Design and Analysis of Bent Functions Using $\mathcal{M}$-Subspaces

Enes Pasalic, Alexandr Polujan, Sadmir Kudin, and Fengrong Zhang

***Abstract*— In this article, we provide the first systematic analysis of bent functions f on $\mathbb{F}_2^n$ in the Maiorana-McFarland class $\mathcal{M}$ regarding the origin and cardinality of their $\mathcal{M}$-*subspaces*, i.e., vector subspaces such that for any two elements a, b from this subspace, the second-order derivative D_aD_bf is the zero function on $\mathbb{F}_2^n$. By imposing restrictions on permutations π of $\mathbb{F}_2^{n/2}$, we specify the conditions so that Maiorana-McFarland bent functions $f(x,y) = x\cdot\pi(y)+h(y)$ admit a unique $\mathcal{M}$-subspace of dimension $n/2$. On the other hand, we show that permutations π with linear structures give rise to Maiorana-McFarland bent functions that do not have this property. In this way, we contribute to the classification of Maiorana-McFarland bent functions, since the number of $\mathcal{M}$-subspaces of a fixed dimension is invariant under equivalence. Additionally, we give several generic methods of specifying permutations π so that $f \in \mathcal{M}$ admits a unique $\mathcal{M}$-subspace. Most notably, using the knowledge about $\mathcal{M}$-subspaces, we show that using the bent 4-concatenation of four suitably chosen Maiorana-McFarland bent functions on $\mathbb{F}_2^{n-2}$, one can in a generic manner generate bent functions on $\mathbb{F}_2^n$ outside the completed Maiorana-McFarland class $\mathcal{M}^\#$ for any even $n \geq 8$. Remarkably, with our construction methods, it is possible to obtain inequivalent bent functions on $\mathbb{F}_2^8$ not stemming from the two primary classes, the partial spread class $\mathcal{PS}$ and $\mathcal{M}$. In this way, we contribute to a better understanding of the origin of bent functions in eight variables, since only a small fraction of about 2^{76} bent functions stems from $\mathcal{PS}$ and $\mathcal{M}$, whereas their total number on $\mathbb{F}_2^8$ is approximately 2^{106}.**

***Index Terms*— Bent function, Maiorana-McFarland class, partial spread class, equivalence, linear structure, permutation, bent 4-concatenation.**

I. Introduction

BENT functions are famous combinatorial objects introduced by Rothaus [23] in the mid-1960s that give rise to various discrete structures. Two known primary classes of bent functions are the Maiorana-McFarland class $\mathcal{M}$ and the Partial Spread class $\mathcal{PS}$, which were introduced in the 1970s in [10] and [17], respectively. On the other hand, the so-called secondary constructions (the reader is referred to [7], [8], [19]) use the known bent functions for the purpose of constructing new ones. However, only a few sporadic works on bent functions analyze the class inclusion properly, being more focused on specifying their explicit univariate/bivariate trace form or construction methods without being precise about whether these functions might belong to the $\mathcal{M}$ class, for instance. This eventually leads to a lack of understanding related to the classification and enumeration of bent functions. For instance, bent functions on $\mathbb{F}_2^8$ belonging to the main two primary classes (approximately 2^{76}) constitute just a small fraction of all bent functions in eight variables (approximately 2^{106}), see [15].

A pioneering work providing bent functions that provably do not belong to $\mathcal{M}$ or $\mathcal{PS}$, up to equivalence, is due to Carlet [5], who introduced two new classes of bent functions, the so-called $\mathcal{C}$ and $\mathcal{D}$ classes. In a recent series of articles [1], [2], [13], [14], [25], the authors specified explicit families of bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed $\mathcal{M}$ class. Nevertheless, apart from the class $\mathcal{D}_0$ of Carlet, these functions are defined on the variable space $n \geq 10$. Thus, the origin of bent functions outside $\mathcal{M}^\# \cup \mathcal{PS}^\#$ on $\mathbb{F}_2^8$ is still unclear. Moreover, the known secondary methods for constructing bent functions commonly employ bent functions on a smaller variable space. For example, in a recent article [20], the authors provided several methods of generating infinite families of bent functions outside $\mathcal{M}^\#$ using the so-called 4-concatenation $f = f_1||f_2||f_3||f_4$ of bent functions f_1, f_2, f_3, f_4 in n variables considered in [4]. Due to the design approach, namely employing bent functions outside $\mathcal{M}^\#$ on a smaller space, these results are significant only for $n \geq 10$ and do not explain the existence of bent functions outside the known primary classes when $n = 8$ since all bent functions in less than 8 variables are in $\mathcal{M}^\#$.

Dillon, in his thesis [10], proved that a given bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ belongs to the $\mathcal{M}^\#$ class if and only if $D_aD_bf(x) = 0$ for all $a, b \in V$ (and for all $x \in \mathbb{F}_2^n$), for at least one $n/2$-dimensional vector subspace V of $\mathbb{F}_2^n$ (see

Manuscript received 26 April 2023; revised 22 October 2023; accepted 30 December 2023. Date of publication 11 January 2024; date of current version 21 May 2024. The work of Enes Pasalic was supported in part by the Slovenian Research Agency under Grant P1-0404, Grant J1-1694, Grant N1-0159, Grant J1-2451, and Grant J1-4084. The work of Sadmir Kudin was supported in part by the Slovenian Research Agency under Grant P1-0404 and Grant J1-4084 and in part by the Young Researchers Grant. The work of Fengrong Zhang was supported in part by the Natural Science Foundation of China under Grant 62372346 and Grant 61972400, in part by the Fundamental Research Funds for the Central Universities under Grant XJS221503, and in part by the Youth Innovation Team of Shaanxi Universities. *(Corresponding author: Alexandr Polujan.)*

Enes Pasalic and Sadmir Kudin are with the FAMNIT and IAM, University of Primorska, 6000 Koper, Slovenia (e-mail: enes.pasalic6@gmail.com; sadmir.kudin@iam.upr.si).

Alexandr Polujan is with the Institute of Algebra and Geometry, Faculty of Mathematics, Otto von Guericke University Magdeburg, 39106 Magdeburg, Germany (e-mail: alexandr.polujan@ovgu.de).

Fengrong Zhang is with the School of Cyber Engineering, Xidian University, Xi'an 710071, China (e-mail: zhfl203@163.com).

Communicated by C. Carlet, Associate Editor for Sequences and Cryptography.

Digital Object Identifier 10.1109/TIT.2024.3352824

also Lemma 2 for details). Vector subspaces of $\mathbb{F}_2^n$ such that for any two elements a, b from the subspace, the second order derivative D_aD_bf is the zero function on $\mathbb{F}_2^n$, were called *$\mathcal{M}$-subspaces* in [22]. The algebraic properties of $\mathcal{M}$-subspaces attracted more attention only recently in a few works, e.g., in [12], [21], and [22].

The main aim of this article is to provide the first systematic investigation of $\mathcal{M}$-subspaces of Boolean bent functions, and using this knowledge, to specify generic construction methods of Boolean bent functions in n variables outside the $\mathcal{M}^\#$ class, for all even $n \geq 8$. Notably, we give a characterization of the bent functions on $\mathbb{F}_2^n$ in the $\mathcal{M}$ class, that have a unique $n/2$-dimensional $\mathcal{M}$-subspace $V = \mathbb{F}_2^{n/2} \times \{0_{n/2}\}$. We show that the property of a Maiorana-McFarland bent function $f(x, y) = x \cdot \pi(y) + h(y)$ to have a *unique $\mathcal{M}$-subspace* of dimension $n/2$ is, in many cases, completely determined by the choice of the permutation π. In the other direction, if a permutation π admits linear structures (implying that its components also do), then $f \in \mathcal{M}$ has at least two $\mathcal{M}$-subspaces of maximal dimension. This characterization not only contributes to the classification of Maiorana-McFarland bent functions, but also partially explains why permutations without linear structures have been efficiently used to specify functions in $\mathcal{C}$ and $\mathcal{D}$ outside $\mathcal{M}^\#$ in some recent works, e.g., [1], [2], [13], and [25]. More precisely, a modification of a bent function $f \in \mathcal{M}$ is easier performed if only one $\mathcal{M}$-subspace of maximal dimension needs to be deprived of this property by adding an indicator function. Using the obtained knowledge about $\mathcal{M}$-subspaces of Maiorana-McFarland bent functions, we provide several design methods of specifying bent functions f_1, f_2, f_3, f_4 on $\mathbb{F}_2^n$ such that the concatenation $f = f_1||f_2||f_3||f_4$ is bent on $\mathbb{F}_2^{n+2}$ and outside $\mathcal{M}^\#$, for all $n \geq 6$. Additionally, we indicate that certain instances of bent functions on $\mathbb{F}_2^8$, obtained with our approach, are outside the $\mathcal{PS}^\#$ class as well, which then contribute to a better understanding of the origin of bent functions in $n = 8$ variables. For a deeper background on bent functions, the reader is referred to the survey article in [8].

The rest of the paper is organized in the following way. In Subsection I-A we recall basic definitions related to Boolean functions, and in Subsection I-B we summarize the algebraic properties of bent 4-concatenation. In Section II, we investigate which classes of permutations π on $\mathbb{F}_2^m$ are suitable for the construction of Maiorana-McFarland bent functions of the form $(x, y) \in \mathbb{F}_2^m \times \mathbb{F}_2^m \mapsto x \cdot \pi(y)$ with several m-dimensional $\mathcal{M}$-subspaces. Particularly, in Subsections II-A and II-B, we show that certain quadratic permutations with linear structures, as well as quadratic permutations, lead to Maiorana-McFarland bent functions with several m-dimensional $\mathcal{M}$-subspaces. In Section III, we study the opposite question; namely, we investigate which classes of permutations π on $\mathbb{F}_2^m$ are suitable for the construction of Maiorana-McFarland bent functions of the form $(x, y) \in \mathbb{F}_2^m \times \mathbb{F}_2^m \mapsto x \cdot \pi(y) + h(y)$ with the unique m-dimensional $\mathcal{M}$-subspace $U = \mathbb{F}_2^m \times \{0_m\}$. In Subsection III-A, we introduce permutations with the (P_1) property as those permutations π on $\mathbb{F}_2^m$ for which $D_vD_w\pi \neq 0_m$, for all linearly independent $v, w \in \mathbb{F}_2^m$. Remarkably, we show that permutations π with this property guarantee that Maiorana-McFarland bent functions of the form $(x, y) \in \mathbb{F}_2^m \times \mathbb{F}_2^m \mapsto x \cdot \pi(y) + h(y)$ have a unique m-dimensional $\mathcal{M}$-subspace, independently of the choice of a Boolean function h on $\mathbb{F}_2^m$. The latter feature provides a variety of different Maiorana-McFarland bent functions with a unique $\mathcal{M}$-subspace of dimension m, even from a single permutation π with this property. In Subsection III-B, we consider permutations π on $\mathbb{F}_2^m$ for which $D_uD_v\pi = 0_m$, for any $u, v \in S$, where $1 \leq \dim(S) \leq m - 1$. Remarkably, we completely characterize such permutations π on $\mathbb{F}_2^m$ giving rise to bent functions $(x, y) \in \mathbb{F}_2^m \times \mathbb{F}_2^m \mapsto x \cdot \pi(y)$ with the unique m-dimensional $\mathcal{M}$-subspace, and refer to them as permutations with (P_2) property in the sequel. In Section IV, we give several explicit constructions of permutations with the (P_1) and (P_2) properties. In Section V, we provide several generic construction methods of bent functions outside the $\mathcal{M}^\#$ class using the bent 4-concatenation. First, in Subsection V-A, we describe the structure of $\mathcal{M}$-subspaces of maximal dimension when the bent 4-concatenation of four Maiorana-McFarland bent functions remains in $\mathcal{M}^\#$. Based on this characterization, we consider two different scenarios of concatenating Maiorana-McFarland bent functions which both lead to bent functions outside $\mathcal{M}^\#$. In Subsection V-B, we show that if Maiorana-McFarland bent functions on $\mathbb{F}_2^n$ do not share a common $\mathcal{M}$-subspace of dimension $n/2 - 1$, then their bent 4-concatenation is outside $\mathcal{M}^\#$. In subsection V-C, we show that even if Maiorana-McFarland bent functions on $\mathbb{F}_2^n$ share a unique $\mathcal{M}$-subspace of dimension $n/2$, then under certain technical conditions it is still possible that their bent 4-concatenation is outside $\mathcal{M}^\#$. Moreover, we indicate that with our approaches, it is possible to construct inequivalent bent functions on $\mathbb{F}_2^8$ outside $\mathcal{M}^\# \cup \mathcal{PS}^\#$. For this purpose, we propose an algorithm for testing the membership in the $\mathcal{PS}^\#$ class which is given in the appendix. In Section VI, we give some concluding remarks, list open problems, and outline potential research directions.

A. Preliminaries

The vector space $\mathbb{F}_2^n$ is the space of all n-tuples $x = (x_1, \ldots, x_n)$, where $x_i \in \mathbb{F}_2 = \{0, 1\}$. For $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_2^n$, the usual scalar (or dot) product over $\mathbb{F}_2$ is defined as $x \cdot y = x_1y_1 + \cdots + x_ny_n$. The Hamming weight of $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, denoted by $wt(x)$, is computed as $wt(x) = \sum_{i=1}^n x_i$. Throughout the paper, we denote by $0_n = (0, 0, \ldots, 0) \in \mathbb{F}_2^n$ the all-zero vector with n coordinates, and by $\mathbb{e}_k \in \mathbb{F}_2^n$ the k-th canonical basis vector. In certain cases, we endow $\mathbb{F}_2^n$ with the structure of the finite field $(\mathbb{F}_{2^n}, \cdot, +)$. An element $\alpha \in \mathbb{F}_{2^n}$ is said to be a *primitive element*, if it is a generator of the multiplicative group $\mathbb{F}_{2^n}^*$. The *absolute trace* $Tr\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ is given by $Tr(x) = \sum_{i=0}^{n-1} x^{2^i}$.

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 $\mathcal{B}_n$. It is well-known that any Boolean function $f \in \mathcal{B}_n$ can be uniquely represented by the *algebraic normal form (ANF)*, which is given by $f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} \lambda_u (\prod_{i=1}^n {x_i}^{u_i})$, where $x_i, \lambda_u \in \mathbb{F}_2$ and $u = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$. The *algebraic degree* of f, denoted by $\deg(f)$, is the maximum Hamming weight of $u \in \mathbb{F}_2^n$ for which $\lambda_u \neq 0$ in its ANF.

