Designs, Codes and Cryptography (2020) 88:1701–1722
https://doi.org/10.1007/s10623-019-00712-y

Cubic bent functions outside the completed Maiorana-McFarland class

Alexandr A. Polujan[1] · **Alexander Pott**[1]

Received: 3 September 2019 / Revised: 21 December 2019 / Accepted: 24 December 2019 /
Published online: 13 February 2020

Abstract
In this paper we prove that in opposite to the cases of 6 and 8 variables, the Maiorana-McFarland construction does not describe the whole class of cubic bent functions in n variables for all $n \geq 10$. Moreover, we show that for almost all values of n, these functions can simultaneously be homogeneous and have no affine derivatives.

Keywords Cubic bent functions · Homogeneous functions · Affine derivatives · Equivalence of Boolean functions · Completed Maiorana-McFarland class

Mathematics Subject Classification 05B10 · 06E30 · 14G50 · 94C30

1 Introduction

Bent functions, introduced by Rothaus in [35], are Boolean functions having the maximum Hamming distance from the set of all affine functions. Being extremal combinatorial objects, they have been intensively studied in the last four decades, due to their broad applications to cryptography, coding theory and theory of difference sets.

Cubic bent functions, i.e. bent functions of algebraic degree three, attracted a lot of attention from researchers, partly because small algebraic degree of these functions allows to investigate them exhaustively, when the number of variables is not too large. For instance, all cubic bent functions in six and eight variables are well-understood: the classification is given in [3,35], the enumeration was obtained in [23,33], and all these functions belong to

The first version of this work [30] was presented in the "Eleventh International Workshop on Coding and Cryptography (WCC 2019)".

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue on Coding and Cryptography 2019".

✉ Alexandr A. Polujan
alexandr.polujan@gmail.com; alexandr.polujan@ovgu.de

Alexander Pott
alexander.pott@ovgu.de

[1] Otto von Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany

the completed Maiorana-McFarland class $\mathcal{M}^{\#}$ [3,10]. A couple of infinite families of cubic bent functions were constructed recently, however, some of them [5,24] are proved to be the members of $\mathcal{M}^{\#}$, while some of them are not analyzed yet [14,28]. Therefore, it is not clear, whether an n-variable cubic bent function can be outside the $\mathcal{M}^{\#}$ class whenever $n \geq 10$. At the same time, cubic bent functions, which are homogeneous or have no affine derivatives, are of a special interest.

A cubic function has no affine derivatives, if all its non-trivial first-order derivatives are quadratic, what makes cryptographic systems with such components more resistant to certain differential attacks. It is well-known that cubic bent functions without affine derivatives exist for all even $n \geq 6, n \neq 8$, as it was shown in in [4,20]. Recently Mandal, Gangopadhyay and Stănică in [26] constructed two classes of cubic bent functions without affine derivatives inside $\mathcal{M}^{\#}$ and proved their mutual inequivalence. They also suggested to find such functions outside the $\mathcal{M}^{\#}$ class and evaluate their significance for cryptographic applications [26, Sect. 1.6].

A Boolean function is called homogeneous, if all the monomials in its algebraic normal form have the same algebraic degree. Homogeneous cubic bent functions were firstly considered by Qu et al. in [34], motivated by faster evaluation in cryptographic systems. The only known homogeneous bent functions are quadratic and cubic, moreover, it is not known, whether homogeneous bent functions of higher degrees exist. While the characterization of homogeneous quadratic bent functions is well-known [25, Chapter 15], it is in general a difficult task to construct a homogeneous cubic bent function. The only known primary construction was given by Seberry et al. in [36]. They proved, that a proper linear transformation of variables can bring special non-homogeneous cubic bent function from $\mathcal{M}^{\#}$ to a homogeneous one. Unfortunately, all functions of this type have many affine derivatives. Another approach is based on the concatenation of homogeneous cubic bent functions in a small number of variables via direct sum. The known computational construction methods of such functions include:

- The tools from the modular invariant theory, as it was shown by Charnes, Rötteler and Beth in [8];
- The significant reduction of the search space, suggested by Meng et al. in [27].

Using these approaches, the mentioned authors constructed a lot of homogeneous cubic bent functions in a small number of variables $6 \leq n \leq 12$. However, since all these examples have not been analyzed with respect to being outside the $\mathcal{M}^{\#}$ class and having no affine derivatives, it is not clear, which properties can the concatenations of these functions have.

The aim of this paper is two-fold. First, we analyze the known homogeneous cubic bent functions in ten and twelve variables from [8,27] and show, that some of these functions do not belong to the the $\mathcal{M}^{\#}$ class and all of them are different from the primary construction of Seberry, Xia and Pieprzyk [36]. Moreover, some of them have no affine derivatives. Secondly, we extend these results for infinite families, by showing, that proper direct sums of these functions inherit the properties of its summands. Consequently, we prove that for any $n \geq 8$ there exist cubic bent functions inside $\mathcal{M}^{\#}$, but different from the primary construction [36]. Further, we consider cubic bent functions with respect to the following three properties: outside $\mathcal{M}^{\#}$, without affine derivatives, and homogeneous. We show, that n-variable cubic bent functions with at least two of the three mentioned properties exist for all $n \geq n_0$, where n_0 depends on the selected combination of properties. In this way, we prove that in general the whole class of cubic bent functions in n variables is not described by the $\mathcal{M}^{\#}$ class, whenever $n \geq 10$. Finally, we show existence of cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$, thus solving a recent open problem by Mandal et al. [26, Sect. 1.6].

The paper is organized in the following way. In Subsect. 1.1 we introduce some basic notions and background on Boolean functions. Section 2 describes geometric invariants of Boolean functions, which we use in the next section in order to distinguish inequivalent functions. Section 3 deals with the construction of new homogeneous cubic bent functions from old. First, in Subsect. 3.1 we survey the known homogeneous bent functions, provide the classification of known examples and show, that some of them are not in the $\mathcal{M}^{\#}$ class. In Subsect. 3.2, we show that proper concatenations of homogeneous cubic functions can never be equivalent to the primary construction. Finally, in Subsect. 3.3 we introduce an approach, aimed to produce many homogeneous functions from a single given one without increasing the number of variables, and illustrate its application for homogeneous cubic bent functions in 12 variables. Section 4 deals with the construction of cubic bent functions outside the $\mathcal{M}^{\#}$ class, using the direct sum. In Subsect. 4.1 we provide a sufficient condition, explaining how one should select bent functions f and g, such that the direct sum $f \oplus g$ is outside $\mathcal{M}^{\#}$. In Subsect. 4.2 we show, that certain cubic bent functions in $6 \leq n \leq 12$ variables satisfy our new sufficient condition and thus lead to infinitely many cubic bent functions outside the $\mathcal{M}^{\#}$ class, which are homogeneous or do not have affine derivatives. The paper is concluded in Sect. 5 and cubic bent functions, used in the paper, are given in the Appendix.

1.1 Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field with two elements and let $\mathbb{F}_2^n$ be the vector space of dimension n over $\mathbb{F}_2$. Mappings $f : \mathbb{F}_2^n \to \mathbb{F}_2$ are called *Boolean functions* in n variables. A Boolean function on $\mathbb{F}_2^n$ can be uniquely expressed as a multivariate polynomial in the ring $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1 \oplus x_1^2, \ldots, x_n \oplus x_n^2)$. This representation is unique and called the *algebraic normal form* (denoted further as ANF), that is,

$$f(\mathbf{x}) = \bigoplus_{\mathbf{v} \in \mathbb{F}_2^n} c_{\mathbf{v}} \left(\prod_{i=1}^{n} x_i^{v_i} \right),$$

where $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, $c_{\mathbf{v}} \in \mathbb{F}_2$ and $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$. The *complement* of a Boolean function f is defined by $\bar{f} := f \oplus 1$. The *algebraic degree* of a Boolean function f, denoted by $\deg(f)$, is the algebraic degree of its ANF. We call a Boolean function *d-homogeneous*, if all the monomials in its ANF have the same degree d, and simply *homogeneous*, if the degree is clear from the context.

