Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-024-01407-9

# Using $P_\tau$ property for designing bent functions provably outside the completed Maiorana–McFarland class

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

Received: 16 August 2023 / Revised: 19 March 2024 / Accepted: 3 April 2024

## Abstract

In this article, we identify certain instances of bent functions, constructed using the so-called $P_\tau$ property, that are provably outside the completed Maiorana–McFarland ($\mathcal{MM}^\#$) class. This also partially answers an open problem in posed by Kan et al. (IEEE Trans Inf Theory, https://doi.org/10.1109/TIT.2022.3140180, 2022). We show that this design framework (using the $P_\tau$ property), can provide instances of bent functions that are outside the known classes of bent functions, including the classes $\mathcal{MM}^\#$, $\mathcal{C}, \mathcal{D}$ and $\mathcal{D}_0$, where the latter three were introduced by Carlet in the early nineties. We provide two generic methods for identifying such instances, where most notably one of these methods uses permutations that may admit linear structures. For the first time, a set of sufficient conditions for the functions of the form $h(y,z) = Tr(y\pi(z)) + G_1(Tr_1^m(\alpha_1 y), \ldots, Tr_1^m(\alpha_k y))G_2(Tr_1^m(\beta_{k+1}z), \ldots, Tr_1^m(\beta_\tau z)) + G_3(Tr_1^m(\alpha_1 y), \ldots, Tr_1^m(\alpha_k y))$ to be bent and outside $\mathcal{MM}^\#$ is specified without a strong assumption that the components of the permutation $\pi$ do not admit linear structures.

**Keywords** Bent functions · $P_\tau$ property · Completed classes · Exclusion from $\mathcal{MM}^\#$ · Linear structures

**Mathematics Subject Classification** 94D10 · 94A60

Communicated by T. Helleseth.

✉ Enes Pasalic
enes.pasalic6@gmail.com

Amar Bapić
amarbapic22@gmail.com

Fengrong Zhang
zhfl203@163.com

Yongzhuang Wei
walker_wyz@guet.edu.cn

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

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

[3] School of Cyber Engineering, Xidian University, Xi'an 710071, People's Republic of China

Published online: 22 April 2024

## 1 Introduction

The concept of bent functions was introduced by Rothaus [22] as a family of Boolean functions possessing several nice combinatorial properties, which allowed for their great range of applications such as in design theory, coding theory, sequences, cryptography to mention a few. An exhaustive survey on bent functions related to their design and properties can be found in [6] and in the recent textbook [17]. For a detailed study of Boolean functions in cryptography we refer to [5]. In general, the design methods of bent functions can be divided into primary and secondary constructions. Whereas the two main primary classes (the partial spread [9] and Maiorana–McFarland class [15]) specify bent functions directly (without involving other bent functions), the known secondary constructions involve other bent functions either on the same or on smaller variable spaces. A non-exhaustive list of various secondary constructions can be found in the following works [3, 4, 7, 11, 16, 30]. However, the question regarding the class inclusion of bent functions stemming from these secondary construction methods is commonly left open, apart from the following works [1–3, 13, 14, 16, 18, 19, 21, 27–29], where some explicit families of bent functions provably outside the completed $\mathcal{MM}$ class are given. Moreover, other combinatorial objects such as bent-negabent and (vectorial) bent functions can also be specified using bent functions outside $\mathcal{MM}^\#$, see for instance [20, 26].

In this article, we consider one generic method of modifying bent functions in the $\mathcal{MM}$ class based on the so-called $P_\tau$ property. More precisely, initially Mesnager [16] provided a necessary and sufficient condition for the function $h(x) = f(x) \oplus Tr(ax)Tr(bx)$ to be bent, where $f$ is a bent function. This approach has later been generalized to involve more trace terms in [24, 25], whereas a more general form $h(x) = f(x) \oplus \sum_{I\subseteq\{1,\dots,\tau\}} a_I \left(\prod_{i\in I} Tr(\mu_i x)\right)$ was considered in [23], where the bentness of $h$ comes from a certain linearity condition on duals, see [23] for more details. An equivalent characterization of the bentness of $h$ on $\mathbb{F}_2^n$ was later stated in terms of the second order derivatives of the dual function of $f$ [30], in brief requiring that $D_{\mu_i} D_{\mu_j} f^* = 0$, for $1 \le i < j \le \tau$, where the elements $\mu_i \in \mathbb{F}_2^n$ build a linear subspace $\mathcal{U}_\tau = \langle \mu_1, \dots, \mu_\tau \rangle$. However, the question about the class membership of derived new families of bent functions was mostly left open. In a recent work [12], this approach was further elaborated and the authors provided an example of a bent function outside $\mathcal{MM}^\#$ specified using this method. In addition, an open problem concerning the identification of all bent functions outside $\mathcal{MM}^\#$ constructed using this method was left open [12, Open problem 2]. We first identify several families of bent functions that are provably outside $\mathcal{MM}^\#$ and can be represented within the construction framework given in [12]. Moreover, we provide an explicit design of such functions and thereby we partially answer this open problem. We remark that the initial conditions (see Theorem 3.2) in our main result are easily satisfied and many families of bent functions outside $\mathcal{MM}^\#$ can be generated.

We then extend our approach and derive a more general framework of using $P_\tau$ property through combining the so-called trivial and non-trivial defining sets. For instance, Example 3.2 demonstrates the fact that $\mathcal{P}_\tau \not\subset (\mathcal{C} \cup \mathcal{SC} \cup \mathcal{D}_0 \cup \mathcal{D} \cup \mathcal{CD})$ and also $\mathcal{P}_\tau \not\subset \mathcal{MM}^\#$. Most notably, we show that permutations with linear structures can be used for this purpose assuming that the defining set is chosen properly. Theorem 4.1 provides a set of sufficient conditions that ensure both bentness and outside $\mathcal{MM}^\#$ property of the proposed family of bent functions, where the standard condition that for a permutation $\pi$ over $\mathbb{F}_{2^m}$ satisfies $Tr_1^m(a\pi(y)) \neq const$ is absent.

The rest of this paper is organized as follows. In Sect. 2, we give some basic definitions related to Boolean functions and in particular we recall certain characterizations related to the completed $\mathcal{MM}$ class. One explicit construction of bent functions outside $\mathcal{MM}^\#$, based on the so-called $P_\tau$ property, is presented in Sect. 3 which also partially answers an open problem raised in [12]. In Sect. 4, we combine trivial and non-trivial defining sets $\mathcal{U}_\tau$ to provide a wider framework for specifying bent functions outside $\mathcal{MM}^\#$ using $P_\tau$ property. In particular, we show that even permutations that admit linear structures can potentially be employed in this method. The class exclusion from the known classes of bent functions is discussed in Sect. 5. Some concluding remarks are given in Sect. 6.

## 2 Preliminaries

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

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 $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented by its associated algebraic normal form (ANF) as follows:

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

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

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

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

and

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

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

### 2.1 The completed Maiorana–McFarland class

The *Maiorana–McFarland class* [15], denoted by $\mathcal{MM}$, is the set of $n$-variable ($n = 2m$) Boolean bent functions of the form

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

where $g$ is an arbitrary Boolean function on $\mathbb{F}_2^m$, and $\pi$ is a *permutation* on $\mathbb{F}_2^m$, i.e., $\pi$ is a bijective mapping from $\mathbb{F}_2^m$ to $\mathbb{F}_2^m$.

**Definition 2.1** A class of bent functions $B_n \subset \mathcal{B}_n$ is *complete* if it is globally invariant under the action of the general affine group (the group of all invertible affine transformations) and under the addition of affine functions (i.e., Boolean functions of degree at most 1). The *completed class*, denoted by $\mathcal{MM}^\#$ in the case of the Maiorana–McFarland class, is the smallest possible complete class that contains the class under consideration.