The *first order-derivative* of a function $f \in \mathcal{B}_n$, in the direction $a \in \mathbb{F}_2^n$, is the mapping $D_a f(x) = f(x+a) + f(x)$. Derivatives of higher orders are defined recursively using $a_1, \ldots, a_k \in \mathbb{F}_2^n$, so that the *k-th order derivative* of a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined by $D_{a_k} D_{a_{k-1}} \cdots D_{a_1} f(x) = D_{a_k}(D_{a_{k-1}} \cdots D_{a_1} f)(x)$. If some a_i are linearly dependent, then $D_{a_k} D_{a_{k-1}} \cdots D_{a_1} f(x) = 0$. For a vector subspace V of $\mathbb{F}_2^n$, we define $D_V f : \mathbb{F}_2^n \to \mathbb{F}_2$ by $D_V f(x) = \sum_{v \in V} f(x+v)$. An element $a \in \mathbb{F}_2^n$ is called a *linear structure* of $f \in \mathcal{B}_n$, if $f(x+a)+f(x) = const.$, for all $x \in \mathbb{F}_2^n$. We say that $f \in \mathcal{B}_n$ *has no linear structures*, if 0_n is the only linear structure of the function f.

For shortness of notation, we usually drop the involved variable which is especially true when using $D_a D_b \pi = 0_m$, for a permutation π over $\mathbb{F}_2^m$. This essentially means that the second-order derivative of π at directions $a, b \in \mathbb{F}_2^m$ is the zero function, for all Boolean coordinate functions $\pi_1, \ldots, \pi_m$ of π, hence $D_a D_b \pi_i(y) = 0$ for all $y \in \mathbb{F}_2^m$, where $\pi(y) = (\pi_1(y), \ldots, \pi_m(y))$.

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

$$\begin{aligned} W_f(a) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x} \quad \text{and} \\ (-1)^{f(x)} &= 2^{-n} \sum_{a \in \mathbb{F}_2^n} W_f(a)(-1)^{a\cdot x}. \end{aligned}$$

For even n, a function $f \in \mathcal{B}_n$ is called *bent* if $W_f(u) = \pm 2^{\frac{n}{2}}$, for all $u \in \mathbb{F}_2^n$. For a bent function $f \in \mathcal{B}_n$, the Boolean function $f^* \in \mathcal{B}_n$ defined by $W_f(u) = 2^{\frac{n}{2}}(-1)^{f^*(u)}$ for all $u \in \mathbb{F}_2^n$, is a bent function and is called the *dual* of f. Two Boolean functions $f, f' \in \mathcal{B}_n$ are called *extended-affine equivalent*, if there exists an affine permutation A of $\mathbb{F}_2^n$ and affine function $l \in \mathcal{B}_n$, such that $f \circ A + l = f'$. It is well known, that extended-affine (EA) equivalence preserves the bent property. In the sequel, when saying two Boolean functions are (in)equivalent, we always mean EA-equivalence, since this is the only type of equivalence we deal with in this article.

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

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

where π is a permutation on $\mathbb{F}_2^m$ and h is an arbitrary Boolean function on $\mathbb{F}_2^m$.

Definition 1: A class of bent functions $B_n \subset \mathcal{B}_n$ is *complete* if it is globally invariant under EA-equivalence. The *completed class*, denoted by $\mathcal{M}^\#$ in the case of the Maiorana-McFarland class $\mathcal{M}$, is the smallest possible complete class that contains the class under consideration.

With the following criterion of Dillon, one can show that a given Boolean bent function $f \in \mathcal{B}_n$ is (not) a member of the completed Maiorana-McFarland class.

Lemma 2 [10, p. 102]: Let $n = 2m$. A Boolean bent function $f \in \mathcal{B}_n$ belongs to $\mathcal{M}^\#$ if and only if there exists an m-dimensional linear subspace V of $\mathbb{F}_2^n$ such that, for any $a, b \in V$,

$$D_a D_b f(x) = f(x) + f(x+a) + f(x+b) + f(x+a+b) = 0,$$

for all $x \in \mathbb{F}_2^n$.

Following the terminology in [22], we introduce the $\mathcal{M}$-subspaces of Boolean (not necessarily bent) functions in the following way.

Definition 3: Let $f \in \mathcal{B}_n$ be a Boolean function. We call a vector subspace V of $\mathbb{F}_2^n$ an $\mathcal{M}$-subspace of f, if we have that $D_a D_b f = 0$, for any $a, b \in V$. We denote by $\mathcal{MS}_r(f)$ the collection of all r-dimensional $\mathcal{M}$-subspaces of f.

It is well known [7], that for a bent function $f \in \mathcal{B}_n$ the maximum possible dimension of an $\mathcal{M}$-subspace is $n/2$; bent functions achieving this bound with equality are exactly the bent functions in $\mathcal{M}^\#$ by Lemma 2. For every Maiorana-McFarland bent function $f(x, y) = x \cdot \pi(y) + h(y)$ on $\mathbb{F}_2^m \times \mathbb{F}_2^m$, the vector space $\mathbb{F}_2^m \times \{0_m\}$ is an $\mathcal{M}$-subspace of f, as observed by Dillon [10]. However, in general, this vector space $\mathbb{F}_2^m \times \{0_m\}$, which we refer to as *the canonical $\mathcal{M}$-subspace*, is not necessarily a unique $n/2$-dimensional $\mathcal{M}$-subspace of f. For instance, for a Maiorana-McFarland bent function f on $\mathbb{F}_2^m \times \mathbb{F}_2^m$, the number of its $\mathcal{M}$-subspaces of maximal dimension m is at most $\prod_{i=1}^m (2^i + 1)$. Moreover, the equality is attained if and only if $f \in \mathcal{B}_{2m}$ is quadratic, as it was deduced in [21] from [12, Theorem 2]. Finally, we note that in [22, Proposition 4.4] it was shown that the number of $\mathcal{M}$-subspaces of a fixed dimension k of a Boolean function $f \in \mathcal{B}_n$ is invariant under equivalence. Consequently, two bent functions with a different number of $\mathcal{M}$-subspaces of dimension $k \le n/2$ are inequivalent. One can determine all $\mathcal{M}$-subspaces of a Boolean function $f \in \mathcal{B}_n$, as described in [22, Algorithm 1].

We note that for vectorial functions, i.e., the mappings $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$, one can essentially extend the definitions related to differential properties (e.g., derivatives, linear structures and $\mathcal{M}$-subspaces) by simply replacing $f \in \mathcal{B}_n$ by $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ in the corresponding definitions. For $b \in \mathbb{F}_2^{m*}$, where $\mathbb{F}_2^{m*} = \mathbb{F}_2^m \setminus \{0_m\}$, the *component function* $F_b \in \mathcal{B}_n$ of $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is defined by $F_b(x) = b \cdot F(x)$ for all $x \in \mathbb{F}_2^n$, where $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is uniquely represented as a collection of Boolean functions $f_i \in \mathcal{B}_n$ in the form $F(x) = (f_1(x), \ldots, f_m(x))$. Notice that the algebraic degree of F is defined as $\deg(F) = \max_{b \in \mathbb{F}_2^{m*}} \deg(F_b)$. A function $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^m$ is called *almost perfect nonlinear (APN)* if, for all $a \in \mathbb{F}_2^{m*}$, $b \in \mathbb{F}_2^m$, the equation $F(x+a) + F(x) = b$ has 0 or 2 solutions $x \in \mathbb{F}_2^m$.

B. Bent 4-Concatenation and Its Algebraic Properties

In the following, we will be mainly interested in the design of bent functions $f \in \mathcal{B}_{n+2}$ from four bent functions $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$ using the *bent 4-concatenation* $f = f_1||f_2||f_3||f_4$, whose ANF is given by

$$\begin{aligned} f(x, y_1, y_2) = {} & f_1(x) + y_1(f_1 + f_3)(x) + y_2(f_1 + f_2)(x) \\ & + y_1 y_2(f_1 + f_2 + f_3 + f_4)(x). \qquad \text{(I.1)} \end{aligned}$$

From this expression, it is not difficult to see that $f_1(x) = f(x, 0, 0)$, $f_2(x) = f(x, 0, 1)$, $f_3(x) = f(x, 1, 0)$ and

$f_4(x) = f(x,1,1)$. Note that if $f_i \in \mathcal{B}_n$ are all bent, then the necessary and sufficient condition that $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is bent as well, is that the *dual bent condition* is satisfied [11], i.e., $f_1^* + f_2^* + f_3^* + f_4^* = 1$.

For the further analysis of the bent 4-concatenation $f = f_1||f_2||f_3||f_4$ in terms of the second-order derivatives, we derive in (I.2), shown at the bottom of the page, the expression for $D_aD_bf(x,y_1,y_2)$, where $a = (a', a_1, a_2)$, $b = (b', b_1, b_2)$, $a', b' \in \mathbb{F}_2^n$, $a_i, b_i \in \mathbb{F}_2$, and the Boolean function $f_{i_1\dots i_k} \in \mathcal{B}_n$ is defined by $f_{i_1\dots i_k} := f_{i_1} + \cdots + f_{i_k}$, for $1 \le i_1 < \ldots < i_k \le 4$.

In this context, the main design goal is to specify suitable $f_i \in \mathcal{B}_n$ so that $f \in \mathcal{B}_{n+2}$ is a bent function, and to ensure that f does not satisfy the $\mathcal{M}^\#$ class membership criterion of Dillon given in Lemma 2.

II. Bent Functions With More Than One $\mathcal{M}$-Subspace of Maximal Dimension

In this section, we derive sufficient conditions that $f(x,y) = x \cdot \pi(y) + h(y) \in \mathcal{B}_{2m}$ admits more than one m-dimensional $\mathcal{M}$-subspace. This feature is disadvantageous from the perspective of constructing bent functions $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{2m+2}$ outside $\mathcal{M}^\#$ from Maiorana-McFarland bent functions $f_i \in \mathcal{B}_{2m}$, since in this case, it is more difficult to ensure that the second-order derivatives of f do not vanish on any $(m+1)$-dimensional subspace of $\mathbb{F}_2^{2m+2}$. Essentially, this property is closely related to the choice of a permutation π on $\mathbb{F}_2^m$ which is then characterized by the presence of non-zero linear structures or by having "many" constant zero second-order derivatives.

A. Permutations With Linear Structures

First, we show that permutations with linear structures give rise to Maiorana-McFarland bent functions with more than one $\mathcal{M}$-subspace of maximal dimension.

Proposition 4: Let π be a permutation of $\mathbb{F}_2^m$ with a non-zero linear structure $s \in \mathbb{F}_2^m$, i.e., for some $v \in \mathbb{F}_2^m$ we have

$$D_s\pi(x) = \pi(x) + \pi(x+s) = v, \quad \text{for all } x \in \mathbb{F}_2^m,$$

and let $h : \mathbb{F}_2^m \to \mathbb{F}_2$ be an arbitrary Boolean function. Then, the function $f \colon \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ defined by

$$f(x,y) = x \cdot \pi(y) + h(y), \quad x, y \in \mathbb{F}_2^m,$$

has at least two m-dimensional $\mathcal{M}$-subspaces.

Proof: Clearly, the canonical $\mathcal{M}$-subspace $\mathbb{F}_2^m \times \{0_m\}$ is the first one. We will now construct another one of dimension m. Let $D_s\pi(y) = v \in \mathbb{F}_2^m$ and $W = \langle v \rangle^\perp \subset \mathbb{F}_2^m$. Also, assign $V = \langle W \times \{0_m\}, (0_m, s)\rangle$, with $s \neq 0_m$. For two different non-zero vectors $a = (a_1, a_2)$ and $b = (b_1, b_2)$ in V, we compute

$$\begin{aligned} D_aD_bf(x,y) =& x \cdot (D_{a_2}D_{b_2}\pi(y)) + a_1 \cdot D_{b_2}\pi(y+a_2) \\ &+ b_1 \cdot D_{a_2}\pi(y+b_2) + D_{a_2}D_{b_2}h(y). \end{aligned}$$

If $a_2 = b_2 = 0_m$, we immediately deduce that $D_{(a_1,a_2)}D_{(b_1,b_2)}f(x,y) = 0$. If $b_2 = s$ and $a_2 = 0_m$, we have

$$D_{(a_1,a_2)}D_{(b_1,b_2)}f(x,y) = a_1 \cdot D_s\pi(y) = a_1 \cdot v = 0,$$

because $a_1 \in W = \langle v \rangle^\perp$. This covers the other cases as well, since $D_aD_bf = D_bD_af = D_{a+b}D_bf$, and we conclude that V is another m-dimensional $\mathcal{M}$-subspace of f. □

However, the condition that permutation π of $\mathbb{F}_2^m$ has no linear structures does not imply that the only m-dimensional $\mathcal{M}$-subspace is $\mathbb{F}_2^m \times \{0_m\}$, as the following example shows.

Example 5: Let $m = 5$ and π be the permutation of $\mathbb{F}_2^m$ defined by its algebraic normal form in the following way:

$$\pi(y) = \begin{bmatrix} y_1 \\ y_2 \\ y_3 + y_1y_3 + y_1y_5 \\ y_1y_3 + y_2y_3 + y_4 \\ y_1y_3 + y_2y_4 + y_5 + y_1y_5 \end{bmatrix}^T. \tag{II.1}$$

It is not difficult to check, that the only linear structure of π is $s = 0_5$. However, the function $g(x,y) = x \cdot \pi(y)$ has exactly two 5-dimensional $\mathcal{M}$-subspaces: the canonical $\mathcal{M}$-subspace $\mathbb{F}_2^5 \times \{0_5\}$ as well as V, which is given by:

$$V = \left\langle \begin{matrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix} \right\rangle.$$

Note that for the permutation π defined in (II.1), there exist a lot of Boolean functions h on $\mathbb{F}_2^5$ such that by adding a Boolean function $h(y)$ on $\mathbb{F}_2^5$ to $g(x,y) = x \cdot \pi(y)$, one gets a bent function $f(x,y) = x \cdot \pi(y) + h(y)$ having only the canonical 5-dimensional $\mathcal{M}$-subspace. A concrete example of such a function is $h(y_1, \ldots, y_5) = y_3y_4y_5$.

B. Quadratic Permutations Inducing More Than One $\mathcal{M}$-Subspace of Maximal Dimension for $f \in \mathcal{M}$

In this subsection, we provide instances of quadratic permutations for which the function defined by $f(x,y) = x \cdot \pi(y)$ has more than one $\mathcal{M}$-subspace of maximal dimension. We will use the following two results from [14].