With a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ one can associate the mapping $D_{\mathbf{a}} f(\mathbf{x}) := f(\mathbf{x} \oplus \mathbf{a}) \oplus f(\mathbf{x})$, which is called the *first-order derivative* of a function f in the *direction* $\mathbf{a} \in \mathbb{F}_2^n$. Derivatives of higher orders are defined recursively, i.e. the *k-th order derivative* of a function f is given by $D_{\mathbf{a}_k} D_{\mathbf{a}_{k-1}} \ldots D_{\mathbf{a}_1} f(\mathbf{x}) := D_{\mathbf{a}_k}(D_{\mathbf{a}_{k-1}} \ldots D_{\mathbf{a}_1} f)(\mathbf{x})$. For instance, the *second-order derivative* of f is given by $D_{\mathbf{a},\mathbf{b}} f(\mathbf{x}) := D_{\mathbf{b}}(D_{\mathbf{a}} f)(\mathbf{x}) = f(\mathbf{x} \oplus \mathbf{a} \oplus \mathbf{b}) \oplus f(\mathbf{x} \oplus \mathbf{a}) \oplus f(\mathbf{x} \oplus \mathbf{b}) \oplus f(\mathbf{x})$. The point $\mathbf{a} \in \mathbb{F}_2^n$ is called a *fast point* of a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ if it satisfies $\deg(D_{\mathbf{a}} f) < \deg(f) - 1$ and a *slow point*, if $\deg(D_{\mathbf{a}} f) = \deg(f) - 1$. The set of fast points $\mathbb{FP}_f$ forms a vector subspace and its dimension is bounded by $\dim(\mathbb{FP}_f) \leq n - \deg(f)$, as it was shown in [15]. A cubic function has *no affine derivatives*, if $\dim(\mathbb{FP}_f) = 0$, i.e. all its non-trivial first-order derivatives are quadratic functions.

The *direct sum* of two functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and $g : \mathbb{F}_2^m \to \mathbb{F}_2$ is a function $h : \mathbb{F}_2^{n+m} \to \mathbb{F}_2$, defined by $h(\mathbf{x}, \mathbf{y}) := f(\mathbf{x}) \oplus g(\mathbf{y})$. We also define the *$k$-fold direct sum* $k \cdot f : \mathbb{F}_2^{k \cdot n} \to \mathbb{F}_2$ as $k \cdot f(\mathbf{x}_1, \ldots, \mathbf{x}_k) := f(\mathbf{x}_1) \oplus \cdots \oplus f(\mathbf{x}_k)$, for $\mathbf{x}_i \in \mathbb{F}_2^n$.

Definition 1.1 A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called *bent*, if for all $\mathbf{a} \in \mathbb{F}_2^n$ with $\mathbf{a} \neq \mathbf{0}$ and all $b \in \mathbb{F}_2$ the equation $D_{\mathbf{a}} f(\mathbf{x}) = b$ has 2^{n-1} solutions $\mathbf{x} \in \mathbb{F}_2^n$.

Remark 1.2 It is well-known, that bent functions in n variables exist only for n even and have degree at most $n/2$ (see [35]).

On the set of all Boolean functions one can introduce an equivalence relation in the following way: two functions $f, f' \colon \mathbb{F}_2^n \to \mathbb{F}_2$ are called *equivalent*, if there exists a non-degenerate affine transformation $A \in AGL(n, 2)$ and an affine function $l(\mathbf{x}) = \langle \mathbf{a}, \mathbf{x} \rangle_n \oplus b$ on $\mathbb{F}_2^n$ (where $\mathbf{x} \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$ and $\langle \cdot, \cdot \rangle_n$ is a non-degenerate bilinear form on $\mathbb{F}_2^n$), such that $f'(\mathbf{x}) = f(\mathbf{x}A) \oplus l(\mathbf{x})$ holds for all $\mathbf{x} \in \mathbb{F}_2^n$.

Further we will analyze inequivalence of Boolean functions with the help of incidence structures and linear codes. Recall that an *incidence structure* is a triple $\mathbb{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, where $\mathcal{P} = \{p_1, \ldots, p_v\}$ is a set of elements called *points* and $\mathcal{B} = \{B_1, \ldots, B_b\}$ is a set of elements called *lines*, and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ is a binary relation, called *incidence relation*. The *incidence matrix* of $M(\mathbb{S}) = (m_{ij})$ of $\mathbb{S}$ is a binary $b \times v$ matrix with $m_{ij} = 1$ if $p_j \in B_i$ and $m_{ij} = 0$ otherwise. Two incidence structures $\mathbb{S}$ and $\mathbb{S}'$ are *isomorphic*, if there are permutation matrices P and Q such that $P \cdot M(\mathbb{S}) \cdot Q = M(\mathbb{S}')$.

The *linear code* of $\mathbb{S}$ over $\mathbb{F}_2$ is the subspace $\mathcal{C}(\mathbb{S})$ of $\mathbb{F}_2^v$, spanned by the row vectors of the incidence matrix $M(\mathbb{S})$. It is clear, that the incidence matrix $M(\mathbb{S})$ and the linear code $\mathcal{C}(\mathbb{S})$ depend on the labeling of the points and lines of $\mathbb{S}$, however these objects are essentially unique up to row and column permutations. We refer to [12,13] about incidence structures and their linear codes.

Finally, we will use the following notation for vectors and matrices: $\mathbf{j}_n$ is the *all-one-vector* of length n, by $\mathbf{I}_n$ and $\mathbf{J}_n$ we denote the *identity matrix* and the *all-one-matrix* of order n. The *all-zero-matrix* of order n and size $r \times s$ is denoted by $\mathbf{O}_n$ and $\mathbf{O}_{r,s}$ respectively.

1.2 The completed generalized Maiorana-McFarland class of Boolean functions

The *generalized Maiorana-McFarland class* $\mathcal{M}_{r,s}$ of Boolean functions in $n = r + s$ variables [7, p. 354] is the set of Boolean functions of the form

$$f_{\pi,\phi}(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \pi(\mathbf{y}) \rangle_r \oplus \phi(\mathbf{y}), \tag{1.1}$$

where $\mathbf{x} \in \mathbb{F}_2^r$, $\mathbf{y} \in \mathbb{F}_2^s$, ϕ is an arbitrary Boolean function on $\mathbb{F}_2^s$ and $\pi : \mathbb{F}_2^s \to \mathbb{F}_2^r$ is some mapping. A function f belongs to the *completed generalized Maiorana-McFarland class* $\mathcal{M}_{r,s}^{\#}$, if it is equivalent to some function from $\mathcal{M}_{r,s}$. In the case $r = s$, which corresponds to the *original Maiorana-McFarland class* of bent functions $\mathcal{M}$, a function f is bent if and only if the mapping π is a permutation [7, p. 325]. The completed version of $\mathcal{M}$ is denoted by $\mathcal{M}^{\#}$. We will call (1.1) a *Maiorana-McFarland representation* of a given function f on $\mathbb{F}_2^n$, if there exists a non-degenerate linear transformation A, such that $f(\mathbf{z}A) = f_{\pi,\phi}(\mathbf{x}, \mathbf{y})$ for some mappings π and ϕ.

A characterization of the completed Maiorana-McFarland class $\mathcal{M}^{\#}$ of bent functions is given in [11, p. 102] and [6, Lemma 33]. In the case of the $\mathcal{M}_{r,s}^{\#}$ class, the proof is similar.