The first-order derivative of a function $f$ in the direction $a \in \mathbb{F}_2^n$ is given by $D_a f(x) = f(x) \oplus f(x \oplus a)$. If $D_a f(x) = const \in \mathbb{F}_2$, for all $x \in \mathbb{F}_2^n$, then $a \in \mathbb{F}_2^n$ is said to be a *linear structure* of $f$. Derivatives of higher order are defined recursively, i.e., the *k-th order derivative* of a function $f \in \mathcal{B}_n$ is defined by $D_V f(x) = D_{a_k} D_{a_{k-1}} \dots D_{a_1} f(x) = D_{a_k}(D_{a_{k-1}} \dots D_{a_1} f)(x)$, where $V = \langle a_1, \dots, a_k \rangle$ is a vector subspace of $\mathbb{F}_2^n$ spanned by elements $a_1, \dots, a_k \in \mathbb{F}_2^n$. If a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ satisfies $\deg(D_c f) \leq \deg(f) - 2$, then $c$ is called a fast point (FP) of $f$ [10]. The set of all fast points of a Boolean function $f$, building a linear subspace of $\mathbb{F}_2^n$, is denoted by $\mathbb{FP}_f$. We note the following useful lemma.

**Lemma 2.1** [10] *Let* $f \in \mathcal{B}_n$, *then* $\deg(f) + \dim(\mathbb{FP}_f) \leq n$.

The following lemma, due to Dillon [9], is of crucial importance for the discussion on class inclusion.

**Lemma 2.2** [9, p. 102] *A bent function $f$ in $n$ variables belongs to $\mathcal{MM}^\#$ if and only if there exists an $n/2$-dimensional linear subspace $V$ of $\mathbb{F}_2^n$ such that the second-order derivatives*

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

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

In the sequel, we call a subspace $V \subset \mathbb{F}_2^n$ of dimension $m \leq n/2$ a vanishing subspace for $f \in \mathcal{B}_n$ (also called an $\mathcal{M}$-subspace in [21]), whenever $D_\alpha D_\beta f(x) = 0$ for all $\alpha, \beta \in V$.

***Remark 2.1*** Using the isomorphism between the vector space $\mathbb{F}_2^n$ and the finite field $\mathbb{F}_{2^n}$, for convenience and precision, we sometimes write vanishing subspaces in the vector space notation even though the function $f(x, y) = Tr_1^m(x\pi(y))$ is defined for $x, y \in \mathbb{F}_{2^m}$ (corresponding to $f(x, y) = x \cdot \pi(y)$, with $x, y \in \mathbb{F}_2^m$), with $n = 2m$. Here, $Tr_1^m(\cdot)$ denotes the absolute trace function $Tr_1^m : \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined as $Tr_1^m(x) = x + x^{2^1} + \cdots + x^{2^{m-1}}$. Moreover, the all-zero vector $0 \in \mathbb{F}_2^m$ is denoted simply by 0 when considered as an element of $\mathbb{F}_{2^m}$.

## 3 Specifying bent functions outside $\mathcal{MM}^\#$ using $P_\tau$ property

As already mentioned, apart from various initial works in [23–25], the bent property of modified functions in the $\mathcal{MM}$ class through addition of certain indicators was analyzed in [30] in terms of the second-order derivatives of the dual bent function. More precisely, denoting by $f^*$ the dual function of a bent function $f \in \mathcal{B}_n$, it was deduced that $h(x) = f(x) + \sum_{I \subseteq \{1,\dots,\tau\}} a_I \left( \prod_{i \in I} Tr_1^n(\mu_i x) \right)$ can preserve the bent property provided that $D_{\mu_i} D_{\mu_j} f^* = 0$, for $1 \leq i < j \leq \tau$. This condition was sometimes called the $P_\tau$ property, referring to the cardinality of the linearly independent vectors $\mu_i \in \mathbb{F}_2^n$ for which $D_{\mu_i} D_{\mu_j} f^* = 0$. In the sequel, we use the "+" sign to denote the addition of elements in the finite field $\mathbb{F}_{2^n}$ instead of "$\oplus$" reserved for the vector space notation in $\mathbb{F}_2^n$.

In this section, we will address this construction method more thoroughly in terms of the class membership of the generated bent functions. In particular, we partially answer an open problem stated recently in [12] that concerns a complete classification of bent functions given in Proposition 3.1 below, with respect to the property of being outside $\mathcal{MM}^\#$.

**Proposition 3.1** (Proposition 1 in [12]) *Let $\alpha \in \mathbb{F}_{2^m}^*$ and $\omega \in \mathbb{F}_{2^n}$ with $\omega + \omega^{2^m} = 1$, where $n = 2m$. Let $\pi$ be a permutation of $\mathbb{F}_{2^m}$ and $g$ be a Boolean function over $\mathbb{F}_{2^m}$. Then, the Boolean function*

$$f(x) = Tr_1^n(\alpha\omega^{2^m} x\pi(x + x^{2^m})) + g(x + x^{2^m}), \quad \text{for all } x \in \mathbb{F}_{2^n}, \tag{3}$$

*is bent on $\mathbb{F}_{2^n}$ and the dual of $f$ is given by*

$$f^*(x) = Tr_1^n(\omega x\pi^{-1}(\alpha^{-1}(x + x^{2^m}))) + g(\pi^{-1}(\alpha^{-1}(x + x^{2^m}))).$$

**Theorem 3.1** (Theorem 8 in [12]) *Let $f$ be a bent function on $\mathbb{F}_{2^n}$ generated by Proposition 3.1, which is in $\mathcal{MM}$, and let $\mu_1, \mu_2, \dots, \mu_\tau \in \mathbb{F}_{2^n}$ be such that $D_{\mu_i} D_{\mu_j} f^* = 0$ for any $1 \le i < j \le \tau$. Then, for any $a_I \in \mathbb{F}_2$, the $n$-variable Boolean function*

$$h(x) = f(x) + F(Tr_1^n(\mu_1 x), Tr_1^n(\mu_2 x), \dots, Tr_1^n(\mu_\tau x)) \tag{4}$$

*is a bent function, where $F(X_1, X_2, \dots, X_\tau) = \sum_{I \subseteq [\tau]} a_I(\prod_{i \in I} X_i)$.*

We note that each product $\prod_{i \in I} X_i$, $I \subseteq [\tau] = \{1, 2, \dots, \tau\}$, corresponds to the indicator of some $(n - |I|)$-dimensional affine subspace of $\mathbb{F}_{2^n}$. Hence, the function $F$ can be represented as a sum of indicator functions of affine subspaces not necessarily of the same dimension.

The particular problem that was left open in [12] is stated as follows.

**Open Problem 1** [12] *Determine all the bent functions defined as in Theorem 3.1 which are outside the completed Maiorana–McFarland class.*

We now first identify certain families of bent functions that are outside $\mathcal{MM}^\#$ and fall into this framework. More precisely, we specify a new family of bent functions outside $\mathcal{MM}^\#$ which also satisfies the above form and thereby provides a partial answer to the open problem above.

Note that any $x \in \mathbb{F}_{2^n}$, $n = 2m$, can be represented as $x = y + z\omega$, where $y, z \in \mathbb{F}_{2^m}$ and $\omega \in \mathbb{F}_{2^n}$ with $\omega + \omega^{2^m} = 1$. Thus, the function (3) can be written as

$$f(x) = f(y, z) = Tr_1^m(\alpha y\pi(z)) + g(z), \tag{5}$$

where $\alpha \in \mathbb{F}_{2^m}^*$. In [12], the authors provided one example of functions of the form (4) which is provably outside $\mathcal{MM}^\#$.

For simplicity, we will assume that $\alpha = 1$ and $g \cong 0$ in (5), i.e. we will consider functions $f \in \mathcal{B}_{2m}$ of the form $f(y, z) = Tr_1^m(y\pi(z))$ which belong to $\mathcal{MM}$. Note that any linear function from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ can be written as $(y, z) \mapsto Tr_1^m(\alpha y + \beta z)$, where $\mu = (\alpha, \beta) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Hence, the function given by (4), with the above restrictions, can be written in bivariate form as

$$h(y, z) = f(y, z) + F(Tr_1^m(\alpha_1 y + \beta_1 z), \dots, Tr_1^m(\alpha_\tau y + \beta_\tau z)), \tag{6}$$

where $f(y, z) = Tr_1^m(y\pi(z))$ and $F(X_1, X_2, \dots, X_\tau) = \sum_{I \subseteq [\tau]} a_I(\prod_{i \in I} X_i)$, with $\mu_i = (\alpha_i, \beta_i) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ and $D_{\mu_i} D_{\mu_j} f^* = 0$ for any $1 \le i < j \le \tau \le m$. Notice that $X_i = Tr_1^m(\alpha_i y + \beta_i z)$, thus it represents a linear function.