Lemma 6 [14]: Let $G : \mathbb{F}_2^m \to \mathbb{F}_2^t$ be a vectorial Boolean function. If there exists an $(m-k)$-dimensional subspace H of $\mathbb{F}_2^m$ such that $D_aD_bG = 0_t$ for all $a, b \in H$, then the algebraic degree of G is at most $k+1$.

$$\begin{aligned} D_aD_bf(x,y_1,y_2) = {}& D_{a'}D_{b'}f_1(x) + y_1D_{a'}D_{b'}f_{13}(x) + y_2D_{a'}D_{b'}f_{12}(x) + y_1y_2D_{a'}D_{b'}f_{1234}(x) \\ &+ a_1D_{b'}f_{13}(x+a') + b_1D_{a'}f_{13}(x+b') + a_2D_{b'}f_{12}(x+a') + b_2D_{a'}f_{12}(x+b') \\ &+ (a_1y_2 + a_2y_1 + a_1a_2)D_{b'}f_{1234}(x+a') + (b_1y_2 + b_2y_1 + b_1b_2)D_{a'}f_{1234}(x+b') \\ &+ (a_1b_2 + b_1a_2)f_{1234}(x+a'+b') \end{aligned} \tag{I.2}$$

Lemma 7 *[14]:* Let $\pi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ be a permutation such that there is a linear hyperplane V of $\mathbb{F}_2^m$, on which π is affine. Let $\mathbb{1}_V(x)$ be the affine Boolean function that defines V, that is, $\mathbb{1}_V(x) = 1$ if and only if $x \in V$. Then, $\mathbb{1}_V(x)$ or $\mathbb{1}_V(x) + 1$ is a component function of π.

Lemma 8: Let π be a permutation of $\mathbb{F}_2^m$, such that there exists an $(m-1)$-dimensional subspace $S \subset \mathbb{F}_2^m$ for which $D_a D_b \pi = 0_m$, for all $a, b \in S$. Then, π is at most quadratic and $\mathbb{1}_S(y)$ or $\mathbb{1}_S(y) + 1$ is a component function of π.

Proof: The fact that π is at most quadratic follows directly from Lemma 6. Let a, b be two arbitrary vectors from S. Since $D_a D_b \pi(y) = 0_m$, for all $y \in \mathbb{F}_2^m$, setting $y = 0_m$ we get:

$$\pi(a+b) + \pi(a) + \pi(b) + \pi(0_m) = 0_m.$$

Since $a, b \in S$ were arbitrary, we deduce that π is affine on the linear hyperplane S, and from Lemma 7 it follows that $\mathbb{1}_S(y)$ or $\mathbb{1}_S(y) + 1$ is a component function of π. □

Proposition 9: Let π be a permutation of $\mathbb{F}_2^m$, such that there exists an $(m-1)$-dimensional subspace $S \subset \mathbb{F}_2^m$ for which $D_a D_b \pi = 0_m$, for all $a, b \in S$. Let $f \colon \mathbb{F}_2^m \times \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ be the function defined by:

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

Then, f has at least two m-dimensional $\mathcal{M}$-subspaces.

Proof: It is obvious that $\mathbb{F}_2^m \times \{0_m\}$ is one m-dimensional $\mathcal{M}$-subspace for f. Let $\mathbb{1}_S : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ be the affine Boolean function that defines S, that is, $\mathbb{1}_S(y) = 1$ if and only if $y \in S$. From Lemma 8, we deduce that $\mathbb{1}_S(y)$ or $\mathbb{1}_S(y)+1$ is a component function of π. Let $c \in \mathbb{F}_2^m$ be such that $c \cdot \pi$ is equal to $\mathbb{1}_S$ or $\mathbb{1}_S + 1$. Let S' denote the subspace $S' = \{0_m\} \times S$, and let V be the m-dimensional subspace of $\mathbb{F}_2^{2m}$ defined by $V = \langle (c, 0_m), S' \rangle$. We will show that V is also an $\mathcal{M}$-subspace for f. If $v = (v_1, v_2)$ and $w = (w_1, w_2)$ are from V such that $v_1 = w_1 = 0_m$, that is $v, w \in S'$, then v_2, w_2 are in S, and

$$D_v D_w f(x, y) = x \cdot D_{v_2} D_{w_2} \pi(y) = 0.$$

Assume now that $v = (c, 0_m)$ and $w \in S'$. Then,

$$\begin{aligned} D_v D_w f(x, y) &= D_w(D_v f(x, y)) = D_w(c \cdot \pi(y)) \\ &= \mathbb{1}_S(y + w_2) + \mathbb{1}_S(y). \end{aligned}$$

Since w_2 is in S, then $y + w_2$ is in S if and only if y is in S, hence $\mathbb{1}_S(y + w_2) = \mathbb{1}_S(y)$, for all $y \in \mathbb{F}_2^m$. Consequently,

$$D_v D_w f(x, y) = \mathbb{1}_S(y + w_2) + \mathbb{1}_S(y) = 0.$$

We conclude that $D_v D_w f = 0$ for all $v, w \in V$, and hence that V is also an $\mathcal{M}$-subspace for f of dimension m. □

III. BENT FUNCTIONS IN $\mathcal{M}$ WITH THE UNIQUE CANONICAL $\mathcal{M}$-SUBSPACE

In this section, we characterize more precisely permutations that give rise to the bent functions $f(x, y) = x \cdot \pi(y) + h(y)$ with the unique canonical $\mathcal{M}$-subspace of maximal dimension, namely $\mathbb{F}_2^m \times \{0_m\}$. This is achieved through two useful properties called (P_1) and (P_2), which classify permutations with respect to $\mathcal{M}$-subspaces of its second-order derivatives $D_a D_b \pi$. In Section IV, we will provide some generic methods of specifying permutations satisfying these properties, including a generic class of APN permutations that necessarily satisfy the (P_1) property.

A. Bent Functions From Permutations Satisfying the (P_1) Property

In the following statement, we provide a sufficient condition on permutations π of $\mathbb{F}_2^m$, so that the subspace $\mathbb{F}_2^m \times \{0_m\}$ is the unique $\mathcal{M}$-subspace of $f(x, y) = x \cdot \pi(y) + h(y) \in \mathcal{B}_{2m}$ of dimension m, independently on the choice of a function h on $\mathbb{F}_2^m$.

Theorem 10: Let π be a permutation of $\mathbb{F}_2^m$ which has the following property:

$$D_v D_w \pi \neq 0_m, \quad \text{for all linearly independent } v, w \in \mathbb{F}_2^m. \tag{P_1}$$

Define $f \colon \mathbb{F}_2^m \times \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ by $f(x, y) = x \cdot \pi(y) + h(y)$, for all $x, y \in \mathbb{F}_2^m$, where $h \colon \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ is an arbitrary Boolean function. Then, the following hold:

1) Permutation π has no linear structures.
2) The vector space $V = \mathbb{F}_2^m \times \{0_m\}$ is the only m-dimensional $\mathcal{M}$-subspace of f.

Proof: 1) Assume that π has a non-zero linear structure $a \in \mathbb{F}_2^m$, i.e., for some $v \in \mathbb{F}_2^m$ it holds that $D_a \pi(y) = v$, for all $y \in \mathbb{F}_2^m$. Then, taking any $b \in \mathbb{F}_2^m \setminus \{0_m, a\}$, we get that $D_a D_b \pi = 0_m$, which contradicts the property (P_1).

2) Let V be an m-dimensional subspace of $\mathbb{F}_2^{2m}$ such that $D_a D_b f = 0$, for all $a, b \in V$. Define the linear mapping $L : V \rightarrow \mathbb{F}_2^m$ by $L(x, y) = y$, for all $(x, y) \in V$.

In general, denoting $a = (a_1, a_2)$ and $b = (b_1, b_2)$, we have

$$\begin{aligned} &D_{(a_1,a_2)} D_{(b_1,b_2)} f(x, y) = x \cdot (D_{a_2} D_{b_2} \pi(y)) + \\ &a_1 \cdot D_{b_2} \pi(y + a_2) + b_1 \cdot D_{a_2} \pi(y + b_2) + D_{a_2} D_{b_2} h(y). \end{aligned} \tag{III.1}$$

If $a_2, b_2 \in \mathbb{F}_2^m \setminus \{0_m\}$ and $a_2 \neq b_2$, then $D_{a_2} D_{b_2} \pi(y) \neq 0_m$. Hence, $D_{(a_1,a_2)} D_{(b_1,b_2)} f \neq 0$ because $x \cdot (D_{a_2} D_{b_2} \pi(y)) \neq 0$. Since for all $a, b \in V$ we have assumed that $D_a D_b f = 0$, we deduce that, for all $a, b \in V$, either $L(a) = a_2 = 0_m$, or $L(b) = b_2 = 0_m$, or $L(a) = a_2 = b_2 = L(b)$. This means that $\dim(Im(L)) \leq 1$. From the rank-nullity theorem, we get that $\dim(Ker(L)) \geq m - 1$. If $\dim(Ker(L)) = m$, then $V = \mathbb{F}_2^m \times \{0_m\}$.

Assume now that $\dim(Ker(L)) = m - 1$, and let $b = (b_1, b_2) \in V$ be such that $b_2 \neq 0_m$. For all $a = (a_1, a_2) \in Ker(L)$, we have $a_2 = 0_m$ and hence

$$D_{(a_1,a_2)} D_{(b_1,b_2)} f(x, y) = a_1 \cdot D_{b_2} \pi(y) = 0, \text{ for all } y \in \mathbb{F}_2^m. \tag{III.2}$$

Denote by S_b the subspace of $\mathbb{F}_2^m$ generated by $\{D_{b_2} \pi(y) \colon y \in \mathbb{F}_2^m\}$. Notice that, since π is a permutation and $b_2 \neq 0_m$, the function $D_{b_2} \pi(y) = \pi(y) + \pi(y + b_2)$ is never equal to 0_m, for any $y \in \mathbb{F}_2^m$. This means that if $\dim(S_b) = 1$, then $D_{b_2} \pi(y)$ is constant, which is in contradiction with the assumption that π has no linear structures.

This implies that $\dim(S_b) \geq 2$, and hence $\dim(S_b^{\perp}) \leq m-2$. From Eq. (III.2) we have that for every $a = (a_1, a_2) \in Ker(L)$ the vector a_1 is in $S_b^{\perp}$, hence $\{a_1 \colon a = (a_1, a_2) \in Ker(L)\} \subseteq S_b^{\perp}$. However,

$$\dim(\{a_1 \colon a = (a_1, a_2) \in Ker(L)\}) = \dim(Ker(L)) = m-1,$$

and this is a contradiction, because $\dim(S_b^{\perp}) \leq m-2$. This means that the case $\dim(Ker(L)) = m-1$ is not possible. Hence, the only m-dimensional subspace of $\mathbb{F}_2^{2m}$ such that $D_aD_bf = 0$, for all $a, b \in V$, is $V = \mathbb{F}_2^m \times \{0_m\}$. □

Imposing an additional condition on the permutation π, it is possible to completely specify the structure of $\mathcal{M}$-subspaces for this specific family of bent functions in $\mathcal{M}$.

Corollary 11: Let π be a permutation of $\mathbb{F}_2^m$ with the property (P_1) and such that $\gamma \cdot \pi$ has no linear structures for $\gamma \in \mathbb{F}_2^m \setminus \{0_m\}$. Let $f \colon \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ be the function defined by $f(x, y) = x \cdot \pi(y) + h(y)$, for all $x, y \in \mathbb{F}_2^m$, where $h : \mathbb{F}_2^m \to \mathbb{F}_2$ is an arbitrary Boolean function. If S is a subspace of $\mathbb{F}_2^m \times \mathbb{F}_2^m$ such that $\dim(S) > 1$ and $D_aD_bf = 0$, for all $a, b \in S$, then S is a subspace of $\mathbb{F}_2^m \times \{0_m\}$.

Proof: Notice that since π has the (P_1) property, then for any distinct nonzero elements $a, b \in \mathbb{F}_2^m$ we have $D_aD_b\pi(y) \neq 0_m$.

Then, denoting $a = (a_1, a_2)$, $b = (b_1, b_2) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$, the term $x \cdot (D_{a_2}D_{b_2}\pi(y))$ in Eq. (III.1) cannot be canceled unless $a_2 = 0_m$ or $b_2 = 0_m$, alternatively $a_2 = b_2 \neq 0_m$.

Assume first that $a, b \in S$, where $a_2 = 0_m$ and $b_2 \neq 0_m$ so that $S \not\subset \mathbb{F}_2^m \times \{0_m\}$. Eq. (III.1) then reduces to $D_{(a_1,a_2)}D_{(b_1,b_2)}f(x, y) = a_1 \cdot D_{b_2}\pi(y)$, which implies that $a_1 = 0_m$ and therefore $a = (a_1, a_2) = (0_m, 0_m)$, a contradiction. The case $a_2 = b_2 \neq 0_m$, implying also that $a_1 \neq b_1$ since $\dim(S) > 1$, gives $D_{(a_1,a_2)}D_{(b_1,b_2)}f(x, y) = (a_1+b_1) \cdot D_{a_2}\pi(y+a_2)$ which is nonzero by assumption, and consequently $D_{(a_1,a_2)}D_{(b_1,b_2)}f(x, y) \neq 0$. □

The following result specifies both the necessary and sufficient condition for a permutation π on $\mathbb{F}_2^m$, when the function $h(y) = \delta_0(y) = \prod_{i=1}^m (y_i + 1)$ is used to define $f(x, y) = x \cdot \pi(y) + h(y)$, so that f admits only the canonical $\mathcal{M}$-subspace $\mathbb{F}_2^m \times \{0_m\}$.

Proposition 12: Let π be a permutation of $\mathbb{F}_2^m$ with $\deg(\pi) < m-1$, and let $f \colon \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ be the function defined by

$$f(x, y) = x \cdot \pi(y) + \delta_0(y), \text{ for all } x, y \in \mathbb{F}_2^m.$$

Then, f has only one m-dimensional $\mathcal{M}$-subspace if and only if π has no linear structures.

Proof: If π has linear structures, then the fact that f has at least two $\mathcal{M}$-subspaces follows from Proposition 4.

Assume now that π has no linear structures. Let $V \neq \mathbb{F}_2^m \times \{0_m\}$ be an m-dimensional subspace of $\mathbb{F}_2^{2m}$ such that $D_aD_bf = 0$, for all $a, b \in V$. Define the linear mapping $L : V \to \mathbb{F}_2^m$ by $L(x, y) = y$, for all $(x, y) \in V$. Similarly to (III.1), replacing $h(y)$ by $\delta_0(y)$ and denoting $a = (a_1, a_2)$, $b = (b_1, b_2) \in V$, we have

$$\begin{aligned} &D_{(a_1,a_2)}D_{(b_1,b_2)}f(x, y) = x \cdot (D_{a_2}D_{b_2}\pi(y)) + \\ &a_1 \cdot D_{b_2}\pi(y+a_2) + b_1 \cdot D_{a_2}\pi(y+b_2) + D_{a_2}D_{b_2}\delta_0(y). \end{aligned} \tag{III.3}$$

Assume first that $\dim(Im(L)) \geq 2$. Let $(c_1, c_2), (d_1, d_2) \in V$ be such that c_2 and d_2 are two different nonzero elements in $\mathbb{F}_2^m$. Since $\deg(D_{c_2}D_{d_2}\delta_0(y)) = m-2$ and $\deg(\pi) < m-1$, from (III.3) we deduce that the algebraic degree of $D_{(c_1,c_2)}D_{(d_1,d_2)}f$ is $m-2$. Hence, $D_{(c_1,c_2)}D_{(d_1,d_2)}f \neq 0$, a contradiction.