Proposition 1.3 *Let f be a Boolean function on $\mathbb{F}_2^n$ with $n = r + s$. The following statements are equivalent:*

1. *The function f belongs to the $\mathcal{M}_{r,s}^{\#}$ class.*
2. *There exists a vector subspace U of dimension r such that the second order derivatives $D_{\mathbf{a},\mathbf{b}} f$ vanish for all $\mathbf{a}, \mathbf{b} \in U$, that means $D_{\mathbf{a},\mathbf{b}} f = 0$.*
3. *There exists a vector subspace U of dimension r such that the function f is affine on every coset of U.*

Motivated by this characterization, we introduce $\mathcal{M}$-subspaces of Boolean functions, as those, which satisfy the second statement of the Proposition 1.3.

Definition 1.4 We will call a vector subspace U an $\mathcal{M}$-*subspace* of a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, if for all $\mathbf{a}, \mathbf{b} \in U$ the second-order derivatives $D_{\mathbf{a},\mathbf{b}}f$ are constant zero functions, i.e $D_{\mathbf{a},\mathbf{b}}f = 0$. We denote by $\mathcal{MS}_r(f)$ the collection of all r-dimensional $\mathcal{M}$-subspaces of f and by $\mathcal{MS}(f)$ the collection

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

The following invariant, called linearity index [40, p. 82], measures the maximal possible number of variables of linear functions in a Maiorana-McFarland representation (1.1) of a Boolean function.

Definition 1.5 The *linearity index* $\mathrm{ind}(f)$ of a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is the maximal possible r, such that $f \in \mathcal{M}^{\#}_{r,s}$. In terms of $\mathcal{M}$-subspaces, the linearity index of f is given by $\mathrm{ind}(f) = \max_{U \in \mathcal{MS}(f)} \dim(U)$.

Example 1.6 Let $f(\mathbf{x}) := x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_1x_2x_3$ be a cubic Maiorana-McFarland bent function on $\mathbb{F}_2^6$. Second-order derivatives of f are given by the function $D_{\mathbf{a},\mathbf{b}}f(\mathbf{x}) = c_{\mathbf{0}}(\mathbf{a},\mathbf{b}) \oplus (a_3b_2 \oplus a_2b_3)x_1 \oplus (a_3b_1 \oplus a_1b_3)x_2 \oplus (a_2b_1 \oplus a_1b_2)x_3$, where the constant term $c_{\mathbf{0}}(\mathbf{a},\mathbf{b})$ depends on $\mathbf{a}, \mathbf{b}$ and is given by $c_{\mathbf{0}}(\mathbf{a},\mathbf{b}) := a_1(a_2b_3 \oplus a_3b_2 \oplus b_2b_3) \oplus b_1(a_2a_3 \oplus a_2b_3 \oplus a_3b_2) \oplus a_1b_4 \oplus a_2b_5 \oplus a_3b_6 \oplus a_4b_1 \oplus a_5b_2 \oplus a_6b_3$. One can check that the subspace $U = \langle (0,0,0,1,0,0), (0,0,0,0,1,0), (0,0,0,0,0,1)\rangle$ is an $\mathcal{M}$-subspace of f, since its second-order derivatives $D_{\mathbf{a},\mathbf{b}}f$, which correspond to all two-dimensional vector subspaces $\langle \mathbf{a}, \mathbf{b}\rangle$ of U, are constant zero functions

$$\left\langle \begin{matrix} 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 0&0&0&1&0&0 \\ 0&0&0&0&0&1 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 0&0&0&1&1&0 \\ 0&0&0&0&0&1 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \end{matrix} \right\rangle \mapsto 0,$$
$$\left\langle \begin{matrix} 0&0&0&1&0&1 \\ 0&0&0&0&1&0 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 0&0&0&1&0&0 \\ 0&0&0&0&1&1 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 0&0&0&1&0&1 \\ 0&0&0&0&1&1 \end{matrix} \right\rangle \mapsto 0.$$

Now we describe a naive algorithm, which one can use to construct the collection $\mathcal{MS}_r(f)$ for a given function f and a fixed r. For a more efficient algorithm we refer to [6, Algorithm 2].

Algorithm 1 Construct the collection $\mathcal{MS}_r(f)$.

Input: A Boolean function $D_{\mathbf{a},\mathbf{b}}f : \mathbb{F}_2^n \to \mathbb{F}_2$ and $2 \le r \le n$.
Output: The collection $\mathcal{MS}_r(f)$.
1: **Construct** $\mathcal{MS}_2(f) := \{\langle \mathbf{a}, \mathbf{b}\rangle : \dim(U) = 2 \text{ and } D_{\mathbf{a},\mathbf{b}}f = 0\}$.
2: **for all** subspaces $U \in \mathcal{MS}_2(f)$ **do**
3: **repeat**
4: **Determine** subspaces $\tilde{U} = \langle U, \tilde{\mathbf{u}}\rangle$ for all $\tilde{\mathbf{u}} \notin U$, such that for any two-dimensional vector subspace $\langle \mathbf{a}, \mathbf{b}\rangle \subseteq U$ second-order derivatives $D_{\mathbf{a},\mathbf{b}}f = 0$.
5: **Put** $U \leftarrow \tilde{U}$ for the obtained subspaces $\tilde{U}$.
6: **until** $\dim(U) = r$.
7: **Output** subspaces U of dimension r.
8: **end for**

Remark 1.7 Algorithm 1 can be used to compute the linearity index of a given function f in the following way: $\mathrm{ind}(f)$ is the biggest r, for which $\mathcal{MS}_r(f) \neq \varnothing$.

Remark 1.8 For a given $\mathcal{M}$-subspace $U \in \mathcal{MS}_r(f)$ of a function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ one can construct an invertible matrix A_U, which brings f to its Maiorana-McFarland representation (1.1), i.e. $f(\mathbf{z}A_U) = \langle \mathbf{x}, \pi(\mathbf{y})\rangle_r \oplus \phi(\mathbf{y})$, with $\mathbf{z} \in \mathbb{F}_2^n$, $\mathbf{x} \in \mathbb{F}_2^r$ and $\mathbf{y} \in \mathbb{F}_2^s$, in the following way: since the values of $\langle \mathbf{x}, \pi(\mathbf{y})\rangle_r \oplus \phi(\mathbf{y})$ on the coset $\mathbb{F}_2^r \oplus \mathbf{y}$ for $\mathbf{y} \in \mathbb{F}_2^s$ coincide with the values of f on the coset $U \oplus \bar{\mathbf{u}}$ for $\bar{\mathbf{u}} \in \bar{U}$, we can construct A_U using the change of basis formula

$$A_U = \left(\begin{array}{c|c} \mathbf{O}_{r,s} & \mathbf{I}_r \\ \hline \mathbf{I}_s & \mathbf{O}_{s,r} \end{array}\right) \cdot \left(\frac{\mathrm{GJB}(\bar{U})}{\mathrm{GJB}(U)}\right). \tag{1.2}$$

Here $\mathrm{GJB}(U)$ denotes the *Gauss-Jordan basis* of a vector space U and $\bar{U}$ is the *complement* of U, i.e. $\dim(U) + \dim(\bar{U}) = n$ and $U \cap \bar{U} = \{\mathbf{0}\}$, which we compute as in [6, Sect. 4].

2 Geometric invariants of Boolean functions

In this section we study invariants of Boolean functions, which arise from certain binary matrices. We call these invariants *geometric*, since any (0, 1)-matrix defines an incidence structure, and hence a finite geometry, and will use them in the next section to distinguish inequivalent homogeneous cubic bent functions.

2.1 Incidence structures from Boolean functions

For a subset A of an additive group $(G, +)$ the *development* $\mathrm{dev}(A)$ of A is an incidence structure, whose points are the elements in G, and whose lines are the translates $A + g := \{a + g : a \in A\}$. For a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, we will use developments of two types:

- $\mathrm{dev}(D_f)$, the development of the *support* $D_f := \{\mathbf{x} \in \mathbb{F}_2^n\colon f(\mathbf{x}) = 1\}$, and
- $\mathrm{dev}(G_f)$, the development of the *graph* $G_f := \{(\mathbf{x}, f(\mathbf{x})) : \mathbf{x} \in \mathbb{F}_2^n\}$.