***Remark 3.1*** As mentioned above, we can consider the function $h$ in bivariate form and consequently, we can represent the elements $\mu_i$ in the form $\mu_i = (\alpha_i, \beta_i) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Note, that if we want our function $h$ to be outside $\mathcal{MM}^\#$, we cannot have $\alpha_i = 0$ for all $1 \le i \le \tau$. In this case, we would have $h(y, z) = Tr_1^m(y\pi(z)) + G(z) \in \mathcal{MM}$, where $G(z) = F(Tr_1^m(\beta_1 z), \dots, Tr_1^m(\beta_\tau z))$. Hence, to have $h$ outside $\mathcal{MM}^\#$ a necessary condition is that the function $F$ does not entirely depend on the variable $z$.

In the sequel, we will use $\mathcal{U}_\tau$ to denote the set $\{\mu_1, \dots, \mu_\tau\}$. If $f(y, z) = Tr_1^m(y\pi(z))$, then $f^*(y, z) = Tr_1^m(z\pi^{-1}(y))$ (see for instance [5]). It is easy to verify that $D_{\mu_i} D_{\mu_j} f^*(y, z) = 0$ for $\mu_i, \mu_j \in \{0\} \times \mathbb{F}_{2^m}$. However, such a choice of $\mu_i$ will result in $h(y, z) = Tr_1^m(y\pi(z)) + G(z)$, and $h \in \mathcal{MM}$ as remarked above. Because of this, we will say that the set $\mathcal{U}_\tau \subset \{0\} \times \mathbb{F}_{2^m}$ is a *trivial defining set* for $f^*$, otherwise, it will be called *non-trivial*. Notice that depending on the choice of $\pi$ both $f$ and its dual $f^*$ may admit other vanishing subspaces of maximal dimension $m$ but also other ones of a smaller dimension.

For a Boolean function $F \in \mathcal{B}_m$, let us for nonzero distinct elements $\alpha_i, \alpha_j \in \mathbb{F}_{2^m}$, define

$$\Xi(F) := \{i : D_{\alpha_i} D_{\alpha_j} F \neq 0,\ 1 \le i < j \le 2^m - 1\}.$$

***Remark 3.2*** Any nonlinear function $F$ on $\mathbb{F}_2^n$ actually satisfies $|\Xi(F)| \ge 2^{n-1}$, since there must exist an $a \in \mathbb{F}_2^n$ such that $\deg(D_a F) \ge 1$. Now, if $\deg(D_a F) = 1$ then there are exactly $2^{n-1}$ vectors $b \in \mathbb{F}_2^n$ such that $D_a D_b F \neq 0$. Otherwise, if $\deg(D_a F) > 1$ then there are at least $2^{n-1}$ such vectors $b$.

With this notation, we give the following result which gives a partial answer to the Open Problem 1.

**Theorem 3.2** *Let $f$ be a bent function on $\mathbb{F}_{2^n}$, $n = 2m$, defined with $f(y, z) = Tr_1^m(y\pi(z))$, with $y, z \in \mathbb{F}_{2^m}$, and let $\mu_i = (\alpha_i, 0) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ for $1 \le i \le \tau \le m$ be such that $D_{\mu_i} D_{\mu_j} f^* = 0$ for any $i \neq j$, thus constituting a non-trivial defining set for $f^*$. Let $h$ be defined as in (6). If:*

a. *$Tr_1^m(\lambda\pi)$ has no non-zero linear structures for any $\lambda \in \mathbb{F}_{2^m}^*$,*
b. *$|\Xi(F)| \ge 2$,*

*then $h$ is a bent function on $\mathbb{F}_{2^n}$ outside $\mathcal{MM}^\#$.*

***Proof*** For simplicity, let $G(y) = F(Tr_1^m(\alpha_1 y), \dots, Tr_1^m(\alpha_\tau y))$. Let $V$ be any $m$-dimensional subspace of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Let $a = (a_1, a_2), b = (b_1, b_2) \in V$ be arbitrary. The second-order derivative of $h$ (see Lemma 2.2) with respect to $a$ and $b$ can be written as

$$\begin{aligned} D_{(a_1,a_2)} D_{(b_1,b_2)} h(y, z) = Tr_1^m \big(& y D_{a_2} D_{b_2} \pi(z) + a_1 D_{b_2} \pi(z + a_2) \\ & + b_1 D_{a_2} \pi(z + b_2)\big) + D_{a_1} D_{b_1} G(y), \end{aligned}$$

and we need to show that that there always exist $a, b \in V$ such that $D_a D_b h \neq 0$.

We denote the subspace $\{(x, 0) : x \in \mathbb{F}_{2^m}\}$ by $\Delta$. We have the following two cases.

a. $V = \Delta$. Then, we can find two vectors $(a_1, 0), (b_1, 0) \in \Delta$ such that

$$D_{a_1} D_{b_1} G(y) \neq 0,$$

since $|\Xi(G)| = |\Xi(F)| \ge 2$. Consequently,

$$D_a D_b h(y, z) = D_{a_1} D_{b_1} G(y) \neq 0.$$

b. $V \neq \Delta$. We split the proof into two cases, based on the size of $V \cap \Delta$. Let us denote the elements of $V$ with $\{(v_1, u_1), \ldots, (v_{2^m}, u_{2^m})\}$, where $(v_i, u_i) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

(a) $|V \cap \Delta| = 1$. In this case, we have that $u_i \neq u_j$ for $i \neq j$. Otherwise, if there exist two vectors $u_i, u_j$ such that $u_i = u_j$, then $v_i = v_j$ because $(v_i + v_j, 0) \in V \cap \Delta = \{(0, 0)\}$. In other words, we would have that $(v_i, u_i) = (v_j, u_j)$. Further, $|\{u_1, u_2, \ldots, u_{2^m}\}| = |V| = 2^m$, that is, $\{u_1, u_2, \ldots, u_{2^m}\} = \mathbb{F}_{2^m}$. Now, since $Tr_1^m(\lambda\pi)$ has no non-zero linear structures for any $\lambda \in \mathbb{F}_{2^m}^*$, we have $\deg(Tr_1^m(\lambda\pi)) > 2$. This is due to the fact that any quadratic balanced function $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ always admits at least all-one linear structure, so that $D_a f = 1$, for all $x \in \mathbb{F}_{2^m}$ and for some $a \in \mathbb{F}_{2^m}$, see [8, Theorem 6]. Thus, from Lemma 2.1,we can select two vectors $a = (a_1, a_2), b = (b_1, b_2) \in V$ such that $D_{a_2} D_{b_2}\pi(z) \neq const$, since $\{u_1, u_2, \ldots, u_{2^m}\} = \mathbb{F}_{2^m}$.
Furthermore,

$$\begin{aligned} D_a D_b h(y, z) = Tr_1^m \left(y D_{a_2} D_{b_2}\pi(z) + a_1 D_{b_2}\pi(z + a_2) + b_1 D_{a_2}\pi(z + b_2)\right) \\ + D_{a_1} D_{b_1} G(y) \neq 0, \end{aligned}$$

since the term $Tr_1^m \left(y D_{a_2} D_{b_2}\pi(z)\right)$ cannot vanish. Thus, $D_a D_b h \neq 0$ if $|V \cap \Delta| = 1$.

(b) For $|V \cap \Delta| \geq 2$, without loss of generality, let $(a_1, 0) \in V^* \cap \Delta$ where $V^* = V \setminus \{(0, 0)\}$. Set $b \in V \setminus \{0_{2m}, a\}$, then $b_2 \neq 0$. Thus, setting $a_2 = 0$ in $D_{(a_1,a_2)} D_{(b_1,b_2)} h(y, z)$ above, we get

$$D_a D_b h(y, z) = Tr_1^m(a_1 D_{b_2}\pi(z)) + D_{a_1} D_{b_1} G(y) \neq 0, \tag{7}$$

since $Tr_1^m(\lambda\pi)$ has no nonzero linear structure for any $\lambda \in \mathbb{F}_{2^m}^*$.