If $\dim(Im(L)) = 1$, then $\dim(Ker(L)) = m-1$. Let $(a_1, a_2) \in V$ be such that $a_2 \neq 0_m$, and let $(b_1, 0_m) \in V$ be an arbitrary element in $Ker(L)$. Assuming that $D_aD_bf = 0$, for all $a, b \in V$, Eq. (III.3) implies

$$D_{(a_1,a_2)}D_{(b_1,0_m)}f(x, y) = b_1 \cdot D_{a_2}\pi(y) = 0,$$

for all $x, y \in \mathbb{F}_2^m$. This means that the subspace S_{a_2}, generated by the set $\{D_{a_2}\pi(y) \colon y \in \mathbb{F}_2^m\}$, is in the orthogonal complement of b_1, for every b_1 such that $(b_1, 0_m) \in Ker(L)$. Since $\dim(Ker(L)) = m-1$, we deduce that $\dim(S_{a_2}) = 1$. Also, π is a permutation and $a_2 \neq 0_m$, so $D_{a_2}\pi(y) \neq 0_m$, for all $y \in \mathbb{F}_2^m$. Hence, $\{D_{a_2}\pi(y) \colon y \in \mathbb{F}_2^m\} = \{v\}$ for some nonzero $v \in \mathbb{F}_2^m$, and this means that a_2 is a nonzero linear structure of π. However, this is a contradiction, since the assumption is that π has no nonzero linear structures.

We conclude that it has to be the case that $\dim(Im(L)) = 0$, and consequently that the only $\mathcal{M}$-subspace of f is $U = \mathbb{F}_2^m \times \{0_m\}$. □

B. Bent Functions From Permutations Having the $(P_{2)}$ Property

In this section, we show that permutations π on $\mathbb{F}_2^m$, for which $D_aD_b\pi(y) = 0_m$ for all $y \in \mathbb{F}_2^m$ and any $a, b \in S$, where S is an $(m-k)$-dimensional subspace of $\mathbb{F}_2^m$ (with $2 \leq k \leq m-1$), can still be used for the construction of Maiorana-McFarland bent functions on $\mathbb{F}_2^{2m}$ having a unique $\mathcal{M}$-subspace of maximal dimension m. We state this property more formally in the following definition.

Definition 13: Let π be a permutation of $\mathbb{F}_2^m$. Let S be a subspace of $\mathbb{F}_2^m$ of dimension $m-k$, with $1 \leq k \leq m-1$, such that $D_aD_b\pi = 0_m$ for all $a, b \in S$. Then, π satisfies the property (P_2) with respect to S if there does not exist a vector subspace V of $\mathbb{F}_2^m$ with $\dim(V) = k$ such that

$$\begin{aligned} &v \cdot D_a\pi(y) = 0; \text{ for all } a \in S, \text{ all } y \in \mathbb{F}_2^m, \\ &\text{and for all } v \in V. \end{aligned} \tag{P_2}$$

If π satisfies this property with respect to any linear subspace S of $\mathbb{F}_2^m$ of arbitrary dimension $1 \leq \dim(S) \leq m-1$, then we simply say that π satisfies (P_2).

Proposition 14: Let π be a non-affine permutation of $\mathbb{F}_2^m$ and $f(x, y) = x \cdot \pi(y)$ be a bent function on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ in $\mathcal{M}$. Then, the permutation π has the property (P_2) if and only if the only m-dimensional $\mathcal{M}$-subspace of f is $\mathbb{F}_2^m \times \{0_m\}$.

Proof: Assume first that the permutation π has the property (P_2). We will prove that the only m-dimensional $\mathcal{M}$-subspace of f is $\mathbb{F}_2^m \times \{0_m\}$. Assume on contrary, that there exists an m-dimensional $\mathcal{M}$-subspace of f different from $\mathbb{F}_2^m \times \{0_m\}$, and denote one such subspace by V. Let

$L\colon V \longrightarrow \mathbb{F}_2^m$ be the linear mapping defined by $L(x,y)=y$, for all $(x,y)\in V$. Let $a=(a_1,a_2)$, $b=(b_1,b_2)\in V$.

If $\dim(Im(L))=m$, using our assumption that V is an $\mathcal{M}$-subspace of f, we have

$$\begin{aligned} &D_{(a_1,a_2)}D_{(b_1,b_2)}f(x,y)=x\cdot(D_{a_2}D_{b_2}\pi(y))\\ &+a_1\cdot D_{b_2}\pi(y+a_2)+b_1\cdot D_{a_2}\pi(y+b_2)=0, \qquad \text{(III.4)}\end{aligned}$$

for all $(x,y)\in\mathbb{F}_2^m\times\mathbb{F}_2^m$,

implying that $D_{a_2}D_{b_2}\pi=0_m$, for all $a_2,b_2\in Im(L)=\mathbb{F}_2^m$. This would imply that π is affine, which is a contradiction.

If $Im(L))=\{0_m\}$, then $V=\mathbb{F}_2^m\times\{0_m\}$, which is also a contradiction. Hence, $\dim(Im(L))=m-k$, for some $k\in\{1,\dots,m-1\}$. For any $a_2,b_2\in Im(L)$, from (III.4) we get $D_{a_2}D_{b_2}\pi=0_m$. Set $U=\{u\colon(u,0_m)\in V\}$. For any $u\in U$, and any $(a_1,a_2)\in V$, we have $D_{(u,0_m)}D_{(a_1,a_2)}f=0$, hence from (III.4) we get $u\cdot D_{a_2}\pi=0$, i.e., for any $u\in U$ and any $a_2\in Im(L)$ we have $u\cdot D_{a_2}\pi=0$. However, from the rank-nullity theorem, we know that $\dim(U)=k$ since $\dim(Im(L))=m-k$. Thus, we deduce that π does not satisfy the property (P_2) with respect to the subspace $Im(L)$, which is a contradiction. Hence, the only m-dimensional $\mathcal{M}$-subspace of f is $\mathbb{F}_2^m\times\{0_m\}$.

Assume now that the only m-dimensional $\mathcal{M}$-subspace of f is $\mathbb{F}_2^m\times\{0_m\}$, and that there is a subspace S of $\mathbb{F}_2^m$ with $\dim(S)=m-k$, $k\in\{1,\dots,m-1\}$ and linearly independent $u_1,\dots,u_k\in\mathbb{F}_2^m$ such that $D_aD_b\pi=0_m$ and $u_i\cdot D_c\pi=0$, for all $a,b,c\in S$ and $i=1,\dots,k$. Set $V=\langle(u_1,0_m),\dots,(u_k,0_m),\{0_m\}\times S\rangle$. Since $k\le m-1$, V is not equal to $\mathbb{F}_2^m\times\{0_m\}$, and from (III.4) we deduce that $D_{(a_1,a_2)}D_{(b_1,b_2)}f=0$, for all $(a_1,a_2),(b_1,b_2)\in V$. That is, V is an m-dimensional $\mathcal{M}$-subspace of f different from $\mathbb{F}_2^m\times\{0_m\}$, which is a contradiction. We conclude that if the only m-dimensional $\mathcal{M}$-subspace of f is $\mathbb{F}_2^m\times\{0_m\}$, then π satisfies the property (P_2). □

Remark 15: For instance, the permutation π on $\mathbb{F}_2^5$ from Example 5 does not satisfy the conditions in Proposition 14. For this π and $S=\langle(0,0,1,0,0),(0,0,0,1,0),(0,0,0,0,1)\rangle$, we have $\dim(S)=m-2=3$ and one can verify that $D_aD_b\pi=0_5$ for any $a,b\in S$. Furthermore, the vectors $v_1=(1,0,0,0,0)$ and $v_2=(0,1,0,0,0)$ then build $V=\langle v_1,v_2\rangle$ for which $v_i\cdot D_a\pi(y)=0$, for any choice of $a\in S$.

Remark 16: 1. Note that the property (P_1) implies (P_2), but not vice versa.

2. As shown in [3], there exist 75 affine inequivalent quadratic permutations π of $\mathbb{F}_2^5$. Among them, 34 permutations give rise to bent functions $(x,y)\mapsto x\cdot\pi(y)$ with the unique canonical $\mathcal{M}$-subspace. With respect to the properties (P_1), (P_2), they are distributed as follows:

- 2 permutations have the property (P_1), note that these permutations are APN;
- 32 permutations have the property (P_2) (but not (P_1)).
  - For 28 of them there exist a subspace S_i of $\mathbb{F}_2^m$ of dimension $m-3=2$, s.t. $D_aD_b\pi_i=0_5$ for all $a,b\in S_i$. An example of such a permutation π_1 and a subspace S_1 is given by:

$$\pi_1(y)=\begin{bmatrix} y_1\\ y_2+y_1y_2+y_1y_4\\ y_1y_2+y_3+y_2y_4\\ y_2y_3+y_4+y_1y_4+y_2y_4+y_1y_5\\ y_1y_2+y_3y_4+y_5+y_1y_5\end{bmatrix}^T \quad\text{and}$$

$$S_1=\left\langle\begin{matrix}0&0&0&1&0\\0&0&0&0&1\end{matrix}\right\rangle.$$

  - For the remaining 4 permutations, the maximum dimension of S_i s.t. $D_aD_b\pi_i=0_5$ for all $a,b\in S_i$ is equal to $(m-2)=3$. An example of such a permutation π_2 and a subspace S_2 is given by:

$$\pi_2(y)=\begin{bmatrix} y_1\\ y_2+y_1y_2+y_1y_3\\ y_3+y_1y_3+y_1y_5\\ y_1y_2+y_4+y_1y_4\\ y_2y_3+y_1y_4+y_5+y_1y_5\end{bmatrix}^T \quad\text{and}$$

$$S_2=\left\langle\begin{matrix}0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{matrix}\right\rangle.$$

IV. Constructing Permutations With the (P_1) or (P_2) Property

The main aim of this section is to specify certain classes of permutations on $\mathbb{F}_2^m$ satisfying the (P_1) or (P_2) property, and thus to provide constructions of Maiorana-McFarland bent functions in $2m$ variables, with the unique m-dimensional $\mathcal{M}$-subspace, namely $\mathbb{F}_2^m\times\{0_m\}$.

A. APN and APN-Like Permutations

In the following remark, we indicate that APN permutations have the property (P_1). Hence, they can be used for the construction of Maiorana-McFarland bent functions with the unique canonical $\mathcal{M}$-subspace of maximal dimension.

Remark 17: Recall that a function $F\colon\mathbb{F}_2^m\to\mathbb{F}_2^m$ is called *almost perfect nonlinear (APN)* if, for all $a\in\mathbb{F}_2^m\setminus\{0_m\}$ and all $b\in\mathbb{F}_2^m$, the equation $F(x+a)+F(x)=b$ has 0 or 2 solutions $x\in\mathbb{F}_2^m$. Using the same notation as in [16] and [18], for $n\ge 2$, we define the set of all 2-dimensional flats in $\mathbb{F}_2^m$ as follows:

$$\begin{aligned}\mathcal{F}_m=\{\{x_1,x_2,x_3,x_4\}\mid x_1+x_2+x_3+x_4=0_m \text{ and}\\ x_1,x_2,x_3,x_4\in\mathbb{F}_2^m \text{ are distinct}\}.\end{aligned}$$

It is well-known, that a function $F\colon\mathbb{F}_2^m\to\mathbb{F}_2^m$ is APN if and only if for each $\{x_1,x_2,x_3,x_4\}\in\mathcal{F}_m$, it holds that

$$F(x_1)+F(x_2)+F(x_3)+F(x_4)\neq 0_m.$$

Namely, the summation of F over each 2-dimensional flat is non-vanishing. For a function $F\colon\mathbb{F}_2^m\to\mathbb{F}_2^m$, define the set of *vanishing flats* with respect to F as

$$\begin{aligned}\mathcal{VF}_{m,F}=\{\{x_1,x_2,x_3,x_4\}\in\mathcal{F}_m\mid\\ F(x_1)+F(x_2)+F(x_3)+F(x_4)=0_m\}.\end{aligned}$$

With this notation, F is APN on $\mathbb{F}_2^m$ if and only if $\mathcal{VF}_{m,F} = \varnothing$. Therefore, any permutation π of $\mathbb{F}_2^m$, which is APN, satisfies the condition (P_1). For instance, all power APN functions $x \mapsto x^d$ are permutations of $\mathbb{F}_2^m$ for m odd, as shown by Dobbertin, for the proof we refer to [7].

Note that if a function π on $\mathbb{F}_2^m$ is quadratic, then $D_aD_b\pi(y) = const. \in \mathbb{F}_2^m$, for all $a, b \in \mathbb{F}_2^m$. In this way, with the "vanishing flats" characterization of APN functions, we deduce the following characterization of quadratic permutations with the (P_1) property.

Corollary 18: A quadratic permutation π of $\mathbb{F}_2^m$ has the (P_1) property if and only if π is a quadratic APN permutation of $\mathbb{F}_2^m$.

Example 19: Using representatives of equivalence classes of bent functions in six variables [23], one can check with a computer algebra system that every bent function in $n = 6$ variables with the unique 3-dimensional $\mathcal{M}$-subspace is equivalent to a bent function of the form $f(x, y) = Tr(xy^3)$, for $x, y \in \mathbb{F}_{2^3}$. In this case, $y \mapsto y^3$ is an APN permutation of $\mathbb{F}_{2^3}$.

Further, we indicate that the following family of quadratic *APN-like permutations*, i.e., non-APN monomial permutations of the form $\pi(y) = y^{2^t+1}$, whose vanishing flats were analyzed in [16], have the (P_2) property. In this way, they can be used for constructing bent functions in $\mathcal{M}$ having a unique $\mathcal{M}$-subspace of maximal dimension. The following characterization of linear structures of the components of permutation monomials given in [9] (stated only for the binary quadratic case) is useful for our purpose.

Theorem 20 [9]: Let $\delta \in \mathbb{F}_{2^m}$ and $1 \le s \le 2^m - 2$ be such that $f(x) = Tr(\delta x^s)$ is not the zero function on $\mathbb{F}_2^m$. When $wt(s) = 2$, the function f has a linear structure if and only if $s = 2^j(2^i + 1)$, where $0 \le i, j \le m - 1$, $i \notin \{0, m/2\}$.

In this case, $\alpha \in \mathbb{F}_{2^m}$ is a linear structure of f if and only if it satisfies $(\delta^{2^{m-j}}\alpha^{2^i+1})^{2^i-1} + 1 = 0$. More exactly, the space of linear structures Λ of f is as follows. Denote $\sigma = \gcd(m, 2i)$. Then, $\Lambda = \{0\}$ if δ is not a $(2^i + 1)$-th power in $\mathbb{F}_{2^m}$. Otherwise, if $\delta = \beta^{2^j(2^i+1)}$ for some $\beta \in \mathbb{F}_{2^m}$, it holds that $\Lambda = \beta^{-1}\mathbb{F}_{2^\sigma}$.