For the combinatorial properties of supports and graphs of bent functions as well as for their developments we refer to [32, Sect. 3]. We also note the following advantage of $\mathrm{dev}(G_f)$ over $\mathrm{dev}(D_f)$: equivalent Boolean functions f, f' on $\mathbb{F}_2^n$ lead to isomorphic incidence structures $\mathrm{dev}(G_f)$ and $\mathrm{dev}(G_{f'})$, but at the same time $\mathrm{dev}(D_f)$ and $\mathrm{dev}(D_{f'})$ can be non-isomorphic [21, Example 9.3.28]. For this reason we will mostly be interested in combinatorial invariants, like p-ranks [16, p. 787] or Smith normal forms [19, p. 494], of the incidence matrix $M(\mathrm{dev}(G_f))$.

Definition 2.1 A diagonal matrix D with non-negative entries $d_1, d_2, \ldots, d_n$ such that $d_1 | d_2 | \cdots | d_n$ is called the *Smith normal form* of an integral matrix A of order n, if there exist integral matrices U and V with $\det(U), \det(V) = \pm 1$, such that $UAV = D$. The diagonal entries d_i are called *elementary divisors* of A. The p-rank of A is the rank of A over the field $\mathbb{F}_p$.

Throughout the paper we will use the following *geometric invariants* of Boolean functions $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, which are defined as follows:

- 2-rank(f) is the 2-rank of $M(\mathrm{dev}(D_f))$, for bent functions 2-ranks have been extensively studied in [37,38];

– Γ-rank(f) is the 2-rank of $M(\mathrm{dev}(G_f))$, Γ-ranks(f) were mostly studied in the context of inequivalence of vectorial mappings [17,18];
– SNF(f) is the Smith normal form of the incidence matrix $M(\mathrm{dev}(G_f))$, given by the multiset $\mathrm{SNF}(f) = \{*d_1^{m_1}, \ldots, d_k^{m_k}*\}$, where $d_i | d_{i+1}$ and m_i is the multiplicity of d_i.

Finally we emphasize, that Γ-rank(f) and SNF(f) are invariants under equivalence for all Boolean functions $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, while 2-rank$(f)$ is invariant under equivalence only for Boolean functions f with $\deg(f) \geq 2$.

2.2 The relation between geometric invariants

In this subsection we show, that Γ-rank and 2-rank coincide for all non-constant Boolean functions. We also show, how a small modification of the incidence matrix $M(\mathrm{dev}(D_f))$ can help to compute the Smith normal form of a Boolean function f in a more efficient way. Finally, we partially specify elementary divisors for bent functions.

First, we will use the following notation for incidence matrices of developments

$$M_f := M(\mathrm{dev}(D_f)) = (f(\mathbf{x} \oplus \mathbf{y}))_{\mathbf{x},\mathbf{y} \in \mathbb{F}_2^n} \text{ and } N_f := M(\mathrm{dev}(G_f)).$$

Note that, since $(\mathbf{x} \oplus \mathbf{y}, 1) \in G_f \Leftrightarrow f(\mathbf{x} \oplus \mathbf{y}) = 1$ and $(\mathbf{x} \oplus \mathbf{y}, 0) \in G_f \Leftrightarrow \bar{f}(\mathbf{x} \oplus \mathbf{y}) = 1$, we can write N_f without loss of generality as the following block-matrix, where $V_i := \{(\mathbf{x}, i)\colon \mathbf{x} \in \mathbb{F}_2^n\}$ for a fixed $i \in \mathbb{F}_2$:

$$N_f = \begin{array}{c} \begin{matrix} V_1 & V_0 \end{matrix} \\ \begin{pmatrix} M_f & M_{\bar{f}} \\ M_{\bar{f}} & M_f \end{pmatrix} \end{array} \begin{matrix} V_0 \\ V_1 \end{matrix}. \tag{2.1}$$

Now we summarize some well-known statements about higher-order derivatives, which we will use to show the connection between geometric invariants of Boolean functions.

Result 2.2 [22] *Let f be a Boolean function on $\mathbb{F}_2^n$ and $\mathbf{a}_1, \ldots, \mathbf{a}_k \in \mathbb{F}_2^n$.*

1. *If $\mathbf{a}_1, \ldots, \mathbf{a}_k$ are linearly dependent, then $D_{\mathbf{a}_k} D_{\mathbf{a}_{k-1}} \ldots D_{\mathbf{a}_1} f = 0$.*
2. *Let now $\mathbf{a}_1, \ldots, \mathbf{a}_k$ be linearly independent. The derivatives of f are independent of the order in which the derivation is taken, i.e. the equality*

$$D_{\mathbf{a}_k} D_{\mathbf{a}_{k-1}} \ldots D_{\mathbf{a}_1} f(\mathbf{x}) = D_{\mathbf{a}_{\pi(k)}} D_{\mathbf{a}_{\pi(k-1)}} \ldots D_{\mathbf{a}_{\pi(1)}} f(\mathbf{x}) = \bigoplus_{\mathbf{a} \in \langle \mathbf{a}_1, \ldots, \mathbf{a}_k \rangle} f(\mathbf{x} \oplus \mathbf{a})$$

holds for any permutation π on $\{1, \ldots, k\}$.

In the next theorem we prove that for Boolean functions of degree at least two the Γ-rank and 2-rank coincide and show, that all the information about the SNF(f) can be recovered from a matrix obtained through a small modification of M_f.

Theorem 2.3 *Let f be a Boolean function on $\mathbb{F}_2^n$. Then the following hold:*

1. *If $\deg(f) \geq 1$, then the all-one-vector $\mathbf{j}_{2^n}$ can be expressed as a sum of an even number of vectors from the linear code $\mathcal{C}(\mathrm{dev}(D_f))$.*
2. *If $\deg(f) < 1$, then Γ-rank$(f) = 2$, otherwise Γ-rank$(f) = 2 - \mathrm{rank}(f)$.*
3. *$\mathrm{SNF}(f) = \{*d_1^{m_1}, \ldots, d_k^{m_k}, 0^{2^n-1}*\}$, where all d_i's are elementary divisors of the matrix $\begin{pmatrix} M_f & \mathbf{j}_{2^n}^T \\ \mathbf{j}_{2^n} & 2 \end{pmatrix}$.*

Proof *1.* It was shown in [37, Lemma 3.1], that $\mathbf{j}_{2^n} \in \mathcal{C}(\mathrm{dev}(D_f))$. We will prove this statement, by expressing $\mathbf{j}_{2^n}$ as a sum of an even number of vectors from the linear code $\mathcal{C}(\mathrm{dev}(D_f))$. Let d denotes the degree of a function f. First, we observe that the number of slow points of a function f is bounded from below by $2^n - 2^{n-d}$. Thus there exist a sequence of slow points $\mathbf{a}_1, \ldots, \mathbf{a}_d$, such that the d-th order derivative $D_{\mathbf{a}_d} D_{\mathbf{a}_{d-1}} \ldots D_{\mathbf{a}_1} f$ is the constant one function. Finally since the following equality holds for all $\mathbf{x} \in \mathbb{F}_2^n$ due to Result 2.2

$$D_{\mathbf{a}_d} D_{\mathbf{a}_{d-1}} \ldots D_{\mathbf{a}_1} f(\mathbf{x}) = \bigoplus_{\mathbf{a} \in \langle \mathbf{a}_1, \ldots, \mathbf{a}_d \rangle} f(\mathbf{x} \oplus \mathbf{a}) = 1,$$

one can see, the all-one-vector $\mathbf{j}_{2^n}$ is as a sum of 2^d elements of $\mathcal{C}(\mathrm{dev}(D_f))$.