Combining the cases $V = \Delta$ and $V \neq \Delta$, we deduce that $f$ does not belong to $\mathcal{MM}^\#$. □

***Remark 3.3*** Notice that the assumptions in Theorem 3.2 can be easily satisfied. For the condition on the second-order derivatives of dual $f^*$, see also Remark 3.4 below. Permutations whose components are without linear structures have been recently specified in [14]. On the other hand, the condition that $Tr_1^m(\lambda\pi)$ has no nonzero linear structures is only sufficient but not necessary. Notice that (7) implies that $G$ can be chosen so that $D_{a_1} D_{b_1} G(y) \neq 0$, unless $a_1 = b_1$. Then, considering the choice $a = (a_1, 0)$ and $b = (b_1, b_2)$, where $a_1 = b_1$, implies that $(0, b_2)$ belongs to $V$. For these particular $a = (a_1, 0)$ and $b = (0, b_2)$, it is enough that $Tr_1^m(a_1 D_{b_2}\pi(z)) \neq 0$ so that $f \notin \mathcal{MM}^\#$.

***Example 3.1*** Let us consider the bent function $f(y, z) = Tr_1^6(yz^{38})$, $y, z \in \mathbb{F}_{2^6}$. Using Sage, we obtained that $\mathcal{U}_2 = \{\omega^6, \omega^{27}\} \times \{0\} = \{\alpha_1, \alpha_2\} \times \{0\}$ is a non-trivial defining set for $f^*$, where $\omega$ is a primitive element in $\mathbb{F}_{2^6}$ such that $\omega^6 + \omega^4 + \omega^3 + \omega + 1 = 0$. We further confirmed that this was the maximal size for such a set of linearly independent elements. Thus, the only function which can be constructed using Theorem 3.1 is of the form $h(y, z) = Tr_1^6(yz^{38}) + Tr_1^6(\omega^6 y) Tr_1^6(\omega^{27} y)$, which belongs to the $\mathcal{C}$ class of bent functions, see below. From [29], we know that it is also outside $\mathcal{MM}^\#$ since $\pi(z) = z^{38}$ is of degree 3 and its components do not admit linear structures.

Carlet [3] introduced the so-called $\mathcal{C}$ class of bent functions that contains all functions of the form

$$f(x, y) = x \cdot \pi(y) \oplus \mathbf{1}_{L^\perp}(x), \tag{8}$$

where $L$ is any linear subspace of $\mathbb{F}_2^n$, $\mathbf{1}_{L^\perp}$ is the indicator function of the space $L^\perp$, and $\pi$ is any permutation on $\mathbb{F}_2^n$ such that:

$$(C) \quad \phi(a + L) \text{ is a flat (affine subspace), for all } a \in \mathbb{F}_2^n, \text{ where } \phi := \pi^{-1}.$$

The permutation $\phi$ and the subspace $L$ are then said to satisfy the $(C)$ property, or for short $(\phi, L)$ *has property* $(C)$.

Let us also consider the following example, which gives functions of a different form than those contained in the $\mathcal{C}$ class.

***Example 3.2*** Let us consider the bent function $f(y,z) = Tr_1^9(yz^{284}),\ y, z \in \mathbb{F}_{2^9}$. The set $\mathcal{U}_3 = \{1, \omega^{73}, \omega^{146}\} \times \{0\} = \{\alpha_1, \alpha_2, \alpha_3\} \times \{0\}$ is a non-trivial defining set for $f^*$, where $\omega$ is a primitive element in $\mathbb{F}_{2^9}$ such that $\omega^9 + \omega^4 + 1 = 0$. Then, for any polynomial $G \in \mathbb{F}_2[Y_1, Y_2, Y_3]$ the function $h(y,z) = Tr_1^9(yz^{284}) + G(Tr_1^9(y), Tr_1^9(\omega^{73}y), Tr_1^9(\omega^{146}y))$ is a bent function in 18 variables. Specifically, if we take $G(Y_1, Y_2, Y_3) = Y_1Y_2Y_3 + Y_1Y_2 + Y_1Y_3$ then

$$\begin{aligned} G(Y_1, Y_2, Y_3) = {} & Tr_1^9(y)Tr_1^9(\omega^{73}y)Tr_1^9(\omega^{146}y) + Tr_1^9(y)Tr_1^9(\omega^{73}y) \\ & + Tr_1^9(\omega^{73}y)Tr_1^9(\omega^{146}y). \end{aligned}$$

We note that $|\Xi(G)| \geq 2$ and since $\pi(z) = z^{284}$ has no non-zero linear structures, from Theorem 3.2, the function $h$ is outside $\mathcal{MM}^{\#}$. Using Sage we observed that the function $G$, as a 9-variable Boolean function, contains the value 1 exactly 192 times in its truth table. This means that we have modified the values of $f \in \mathcal{MM}$ at $192 \cdot 2^9$ places. As 192 is not a power of 2, then $h$ is obviously not a function in the $\mathcal{C}$ class.

The following remark further clarifies the possibility of finding a set of linearly independent vectors $\mu_1, \ldots, \mu_\tau \in \mathbb{F}_2^n$ satisfying the so-called $P_\tau$ property in Theorem 3.1.

***Remark 3.4*** Since the dual $f^*(y,z) = Tr_1^m(z\pi^{-1}(y))$ of $f(y,z) = Tr_1^m(y\pi(z))$ is also in $\mathcal{MM}^{\#}$, the dual $f^*$ admits at least the canonical (trivial) defining set $\{0\} \times \mathbb{F}_{2^m}$. However, depending on $\pi$, there might exist other non-trivial vanishing subspaces $\langle \mu_1, \ldots, \mu_\tau \rangle$ (see also Remark 3.1 and the discussion after Remark 4.2) so that $D_{\mu_i}D_{\mu_j}f^* = 0$ for all $\mu_i, \mu_j$ in $\langle \mu_1, \ldots, \mu_\tau \rangle$. For instance, if the permutation $\pi^{-1}$ on $\mathbb{F}_2^5$ is given as

$$\pi^{-1}(y) = \begin{pmatrix} y_1 \\ y_2 \\ y_3 + y_1y_3 + y_1y_5 \\ y_1y_3 + y_2y_3 + y_4 \\ y_1y_3 + y_2y_4 + y_5 + y_1y_5 \end{pmatrix}, \tag{9}$$

then the only linear structure of $\pi$ is $s = 0$ but $\pi^{-1}$ has components that admit linear structures. However, the function $f^*(y,z) = z \cdot \pi^{-1}(y)$ has exactly two $\mathcal{M}$-subspaces of maximal dimension 5: the canonical $\mathcal{M}$-subspace $\{0_5\} \times \mathbb{F}_2^5$ as well as $V$, which is given by:

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

Consequently, the basis of $V$ can be identified with $\langle \mu_1, \ldots, \mu_5 \rangle$ which can be used to define a non-trivial defining set, say $\mathcal{U}_2 = \{\alpha_1, \alpha_2\} \times \{0_5\}$ corresponding to the first two rows of $V$, see also Example 3.1.

## 4 Extending non-trivial defining sets

In what follows, we extend the above result in a more generic way by combining a non-trivial defining set as in Theorem 3.2 with a defining set that uses both variables. That is, we consider the function $F$ in (6) to be of the form

$$\begin{aligned} F(X_1, X_2, \dots, X_\tau) = {} & G_1(Tr_1^m(\alpha_1 y), \dots, Tr_1^m(\alpha_k y))G_2(Tr_1^m(\beta_{k+1} z), \dots, Tr_1^m(\beta_\tau z)) \\ & + G_3(Tr_1^m(\alpha_1 y), \dots, Tr_1^m(\alpha_k y)), \end{aligned} \tag{10}$$

where $G_1, G_3$ and $G_2$ are in $\mathbb{F}_2[X_1, \dots, X_r]$ for $r = k$ and $r = \tau - k$, respectively. Because the polynomials $G_1, G_2, G_3$ are arbitrary, we would like to note that we do not need to consider all variables. That is, the polynomials can depend on any subset of $\{X_1, \dots, X_r\}$. Nevertheless, we can still obtain bent functions outside $\mathcal{MM}^\#$, thus providing an additional partial solution to Open Problem 1. With respect to $f(y, z) = Tr_1^m(y\pi(z))$ and its dual $f^*(y, z) = Tr_1^m(z\pi^{-1}(y))$, we define

$$A = \{a_i = (\alpha_i, 0) : 1 \le i \le k, \alpha_i \in \mathbb{F}_{2^m}\}; \quad B = \{b_j = (0, \beta_j) : k+1 \le j \le \tau, \beta_j \in \mathbb{F}_{2^m}\} \tag{11}$$

such that $D_{a_i} D_{a_{i'}} f^* = D_{b_j} D_{b_{j'}} f^* = 0$ for any $a_i, a_{i'} \in A, b_j, b_{j'} \in B$, where $i \ne i'$ and $j \ne j'$.