Proposition 21: Let $\pi(y) = y^{2^t+1}$ for $y \in \mathbb{F}_{2^m}$, where $s = \gcd(t, m) = 2$, $m = 2r$ and $r \ge 3$ is odd. Then, π is a permutation and it has the property (P_2).

Proof: From [24], it is known that π is a permutation. To prove that π has the property (P_2), let S be a vector subspace of $\mathbb{F}_{2^m}$, $1 \le \dim(S) \le m - 1$, such that $D_aD_b\pi(y) = 0$, for all $a, b \in S$.

First, assume that $1 \le \dim(S) \le 2$, and let $a \in S \setminus \{0\}$. Let $u_1, \ldots, u_4$ be any 4 linearly independent elements in $\mathbb{F}_{2^m}$. From Theorem 20, we deduce that the space of linear structures of $Tr(\delta y^{2^t+1})$ is $\beta^{-1}\mathbb{F}_{2^2}$,

where β is such that $\delta = \beta^{2^t+1}$. This means that the space of linear structures of $Tr(u_iy^{2^t+1})$ is $\beta_i^{-1}\mathbb{F}_{2^2}$, where $u_i = \beta_i^{2^t+1}$, for $i = 1, \ldots, 4$. Notice that $\beta_1^{-1}, \beta_2^{-1}, \beta_3^{-1}, \beta_4^{-1}$ are different nonzero elements of $\mathbb{F}_{2^m}$, because $u_1, \ldots, u_4$ are linearly independent. Since $a \in \mathbb{F}_{2^m}^*$, there exists some $i_0 \in \{1, \ldots, 4\}$, such that $a \notin \beta_{i_0}^{-1}\mathbb{F}_{2^2}$, (otherwise, we would have $\beta_i^{-1} = \beta_j^{-1}$, for some different $i, j \in \{1, \ldots, 4\}$). Then, since $\beta_{i_0}^{-1}\mathbb{F}_{2^2}$ is the space of linear structures of $Tr(u_{i_0}y^{2^t+1})$, we have that $D_a(Tr(u_{i_0}y^{2^t+1}))$ is not constant. Since $u_1, \ldots, u_4$ were arbitrary linearly independent elements from $\mathbb{F}_{2^m}$, we deduce that there do not exist linearly independent $u_1, \ldots, u_4 \in \mathbb{F}_{2^m}$ for which $Tr(u_iD_a\pi) = D_a(Tr(u_i\pi)) = 0$, for all $i = 1, \ldots, 4$. That is, because $4 \le m - 2 < m - 1$, the permutation π has the property (P_2) with respect to the subspace S.

Assume now that $\dim(S) = t$, where $3 \le t \le m - 1$, and assume that there exist $u_1, \ldots, u_{m-t} \in \mathbb{F}_{2^m}$ such that $Tr(u_iD_a\pi) = D_a(Tr(u_i\pi)) = 0$, for all $a \in S$ and all $i = 1, \ldots, m - t$. From Theorem 20, we have that the space of linear structures of $Tr(u_iy^{2^t+1})$ is $\beta_i^{-1}\mathbb{F}_{2^2}$, where $u_i = \beta_i^{2^t+1}$, for $i = 1, \ldots, m - t$. Since $\dim(S) \ge 3$, there exists $a \in S$ such that $a \ne \beta_1^{-1}\mathbb{F}_{2^2}$. This means that $a \in S$ is not in the space of linear structures of $Tr(u_1y^{2^t+1})$, hence $D_a(Tr(u_1y^{2^t+1}))$ is not constant, which is in contradiction with our assumption $D_a(Tr(u_1\pi)) = 0$. □

B. Piecewise Permutations Having the (P_1) Property

Now, we provide a secondary construction of permutations with the (P_1) property. In this way, we obtain infinite families of permutations with the (P_1) property in all dimensions. We also indicate that permutations with the (P_1) property are not necessarily APN, see Remark 24.

Proposition 22: Let σ_1 and σ_2 be two permutations of $\mathbb{F}_2^m$ such that $D_uD_v\sigma_1 \ne D_uD_v\sigma_2$, for any distinct elements $u, v \in \mathbb{F}_2^{m*}$. Define the function $\pi\colon \mathbb{F}_2^{m+1} \to \mathbb{F}_2^{m+1}$ by

$$\pi(y, y_{m+1}) = (\sigma_1(y) + y_{m+1}(\sigma_1(y) + \sigma_2(y)), y_{m+1}),$$

for all $y \in \mathbb{F}_2^m, y_{m+1} \in \mathbb{F}_2$. Then, π is a permutation of $\mathbb{F}_2^{m+1}$ such that $D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi \ne 0_{m+1}$ for any two different vectors $(a, a_{m+1}), (b, b_{m+1}) \in \mathbb{F}_2^{m+1*}$, that is, π satisfies the (P_1) property.

Proof: Since $\pi(y, 0) = (\sigma_1(y), 0)$ and $\pi(y, 1) = (\sigma_2(y), 1)$ and since σ_1 and σ_2 are permutations, π is a permutation as well.

Take two linearly independent vectors (a, a_{m+1}) and $(b, b_{m+1}) \in \mathbb{F}_2^{m+1}$, where $a, b \in \mathbb{F}_2^m$ and $a_{m+1}, b_{m+1} \in \mathbb{F}_2$.

1) Assume first that $a_{m+1} = b_{m+1} = 0$. Then,

$$\begin{aligned}&D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y, y_{m+1}) = \\ &(D_aD_b\sigma_1(y) + y_{m+1}(D_aD_b\sigma_1(y) + D_aD_b\sigma_2(y)), 0).\end{aligned}$$

Since (a, a_{m+1}) and (b, b_{m+1}) are linearly independent and $a_{m+1} = b_{m+1} = 0$, the vectors a and b are linearly independent. If $D_aD_b\sigma_1(y) \ne 0_m$, then $D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y, 0) = (D_aD_b\sigma_1(y), 0) \ne 0_{m+1}$, hence $D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y, y_{m+1}) \ne 0_{m+1}$. If $D_aD_b\sigma_1(y) = 0_m$, then, since from the assumption $D_aD_b\sigma_2(y) \ne D_aD_b\sigma_1(y) = 0_m$, we have that

$$D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y, 1) = (D_aD_b\sigma_2(y), 0) \ne 0_{m+1}.$$

Hence, $D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y, y_{m+1}) \ne 0_{m+1}$. We conclude that in any case, when $a_{m+1} = b_{m+1} = 0$, we have $D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y, y_{m+1}) \ne 0_{m+1}$.

2) Now assume that $a_{m+1}+b_{m+1}=1$. W.l.o.g, we assume that $b_{m+1}=1$ and $a_{m+1}=0$. Computing the second-order derivative of π, we get

$$\begin{aligned}&D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y,y_{m+1}) = D_{(b,1)}(D_a\sigma_1(y)\\&+y_{m+1}(D_a\sigma_1(y)+D_a\sigma_2(y)),0)\\&=(D_aD_b\sigma_1(y)+y_{m+1}(D_aD_b\sigma_1(y)+D_aD_b\sigma_2(y))\\&+D_a\sigma_1(y+b)+D_a\sigma_2(y+b),0),\end{aligned}$$

for all $y\in\mathbb{F}_2^m, y_{m+1}\in\mathbb{F}_2$. Setting $y_{m+1}=0$, we have

$$\begin{aligned}&D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y,0)=\\&(D_aD_b\sigma_1(y)+D_a\sigma_1(y+b)+D_a\sigma_2(y+b),0).\end{aligned}$$

If $D_aD_b\sigma_1(y)+D_a\sigma_1(y+b)+D_a\sigma_2(y+b)\neq 0_m$, we deduce that $D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y,0)\neq 0_{m+1}$, hence $D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y,y_{m+1})\neq 0_{m+1}$. If however, $D_aD_b\sigma_1(y)+D_a\sigma_1(y+b)+D_a\sigma_2(y+b)=0_m$, then we compute

$$D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y,1)=(D_aD_b\sigma_1(y)+D_aD_b\sigma_2(y),0).$$

From the assumption $D_aD_b\sigma_2(y)\neq D_aD_b\sigma_1(y)$, we have $D_aD_b\sigma_2(y)+D_aD_b\sigma_1(y)\neq 0_m$, hence $D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y,1)\neq 0_{m+1}$, and consequently $D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y,y_{m+1})\neq 0_{m+1}$.

3) Finally, we have the case $a_{m+1}=b_{m+1}=1$. Since

$$\begin{aligned}&D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y,y_{m+1})=\\&D_{(a+b,a_{m+1}+b_{m+1})}D_{(b,b_{m+1})}\pi(y,y_{m+1}),\end{aligned}$$

from the case 2) we have that

$$D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y,y_{m+1})\neq 0_{m+1}.$$

We deduce that $D_{(a,a_{m+1})}D_{(b,b_{m+1})}\pi(y,y_{m+1})\neq 0_{m+1}$, what concludes the proof. □

Corollary 23: Let σ be a permutation of $\mathbb{F}_2^m$ such that $D_V\sigma\neq 0_m$ for all 2-dimensional subspaces V of $\mathbb{F}_2^m$, thus satisfying the (P_1) property. Define the function $\pi\colon\mathbb{F}_2^{m+1}\to\mathbb{F}_2^{m+1}$ by

$$\pi(y,y_{m+1})=(y+y_{m+1}(\sigma(y)+y),y_{m+1}), \qquad \text{(IV.1)}$$

for all $y\in\mathbb{F}_2^m, y_{m+1}\in\mathbb{F}_2$. Then, π is a permutation of $\mathbb{F}_2^{m+1}$ such that $D_W\pi\neq 0_{m+1}$ for all two dimensional subspaces W of $\mathbb{F}_2^{m+1}$, thus it satisfies the (P_1) property.

Proof: Set $\sigma_1(y)=y$ and $\sigma_2(y)=\sigma(y)$, for all $y\in\mathbb{F}_2^m$. Then, $D_V\sigma_1(y)=0_m\neq D_V\sigma_2(y)$, for all two dimensional subspaces V of $\mathbb{F}_2^m$. The result then follows from Proposition 22. □

Note that, with the same assumptions as in Corollary 23, using Proposition 22 and setting $\sigma_1(y)=\sigma(y)$ and $\sigma_2(y)=y$, we can deduce in the same way that

$$\pi'(y,y_{m+1})=(\sigma(y)+y_{m+1}(\sigma(y)+y),y_{m+1})$$

is also a permutation such that $D_W\pi'\neq 0_{m+1}$, for all two dimensional subspaces W of $\mathbb{F}_2^{m+1}$.

In the following remark, we indicate that the APN-ness of permutations π on $\mathbb{F}_2^m$ with the (P_1) property, plays a very important role for $\mathcal{M}$-subspaces for bent functions in $\mathcal{M}$.

Remark 24: Let σ be a permutation on $\mathbb{F}_2^m$ satisfying the property (P_1). Define the permutation $\pi\colon\mathbb{F}_2^{m+1}\to\mathbb{F}_2^{m+1}$, as in Corollary 23, by

$$\pi(y,y_{m+1})=(y+y_{m+1}(\sigma(y)+y),y_{m+1}),$$

for all $y\in\mathbb{F}_2^m, y_{m+1}\in\mathbb{F}_2$. Clearly, the permutation π is not APN, since the last coordinate is linear, see for instance [6, Proposition 13]. Define the function $f\colon\mathbb{F}_2^{2m+2}\to\mathbb{F}_2$ by

$$f(x,x_{m+1},y,y_{m+1})=(x,x_{m+1})\cdot\pi(y,y_{m+1}),$$

for all $x,y\in\mathbb{F}_2^m$ and $x_{m+1},y_{m+1}\in\mathbb{F}_2$. From Corollary 23 and Theorem 10, we deduce that π has the property (P_1), and $\mathbb{F}_2^{m+1}\times\{0_{m+1}\}$ is the unique $\mathcal{M}$-subspace of f.

Now, define $a_1=\mathbb{e}_{m+1}\in\mathbb{F}_2^{m+1}, a_2=0_{m+1}\in\mathbb{F}_2^{m+1}$ and $b_1=0_{m+1}\in\mathbb{F}_2^{m+1}$, $b_2=(b,0)\in\mathbb{F}_2^{m+1}$, where b is a nonzero vector in $\mathbb{F}_2^m$. From (III.1), we have

$$\begin{aligned}&D_{(a_1,a_2)}D_{(b_1,b_2)}f(x,x_{m+1},y,y_{m+1})\\&=(x,x_{m+1})\cdot D_{a_2}D_{b_2}\pi(y,y_{m+1})\\&+a_1\cdot D_{b_2}\pi((y,y_{m+1})+a_2)+b_1\cdot D_{a_2}\pi((y,y_{m+1})+b_2)\\&=\mathbb{e}_{m+1}\cdot D_{(b,0)}\pi(y,y_{m+1})\\&=\mathbb{e}_{m+1}\cdot(b+y_{m+1}(D_b\sigma(y)+b),0)=0.\end{aligned}$$

However, $\dim(\langle(a_1,a_2),(b_1,b_2)\rangle)=2$, and since $b_2=(b,0)\neq 0_{m+1}$ it is not a subspace of $\mathbb{F}_2^{m+1}\times\{0_{m+1}\}$. This means that not every permutation π with the (P_1) property defines a bent function $(x,y)\mapsto x\cdot\pi(y)$ with the vanishing behavior as in Corollary 11.

The problem of preserving the (P_2) property for the class of permutations defined by (IV.1) appears to be harder. One can eventually show that the (P_2) property for π is inherited from σ for some particular subspaces, whereas it remains an open problem to show that π fully satisfies the (P_2) property when σ does. Notice that, as indicated in Remark 16, permutations satisfying the (P_2) property stand for the majority among quadratic permutations over $\mathbb{F}_2^5$, for which the associated bent function $f(x,y)=x\cdot\pi(y)+h(y)$ only admits the unique canonical $\mathcal{M}$-subspace of maximal dimension.

Open Problem 1: Find more constructions of permutations with the (P_2) property.

V. Generic Methods of Constructing Bent Functions Outside $\mathcal{M}^\#$

In this section, we provide a theoretical analysis regarding $\mathcal{M}$-subspaces of f with respect to the bent 4-concatenation $f=f_1||f_2||f_3||f_4$. Based on this analysis, we consequently provide two generic methods of constructing bent functions outside $\mathcal{M}^\#$, for even $n\geq 8$. Our first approach is based on the concatenation of bent functions $f_1,f_2,f_3,f_4\in\mathcal{B}_n$ that *do not share any $\mathcal{M}$-subspace of dimension $n/2-1$*, i.e, $\bigcap_{i=1}^4\mathcal{MS}_{n/2-1}(f_i)=\varnothing$. Our second approach is based on the concatenation of bent functions $f_1,f_2,f_3,f_4\in\mathcal{B}_n$ that *share a unique $\mathcal{M}$-subspace of dimension $n/2$*, i.e, $|\bigcap_{i=1}^4\mathcal{MS}_{n/2}(f_i)|=1$. Finally, using our algorithm for checking the membership in the completed partial spread class $\mathcal{PS}^\#$ (given in the appendix), we demonstrate that with our approaches it is possible to construct inequivalent bent functions in $\mathcal{B}_8$ outside $\mathcal{M}^\#\cup\mathcal{PS}^\#$.