2. Assume that the matrix N_f is of the form (2.1). Performing elementary row and column operations one can bring the matrix N_f to the form

$$N_f \overset{\text{(I)}}{\rightsquigarrow} \begin{pmatrix} M_f & M_{\bar{f}} \\ \mathbf{J}_{2^n} & \mathbf{J}_{2^n} \end{pmatrix} \overset{\text{(II)}}{\rightsquigarrow} \begin{pmatrix} M_f & \mathbf{J}_{2^n} \\ \mathbf{J}_{2^n} & \mathbf{O}_{2^n} \end{pmatrix}.$$

Note, that elementary column operations change the linear code $\mathcal{C}(\mathrm{dev}(D_f))$, however its dimension, which is equal to Γ-rank(f), remains the same. If $\deg(f) < 1$, i.e. f is a constant function, clearly Γ-rank$(f) = 2$. By the previous statement $\mathbf{j}_{2^n}$ can be expressed as a sum of an even number of rows of M_f. Since the matrix M_f is symmetric, the vector $\mathbf{j}_{2^n}^T$ can be expressed as a sum of an even number of columns of the matrix M_f. In this way, the matrix N_f can be brought to the form

$$N_f \overset{\text{(I)-(II)}}{\rightsquigarrow} \begin{pmatrix} M_f & \mathbf{J}_{2^n} \\ \mathbf{J}_{2^n} & \mathbf{O}_{2^n} \end{pmatrix} \overset{\text{(III)}}{\rightsquigarrow} \begin{pmatrix} M_f & \mathbf{O}_{2^n} \\ \mathbf{O}_{2^n} & \mathbf{O}_{2^n} \end{pmatrix}$$

and hence Γ-rank$(f) = \mathrm{rank}(f)$.

3. Performing elementary row and column operations, as in the proof of the previous statement, but over the ring $\mathbb{Z}$, one can bring the matrix N_f to the form

$$N_f \rightsquigarrow \left(\begin{array}{cc|c} M_f & \mathbf{j}_{2^n}^T & \mathbf{O}_{2^n+1,2^n-1} \\ \mathbf{j}_{2^n} & 2 & \\ \hline \mathbf{O}_{2^n-1,2^n+1} & & \mathbf{O}_{2^n-1,2^n-1} \end{array}\right).$$

In this way, $\mathrm{SNF}(f) = \{*d_1^{m_1}, \ldots, d_k^{m_k}, 0^{2^n-1}*\}$, where d_i's are elementary divisors of the matrix $\begin{pmatrix} M_f & \mathbf{j}_{2^n}^T \\ \mathbf{j}_{2^n} & 2 \end{pmatrix}$. □

In the following proposition we partially specify the SNF of a bent function.

Proposition 2.4 *Let f be a bent function on $\mathbb{F}_2^n$ and its Smith normal form given by* $\mathrm{SNF}(f) = \{*d_1^{m_1}, \ldots, d_k^{m_k}, 0^{2^n-1}*\}$. *Then the following holds.*

1. *All elementary divisors d_i in the* $\mathrm{SNF}(f)$ *are powers of two.*
2. Γ-rank$(f) = m_1$, *where m_1 is the multiplicity of one in the* $\mathrm{SNF}(f)$.

Proof *1.* Let $d_1 | d_2 | \ldots | d_{2^{n+1}}$ be elementary divisors and $\alpha_1, \alpha_2, \ldots, \alpha_{2^{n+1}}$ be eigenvalues of the matrix N_f respectively. By [29, Theorem 6], for all $1 \le i_1 < \cdots < i_k \le 2^{n+1}$ and $k = 1, \ldots, 2^{n+1} - 1$ the following relation between products of elementary divisors and eigenvalues holds: $d_1 \cdots d_k | \alpha_{i_1} \cdots \alpha_{i_k}$. Since $\alpha_{i_1} \cdots \alpha_{i_k} | \alpha_{i_1}^2 \cdots \alpha_{i_k}^2$ it is enough to show, that

all nonzero α_i^2 are powers of two. Since N_f is symmetric, we have $N_f^2 = N_f N_f^T$. By [31, Lemma 1.1.4], the matrix $N_f N_f^T$ has eigenvalue 2^{2n} (multiplicity 1), 2^n (multiplicity 2^n) and 0 (multiplicity $2^n - 1$). Thus the product of any k nonzero elementary divisors of N_f is 2^l for some l, and hence all d_i are powers of two. Finally, since the p-rank is the number of elementary divisors, coprime with p and all elementary divisors are powers of two, we conclude that Γ-rank$(f) = m_1$. □

Remark 2.5 We computed SNF(f) for many n-variable bent functions of different degrees on $\mathbb{F}_2^n$ with $6 \le n \le 12$. Based on our numerical experiments, we observe the following kind of symmetry in the SNF(f) of a bent function f on $\mathbb{F}_2^n$:

1. SNF$(f) = \{*d_1^{m_1}, \ldots, d_n^{m_n}, 0^{2^n-1}*\}$, where all elementary divisors d_i are of the form $d_i = 2^{i-1}$ for $i = 1, \ldots, n$.
2. Multiplicities of elementary divisors m_i satisfy $m_n = 1$, $m_{n-1} = m_1 - 2$ and $m_{n/2-i} = m_{n/2+i}$ for $i = 1, \ldots, n/2 - 2$.

We do not know how to prove this statement in general and we make the following conjecture.

Conjecture 2.6 The SNF(f) of a bent function f on $\mathbb{F}_2^n$ satisfies Remark 2.5.

3 Homogeneous cubic bent functions

In this section we first survey the known homogeneous cubic bent functions. We also classify the known examples in 10 and 12 variables, constructed in [8,27] by using sophisticated computational approaches, and show that:

- Some of them are not covered by the Maiorana-McFarland construction;
- All of them are not equivalent to the only one known analytic construction (for this reason we will call it later "the primary construction") of Seberry, Xia and Pieprzyk, given in [36].

Subsequently, we extend the latter result to an arbitrary number of variables, by proving, that proper concatenations of homogeneous cubic bent functions in a small number of variables can never be equivalent to the primary construction. Finally we provide a construction method, aimed to generate a lot of homogeneous bent functions from a single given example. Using this approach we construct many new homogeneous cubic bent functions in 12 variables and show, that some of them are not equivalent to all the previously known ones.

3.1 The known examples and constructions

The existence of homogeneous cubic bent functions on $\mathbb{F}_2^n$ for all $n \ge 6$ was shown in two independent ways. Seberry, Xia and Pieprzyk in [36, Theorem 8] proved that one can construct such functions on $\mathbb{F}_2^n$ for all even $n \ne 8$, from special Maiorana-McFarland functions by a proper change of basis. We will call their construction *primary* and denote any n-variable function of this type by $h_{pr.}^n$.

Result 3.1 [36, Theorem 6] *Let $f_{id,\phi}$ be a Maiorana-McFarland bent function on $\mathbb{F}_2^{2m}$ where ϕ is a homogeneous cubic function without affine derivatives on $\mathbb{F}_2^m$. Then there exists a nonsingular matrix T, such that $h_{pr.}^n(\mathbf{x}, \mathbf{y}) := f_{id,\phi}((\mathbf{x}, \mathbf{y})T)$ is a homogeneous cubic bent function.*

Table 1 First $n/2$ elementary divisors of the Smith normal form $\mathrm{SNF}(h_i^n)$ for the known homogeneous cubic bent functions from [8, p. 149] and [27, p. 15]

h_i^{10}	$\mathrm{SNF}(h_i^{10})$
h_1^{10}	$\{*1^{20}, 2^{86}, 4^{130}, 8^{143}, 16^{268}, \cdots *\}$
h_2^{10}	$\{*1^{20}, 2^{78}, 4^{138}, 8^{147}, 16^{260}, \cdots *\}$
h_3^{10}	$\{*1^{20}, 2^{108}, 4^{110}, 8^{129}, 16^{292}, \cdots *\}$
h_4^{10}	$\{*1^{22}, 2^{154}, 4^{90}, 8^{81}, 16^{332}, \cdots *\}$
h_i^{12}	$\mathrm{SNF}(h_i^{12})$
h_1^{12}	$\{*1^{22}, 2^{142}, 4^{276}, 8^{493}, 16^{630}, 32^{972}, \cdots *\}$
h_2^{12}	$\{*1^{22}, 2^{126}, 4^{276}, 8^{517}, 16^{646}, 32^{924}, \cdots *\}$
h_3^{12}	$\{*1^{24}, 2^{127}, 4^{260}, 8^{525}, 16^{674}, 32^{878}, \cdots *\}$
h_4^{12}	$\{*1^{22}, 2^{104}, 4^{256}, 8^{525}, 16^{698}, 32^{888}, \cdots *\}$
h_5^{12}	$\{*1^{26}, 2^{196}, 4^{392}, 8^{419}, 16^{490}, 32^{1052}, \cdots *\}$

Another approach, suggested by Charnes et al. in [8], consists of two steps. First, they constructed homogeneous cubic bent functions in a small number of variables using the tools from modular invariant theory, and second, they extended these examples to an arbitrary number of variables, using the direct sum construction.