The following result ensures the bentness of the function $h$ defined by (6) if $F$ is defined by (10).

**Lemma 4.1** *Let $f$ be a bent function on $\mathbb{F}_{2^n}$, $n = 2m$, defined by $f(y, z) = Tr_1^m(y\pi(z))$ with the dual $f^*(y, z) = Tr_1^m(z\pi^{-1}(y))$. Let $h$ be defined as in (6) with $F$ as in (10), where the functions $G_i$ are defined using $A$ and $B$ in (11). The function $h$ is bent if*

$$\{D_{\alpha_i} \pi^{-1}(y) : y \in \mathbb{F}_{2^m}, (\alpha_i, 0) \in A\} \subseteq \langle \beta_i : (0, \beta_i) \in B\rangle^\perp. \tag{12}$$

***Proof*** Suppose $G_1 G_2 = 0$, i.e. at least one of the functions $G_1$ and $G_2$ is zero. Then $F = G_3$ and the result follows from the property of the set $A$. Let $G_1 G_2 \ne 0$, i.e. we are now "mixing" the elements from $A$ and $B$. Let $a_i = (\alpha_i, 0) \in A$ and $b_j = (0, \beta_j) \in B$ be arbitrary. Then,

$$D_{a_i} D_{b_j} f^*(y, z) = D_{(\alpha_i, 0)} D_{(0, \beta_j)}(Tr_1^m(z\pi^{-1}(y))) = Tr_1^m(\beta_j D_{\alpha_i} \pi^{-1}(y)) = 0,$$

for all $y \in \mathbb{F}_{2^m}$ as

$$\left\{D_{\alpha_i} \pi^{-1}(y) : y \in \mathbb{F}_{2^m}, (\alpha_i, 0) \in A\right\} \subseteq \langle \beta_i : (0, \beta_i) \in B\rangle^\perp.$$

The conclusion follows from Theorem 3.1. □

***Remark 4.1*** Referring to Remark 3.4, the choice of $A$ and $B$ and the associated functions $G_i$ can be deduced from the non-trivial vanishing subspace $V$ of $f^*$. More precisely, the set $A$ can be potentially defined using $(\alpha_1, 0)$ and $(\alpha_2, 0)$ (corresponding to the first two rows of $V$) whereas $B$ corresponds to the last three rows of $V$.

Even though the choice of $A$ and $B$ is relatively easy, the main difficulty in ensuring the bentness of $h$ in Lemma 4.1 is the condition given in Eq. (12) related to the first-order derivatives of $\pi^{-1}$, which is not easily satisfied.

**Theorem 4.1** *Let $f$ be a bent function on $\mathbb{F}_2^n$, $n = 2m$, defined with $f(y, z) = Tr_1^m(y\pi(z))$ and let $A$ and $B$ be defined by (11) so that $D_{a_i} D_{a_j} f^* = D_{b_i} D_{b_j} f^* = 0$, for any $a_i, a_j \in A, b_i, b_j \in B$ for $i \ne j$, where $a_i = (\alpha_i, 0)$ and $b_j = (0, \beta_j)$ for $\alpha_i, \beta_j \in \mathbb{F}_{2^m}$. Assume that $\{D_{\alpha_i} \pi^{-1}(x) : x \in \mathbb{F}_{2^m}\} \subseteq \langle B\rangle^\perp$ for all $1 \le i \le k$ and define $h$ as in (6) with $F$ as in (10). If:*

(a) $D_a G_1(y) \neq const$, *for all nonzero* $a \in \mathbb{F}_2^m$,
(b) $\deg(G_2) > 2$ *and* $D_a G_2(y) \neq const$, *for all nonzero* $a \in \mathbb{F}_2^m$,

*then* $h$ *is a bent function outside* $\mathcal{MM}^{\#}$.

***Proof*** From Lemma 4.1, we have that $h$ is a bent function. For simplicity, we denote $F(y, z) = G_1(y)G_2(z) + G_3(y)$ using the dependency through the formal variables $X_i$ as in (10). Let $V$ be any $m$-dimensional subspace of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Let $a = (a_1, a_2), b = (b_1, b_2) \in V$ be arbitrary. The second-order derivative of $h$ with respect to $a$ and $b$ can be written as:

$$\begin{aligned} & D_{(a_1,a_2)} D_{(b_1,b_2)} h(y, z) \\ & \quad = Tr_1^m(y\left(D_{a_2} D_{b_2} \pi(z)\right) + a_1 D_{b_2} \pi(z + a_2) + b_1 D_{a_2} \pi(z + b_2)) \\ & \qquad + D_a D_b G_1(y) G_2(z) + D_{a_1} D_{b_1} G_3(y) \\ & \quad = Tr_1^m(y\left(D_{a_2} D_{b_2} \pi(z)\right) + a_1 D_{b_2} \pi(z + a_2) + b_1 D_{a_2} \pi(z + b_2)) \\ & \qquad + G_1(y) D_{a_2} D_{b_2} G_2(z) + G_2(z + a_2) D_{a_1} G_1(y) \\ & \qquad + G_2(z + b_2) D_{b_1} G_1(y) + G_2(z + a_2 + b_2) D_{a_1+b_1} G_1(y) \\ & \qquad + D_{a_1} D_{b_1} G_3(y). \end{aligned} \tag{13}$$

We denote the set $\{(y, 0) \mid y \in \mathbb{F}_{2^m}\}$ by $\Delta$, and consider two cases $V = \Delta$ and $V \neq \Delta$.

a. For $V = \Delta$, there exist two vectors $(a_1, 0), (b_1, 0) \in \Delta$ such that $D_{a_1} D_{b_1} G_1(y) \neq 0$ since $\Delta = \{(y, 0) \mid y \in \mathbb{F}_{2^m}\}$ and $G_1$ has no nonzero linear structure. That is, since $D_{a_1} G_1(y) \neq const$, for all $a_1 \in \mathbb{F}_{2^m}$, then there must exist $b_1 \in \mathbb{F}_{2^m}$ such that $D_{a_1} D_{b_1} G_1(y) \neq 0$. From (13), we get:

$$\begin{aligned} D_{(a_1,0)} D_{(b_1,0)} h(y, z) &= G_2(z)[D_{a_1} G_1(y) + D_{b_1} G_1(y) \\ & \quad + D_{a_1+b_1} G_1(y)] + D_{a_1} D_{b_1} G_3(y) \\ &= G_2(z) D_{a_1} D_{b_1} G_1(y) + D_{a_1} D_{b_1} G_3(y) \neq 0, \end{aligned} \tag{14}$$

since $D_{a_1} D_{b_1} G_1(y) \neq 0$. Notice that in (14) we used the fact that $D_{a_1} D_{b_1} G_1(y) = G_1(y) + G_1(y + a_1) + G_1(y + b_1) + G_1(y + a_1 + b_1) = D_{a_1} G_1(y) + D_{b_1} G_1(y) + D_{a_1+b_1} G_1(y)$.

b. For $V \neq \Delta$, we split the proof into two cases depending on the cardinality of $V \cap \Delta$. We set $V = \left\{(v_1^{(1)}, v_2^{(1)}), (v_1^{(2)}, v_2^{(2)}), \ldots, (v_1^{(2^m)}, v_2^{(2^m)}\right\}$,

(a) For $|V \cap \Delta| = 1$, we have $v_2^{(i)} \neq v_2^{(j)}$ for any $i \neq j$. As in the proof of Theorem 3.2, we have that $\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^m)}\} = \mathbb{F}_{2^m}$.
Thus, from Lemma 2.1,we can find two vectors $a, b \in V$ such that $D_{a_2} D_{b_2} G_2(z) \neq 0$, since $\deg(G_2) > 2$.
From (13), we have

$$D_{(a_1,a_2)} D_{(b_1,b_2)} h(y, z) \neq 0,$$

since $G_1(y) D_{a_2} D_{b_2} G_2(z) \neq 0$, $\deg(G_1) > 1$ and $\deg(G_1) > \deg(D_c(G_1))$, for any $c \in \mathbb{F}_{2^m}$.