A. Possible $\mathcal{M}$-Subspaces for the Bent 4-Concatenation

The following result is crucial in understanding the structural properties of bent functions in $\mathcal{M}^{\#}$, in terms of 4-concatenation. Notice that when considering $f = f_1||f_2||f_3||f_4$, we do not assume that f_i are bent functions.

Proposition 25: Let $f_1, \ldots, f_4$ be four Boolean functions in n variables, not necessarily bent, such that $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is a bent function in $\mathcal{M}^{\#}$. Let W be an $\mathcal{M}$-subspace of f of maximal dimension $(n/2+1)$. Then, there is an $(n/2-1)$-dimensional subspace V of $\mathbb{F}_2^n$ such that:

1) $V \times \{(0,0)\}$ is a subspace of W,
2) V is an $\mathcal{M}$-subspace of f_i, for all $i = 1, \ldots, 4$.

Proof: Let W be an $\mathcal{M}$-subspace of f of dimension $(n/2+1)$ (we know that it exists since f is in $\mathcal{M}^{\#}$). We have

$$\dim(W \cap (\mathbb{F}_2^n \times \{(0,0)\})) = \dim(W) + \dim(\mathbb{F}_2^n \times \{(0,0)\}) - \dim(\langle W, \mathbb{F}_2^n \times \{(0,0)\}\rangle).$$

Because $\dim(\langle W, \mathbb{F}_2^n \times \{(0,0)\}\rangle) \leq n+2$, we have

$$\dim(W \cap (\mathbb{F}_2^n \times \{(0,0)\})) \geq (n/2+1) + n - (n+2) = n/2-1.$$

Hence, there is an $(n/2-1)$-dimensional subspace V of $\mathbb{F}_2^n$ such that $V \times \{(0,0)\}$ is a subspace of W. Let a and b be two arbitrary vectors from V. Then, $(a,0,0)$ and $(b,0,0)$ are in W, so $D_{(a,0,0)}D_{(b,0,0)}f = 0$. Using (I.2), we compute:

$$\begin{aligned} &D_{(a,0,0)}D_{(b,0,0)}f(x,z_1,z_2) = D_aD_bf_1(x) + \\ &z_1(D_aD_b(f_1+f_2)(x)) + z_2(D_aD_b(f_1+f_3)(x)) + \\ &z_1z_2(D_aD_b(f_1+f_2+f_3+f_4)(x)) = 0, \end{aligned} \tag{V.1}$$

for all $(x, z_1, z_2) \in \mathbb{F}_2^{n+2}$. From this, we deduce that

$$\begin{aligned} &D_aD_bf_1(x) = D_aD_b(f_1+f_2)(x) = D_aD_b(f_1+f_3)(x) = \\ &D_aD_b(f_1+f_2+f_3+f_4)(x) = 0, \end{aligned} \tag{V.2}$$

for all $x \in \mathbb{F}_2^n$, and consequently, that $D_aD_bf_1 = D_aD_bf_2 = D_aD_bf_3 = D_aD_bf_4 = 0$. Since a and b were two arbitrary elements from V, this completes the proof. □

The following important result describes the form of $\mathcal{M}$-subspaces of maximal dimension for $f = f_1||f_2||f_3||f_4$, where $f_i \in \mathcal{B}_{2m}$ are bent functions in $\mathcal{M}$. Notice that when f_i share the same unique canonical $\mathcal{M}$-subspace $U = \mathbb{F}_2^m \times \{0_m\}$, which we address later in this section, is a special case of this result.

Proposition 26: Let $f_1, \ldots, f_4$ be bent functions in $\mathcal{B}_n$, $n = 2m$, and assume that for at least one $k \in \{1, \ldots, 4\}$ the function f_k admits the unique (canonical) m-dimensional $\mathcal{M}$-subspace $U = \mathbb{F}_2^m \times \{0_m\}$. Then, any $(n/2+1)$-dimensional $\mathcal{M}$-subspace W of $f = f_1||f_2||f_3||f_4$ must have one of the following forms:

i) $W = \langle U \times (0,0), (a,b,c_1,c_2)\rangle$, where $a, b \in \mathbb{F}_2^m$, $c_1, c_2 \in \mathbb{F}_2$ and $(c_1, c_2) \neq 0_2$.
ii) $W = \langle V \times (0,0), (a,b,c_1,c_2), (u,v,d_1,d_2)\rangle$, where $V \subset \mathbb{F}_2^m$, $\dim(V) = n/2-1$; $a, b, u, v \in \mathbb{F}_2^m$, $c_1, c_2, d_1, d_2 \in \mathbb{F}_2$, and $(c_1, c_2) \neq 0_2, (d_1, d_2) \neq 0_2, (c_1, c_2) \neq (d_1, d_2)$.

Proof: Let W be an $(n/2+1)$-dimensional $\mathcal{M}$-subspace of f. Similarly as in the proof of Proposition 25, we have

$$\dim(W \cap (\mathbb{F}_2^n \times \{(0,0)\})) \geq n/2-1.$$

If $\dim(W \cap (\mathbb{F}_2^n \times \{(0,0)\})) = n/2-1$, then W is of the form stated in ii). By assumption, there exists at least one $k \in \{1, \ldots, 4\}$ such that the only m-dimensional $\mathcal{M}$-subspace of f_k is $U = \mathbb{F}_2^m \times \{0_m\}$. Hence, if $\dim(W \cap (\mathbb{F}_2^n \times \{(0,0)\})) = n/2$, then W is of the form stated in i). Since $f_i \in \mathcal{B}_n$ are bent, the maximum dimension of an $\mathcal{M}$-subspace of any f_i is $n/2$. Hence, the case $\dim(W \cap (\mathbb{F}_2^n \times \{(0,0)\})) = n/2+1$ is not possible because it would imply that there is an $(n/2+1)$-dimensional $\mathcal{M}$-subspace of f_i. □

B. Concatenating f_i on $\mathbb{F}_2^n$ With No Common $(n/2-1)$-Dimensional $\mathcal{M}$-Subspace

In this section, we provide some generic construction methods of bent functions outside the $\mathcal{M}^{\#}$ class, which are easily derived from Proposition 25.

The following results is fundamental for the design of bent functions outside $\mathcal{M}^{\#}$ based on the 4-concatenation, and most notably the ingredient functions are not necessarily bent (hence they can be disjoint spectra semi-bent functions or suitable five-valued spectra functions).

Theorem 27: Let $f_1, \ldots, f_4 \in \mathcal{B}_n$ be four Boolean functions, not necessarily bent, such that $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is a bent function. Assume that there is no $(n/2-1)$-dimensional subspace V of $\mathbb{F}_2^n$ such that $D_aD_bf_i = 0$, for all $a, b \in V$ and all $i \in \{1, \ldots, 4\}$. Then, $f \in \mathcal{B}_{n+2}$ is a bent function outside $\mathcal{M}^{\#}$.

Proof: The result is a direct consequence of Proposition 25. □

With this result, we can now demonstrate how one can construct bent functions on $\mathbb{F}_2^8$ outside the $\mathcal{M}^{\#}$ class from four bent functions on $\mathbb{F}_2^6$ (necessarily) in $\mathcal{M}^{\#}$. We emphasize that this is the first attempt in the literature towards our better understanding of the origin of bent functions on $\mathbb{F}_2^8$.

Example 28: Let π be a quadratic APN permutation of $\mathbb{F}_2^3$, which, in turn, has the (P_1) property:

$$\pi(y_1,y_2,y_3) = \begin{bmatrix} y_2y_3 + y_1 + y_2 + y_3 \\ y_1y_2 + y_1y_3 + y_2 \\ y_1y_2 + y_3 \end{bmatrix}^T. \tag{V.3}$$

Define four bent functions $f_1, \ldots, f_4 \in \mathcal{B}_6$, which all belong to $\mathcal{M}^{\#}$, as follows:

$$\begin{aligned} f_1(x,y) &= x \cdot y + \delta_0(x), \quad f_2(x,y) = x \cdot \pi(y) + \delta_0(x), \\ f_3(x,y) &= x \cdot y, \quad f_4(x,y) = x \cdot \pi(y) + 1. \end{aligned} \tag{V.4}$$

One can check that for the bent functions defined in (V.4), the dual bent condition is satisfied. Therefore, $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_8$ is bent. Its ANF is given by

$$\begin{aligned} f(z) = {} & 1 + z_1 + z_2 + z_1z_2 + z_3 + z_1z_3 + z_2z_3 + \\ & z_1z_2z_3 + z_3z_4 + z_1z_5 + z_2z_6 + z_7 + z_1z_7 + z_2z_7 + \\ & z_1z_2z_7 + z_3z_7 + z_1z_3z_7 + z_2z_3z_7 + z_1z_2z_3z_7 + z_1z_4z_8 + \\ & z_2z_4z_5z_8 + z_1z_6z_8 + z_1z_4z_6z_8 + z_2z_5z_6z_8 + z_3z_5z_6z_8 + \\ & z_7z_8. \end{aligned}$$

Finally, we confirm that the functions $f_1, \ldots, f_4$ satisfy the conditions of Theorem 27. Due to the APN-ness of π, we have that $D_aD_bf_4 = 0$ if and only if 2-dimensional subspace $\langle a, b\rangle$ is a subspace of $S = \mathbb{F}_2^3 \times$

$\{0_3\}$. On the other hand, $D_aD_bf_1 \neq 0$ for any two dimensional subspace $\langle a, b\rangle$ of $S = \mathbb{F}_2^3 \times \{0_3\}$. In this way, we conclude that $f \notin \mathcal{M}^\#$. Using Algorithm .1 in the appendix, we also confirm that $f \notin \mathcal{PS}^\#$. Thus, we have that $f \notin (\mathcal{M}^\# \cup \mathcal{PS}^\#)$.

Another generic method of constructing bent functions outside $\mathcal{M}^\#$, where nonlinear permutations are used to specify f_i, is given in the following example.

Example 29: Let π be the APN permutation defined by (V.3) and σ be another APN permutation of $\mathbb{F}_2^3$, given by its algebraic normal form as:

$$\sigma(x) = \begin{bmatrix} x_1 + x_2 + x_3 + x_2x_3 \\ x_2 + x_3 + x_1x_3 \\ x_2 + x_1x_2 + x_1x_3 \end{bmatrix}^T.$$

Let $h_1, h_2 \in \mathcal{B}_3$ be arbitrary Boolean functions. Define four bent functions $f_i \in \mathcal{B}_6$, for $i = 1, \ldots, 4$, as in (V.5) below, which all belong to $\mathcal{M}^\#$. Then, the function $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_8$ is a bent function outside $\mathcal{M}^\#$ (independently of the choice of h_1 and h_2). This follows from Theorem 27, by noting that f_1 and f_3 do not share any 2-dimensional subspace V for which $D_aD_bf_1 = D_aD_bf_3 = 0$, for $a, b \in V$. Indeed, the only 3-dimensional $\mathcal{M}$-subspace of f_1 and f_3 are $\mathbb{F}_2^3 \times \{0_3\}$ and $\{0_3\} \times \mathbb{F}_2^3$, respectively. Due to the APN property of π and σ, $\mathcal{M}$-subspaces of smaller dimension for f_1 and f_3 are subspaces of $\mathbb{F}_2^3 \times \{0_3\}$ and $\{0_3\} \times \mathbb{F}_2^3$, respectively, and cannot be shared.

Now, set $h_1(y) = y_1y_2y_3 + y_1y_2 + y_1y_3 + y_2y_3 + y_1 + y_2 + y_3$ and $h_2(y) = y_1y_2y_3 + y_1y_3 + y_2y_3 + 1$. Then, the algebraic normal form of $f = f_1||f_2||f_3||f_4$ is given as follows:

$$f(z) = z_4 + z_1z_4 + z_5 + z_1z_5 + z_2z_5 + z_4z_5 + z_2z_4z_5 + z_3z_4z_5 + z_6 + z_1z_6 + z_3z_6 + z_4z_6 + z_2z_4z_6 + z_5z_6 + z_1z_5z_6 + z_4z_5z_6 + z_1z_3z_7 + z_2z_3z_7 + z_1z_2z_3z_7 + z_4z_7 + z_2z_4z_7 + z_3z_4z_7 + z_2z_3z_4z_7 + z_5z_7 + z_1z_5z_7 + z_1z_2z_5z_7 + z_1z_3z_5z_7 + z_4z_5z_7 + z_2z_4z_5z_7 + z_3z_4z_5z_7 + z_6z_7 + z_1z_6z_7 + z_1z_2z_6z_7 + z_4z_6z_7 + z_2z_4z_6z_7 + z_5z_6z_7 + z_1z_5z_6z_7 + z_4z_5z_6z_7 + z_7z_8.$$

Using Algorithm .1 in the appendix, we confirm that $f \notin \mathcal{PS}^\#$, and hence $f \notin (\mathcal{M}^\# \cup \mathcal{PS}^\#)$.

Now, we provide one generic method of specifying $f = f_1||f_2||f_3||f_4$ outside $\mathcal{M}^\#$, where f_i are bent functions within or outside $\mathcal{M}^\#$. The dual bent condition $f_1^* + f_2^* + f_3^* + f_4^* = 1$ can be satisfied if we simply select, e.g., $f_1 = f_2$ and $f_4 = 1 + f_3$, where $f_i \in \mathcal{B}_n$ are bent.

Theorem 30: Let π be a permutation of $\mathbb{F}_2^m$, where $m \geq 4$, having the property (P_1). Let σ a permutation of $\mathbb{F}_2^m$ such that there is no $(m-2)$-dimensional subspace S of $\mathbb{F}_2^m$ for which $D_aD_b\sigma = 0_m$, for all $a, b \in S$. Let $h_1, h_2 \in \mathcal{B}_m$ be two arbitrary Boolean functions. Let $f_i \in \mathcal{B}_{2m}$ with $i = 1, \ldots, 4$, be the functions defined by

$$\begin{aligned} f_1(x,y) &= f_2(x,y) = x \cdot \pi(y) + h_1(y), \\ f_3(x,y) &= f_4(x,y) + 1 = y \cdot \sigma(x) + h_2(x), \end{aligned} \tag{V.5}$$

for all $x, y \in \mathbb{F}_2^m$. Then, $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{2m+2}$ is a bent function outside the $\mathcal{M}^\#$ class.