Result 3.2 [36, Theorem 2] *The direct sum $h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}) \oplus g(\mathbf{y})$ is bent and d-homogeneous on $\mathbb{F}_2^{n+m}$ if and only if the functions f and g are bent and d-homogeneous on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ respectively.*

Further we classify the known homogeneous cubic bent functions in a small number of variables and show, that some of them are not the members of the $\mathcal{M}^\#$ class.

Theorem 3.3 *The homogeneous cubic bent functions in $n = 10$ or $n = 12$ variables from* [8, p. 149] *and* [27, p. 15] *satisfy:*

1. *If $n = 10$, there are 4 equivalence classes, with 2 of them being outside the completed Maiorana-McFarland class $\mathcal{M}^\#$.*
2. *If $n = 12$, there are 5 equivalence classes, which are subclasses of $\mathcal{M}^\#$.*

Proof First, we compute the Smith normal forms for the mentioned homogeneous cubic bent functions and check whether those, having the same ones, are equivalent. We check equivalence of bent functions via equivalence of linear codes [18, Theorem 9] and isomorphism of designs [1, Corollary 10.6] in `Magma` [2]. Consequently, we found 4 and 5 equivalence classes in 10 and 12 variables, respectively. We denote representatives of the obtained classes by h_i^n and list them in the Appendix. We provide only the first $n/2$ elementary divisors for the Smith normal forms of bent functions due to Remark 2.5.
Further we use the parallel implementation of Algorithm 1 in `Mathematica` [39] in order to check, whether the functions h_i^n belong to $\mathcal{M}^\#$. As a result, only functions h_3^{10} and h_4^{10} do not belong to the $\mathcal{M}^\#$ class, while all the functions h_i^{12} are in $\mathcal{M}^\#$. Finally, we list all the $\mathcal{M}$-subspaces of functions from $\mathcal{M}^\#$ in the Appendix. □

3.2 Homogeneous cubic bent functions, different from the primary construction

Using the facts about 2-ranks and the relation between Γ-rank and 2-rank, obtained in the previous section, we derive the following corollary.

Corollary 3.4 *Let f and g be Boolean functions on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively, with* $\deg(f) \geq 1$ *and* $\deg(g) \geq 1$.

1. *Let h be a Boolean function on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ defined as the direct sum of functions f and g, then*

$$\Gamma\text{-rank}(h) = \Gamma\text{-rank}(f) + \Gamma\text{-rank}(g) - 2. \tag{3.1}$$

2. *Let $f_{id,\phi}$ be a Maiorana-McFarland bent function on $\mathbb{F}_2^n$, then*

$$\Gamma\text{-rank}(f_{id,\phi}) = n + 2 \text{ if and only if } \deg(\phi) \leq 3. \tag{3.2}$$

3. *For the primary construction of homogeneous cubic bent functions $h^n_{pr.}$ on $\mathbb{F}_2^n$ we have* $\Gamma\text{-rank}(h^n_{pr.}) = n + 2$.

Proof The first and the second claims hold, since the statements (3.1) and (3.2) were proven in [37,38] for 2-ranks, and by Theorem 2.3 we know, that 2-ranks and Γ-ranks coincide for all non-constant Boolean functions. Finally, the third claim follows from (3.2) and the definition of the primary construction. □

Now we proof the existence of homogeneous cubic bent functions, different from the primary construction.

Theorem 3.5 *There exist homogeneous cubic bent functions on $\mathbb{F}_2^n$, inequivalent to the primary construction $h^n_{pr.}$, whenever $n \geq 8$.*

Proof We construct a homogeneous cubic bent function h_n in $n = 6i + 8j + 10k + 12l$ variables with $j + k + l \neq 0$ as the following concatenation:

$$h_n := i \cdot h^6_* \oplus j \cdot h^8_* \oplus k \cdot h^{10}_* \oplus l \cdot h^{12}_*, \tag{3.3}$$

where h^6_* and h^8_* are arbitrary homogeneous cubic bent functions in 6 and 8 variables respectively, and h^{10}_*, h^{12}_* are arbitrary homogeneous cubic bent functions in 10 and 12 variables from Table 1. Since any homogeneous cubic bent function in 6 variables is equivalent to the primary construction $h^6_{pr.}$, we have $\Gamma\text{-rank}(h^6_*) = 8$. One can check that for any cubic bent function h^8_* in 8 variables we have $\Gamma\text{-rank}(h^8_*) \in \{14, 16\}$. By Proposition 2.4 one can see, that Γ-ranks of functions h^{10}_* and h^{12}_* are multiplicities of the entry one in Table 1. Finally, comparing the lower bound of the $\Gamma\text{-rank}(h_n)$ with $\Gamma\text{-rank}(h^n_{pr.})$, one can see immediately that

$$\begin{aligned}\Gamma\text{-rank}(h_n) &\geq 8i + 14j + 20k + 22l - 2(i + j + k + l - 1)\\ &= n + 2 + 4(j + 2(k + l)) > n + 2 = \Gamma\text{-rank}(h^n_{pr.})\end{aligned}$$

and hence the function h_n is never equivalent to $h^n_{pr.}$ for all $n \geq 8$. □

3.3 Constructing new homogeneous functions from old, without increasing the number of variables

In this subsection we show, that in some cases one can use the power of the Maiorana-McFarland construction to produce a lot of homogeneous bent functions, provided that a single one, member of the $\mathcal{M}^\#$ class, is given. Our approach is based on a generalization of the following observation.

Observation 3.6 *Let $f := h_3^{12}$ and $g := h_4^{12}$. Our computations show, that homogeneous cubic bent functions f and g have a common $\mathcal{M}$-subspace U of dimension 6, which together with its complement $\bar{U}$ is given by:*

$$\mathrm{GJB}(U) = \left(\begin{array}{cc|c|c} 1 & 1 & \mathbf{O}_{1,10} \\ \hline \mathbf{O}_{5,2} & & \mathbf{I}_5 \end{array}\right) \quad \textit{and} \quad \mathrm{GJB}(\bar{U}) = \left(\begin{array}{cc|c|c} 0 & 1 & \mathbf{O}_{1,10} \\ \hline \mathbf{O}_{5,2} & & \mathbf{O}_5 \end{array}\right). \tag{3.4}$$

By Remark 1.8 one can bring functions f and g to their Maiorana-McFarland representations (1.1) using the same linear invertible transformation A_U, given by (1.2):

$$f(\mathbf{z}A_U) = f_{\pi,\phi}(\mathbf{x},\mathbf{y}) \quad \textit{and} \quad g(\mathbf{z}A_U) = g_{\pi,\psi}(\mathbf{x},\mathbf{y}),$$

where $\pi : \mathbb{F}_2^6 \to \mathbb{F}_2^6$ is a permutation and $\phi, \psi : \mathbb{F}_2^6 \to \mathbb{F}_2$ are Boolean functions. In this way, one can construct homogeneous function g from the function f as follows:

$$g(\mathbf{z}) := f_{\pi,\phi\oplus\omega}((\mathbf{x},\mathbf{y})T), \ \textit{where } \omega := \phi \oplus \psi \textit{ and } T := A_U^{-1}. \tag{3.5}$$

Let $h_{\pi,\phi} : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function from the $\mathcal{M}^{\#}_{r,s}$ class, which is equivalent to a d-homogeneous one, i.e. there exist an invertible matrix T of order n, such that $h_{\pi,\phi}((\mathbf{x},\mathbf{y})T)$ is d-homogeneous. We will denote by $\Omega_T(h_{\pi,\phi})$ the set

$$\Omega_T(h_{\pi,\phi}) := \{\omega : \mathbb{F}_2^s \to \mathbb{F}_2 \mid h_{\pi,\phi\oplus\omega}((\mathbf{x},\mathbf{y})T) \text{ is } d\text{-homogeneous bent}\}.$$

This is the set of all Boolean functions ω on $\mathbb{F}_2^s$, which preserve d-homogeneity and bentness of the function $h_{\pi,\phi\oplus\omega}$ with respect to the linear transformation T.