(b) For $|V \cap \Delta| \geq 2$, without loss of generality, let $a = (a_1, 0) \in V^* \cap \Delta$, where $V^* = V \backslash (0)$. Select $b \in V \setminus \{0, a\}$ such that $b_2 \neq 0$. Thus, (13) reduces to

$$\begin{aligned} D_a D_b h(y,z) &= Tr_1^m(a_1 D_{b_2}\pi(z)) + G_1(y)G_2(z) + G_1(y+a_1)G_2(z) \\ &\quad + G_1(y+b_1)G_2(z+b_2) + G_1(y+a_1+b_1)G_2(z+b_2) \\ &\quad + D_{a_1}D_{b_1}G_3(y) \\ &= Tr_1^m(a_1 D_{b_2}\pi(z)) + G_2(z)D_{a_1}G_1(y) + G_2(z+b_2)D_{a_1}G_1(y+b_1) \\ &\quad + D_{a_1}D_{b_1}G_3(y) \\ &= Tr_1^m(a_1 D_{b_2}\pi(z)) + G_2(z)D_{a_1}G_1(y) + G_2(z+b_2)D_{a_1}G_1(y+b_1) \\ &\quad + D_{a_1}D_{b_1}G_3(y) + G_2(z+b_2)D_{a_1}G_1(y) + G_2(z+b_2)D_{a_1}G_1(y) \\ &= Tr_1^m(a_1 D_{b_2}\pi(z)) + D_{b_2}G_2(z)D_{a_1}G_1(y) + G_2(z+b_2)D_{a_1}D_{b_1}G_1(y) \\ &\quad + D_{a_1}D_{b_1}G_3(y). \end{aligned} \tag{15}$$

Since $\deg(D_c G_1) > \deg(D_c D_d(G_1))$, for any distinct $c, d \in \mathbb{F}_{2^m}$, and $G_2$ has no nonzero linear structure, we have that $D_{b_2}G_2(z)D_{a_1}G_1(y) + G_2(z + b_2)D_{a_1}D_{b_2}G_1(y) \neq 0$ (the terms having different nonzero degrees in $z$ and $y$ which cannot be cancelled by the two remaining terms) and thus from (15), we have

$$D_a D_b h(y,z) \neq 0.$$

Summarizing all the cases, we conclude that $h$ is outside $\mathcal{MM}^\#$. □

We emphasize that this is the first time a specific set of conditions for $h$ to be outside $\mathcal{MM}^\#$ has been given without requiring that the component functions of $\pi$ do not admit linear structures. A construction method of bent functions outside $\mathcal{MM}^\#$ that belong to the $\mathcal{C}$ class, whose permutations admit linear structures, was considered for instance in [13].

***Remark 4.2*** Notice the absence of conditions on $G_3$, which can also affect the property that $D_a D_b h \neq 0$. Essentially, the condition $Tr_1^m(a_1 D_{b_2}\pi(z)) + D_{b_2}G_2(z)D_{a_1}G_1(y) + G_2(z + b_2)D_{a_1}D_{b_1}G_1(y) + D_{a_1}D_{b_1}G_3(y)$ for nonzero $a_1, b_2 \in \mathbb{F}_2^m$ and any $b_1 \in \mathbb{F}_2^m$ in (15), can be considered in terms of $G_3$ as well, thus requiring that $D_{a_1}D_{b_1}G_3(y) \neq 0$. The condition that $D_{a_1}D_{b_1}G_3(y) \neq 0$ can be easily satisfied if we specify $G_3(y) = \prod_{i=1}^m(1 + y_i) = \delta_0(y)$, unless $b_1 = 0$ or $a_1 = b_1$. However, it is not clear whether the condition that $D_{a_1}G_1(y) \neq const$ (alternatively that $D_{b_2}G_2(z) \neq const$) in Theorem 4.1 can be then removed.

We notice that it is not necessary to consider the defining sets $A$ and $B$ using the canonical decomposition (as a direct sum) of $\mathbb{F}_2^m \times \mathbb{F}_2^m$ into the disjoint subspaces $\mathbb{F}_2^m \times \{0_m\}$ and $\{0_m\} \times \mathbb{F}_2^m$, so that the elements $a_i = (\alpha_i, 0_m) \in A$ and $b_j = (0_m, \beta_j) \in B$, see (11). We recall that the initial condition on the sets $A$ and $B$ were that $D_a D_{a'} f^* = 0$ and $D_b D_{b'} f^* = 0$, for all $a, a' \in A$ and all $b, b' \in B$. Referring back to Remark 3.4, a non-trivial vanishing subspace $V$ of $f^*$ can be used to define $A = \{(\alpha_i, 0_m)\}$ (taking the first two rows of $V$) and $B = \{(0_m, \beta_j)\}$ (taking the three last rows of $V$). Nevertheless, by taking another basis of $V$ for which we do not necessarily have the above form for the elements in $A$ and $B$, we can satisfy that $D_a D_{a'} f^* = 0$ and $D_b D_{b'} f^* = 0$ even though $a_i = (\alpha_i, u_i)$ and $b_j = (v_j, \beta_j)$. In general, we have $D_{(\alpha_i,u_i)}D_{(v_j,\beta_j)}f^*(y,z) = Tr_1^m(zD_{u_i}D_{\beta_j}\pi^{-1}(y) + \alpha_i D_{\beta_j}\pi(y+u_i) + v_j D_{u_i}\pi(y+\beta_j))$ and it is identically zero for any $(\alpha_i, u_i), (v_j, \beta_j) \in V$, whenever $V$ is a vanishing subspace of $f^*$.

On the other hand, the decomposition of $F$ in Theorem 3.1 as $F(y,z) = G_1(y)G_2(z) + G_3(y)$ is not possible any longer (due to the use of elements of the form $a_i = (\alpha_i, u_i)$ and $b_j = (v_j, \beta_j)$) and the related conditions for $h$ to be outside $\mathcal{MM}^\#$ cannot be stated through the properties of $G_i$. It is an interesting research challenge to provide a set of sufficient conditions on $F(y, z)$ in this general setting (if possible) so that $h(y, z) = f(y, z) + F(y, z)$ is a bent function outside $\mathcal{MM}^\#$.

### 4.1 Specifying non-trivial defining sets using permutations with linear structures

As already illustrated, a suitable selection of $\mu_i$ for a given permutation $\pi$ is easily specified using the vanishing subspaces for the dual $f^*$. However, one generic method of specifying non-trivial defining sets that stem from permutations with linear structures can also be specified.