Proof: Due to the relationship between f_i, we have $f_1^* + f_2^* + f_3^* + f_4^* = 1$, thus f is bent. Assume on the contrary, that f is in the $\mathcal{M}^\#$ class. From Proposition 25, there exists an $(m-1)$-dimensional subspace V of $\mathbb{F}_2^{2m}$ such that $D_aD_bf_i = 0$, for all $a, b \in V$, and all $i = 1, \ldots, 4$.

Define the mapping $L\colon V \to \mathbb{F}_2^m$ by $L(x, y) = y$, for all $(x, y) \in \mathbb{F}_2^{2m}$. Similarly as in the proof of Theorem 10, if $a = (a_1, a_2)$, $b = (b_1, b_2) \in V$ are such that $\dim(\langle a_2, b_2\rangle) = 2$, i.e., if $\dim(Im(L)) \geq 2$, then $x \cdot (D_{a_2}D_{b_2}\pi(y)) \neq 0$ because π has the property (P_1). This implies that $D_aD_bf_1 \neq 0$, which contradicts our assumption that $D_aD_bf_1 = 0$, for all $a, b \in V$. We deduce that $\dim(Im(L)) \leq 1$. From the rank-nullity theorem, we have that $\dim(Ker(L)) \geq m-2$ since $\dim(V) = m-1$. For $a = (a_1, a_2)$, $b = (b_1, b_2)$ in $Ker(L)$, we have $a_2 = b_2 = 0_m$, using the fact that $Ker(L) \subseteq V$ and the assumption that $D_aD_bf_3 = 0$, for all $a, b \in V$. We then get

$$D_aD_bf_3(x, y) = y \cdot D_{a_1}D_{b_1}\sigma(x) + D_{a_1}D_{b_1}h_2(x) = 0,$$

for all $x, y \in \mathbb{F}_2^m$. Consequently, $D_{a_1}D_{b_1}\sigma(x) = 0_m$. Since $\dim(Ker(L)) \geq m-2$, this means that there is a subspace S of $\mathbb{F}_2^m$ of dimension $m-2$ such that $D_{a_1}D_{b_1}\sigma = 0$, for all $a_1, b_1 \in S$. However, this is in contradiction with the assumption on σ. Hence, f is outside $\mathcal{M}^\#$. □

Remark 31: The condition that $m \geq 4$ in Theorem 30 is necessary to avoid the case of considering the nonexistence of $(m-2)$-dimensional subspaces S for which $D_aD_b\sigma = 0_m$, for all $a, b \in S$. When $m = 3$, any 1-dimensional subspace $S = \langle a\rangle$ will satisfy the condition $D_aD_b\sigma = 0_m$, since $b = 0_m$.

Remark 32: It is important to notice that the condition that any $(n/2-1)$-dimensional $\mathcal{M}$-subspace V is not shared between f_i in Theorem 27 is only sufficient, and there exist functions f_i that do share the unique canonical $\mathcal{M}$-subspace $U = \mathbb{F}_2^{n/2} \times \{0_{n/2}\}$ even though $f = f_1||f_2||f_3||f_4$ is outside $\mathcal{M}^\#$, which is discussed in Section V-C.

We notice that bent functions on $\mathbb{F}_2^n$ outside $\mathcal{M}^\#$ do not admit $n/2$-dimensional $\mathcal{M}$-subspaces, and furthermore it was observed in [20] that many instances of bent functions in $\mathcal{PS} \setminus \mathcal{M}^\#$ only have $\mathcal{M}$-subspaces of dimension strictly less than $n/2-1$.

Corollary 33: Let f_1 be an arbitrary Maiorana-McFarland bent function on $\mathbb{F}_2^n$, and let f_3 be a bent function on $\mathbb{F}_2^n$ that only admits $\mathcal{M}$-subspaces of dimension strictly less than $n/2-1$. Set $f_2 = f_1$ and $f_4 = 1 + f_3$. Then, $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is a bent function outside $\mathcal{M}^\#$.

Open Problem 2: The non-sharing property provides a theoretical framework for bent 4-concatenation, however finding such f_i (also satisfying the dual bent condition) appears to be difficult. We leave as an open problem a specification of such quadruples in a generic manner.

C. Concatenating f_i That Share a Unique $\mathcal{M}$-Subspace of Dimension $n/2$

Proposition 26 provides the possibility to analyze the class exclusion of bent functions on $\mathbb{F}_2^n$ (with $n = 2m$) from $\mathcal{M}^\#$, by only considering the subspaces W of dimension $n/2+1$ of the specific form. In particular, this general case is not covered by Proposition 25, when f_i defined on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ share the unique $\mathcal{M}$-subspace $U = \mathbb{F}_2^m \times \{0_m\}$. The analysis can be divided into two cases, namely considering the case that the only common $(m-1)$-dimensional $\mathcal{M}$-subspaces U' for all f_i are such that $U' \subset U$, or alternatively, when there are some $(m-1)$-dimensional $\mathcal{M}$-subspaces U' such that $U' \not\subset U$. The main problem in the analysis of $f = f_1||f_2||f_3||f_4$ is the fact that f_1+f_2, f_1+f_3 or $f_1+f_2+f_3+f_4$ are not bent functions in general, and therefore the analysis of second-order derivatives in (I.2) becomes harder.

Theorem 34: Let $f_1, \dots, f_4$ be four bent functions on $\mathbb{F}_2^n$, with $n = 2m$, such that $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is a bent function. Assume that for any common $(n/2-1)$-dimensional $\mathcal{M}$-subspace $V \subset \mathbb{F}_2^n$ of all f_i, for any $u \in \mathbb{F}_2^n$

there exist $v^{(1)}, v^{(2)}, v^{(3)} \in V$ such that the following three conditions hold simultaneously

1) $D_{v^{(1)}} f_1(x) + D_{v^{(1)}} f_2(x+u) \neq 0$, *or* $D_{v^{(1)}} f_3(x) + D_{v^{(1)}} f_4(x+u) \neq 0$,
2) $D_{v^{(2)}} f_1(x) + D_{v^{(2)}} f_3(x+u) \neq 0$, *or* $D_{v^{(2)}} f_2(x) + D_{v^{(2)}} f_4(x+u) \neq 0$,
3) $D_{v^{(3)}} f_2(x) + D_{v^{(3)}} f_3(x+u) \neq 0$, *or* $D_{v^{(3)}} f_1(x) + D_{v^{(3)}} f_4(x+u) \neq 0$.

Then, the function f is outside $\mathcal{M}^\#$.

Proof: Assume that the function f is in $\mathcal{M}^\#$ and let $W \subset \mathbb{F}_2^{n+2}$ be an $(n/2+1)$-dimensional $\mathcal{M}$-subspace of f. From Proposition 25, we know that there is a common $(n/2-1)$-dimensional $\mathcal{M}$-subspace $V \subset \mathbb{F}_2^n$ of all f_i, $i = 1, \dots, 4$, and furthermore $V \times \{(0,0)\}$ is a subset of W. Moreover, from Proposition 26, we know that there exists a vector $w \in W$ of the form $w = (u, d_1, d_2)$, for some $u \in \mathbb{F}_2^n$ and $(d_1, d_2) \in \mathbb{F}_2^2 \setminus \{(0,0)\}$.

Assume first that $(d_1, d_2) = (0,1)$. For any $v \in V$, we have $D_{(v,0,0)} f = D_v f_1 || D_v f_2 || D_v f_3 || D_v f_4$. Further, we compute $D_{(u,d_1,d_2)} D_{(v,0,0)} f = g_1||g_2||g_3||g_4$, where the functions g_i are given by

$$\begin{aligned} g_1(x) &= D_v f_1(x) + D_v f_2(x+u), \\ g_2(x) &= D_v f_2(x) + D_v f_1(x+u), \\ g_3(x) &= D_v f_3(x) + D_v f_4(x+u), \\ g_4(x) &= D_v f_4(x) + D_v f_3(x+u). \end{aligned} \tag{V.6}$$

For instance, $g_1(x) = D_{(u,d_1,d_2)} D_{(v,0,0)} f(x,0,0)$ and after setting $(d_1, d_2) = (0,1)$ we get

$$\begin{aligned} g_1(x) &= D_{(v,0,0)} f(x,0,0) + D_{(v,0,0)} f(x+u,0,1) \\ &= D_v f_1(x) + D_v f_2(x+u). \end{aligned} \tag{V.7}$$

From the condition 1), we deduce that there exists $v \in V$ such that at least one of the functions g_1 and g_3 is nonzero. From this, we deduce that $D_{(u,d_1,d_2)} D_{(v,0,0)} f \neq 0$, which is a contradiction because (u, d_1, d_2) and $(v,0,0)$ are in W. Similarly, the cases $(d_1, d_2) = (1,0)$ and $(d_1, d_2) = (1,1)$ also lead to a contradiction by using the conditions 2) and 3), respectively.

Thus, the assumption that $f \in \mathcal{M}^\#$ leads to a contradiction, hence we conclude that f is outside $\mathcal{M}^\#$. □

Corollary 35: Let $f_1, \dots, f_4$ be four bent functions on $\mathbb{F}_2^n$, with $n = 2m$, satisfying the following conditions:

a) $f_1, \dots, f_4$ belong to $\mathcal{M}^\#$ and share a unique $\mathcal{M}$-subspace U of dimension m;
b) $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is a bent function.

Let V be an $(n/2-1)$-dimensional subspace of $\mathbb{F}_2^n$ such that $D_a D_b f_i = 0$, for all $a, b \in V$, and all $i = 1, \dots, 4$. If for any $u \in \mathbb{F}_2^n$ and any such $V \subset \mathbb{F}_2^n$, there exist $v^{(1)}, v^{(2)}, v^{(3)} \in V$ such that the following three conditions hold simultaneously

1. $D_{v^{(1)}} f_1(x) + D_{v^{(1)}} f_2(x+u) \neq 0$,
2. $D_{v^{(2)}} f_1(x) + D_{v^{(2)}} f_3(x+u) \neq 0$,
3. $D_{v^{(3)}} f_2(x) + D_{v^{(3)}} f_3(x+u) \neq 0$,

then f is outside $\mathcal{M}^\#$.

In the special case when $f_4 = f_1 + f_2 + f_3$, we have the following corollary.

Corollary 36: With the same notation as in Theorem 34, we assume that $f_4 = f_1 + f_2 + f_3$ and $V \subset U$ for any V of dimension $\dim(V) = n/2 - 1$, where U is a unique $\mathcal{M}$-subspace of dimension $n/2$ shared by all f_i. Then, the following set of sufficient conditions ensures that $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ does not belong to $\mathcal{M}^\#$:
There exists a subspace $S \subset U$, with $\dim(S) = 2$, such that

$$\begin{aligned} D_v f_1(x) + D_v f_2(x+u) \neq 0; \\ D_v f_1(x) + D_v f_3(x+u) \neq 0; \\ D_v f_2(x) + D_v f_3(x+u) \neq 0, \end{aligned} \tag{V.8}$$

for any $v \in S \setminus \{0_n\}$ and any $u \in \mathbb{F}_2^n$.

Proof: If we always have $V \subset U$ for any V, then $\dim(V \cap S) \geq 1$. This follows from the fact that $\dim(S) = 2$, $\dim(V) = n/2-1$, and furthermore $S \subset U$ and $V \subset U$. Thus, for any V of dimension $n/2-1$, we always can find at least one nonzero vector $v' \in V \cap S$. Then, setting $v := v'$ in (V.8), we conclude that f is outside $\mathcal{M}^\#$ using Theorem 34. □

Example 37: Consider the following Boolean bent functions $f_1, \dots, f_4 \in \mathcal{B}_6$, which all belong to $\mathcal{M}^\#$ and are given by their algebraic normal form as follows:

$$\begin{aligned} f_1(x,y) &= x_1(y_2 + y_3 + y_1y_3) + x_2(y_1 + y_1y_3 + y_2y_3) \\ &\quad + x_3(y_1y_2 + y_3) + y_1 + y_2 + y_3, \\ f_2(x,y) &= x_1(y_2 + y_1y_2 + y_1y_3) \\ &\quad + x_2(y_1 + y_2 + y_1y_2 + y_2y_3) \\ &\quad + x_3(y_1 + y_1y_2 + y_3 + y_1y_3 + y_2y_3) + y_3 + 1, \\ f_3(x,y) &= x_1(y_1+y_2+y_1y_2+y_2y_3) + x_2(y_2 + y_3 + y_1y_3) \\ &\quad + x_3(y_1 + y_2 + y_3 + y_2y_3) \\ &\quad + y_2 + y_3 + 1, \\ f_4(x,y) &= x_1(y_1 + y_2 + y_3 + y_2y_3) + x_2(y_1y_2 + y_3) \\ &\quad + x_3(y_2 + y_3 + y_1y_3) + y_1 + 1. \end{aligned} \tag{V.9}$$

One can check that for the bent functions defined by (V.9), the dual bent condition is satisfied. In this way, we have that $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_8$ is bent. Its ANF is given by

$$\begin{aligned} f(z) = {} & z_4 + z_2z_4 + z_5 + z_1z_5 + z_3z_4z_5 + z_6 + z_1z_6 + \\ & z_3z_6 + z_1z_4z_6 + z_2z_4z_6 + z_2z_5z_6 + z_7 + z_4z_7 + z_1z_4z_7 + \\ & z_2z_4z_7 + z_3z_4z_7 + z_2z_5z_7 + z_3z_5z_7 + z_1z_4z_5z_7 + \\ & z_3z_4z_5z_7 + z_1z_6z_7 + z_2z_6z_7 + z_1z_4z_6z_7 + z_1z_5z_6z_7 + \\ & z_2z_5z_6z_7 + z_3z_5z_6z_7 + z_8 + z_4z_8 + z_3z_4z_8 + z_5z_8 + \\ & z_2z_5z_8 + z_1z_4z_5z_8 + z_2z_4z_5z_8 + z_1z_6z_8 + z_2z_4z_6z_8 + \\ & z_3z_4z_6z_8 + z_3z_5z_6z_8 + z_7z_8 + z_6z_7z_8. \end{aligned}$$

Since each f_i is of the form $f_i(x,y) = x \cdot \pi_i(y) + h_i(y)$, where π_i is a quadratic APN permutation, then f_i share the unique canonical $\mathcal{M}$-subspace $U = \mathbb{F}_2^3 \times \{0_3\}$.

Therefore, we cannot apply Theorem 27 for showing that $f \notin \mathcal{M}^\#$. One can check that for every 2-dimensional subspace V of $\mathbb{F}_2^8$ such that $D_aD_bf_i = 0$, for all $a, b \in V$, where $i = 1, \ldots, 4$, the conditions of Theorem 34 are satisfied. Hence, the bent function $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_8$ is outside $\mathcal{M}^\#$. Additionally, using Algorithm .1 in the appendix, we confirm that $f \notin \mathcal{PS}^\#$, and, hence, $f \notin (\mathcal{M}^\# \cup \mathcal{PS}^\#)$.