Proposition 3.7 *Let $h_{\pi,\phi}$ be a Maiorana-McFarland bent function on $\mathbb{F}_2^{2m}$, which is equivalent to a d-homogeneous bent function, i.e. there exist an invertible matrix T, such that $h_{\pi,\phi}((\mathbf{x},\mathbf{y})T)$ is d-homogeneous bent. Then the set $\Omega_T(h_{\pi,\phi})$ is a vector space over $\mathbb{F}_2$.*

Proof Let $\omega_1, \omega_2 \in \Omega_T(h_{\pi,\phi})$ with $\omega_1 \neq \omega_2$ and $\omega := \omega_1 \oplus \omega_2$. We will show that $\omega \in \Omega_T(h_{\pi,\phi})$. Let the invertible matrix T be of the form $T = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with all the submatrices of order m. First, we observe that $0 \in \Omega_T(h_{\pi,\phi})$ and for any $\omega_i \in \Omega_T(h_{\pi,\phi})$ we have

$$h_{\pi,\phi\oplus\omega_i}((\mathbf{x},\mathbf{y})T) = h_{\pi,\phi}((\mathbf{x},\mathbf{y})T) \oplus \omega_i(\mathbf{x}B \oplus \mathbf{y}D),$$

from what follows, that $\omega_i(\mathbf{x}B \oplus \mathbf{y}D)$ is either d-homogeneous or constant zero function, since $h_{\pi,\phi}((\mathbf{x},\mathbf{y})T)$ is d-homogeneous. Thus $\omega \in \Omega_T(h_{\pi,\phi})$, since bentness of $h_{\pi,\phi\oplus\omega}$ is independent on the choice of a function ω on $\mathbb{F}_2^m$ and $\omega(\mathbf{x}B \oplus \mathbf{y}D)$ is a d-homogeneous function. □

Note that for a homogeneous bent function $h_{\pi,\phi} \in \mathcal{M}^{\#}_{r,s}$ the set $\Omega_T(h_{\pi,\phi})$ is not a vector space in general. Nevertheless, for a given homogeneous bent function $h \in \mathcal{M}^{\#}_{r,s}$ one can still construct the set $\Omega_T(h_{\pi,\phi})$, in order to get more, possibly inequivalent, homogeneous functions. We will summarize these ideas in the form of an algorithm below.

Table 2 First $n/2$ elementary divisors of the Smith normal form $\mathrm{SNF}(h_i^n)$ for the new homogeneous cubic bent functions h_6^{12}, h_7^{12} in 12 variables

h_i^{12}	$\mathrm{SNF}(h_i^{12})$
h_6^{12}	$\{*1^{24}, 2^{123}, 4^{292}, 8^{497}, 16^{674}, 32^{878}, \cdots *\}$
h_7^{12}	$\{*1^{24}, 2^{123}, 4^{272}, 8^{516}, 16^{674}, 32^{880}, \cdots *\}$

Algorithm 2 New d-homogeneous bent functions from a single one in $\mathcal{M}^{\#}_{r,s}$.

Input: Homogeneous bent function $h : \mathbb{F}_2^n \to \mathbb{F}_2$, $h \in \mathcal{M}^{\#}_{r,s}$ of degree d.
Output: The set H of new d-homogeneous bent functions from $\mathcal{M}^{\#}_{r,s}$.
1: **Put** $H \leftarrow \{\}$.
2: **for all** $\mathcal{M}$-subspaces $U \in \mathcal{MS}_r(h)$ **do**
3: **Construct** a linear mapping A_U as in Remark 1.8, in order to get the Maiorana-McFarland representation (1.1), i.e. $h_{\pi,\phi}(\mathbf{x}, \mathbf{y}) := h(\mathbf{z}A_U)$.
4: **Put** $H \leftarrow H \cup \{h_{\pi,\phi\oplus\omega}((\mathbf{x}, \mathbf{y})T) : \omega \in \Omega_T(h_{\pi,\phi})\}$, where $T := A_U^{-1}$.
5: **end for**

Remark 3.8 Using Algorithm 2 and the mapping T, defined in (3.5), one can construct $2^{\binom{6}{3}}$ new homogeneous cubic bent functions from any of functions h_3^{12} and h_5^{12}, members of the $\mathcal{M}^{\#}$ class. Such a big number of new functions can be explained in the following way. Let $h \in \{h_3^{12}, h_5^{12}\}$. First, we observe that the image of $\mathbf{y}$ after the linear transformation $\mathbf{y} \mapsto \mathbf{y}' = \mathbf{x}B \oplus \mathbf{y}D$ is given by:

$$\mathbf{y} \mapsto \mathbf{y}' = (x_1 \oplus x_2, x_3 \oplus y_2, x_4 \oplus y_3, x_5 \oplus y_4, x_6 \oplus y_5, y_1 \oplus y_6). \tag{3.6}$$

Since any two coordinates of the vector $\mathbf{y}'$ do not contain common variables x_i and y_j, the linear transformation, defined in (3.6), is homogeneity-preserving. Thus, $\Omega_T(h_{\pi,\phi})$ is generated by monomials $\omega : \mathbb{F}_2^6 \to \mathbb{F}_2$ of degree 3, and hence $|\Omega_T(h_{\pi,\phi})| = 2^{\binom{6}{3}}$. Finally, we note that some of the constructed homogeneous cubic bent functions are not equivalent to any of the known one, since their Smith normal forms, listed in Table 2, are different from those given in Table 1.

Theorem 3.9 *There are at least 7 pairwise inequivalent homogeneous cubic bent functions on $\mathbb{F}_2^{12}$, inequivalent to $h_{pr.}^{12}$.*

Finally we want to emphasize the fundamental difference between the primary construction $h_{pr.}^n$ and functions, constructed in Remark 3.8. For the primary construction of homogeneous cubic bent function $h_{pr.}^n$ one needs to find a special Boolean function ϕ of degree 3, such that the non-homogeneous cubic Maiorana-McFarland function $f_{id,\phi}$ is homogeneous after the change of coordinates. In some sense, the identity permutation id has a "defect", which makes $f_{id,0}$ never equivalent to a homogeneous cubic function. But the specific choice of a cubic function ϕ helps to repair it. Since the functions constructed in Remark 3.8 are in that sense "defect free", it is essential to construct such functions systematically.