**Theorem 4.2** *Let $\pi$ be a permutation of $\mathbb{F}_2^m$ and assume that $S = \langle s_1, \ldots, s_k \rangle$ (with $1 \leq k \leq m - 2$) is a space of linear structures for $\pi^{-1}$, so that $\pi^{-1}(y) + \pi^{-1}(y + s_i) = v_i = const \in \mathbb{F}_2^m$, for all $s \in S$. Then, the dual of $f(y, z) = y \cdot \pi(z))$, where $y, z \in \mathbb{F}_2^m$, defined by $f^*(y, z) = z \cdot \pi^{-1}(y)$, admits a non-trivial vanishing subspace $V = \langle S \times \{0\}, \langle (v_1, 0), \ldots, (v_k, 0) \rangle^\perp \rangle$ of dimension $m$.*

***Proof*** As already mentioned, $D_a D_b f^*(y, z) = 0$ for all $a, b \in \{0_m\} \times \mathbb{F}_2^m$, which is a trivial vanishing subspace of $f^*$ of maximal dimension $m$. Now let $S' = S \times \{0\}$, with $\dim(S') = k$, and extend the basis of $S'$ to $V$ by adjoining the basis of $\langle (v_1, 0_m), \ldots, (v_k, 0_m) \rangle^\perp$, thus adjoining $m - k$ linearly independent elements of the form $(0_m, u_i)$, where $i = 1, \ldots, m - k$. Then, $\dim(V) = m$. For two different non-zero vectors $a = (a_1, a_2)$ and $b = (b_1, b_2)$ in $V$, we compute

$$D_a D_b f^*(y, z) = z \cdot \left( D_{a_1} D_{b_1} \pi^{-1}(y) \right) + a_2 \cdot D_{b_1} \pi^{-1}(y + a_1) + b_2 \cdot D_{a_1} \pi^{-1}(y + b_1).$$

It is clear that for any $a, b \in S'$ we have that $D_a D_b f^*(y, z) = 0$, since $a_2 = b_2 = 0_m$ and furthermore $D_{a_1} D_{b_1} \pi^{-1}(y) = 0$. Selecting $a, b$ to be of the form $(0_m, u_i)$ leads to the same conclusion since $a_1 = b_1 = 0_m$. Finally, if $a \in S'$ and $b = (0_m, u_i)$, then the only term that may not be canceled is $b_2 \cdot D_{a_1} \pi(y)$. However, since $b \in \langle (v_1, 0_m), \ldots, (v_k, 0_m) \rangle^\perp$ and $D_{a_1} \pi(y) = v_i$, we have that $b_2 \cdot D_{a_1} \pi(y) = 0$. □

We notice that permutations $\pi$ on $\mathbb{F}_2^m$, described in Theorem 4.2, need to satisfy the conditions of Theorem 4.1 concerning the bentness of $h$, whereas the property of being outside $\mathcal{MM}^\#$ can be achieved by a proper choice of $G_1$, $G_2$ and $G_3$. More precisely, we need to identify permutations $\pi$ on $\mathbb{F}_2^m$ for which the sets $A$ and $B$ in (11) satisfy that:

- $D_{a_i} D_{a_{i'}} f^* = D_{b_j} D_{b_{j'}} f^* = 0$ for any $a_i, a_{i'} \in A$, $b_j, b_{j'} \in B$, where $i \neq i'$ and $j \neq j'$;
- For any specific choice of $A$ and $B$, Eq. (12) needs to be satisfied.

One possibility of defining (quadratic) permutations that admit more than one linear structure is as follows.

**Proposition 4.1** *Assume that $\sigma$ is a permutation of $\mathbb{F}_2^m$ which admits a nonzero linear structure, so that $\sigma(y) + \sigma(y + a) = v$. Define*

$$\pi(y, y_{m+1}) = (\sigma(y), y_{m+1}), \;\; y_{m+1} \in \mathbb{F}_2,$$

*which is then a permutation over $\mathbb{F}_2^{m+1}$. Then, both $(a, 0)$ and $(a, 1)$ are non-zero linear structures of $\pi$.*

***Proof*** It is clear that $\pi$ is a permutation if $\sigma$ is a permutation. For the linear structures, we check that $(a, 1)$ is a nonzero linear structure of $\pi$. We have,

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

and similarly one can verify the same for $(a, 0)$. □

Since, by Corollary 5 in [8], any quadratic permutation on $\mathbb{F}_2^4$ admits at least one nonzero linear structure, the above result allows as to build larger spaces of linear structures for permutations of $\mathbb{F}_2^m$, where $m > 4$.

**Open Problem 2** *Find generic methods for specifying permutations with or without linear structures and the associated functions $G_i$ so that the conditions in Theorem 4.1 are satisfied.*

## 5 Class inclusion of bent functions obtained via $\mathcal{P}_\tau$ property

In the recent works [1, 2], the authors provided examples of functions outside $\mathcal{MM}^\#$, which they denoted as functions in the $\mathcal{SC}$ and $\mathcal{CD}$ class. Furthermore, in [13], the authors provided conditions for which functions in $\mathcal{D}_0$ are provably outside $\mathcal{MM}^\#$. We summarize the results below and connect them with the representation of $F$ given by (10):

- $\mathcal{D}_0$ case (Theorem 5 in [13]). Let $m \geq 4$ be an integer and let $\pi$ be a permutation on $\mathbb{F}_{2^m}$ with algebraic degree $\deg(\pi) \geq 3$. Then the function $h : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by

$$h(y, z) = Tr_1^m(y\pi(z)) + \prod_{i=1}^{m} \left(Tr_1^m(\alpha^i y) + 1\right) = Tr_1^m(y\pi(z)) + G_3(y),$$

  where $\alpha$ is a primitive element of $\mathbb{F}_{2^m}$, is a bent function in $\mathcal{D}_0$ outside $\mathcal{MM}^\#$.
- $\mathcal{SC}$ case (Proposition 7 in [2]). Let $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a bent function defined by $f(y, z) = Tr_1^m(yz^d)$ where $d(2^s + 1) \equiv 1(\text{mod } 2^m - 1)$ and $wt(d) \geq 3$, $s$ is a positive divisor of $m$ such that $m/s$ is odd. Let $\alpha$ be a primitive element of $\mathbb{F}_{2^s}$ and $\lambda$ a primitive element of $\mathbb{F}_{2^m}$. Then the function

$$\begin{aligned} h(y, z) &= f(y, z) + \prod_{i=1}^{s} \left(Tr_1^m(\alpha^i y) + 1\right) + \prod_{i=1}^{m} \left(Tr_1^m(\lambda^i y) + 1\right) \\ &= f(y, z) + G_3^{(1)}(y) + G_3^{(2)}(y) \end{aligned}$$

  is a bent function outside $\mathcal{MM}^\#$.
- $\mathcal{CD}$ case ([2, Theorem 11]). Let $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a bent function defined by $f(y, z) = Tr_1^m(yz^d)$ where $d(2^s + 1) \equiv 1(\text{mod } 2^m - 1)$ and $wt(d) \geq 3$, $s$ is a positive divisor of $m$ such that $m/s$ is odd. Let $E_2$ be a subfield of $\mathbb{F}_{2^s}$ (which corresponds to a subspace of $\mathbb{F}_{2^m}$), $E_1 = E_2^\perp$ and $L \subset E_2$ be any subspace of $\mathbb{F}_{2^m}$. Then, the function

$$\begin{aligned} h(y, z) = f(y, z) &+ \prod_{\mu_1 \in \mathbf{b}(E_1)} \left(Tr_1^m(\mu_1 y) + 1\right) \prod_{\mu_2 \in \mathbf{b}(E_2)} \left(Tr_1^m(\mu_2 z) + 1\right) \\ &+ \prod_{\mu \in \mathbf{b}(L)} \left(Tr_1^m(\mu y) + 1\right) \\ &= f(y, z) + G_1(y)G_2(z) + G_3(y) \end{aligned}$$

  is a bent function outside $\mathcal{MM}^\#$, where $\mathbf{b}(\cdot)$ denotes the basis of a given subspace.

Let us now discuss the relationship between the class $\mathcal{P}_\tau$ (the class of all bent functions obtained via Theorem 3.1) and the classes $\mathcal{SC}$, $\mathcal{CD}$, $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}_0$. First of all, we notice that the so-called superclasses $\mathcal{SC}$, $\mathcal{CD}$ are defined using the addition of exactly two very particular indicators. On the other hand, Theorem 4.1 provides much more general framework since a larger number of suitable indicators can be added to $f(y,z) = Tr_1^m(yz)$. In this context, we observe the following differences and similarities between these classes.