Remark 38: The examples in this section indicate that the concatenation $f = f_1||f_2||f_3||f_4$ of four bent functions $f_i \in \mathcal{M}^\#$ can generate new bent functions $f \notin (\mathcal{M}^\# \cup \mathcal{PS}^\#)$. Notice also that all functions $f \in \mathcal{B}_8$ obtained in Examples 28, 29 and 37 are pairwise inequivalent. The latter was checked with Magma using the design isomorphism, as described in [22].

The comments given in the above remark motivate the following research problem.

Open Problem 3: Find other explicit families of bent functions $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$ satisfying the dual bent condition, i.e., $f_1^* + f_2^* + f_3^* + f_4^* = 1$, such that $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is bent and outside $\mathcal{M}^\#$. Particularly, specify these quadruples when all $f_i \in \mathcal{M}^\#$ share a unique $\mathcal{M}$-subspace of maximal dimension.

VI. Conclusion and Open Problems

In this article, we have analyzed the structure of bent functions in the Maiorana-McFarland class with respect to their inherent $\mathcal{M}$-subspaces, thus contributing to the analysis of inequivalent Maiorana-McFarland bent functions. Moreover, we provided generic construction methods of bent functions outside $\mathcal{M}^\#$, for any $n \geq 8$ using the bent 4-concatenation. Most notably, our results indicate that it is possible to construct bent functions outside $\mathcal{M}^\# \cup \mathcal{PS}^\#$, thus we contribute to a better understanding of the origin of bent functions in $n = 8$ variables.

To conclude, we believe that answering the following questions (in addition to the already mentioned open problems) will help to shed more light on the classification of bent functions as well as to develop new generic construction methods of these functions:

1) As we mentioned in the introduction, for a Maiorana-McFarland bent function $f \in \mathcal{B}_n$, the number of its $\mathcal{M}$-subspaces of dimension $n/2$ is at most $\prod_{i=1}^{n/2}\left(2^i + 1\right)$ and the equality is attained if and only if f is quadratic. What is the maximum number of $\mathcal{M}$-subspaces of dimension $n/2$ for a bent function $f \in \mathcal{B}_n$ in $\mathcal{M}$ of a fixed degree $d > 2$, and is it possible to characterize the functions achieving this bound? Our computational results indicate, that bent functions of the form $(x, y) \mapsto x \cdot y + y_1y_2 \cdots y_d$ have the maximum number of $\mathcal{M}$-subspaces of maximal dimension among all Maiorana-McFarland bent function of a fixed degree $d > 2$.
2) In this article, we analyzed certain properties of permutations π which guarantee that Maiorana-McFarland bent functions $x \cdot \pi(y) + h(y)$ have either one or many $\mathcal{M}$-subspaces of maximal dimension. For example, if π has the (P_1) property, we know that (independently of the choice of the function h) the bent function $x \cdot \pi(y) + h(y)$ has the unique canonical $\mathcal{M}$-subspace $U = \mathbb{F}_2^m \times \{0_m\}$. However, if the (P_1) property is relaxed, then the properties of the function h become crucial to guarantee the uniqueness of the canonical $\mathcal{M}$-subspace. We think it is important to understand in general, how the choice of a pair (π, h) affects the number of $\mathcal{M}$-subspaces of maximal dimension of the corresponding Maiorana-McFarland function.
3) An efficient way to satisfy the dual bent condition (we have to ensure that $f_1^* + f_2^* + f_3^* + f_4^* = 1$ so that $f = f_1||f_2||f_3||f_4$ is bent) is to use $f_1 = f_2$ and $f_3 = 1 + f_4$, which we employed in Theorem 30. However, there exist other possibilities to satisfy the dual bent condition which need to be examined further with regard to the class membership of the designed bent functions. We notice that Proposition 25 does not require that the functions f_i that define $f = f_1||f_2||f_3||f_4$ are bent. Therefore, another interesting research problem is to apply a similar approach, as taken in Theorem 30, to semi-bent and 5-valued spectra functions.

Appendix

For convenience of the reader, before presenting the algorithm, we first provide some basic facts about the partial spread class of bent functions. Recall that a partial spread of order s in $\mathbb{F}_2^n$, with $n = 2m$, is a set of s vector subspaces $U_1, \ldots, U_s$ of $\mathbb{F}_2^n$ of dimension m each, such that $U_i \cap U_j = \{0_n\}$ for all $i \neq j$. The partial spread of order $s = 2^m + 1$ in $\mathbb{F}_2^n$ is called a spread.

The *partial spread class* $\mathcal{PS}$ of bent functions on $\mathbb{F}_2^n$ is the union of the following two classes [10]: the $\mathcal{PS}^+$ *class* is the set of Boolean bent functions of the form $f(x) = \sum_{i=1}^{2^{m-1}+1} 1_{U_i}(x)$, where $U_i \cap U_j = \{0_n\}$ for all $i \neq j$; the $\mathcal{PS}^-$ *class* is the set of Boolean bent functions of the form $f(x) = \sum_{i=1}^{2^{m-1}} 1_{U_i^*}(x)$, where $U_i^* := U_i \setminus \{0\}$ and $U_i \cap U_j = \{0_n\}$ for all $i \neq j$. The *Desarguesian partial spread* class $\mathcal{PS}_{ap} \subset \mathcal{PS}^-$ is the set of Boolean bent functions f on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ of the form $f\colon (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mapsto h(x/y)$, where $\frac{x}{0} = 0$, for all $x \in \mathbb{F}_{2^m}$, and $h\colon \mathbb{F}_{2^m} \to \mathbb{F}_2$ is a balanced Boolean function with $h(0) = 0$. However, the property of a bent function to be a member of the partial spread class is not invariant under equivalence. If f is a partial spread function on $\mathbb{F}_2^n$, i.e., $f(x) = \sum_{i=1}^{s} 1_{U_i}(x)$ for a partial spread $\{U_1, \ldots, U_s\}$ of order s in $\mathbb{F}_2^n$, then for an invertible $n \times n$-matrix A, the function $g\colon x \in \mathbb{F}_2^n \mapsto f(xA)$ is a partial spread function as well, since $g(x) = \sum_{i=1}^{s} 1_{U_iA^{-1}}(x)$ for the partial spread $\{U_1A^{-1}, \ldots, U_sA^{-1}\}$. However, translations of the input $x \mapsto x+b$ for $b \in \mathbb{F}_2^n$ and additions of affine functions l on $\mathbb{F}_2^n$ to the output of a partial spread function f on $\mathbb{F}_2^n$ may lead to functions $g\colon x \mapsto f(x + b)$ and $h\colon x \mapsto f(x) + l(x)$ on $\mathbb{F}_2^n$, respectively, which do not belong to the partial spread class $\mathcal{PS}$. Using these observations, in Algorithm .1 below we describe how to check computationally the membership of a given bent function f on $\mathbb{F}_2^n$ in the $\mathcal{PS}$ class.

Remark 39: Note that, it is possible to establish with Algorithm .1 whether a bent function $f \in \mathcal{B}_n$ belongs to the

Algorithmus .1 Membership in the Partial Spread Class $\mathcal{PS}$

```
Require: Bent function $f \in \mathcal{B}_n$.
Ensure: True, $f$ is a partial spread function and false, otherwise.
if $f(0) = 1$ then                                    ▷ The case $\mathcal{PS}^+$
    Assign $s := 2^{n/2-1} + 1$ and $V := \mathrm{supp}(f)$ (the support of $f$).
else                                                  ▷ The case $\mathcal{PS}^-$
    Assign $s := 2^{n/2-1}$ and $V := \mathrm{supp}(f) \bigcup \{0_n\}$.
end if
Construct the graph $G = (V, E)$, for which the relation between vertices in $V$ and edges in $E$ is determined by the incidence matrix $[f(x+y)]_{x,y \in V}$.
Find the set $S$ of cliques of the size $2^{n/2}$ in $G$.
Construct the set $V'$ of cliques in $S$, whose elements form an $n/2$-dimensional vector space.
if $|V'| < s$ then
    Return false.
end if
Construct the graph $G' = (V', E')$, for which the relation between vertices in $V'$ and edges in $E'$ is determined by the incidence matrix $(a_{i,j})$, where $a_{i,j} = 1$, if for $U_i, U_j \in S$ holds $U_i \cap U_j = \{0_n\}$, and 0 otherwise.
Return true, $f$ is a partial spread function, if the graph $G'$ contains a clique of size $s$, and false otherwise.
```

completed partial spread class $\mathcal{PS}^{\#}$. If for a vector $b \in \mathbb{F}_2^n$ and an affine function l on $\mathbb{F}_2^n$ the function $g\colon x \mapsto f(x+b)+l(x)$ on $\mathbb{F}_2^n$ is a member of the $\mathcal{PS}$ class, we have $f \in \mathcal{PS}^{\#}$, otherwise $f \notin \mathcal{PS}^{\#}$.

Acknowledgment

The authors would like to thank the anonymous reviewers and the associate editor Dr. Claude Carlet for their valuable comments and suggestions that helped to improve the quality of the paper.

References

[1] A. Bapić, E. Pasalic, F. Zhang, and S. Hodžić, "Constructing new superclasses of bent functions from known ones," *Cryptogr. Commun.*, vol. 14, no. 6, pp. 1229–1256, Nov. 2022.

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

[3] D. Božilov, B. Bilgin, and H. A. Sahin, "A note on 5-bit quadratic Permutations' classification," *IACR Trans. Symmetric Cryptol.*, vol. 2017, no. 1, pp. 398–404, Mar. 2017.

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

[5] C. Carlet, "Two new classes of bent functions," in *Advances in Cryptology—EUROCRYPT*, T. Helleseth, Ed. Berlin, Germany: Springer, 1994, pp. 77–101.

[6] C. Carlet, "Vectorial Boolean functions for cryptography," in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* (Encyclopedia of Mathematics and its Applications. Cambridge, U.K.: Cambridge Univ. Press, 2010, ser. 134, pp. 398–469.

[7] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2021.

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

[9] P. Charpin and G. M. Kyureghyan, "Monomial functions with linear structure and permutation polynomials," in *Finite Fields: Theory and Applications* (Contemporary Mathematics), vol. 518, Providence, RI, USA: AMS, 2010, pp. 99–111.

[10] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, Dept. Math., Univ. Maryland, College Park, MD, USA, 1974.

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

[12] N. Kolomeec, "The graph of minimal distances of bent functions and its properties," *Designs, Codes Cryptogr.*, vol. 85, no. 3, pp. 395–410, Dec. 2017.

[13] S. Kudin, E. Pasalic, N. Cepak, and F. Zhang, "Permutations without linear structures inducing bent functions outside the completed Maiorana–McFarland class," *Cryptogr. Commun.*, vol. 14, no. 1, pp. 101–116, Jan. 2022.

[14] S. Kudin and E. Pasalic, "A complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^{\#}$ and a general framework for specifying bent functions in $\mathcal{C}$ outside $\mathcal{M}$," *Designs, Codes Cryptogr.*, vol. 90, no. 8, pp. 1783–1796, Aug. 2022.

[15] P. Langevin and G. Leander, "Counting all bent functions in dimension eight 99270589265934370305785861242880," *Designs, Codes Cryptogr.*, vol. 59, nos. 1–3, pp. 193–205, Apr. 2011.

[16] S. Li, W. Meidl, A. Polujan, A. Pott, C. Riera, and P. Stanica, "Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application," *IEEE Trans. Inf. Theory*, vol. 66, no. 11, pp. 7101–7112, Nov. 2020.

[17] R. L. McFarland, "A family of difference sets in non-cyclic groups," *J. Combinat. Theory A*, vol. 15, no. 1, pp. 1–10, Jul. 1973.

[18] W. Meidl, A. Polujan, and A. Pott, "Linear codes and incidence structures of bent functions and their generalizations," *Discrete Math.*, vol. 346, no. 1, Jan. 2023, Art. no. 113157.

[19] S. Mesnager, *Bent Functions: Fundamentals and Results*, 1st ed. Cham, Switzerland: Springer, 2016.

[20] E. Pasalic, A. Bapić, F. Zhang, and Y. Wei, "Explicit infinite families of bent functions outside the completed Maiorana-McFarland class," *Designs, Codes Cryptogr.*, vol. 91, pp. 2365–2393, Mar. 2023.

[21] A. Polujan, "Boolean and vectorial functions: A design-theoretic point of view," Ph.D. dissertation, Otto-von-Guericke-Universität Magdeburg, Fakultät für Mathematik, Magdeburg, Germany, 2021.

[22] A. A. Polujan and A. Pott, "Cubic bent functions outside the completed Maiorana–McFarland class," *Designs, Codes Cryptogr.*, vol. 88, no. 9, pp. 1701–1722, Sep. 2020.

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

[24] Z. Zha, L. Hu, and S. Sun, "Constructing new differentially 4-uniform permutations from the inverse function," *Finite Fields Appl.*, vol. 25, pp. 64–78, Jan. 2014.

[25] F. Zhang, E. Pasalic, N. Cepak, and Y. Wei, "Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana–McFarland class," in *Codes, Cryptology and Information Security*, S. El Hajji, A. Nitaj, and E. M. Souidi, Eds. Cham, Switzerland: Springer, 2017, pp. 298–313.

[26] 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 $\mathcal{M}^{\#}$," *Discrete Appl. Math.*, vol. 285, pp. 458–472, Oct. 2020.

Enes Pasalic received the Ph.D. degree in cryptology from Lund University, Lund, Sweden, in 2003. Since May 2003, he has been a Post-Doctoral Researcher with INRIA (Versaille, France) Crypto Group, and later with the Technical University of Denmark, Lyngby, in 2005. He is currently with the FAMNIT and IAM, University of Primorska, Koper, Slovenia. His main research interests include cryptology and in particular the design and analysis of symmetric encryption schemes.

Alexandr Polujan received the Ph.D. degree in mathematics from Otto von Guericke University Magdeburg, Germany, in 2021. He is currently a Post-Doctoral Researcher with Otto von Guericke University Magdeburg. His research interests include Boolean functions, design theory, and coding theory.

Sadmir Kudin received the B.S. and M.S. degrees in mathematics from the University of Sarajevo, Sarajevo, Bosnia and Herzegovina, in 2016 and 2018, respectively, and the Ph.D. degree in mathematics from the University of Primorska, Koper, Slovenia, in 2023. His current research interests include symmetric cryptography, Boolean functions, and linear codes.

Fengrong Zhang received the B.S. degree in mathematics from the Hebei University of Science and Technology, Shijiazhuang, China, in 2006, and the M.S. degree in mathematics and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2009 and 2012, respectively. In 2012, he joined the School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, China, as a Lecturer, where he has been an Associate Professor since 2015. From 2017 to 2018, he was a Visiting Scholar with the Department of Mathematics, University of Paris VIII, Paris, France. He is currently a Professor with the School of Cyber Engineering, Xidian University. His current research interests include Boolean functions, cryptography, and coding theory.