{F}_2^5$ *be defined by*

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

for $j = 1, \ldots, 4$. *If* $T_0 = \{\phi_0(\eta) : \eta \in E_0\}$, *then* $T_0 \subset \mathbb{F}_2 \times \overline{T_1}$ *(as required in Theorem 4.1-(a)). 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,* $f^*_{[2],1} \oplus \ldots \oplus f^*_{[2],4} = 1$. *Hence, by Theorem 2.1, 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:*

$$f(x_0, \ldots, x_9) = x_0x_1x_2x_3x_4 \oplus x_0x_1x_2x_3x_9 \oplus x_0x_1x_2x_4x_8 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_9 \oplus x_0x_1x_4x_8 \oplus x_0x_1x_4 \oplus x_0x_1x_6 \oplus x_0x_1x_7 \oplus x_0x_2x_4 \oplus x_0x_2x_5x_8 \oplus x_0x_2x_5 \oplus x_0x_2x_6 \oplus$$

$x_0x_4 \oplus x_0x_5x_8 \oplus x_1x_2x_5 \oplus x_1x_2x_6x_8 \oplus x_1x_5 \oplus x_1x_6x_8 \oplus x_1x_6 \oplus x_2x_3x_4 \oplus x_2x_3x_9 \oplus x_2x_4x_8 \oplus x_2x_5x_8 \oplus x_2x_6x_8 \oplus x_2x_7 \oplus x_3x_9 \oplus x_4x_8 \oplus x_5x_8 \oplus x_5 \oplus x_6x_8 \oplus x_7 \oplus x_8x_9 \oplus x_8 \oplus x_9 \oplus 1$.

Nevertheless, using our algorithm in Section 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. We assume that all sets are ordered lexicographically and we denote $\mathbb{F}_2^n = \{\mathbf{v}_0^{(n)}, \mathbf{v}_1^{(n)}, \ldots, \mathbf{v}_{2^n-1}^{(n)}\}$.

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

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

and let $\phi_0^{(j)} : E_0 \to \mathbb{F}_2^{m+1}$ *be defined by*

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

for $j = 1, 2, 3, 4$ *and* $\Gamma = \mathbb{F}_2 \times (\mathbb{F}_2^m \setminus T_1)$, *where* $T_1 = \{\phi_1(\theta) : \theta \in E_1\}$. *Now 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* $j = 1, 2, 3, 4$, $f^{(j)} \in \mathcal{B}_n$ *is defined as follows:*

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

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 $j = 1, 2, 3, 4$. It remains to show that these functions satisfy Theorem 2.1-(iii). From [16, Theorem V.6], we have that $W_{f^{(j)}}(X) = \pm 2^{m+1}$ if $\phi_0^{(j)^{-1}}(X_{(0,m-2)})$ exists, and $W_{f^{(j)}}(X) = \pm 2^m$ if $\phi_1^{-1}(X_{(0,m-1)})$ exists. Let $S_{f^{(j)}}^{[1]} = \{\mathbf{x} \in \mathbb{F}_2^n : |W_{f^{(j)}}(\mathbf{x})| = 2^{m+1}$ and $S_{f^{(j)}}^{[2]} = \{\mathbf{x} \in \mathbb{F}_2^n : |W_{f^{(j)}}(\mathbf{x})| = 2^m$. 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 and consequently the sets $S_{f^{(j)}}^{[1]}$ are pairwise disjoint for $j = 1, 2, 3, 4$. As the function ϕ_1 is the same for all $f^{(j)}$, it follows that all sets $S_{f^{(j)}}^{[2]}$ are equal. The condition that the bent duals defined on $S_{f^{(j)}}^{[2]}$ 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 $j = 1$. □

Remark 4.1. *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 increases the cardinality of bent functions provably outside the completed Maiorana-McFarland class by specifying many infinite families of such functions, which can additionally be combined for the same purpose. 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.

Acknowledgment: 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).

References

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

[2] A. Bapić, E. Pasalic, F. Zhang and S. Hodžić. "Constructing new superclasses of bent functions from known ones." *Cryptography and Communications*, SI Boolean Functions and Their Applications VI, pp. 1–28 (2022).

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

[4] C. Carlet. "Two new classes of bent functions." In *Lecture Notes in Computer Science*, volume 765, pages 77–101, 1993.

[5] C. Carlet. "Boolean Functions for Cryptography and Coding Theory." Cambridge University Press, 2021.

[6] C. Carlet. "Partially bent functions." *Designs, Codes and Cryptography*, vol. 3, no. 2, pp. 135–145, 1993.