Let us consider the function $f \in \mathcal{B}_{2m}$ defined by $f(y,z) = Tr_1^m(yz) + \delta_0(y)$. It is easy to note that $f$ is contained in all of the above mentioned classes. In other words,

$$\mathcal{P}_\tau \cap \mathcal{C} \cap \mathcal{SC} \cap \mathcal{D}_0 \cap \mathcal{D} \cap \mathcal{CD} \neq \emptyset.$$

From Example 3.2, we observed that the truth table of the function $f(y,z) = Tr_1^9(yz^{284}) \in \mathcal{MM}$ on $\mathbb{F}_2^9 \times \mathbb{F}_2^9$ was modified in $2^9 \cdot 192$ places. Thus, it was not modified on a subspace, which implies that $h \notin \mathcal{D}_0, \mathcal{D}$ or $\mathcal{C}$. On the other hand, functions in $\mathcal{SC}$ modify a function in $\mathcal{MM}$ in $2^m(2^r - 1)$ places [1] which does not correspond to this number either. This is a consequence of the fact that the class $\mathcal{SC}$ uses the addition of two indicators (of two suitable subspaces), whereas the function $h$ in Example 3.2 is defined as

$$\begin{aligned} h(y,z) &= Tr_1^9\left(yz^{284}\right) + Tr_1^9(y) Tr_1^9\left(\omega^{73}y\right) Tr_1^9\left(\omega^{146}y\right) + Tr_1^9(y) \\ &\quad + Tr_1^9\left(\omega^{73}y\right) Tr_1^9\left(\omega^{73}y\right) Tr_1^9\left(\omega^{146}y\right), \end{aligned}$$

which corresponds to the addition of three different indicators. Thus, the function $h \notin \mathcal{SC}$. By noting that $h(y,z) = f(y,z) + G_1(y) + G_2(y) + G_3(y)$ uses the indicators that do not depend on the $z$ variable, we conclude that $h \notin \mathcal{CD}$. In other words,

$$\mathcal{P}_\tau \not\subset (\mathcal{C} \cup \mathcal{SC} \cup \mathcal{D}_0 \cup \mathcal{D} \cup \mathcal{CD}).$$

## 6 Conclusions

In this article, we have analyzed the properties of the so-called $\mathcal{P}_\tau$ method of constructing bent functions. We partially answer an open problem in [12] posed by Kan et al. (IEEE Trans Inf Theory, https://doi.org/10.1109/TIT.2022.3140180, 2022) by identifying those instances of bent functions that are provably outside $\mathcal{MM}^\#$ within this framework. We also demonstrate that the family of bent functions obtained using the $\mathcal{P}_\tau$ method is neither included in the classes $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}_0$ nor in the recently introduced classes $\mathcal{SC}$ and $\mathcal{CD}$. Even though we have provided a theoretical framework for using permutations whose components do not admit linear structures, it remains to specify some generic methods of identifying suitable permutations $\pi$ that satisfy (12) and the associated functions $G_i$ that ensure both bentness and the outside $\mathcal{MM}^\#$ property of the generated functions.

**Acknowledgements** Enes Pasalic is partly supported by the Slovenian Research Agency (research program P1-0404 and research Projects N1-0159, J1-2451 and J1-4084). Fengrong Zhang is supported in part by the Natural Science Foundation of China (Grant Nos. 62372346 and 61972400) and the Youth Innovation Team of Shaanxi Universities. Yongzhuang Wei is supported by the Guangxi Natural Science Foundation (Grant No. 2019GXNSFGA245004).

## Declarations

**Conflict of interest** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References

1. Bapić A., Pasalic E.: Constructions of (vectorial) bent functions outside the completed Maiorana–McFarland class. Discret. Appl. Math. **314**, 197–212 (2022).
2. Bapić A., Pasalic E., Zhang F., Hodžić S.: Constructing new superclasses of bent functions from known ones. Cryptogr. Commun. (2022). https://doi.org/10.1007/s12095-022-00566-7.
3. Carlet C.: Two new classes of bent functions. In: Proc. EUROCRYPT '93, in Lecture Notes in Computer Science, vol. e 765, pp. 77–101 (1993).
4. Carlet C.: On the secondary constructions of resilient and bent functions. In: Proc. Coding, Cryptograph. Combinat., published by Birkhäuser Verlag, vol. 23, pp. 3–28 (2004).
5. Carlet C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2021).
6. Carlet C., Mesnager S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5–50 (2016).
7. Carlet C., Zhang F., Hu Y.: Secondary constructions of bent functions and their enforcement. Adv. Math. Commun. **6**, 305–314 (2012).
8. Charpin P., Sarkar S.: Polynomials with linear structure and Maiorana–McFarland construction. IEEE Trans. Inf. Theory **49**(8), 2004–2019 (2011).
9. Dillon J.F.: Elementary Hadamard difference sets. Ph.D. dissertation. University of Maryland, College Park, MD, USA (1974).
10. Duan M., Yang M., Sun X., Zhu B., Lai X.: Distinguishing properties and applications of higher order derivatives of Boolean functions. Inf. Sci. **271**, 224–235 (2014).
11. Hodžić S., Pasalic E., Wei Y.: A general framework for secondary constructions of bent and plateaued functions. Des. Codes Cryptogr. **88**(10), 2007–2035 (2020).
12. Li Y., Kan H., Mesnager S., Peng J., Tan C.H., Zheng L.: Generic constructions of (Boolean and vectorial) bent functions and their consequences. IEEE Trans. Inf. Theory (2022). https://doi.org/10.1109/TIT.2022.3140180.
13. Kudin S., Pasalic E.: A complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^\#$ and a general framework for specifying bent functions in $\mathcal{C}$ outside $\mathcal{M}^\#$. Des. Codes Cryptogr. **90**(10), 1783–1796 (2022).
14. Kudin S., Pasalic E., Cepak N., Zhang F.: Permutations without linear structures inducing bent functions outside the completed Maiorana–McFarland class. Cryptogr. Commun. **14**, 101–116 (2022).
15. McFarland R.L.: A family of noncyclic difference sets. J. Comb. Theory Ser. A **15**, 1–10 (1973).
16. Mesnager S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inf. Theory **60**(7), 4397–4407 (2014).
17. Mesnager S.: Bent Functions—Fundamentals and Results. Springer, Cham (2016).
18. Pasalic E., Zhang F., Kudin S., Wei Y.: Vectorial bent functions weakly/strongly outside the completed Maiorana–McFarland class. Discret. Appl. Math. **294**, 138–151 (2021).
19. Pasalic E., Bapić A., Zhang F., Wei Y.: Explicit infinite families of bent functions outside $\mathcal{MM}^\#$. Des. Codes Cryptogr. **91**, 2365–2393 (2023).
20. Pasalic E., Kudin S., Polujan A., Pott A.: Vectorial Bent-Negabent functions—their constructions and bounds. IEEE Trans. Inf. Theory **69**(4), 2702–2712 (2023).
21. Polujan A.A., Pott A.: Cubic bent functions outside the completed Maiorana–McFarland class. Des. Codes Cryptogr. **88**, 1701–1722 (2020).
22. Rothaus O.S.: On 'bent' functions. J. Comb. Theory Ser. A **20**(3), 300–305 (1976).
23. Tang C., Zhou Z., Qi Y., Zhang X., Fan C., Helleseth T.: Generic construction of bent functions and bent idempotents with any possible algebraic degrees. IEEE Trans. Inf. Theory **63**(10), 6149–6157 (2017).
24. Wang L., Wu B., Liu Z., Lin D.: Three new infinite families of bent functions. Sci. China Inf. Sci. **61**, 032104 (2018).

25. Xu G., Cao X., Xu S.: Several new classes of Boolean functions with few Walsh transform values. Appl. Algebra Eng. Commun. Comput. **28**(2), 155–176 (2017).
26. Zhang F., Wei Y., Pasalic E.: Constructions of Bent–Negabent functions and their relation to the completed Maiorana–McFarland class. IEEE Trans. Inf. Theory **61**(3), 1496–1506 (2015).
27. Zhang F., Pasalic E., Cepak N., Wei Y.: Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana–McFarland class. In: Pro. Codes, Cryptology and Information Security, LNCS 10194, Springer, pp. 298–313 (2017).
28. Zhang F., Pasalic E., Wei Y., Cepak N.: Constructing bent functions outside the Maiorana–McFarland class using a general form of Rothaus. IEEE Trans. Inf. Theory **63**(8), 5336–5349 (2017).
29. Zhang F., Cepak N., Pasalic E., Wei Y.: Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^{\#}$. Discret. Appl. Math. **285**(1), 458–472 (2020).
30. Zheng L., Peng J., Kan H., Li Y.: Several new infinite families of bent functions via second order derivatives. Cryptogr. Commun. **12**, 1143–1160 (2020).

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.