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

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

[9] C. Carlet and S. Mesnager. "Four decades of research on bent functions." *Designs, Codes and Cryptogr.*, 78(1): 5–50 (2016)

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

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

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

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

[15] S. Hodžić, E. Pasalic, and Y. Wei. "A general framework for secondary constructions of bent and plateaued functions." *Designs, Codes and Cryptogr.*, 88(10): 2007-2035 (2020)

[16] S. Hodžić, E. Pasalic, W. G. Zhang. "Generic constructions of five-valued spectra Boolean functions". *IEEE Trans. Inf. Theory* 65(11): 7554–7565 (2019)

[17] S. Hodžić, E. Pasalic, Y. Wei, and F. Zhang. "Designing plateaued Boolean functions in spectral domain and their classification." *IEEE Trans. Inf. Theory*, 65(9): 5865–5879 (2019)

[18] S. Kudin, E. Pasalic, N. Cepak, F. Zhang. "Permutations without linear structures inducing bent functions outside the completed Maiorana-McFarland class". *Cryptography and Communications*, https://doi.org/10.1007/s12095-021-00523-w (2021).

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

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

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

[22] Y. Wei, E. Pasalic, F. Zhang, W. Wu, and C.-X. Wang. "New constructions of resilient functions with strictly almost optimal nonlinearity via non-overlap spectra functions." *Inform. Sci.*, vol. 415–416, pp. 377–396, 2017.

[23] L. Wang, B. Wu, Z. Liu, D. Lin. "Three new infinite families of bent functions". *Sci. China Inf. Sci.*, vol. 61, 032104, 2018, doi:10.1007/s11432-016-0624-x.

[24] F. Zhang, N. Cepak, E. Pasalic, and Y. Wei. "Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^{\#}$." *Discret. Appl. Math.*, 285(1): 458–472, 2020.

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

[26] F. Zhang, E. Pasalic, Y. Wei, N. Cepak. "Constructing bent functions outside the Maiorana-McFarland class using a general form of Rothaus". *IEEE Trans. Inf. Theory*, 63(8): 5336–5349 (2017)

[27] Y. Zheng and X. M. Zhang. "On plateaued functions." *IEEE Trans. Inf. Theory*, 47(3): 1215–1223 (2001).

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

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

$$x_0x_1x_2x_4 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3x_7 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_7 \oplus x_0x_1x_6x_7 \oplus x_0x_2x_3x_6 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_5x_6 \oplus x_0x_2x_5x_7 \oplus x_0x_2x_5 \oplus x_0x_2x_6x_7 \oplus x_0x_3x_4x_6 \oplus x_0x_3x_4x_7 \oplus x_0x_3x_4 \oplus x_0x_3x_5x_7 \oplus x_0x_3x_6x_7 \oplus x_0x_3x_6 \oplus x_0x_3x_7 \oplus x_0x_4x_5x_6 \oplus x_0x_4x_5 \oplus x_0x_4x_6 \oplus x_0x_5x_6x_7 \oplus x_0x_5x_6 \oplus x_0x_5x_7 \oplus x_0x_7 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_6 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_4 \oplus x_1x_2x_5x_6 \oplus x_1x_2x_5 \oplus x_1x_2x_6x_7 \oplus x_1x_2x_7 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_5x_6 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_4x_6x_7 \oplus x_1x_4x_7 \oplus x_1x_4 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_1x_6 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_5x_7 \oplus x_2x_3x_5 \oplus x_2x_4x_5x_6 \oplus x_2x_4x_5x_7 \oplus x_2x_4x_5 \oplus x_2x_4x_7 \oplus x_2x_4 \oplus x_2x_6x_7 \oplus x_2x_7 \oplus x_3x_4x_5x_7 \oplus x_3x_4x_6x_7 \oplus x_3x_5x_6 \oplus x_3x_5 \oplus x_3x_6x_7 \oplus x_3x_6 \tag{19}$$

$$x_0x_1x_2x_6+x_0x_1x_2x_7+x_0x_1x_2x_8x_9+x_0x_1x_2x_8x_{10}+x_0x_1x_2x_9x_{11}+x_0x_1x_2x_{10}x_{11}+x_0x_1x_3x_4+x_0x_1x_3x_5+x_0x_1x_4+x_0x_1x_7+x_0x_1x_8x_9+x_0x_1x_8x_{10}+x_0x_1x_9x_{11}+x_0x_1x_{10}x_{11}+x_0x_2x_3x_6+x_0x_2x_4+x_0x_2x_5+x_0x_2x_7+x_0x_2x_8x_9+x_0x_2x_8x_{10}+x_0x_2x_9x_{11}+x_0x_2x_{10}x_{11}+x_0x_3x_4+x_0x_3x_5+x_0x_3x_6+x_0x_3x_7+x_0x_3x_8x_9+x_0x_3x_8x_{10}+x_0x_3x_9x_{11}+x_0x_3x_{10}x_{11}+x_0x_6+x_1x_2x_3x_4+x_1x_2x_4+x_1x_2x_6+x_1x_3x_5+x_1x_3x_6+x_1x_5+x_1x_6+x_1x_7+x_1x_8x_9+x_1x_8x_{10}+x_1x_9x_{11}+x_1x_{10}x_{11}+x_2x_3x_4+x_2x_3x_5+x_2x_3x_6+x_2x_4+x_2x_6+x_2x_7+x_2x_8x_9+x_2x_8x_{10}+x_2x_9x_{11}+x_2x_{10}x_{11}+x_3x_4+x_4x_5x_6x_7+x_4x_5x_6x_8x_9+x_4x_5x_6x_8x_{10}+x_4x_5x_6x_9x_{11}+x_4x_5x_6x_{10}x_{11}+x_4x_5x_6+x_4x_5x_7+x_4x_5x_8x_9+x_4x_5x_8x_{10}+x_4x_5x_9x_{11}+x_4x_5x_{10}x_{11}+x_4x_5+x_4x_6x_7+x_4x_6x_8x_9+x_4x_6x_8x_{10}+x_4x_6x_9x_{11}+x_4x_6x_{10}x_{11}+x_4x_6+x_4x_7+x_4x_8x_9+x_4x_8x_{10}+x_4x_9x_{11}+x_4x_{10}x_{11}+x_4+x_5x_6x_7+$$

$$x_5x_6x_8x_9 + x_5x_6x_8x_{10} + x_5x_6x_9x_{11} + x_5x_6x_{10}x_{11} + x_5x_6 + x_5x_7 + x_5x_8x_9 + x_5x_8x_{10} + x_5x_9x_{11} + x_5x_{10}x_{11} + x_5 + x_6x_7 + x_6x_8x_9 + x_6x_8x_{10} + x_6x_9x_{11} + x_6x_{10}x_{11} + x_6 + x_7 + x_8x_{10} + x_9x_{11} + 1 \tag{20}$$

$$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} \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_9x_{11} \oplus x_3x_6x_{10}x_{11} \oplus x_3x_6 \oplus x_8x_9 \oplus x_{10}x_{11} \tag{21}$$

$$\mathfrak{f}(x_0, \ldots, x_{11}) = x_0x_1x_2x_3x_8 \oplus x_0x_1x_2x_3x_9 \oplus x_0x_1x_2x_4x_8 \oplus x_0x_1x_2x_4x_9 \oplus x_0x_1x_2x_5x_8 \oplus x_0x_1x_2x_5x_9 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2x_6x_8 \oplus x_0x_1x_2x_6x_9 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_2x_7x_8 \oplus x_0x_1x_2x_7x_9 \oplus x_0x_1x_2x_7 \oplus x_0x_1x_2x_8 \oplus x_0x_1x_2x_9 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_6x_8 \oplus x_0x_1x_3x_6x_9 \oplus x_0x_1x_3x_6 \oplus x_0x_1x_3x_8 \oplus x_0x_1x_3x_9 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_6x_8 \oplus x_0x_1x_4x_6x_9 \oplus x_0x_1x_4x_6 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4x_8 \oplus x_0x_1x_4x_9 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_6x_8 \oplus x_0x_1x_5x_6x_9 \oplus x_0x_1x_5x_6 \oplus x_0x_1x_5x_8 \oplus x_0x_1x_5x_9 \oplus x_0x_1x_6x_7x_8 \oplus x_0x_1x_6x_7x_9 \oplus x_0x_1x_6x_7 \oplus x_0x_1x_6x_8 \oplus x_0x_1x_6x_9 \oplus x_0x_1x_6 \oplus x_0x_1x_7x_8 \oplus x_0x_1x_7x_9 \oplus x_0x_1x_7 \oplus x_0x_1x_8 \oplus x_0x_1x_9 \oplus x_0x_2x_3x_4x_8 \oplus x_0x_2x_3x_4x_9 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_3x_6x_8 \oplus x_0x_2x_3x_6x_9 \oplus x_0x_2x_3x_6 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_3x_8 \oplus x_0x_2x_3x_9 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5x_8 \oplus x_0x_2x_4x_5x_9 \oplus x_0x_2x_4x_7x_8 \oplus x_0x_2x_4x_7x_9 \oplus x_0x_2x_4x_8 \oplus x_0x_2x_4x_9 \oplus x_0x_2x_4 \oplus x_0x_2x_5x_6x_8 \oplus x_0x_2x_5x_6x_9 \oplus x_0x_2x_5x_6 \oplus x_0x_2x_5x_7 \oplus x_0x_2x_5x_8 \oplus x_0x_2x_5x_9 \oplus x_0x_2x_6x_7x_8 \oplus x_0x_2x_6x_7x_9 \oplus x_0x_2x_6x_7 \oplus x_0x_2x_6x_8 \oplus$$

$$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 \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 \tag{22}$$