Open Problem 3.10 *Are there infinite families of permutations $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$, such that for some non-degenerate linear transformation T the function, defined by $(\mathbf{x}, \mathbf{y}) \mapsto f_{\pi,\psi}((\mathbf{x}, \mathbf{y})T)$, is homogeneous cubic bent for all homogeneous cubic functions $\psi : \mathbb{F}_2^m \to \mathbb{F}_2$?*

4 Bent functions outside the $\mathcal{M}^{\#}$ class via direct sum construction

In this section we show how one can choose bent functions f and g, such that the direct sum $f \oplus g$ is not a member of the completed Maiorana-McFarland class $\mathcal{M}^{\#}$. The idea of the approach is based on the following observation: if one can measure the maximum dimension of *relaxed* $\mathcal{M}$*-subspaces* (which we introduce below) of the components f and g, then one can provide an upper bound for the linearity index $\mathrm{ind}(f \oplus g)$ and if it small enough, then $f \oplus g \notin \mathcal{M}^{\#}$.

Finally, using this recursive approach, we prove the series of results about the existence of cubic bent functions outside the $\mathcal{M}^{\#}$ class, which can simultaneously be homogeneous and have no affine derivatives.

4.1 The sufficient condition in terms of relaxed $\mathcal{M}$-subspaces

Further, we identify $\mathbb{F}_2^{n+m}$ with $\mathbb{F}_2^n \times \mathbb{F}_2^m$. In this way, any vector $\mathbf{v} \in \mathbb{F}_2^{n+m}$ is uniquely represented by a pair $(\mathbf{v_x}, \mathbf{v_y})$, where $\mathbf{v_x} \in \mathbb{F}_2^n$ and $\mathbf{v_y} \in \mathbb{F}_2^m$. Now let $U \in \mathcal{MS}(h)$, i.e. for all $\mathbf{a}, \mathbf{b} \in U$ we have, that second-order derivatives satisfy $D_{\mathbf{a},\mathbf{b}}h = 0$. This takes place if and only if $D_{\mathbf{a_x},\mathbf{b_x}}f = D_{\mathbf{a_y},\mathbf{b_y}}g = c_{\mathbf{a},\mathbf{b}}$, where $c_{\mathbf{a},\mathbf{b}} \in \mathbb{F}_2$ is a constant, depending on $\mathbf{a}$ and $\mathbf{b}$, since g and h do not have common variables. This observation leads to the following generalization of $\mathcal{M}$-subspaces (see Definition 1.4).

Definition 4.1 We will call a vector subspace U a *relaxed* $\mathcal{M}$*-subspace* of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, if for all $\mathbf{a}, \mathbf{b} \in U$ second order derivatives $D_{\mathbf{a},\mathbf{b}}f$ are either constant zero or constant one functions, i.e $D_{\mathbf{a},\mathbf{b}}f = 0$ or $D_{\mathbf{a},\mathbf{b}}f = 1$. We denote by $\mathcal{RMS}_r(f)$ the collection of all r-dimensional relaxed $\mathcal{M}$-subspaces of f and by $\mathcal{RMS}(f)$ the collection

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

While the linearity index of a Boolean function (see Definition 1.5) is defined as the maximal possible dimension of its $\mathcal{M}$-subspace, it is reasonable to define its analogue for relaxed $\mathcal{M}$-subspaces.

Definition 4.2 For a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ its *relaxed linearity index* $\text{r-ind}(f)$ is defined by $\text{r-ind}(f) := \max_{U \in \mathcal{RMS}(f)} \dim(U)$.

Example 4.3 Let $f : \mathbb{F}_2^6 \to \mathbb{F}_2$ be the function from Example 1.6. One can check, that the subspace $U = \langle (0,1,0,0,0,1), (0,0,0,1,0,0), (0,0,0,0,1,1) \rangle$ is a relaxed $\mathcal{M}$-subspace of f, since its second-order derivatives $D_{\mathbf{a},\mathbf{b}}f$, which correspond to all two-dimensional vector subspaces $\langle \mathbf{a}, \mathbf{b} \rangle$ of U, are constant zero or constant one functions

$$\left\langle \begin{smallmatrix} 0&0&0&1&0&0 \\ 0&0&0&0&1&1 \end{smallmatrix} \right\rangle \mapsto 0, \left\langle \begin{smallmatrix} 0&1&0&0&0&1 \\ 0&0&0&0&1&1 \end{smallmatrix} \right\rangle \mapsto 1, \left\langle \begin{smallmatrix} 0&1&0&1&0&1 \\ 0&0&0&0&1&1 \end{smallmatrix} \right\rangle \mapsto 1, \left\langle \begin{smallmatrix} 0&1&0&0&0&1 \\ 0&0&0&1&0&0 \end{smallmatrix} \right\rangle \mapsto 0,$$
$$\left\langle \begin{smallmatrix} 0&1&0&0&1&0 \\ 0&0&0&1&0&0 \end{smallmatrix} \right\rangle \mapsto 0, \left\langle \begin{smallmatrix} 0&1&0&0&0&1 \\ 0&0&0&1&1&1 \end{smallmatrix} \right\rangle \mapsto 1, \left\langle \begin{smallmatrix} 0&1&0&0&1&0 \\ 0&0&0&1&1&1 \end{smallmatrix} \right\rangle \mapsto 1.$$

Now we present some properties of collections of $\mathcal{M}$-subspaces as well as of relaxed ones.

Proposition 4.4 *Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function and let $n = r + s$. The following hold:*

1. $\mathcal{MS}(f) \subseteq \mathcal{RMS}(f)$.
2. $|\mathcal{MS}_r(f)|$ *and* $|\mathcal{RMS}_r(f)|$ *as well as* $\mathrm{ind}(f)$ *and* $\text{r-ind}(f)$ *are invariants under equivalence.*
3. $\mathrm{ind}(f) \le \text{r-ind}(f)$ *and* $f \notin \mathcal{M}^{\#}_{r,s}$ *for all* $r > \text{r-ind}(f)$.

Proof *1.* This follows from the definitions of collections $\mathcal{MS}(f)$ and $\mathcal{RMS}(f)$.

2. Let f and f' be equivalent, i.e. $f'(\mathbf{x}) = f(\mathbf{x}A) \oplus l(\mathbf{x})$. Assume $U \in \mathcal{RMS}_r(f)$ and let $U' = UA^{-1}$ with $\mathbf{a}', \mathbf{b}' \in U'$. Denoting $\mathbf{y} = \mathbf{x}A$, one can see from the following computations

$$\begin{aligned} D_{\mathbf{a}',\mathbf{b}'} f'(\mathbf{x}) &= f'(\mathbf{x} \oplus \mathbf{a}' \oplus \mathbf{b}') \oplus f'(\mathbf{x} \oplus \mathbf{a}') \oplus f'(\mathbf{x} \oplus \mathbf{b}') \oplus f'(\mathbf{x}') \\ &= f(\mathbf{y} \oplus \mathbf{a} \oplus \mathbf{b}) \oplus f(\mathbf{y} \oplus \mathbf{a}) \oplus f(\mathbf{y} \oplus \mathbf{b}) \oplus f(\mathbf{y}) = D_{\mathbf{a},\mathbf{b}} f(\mathbf{y}) \end{aligned}$$

that $U' \in \mathcal{RMS}_r(f')$. Since A^{-1} maps different subspaces to different ones, we have that $|\mathcal{RMS}_r(f)| = \left|\mathcal{RMS}_r(f')\right|$ and $|\mathcal{MS}_r(f)| = \left|\mathcal{MS}_r(f')\right|$. Since $\dim(U) = \dim(U')$, we have $\mathrm{ind}(f) = \mathrm{ind}(f')$ and $\text{r-ind}(f) = \text{r-ind}(f')$.
3. First, since $\mathcal{MS}(f) \subseteq \mathcal{RMS}(f)$ the inequality $\mathrm{ind}(f) \le \text{r-ind}(f)$ holds. The statement $f \notin \mathcal{M}^{\#}_{r,s}$ for all $r > \text{r-ind}(f)$ now follows from the maximality of the linearity index. □

In the next theorem we will show, that each relaxed $\mathcal{M}$-subspace of $f \oplus g$ is contained in another relaxed $\mathcal{M}$-subspace from $\mathcal{RMS}(f \oplus g)$, constructed via the direct product of relaxed $\mathcal{M}$-subspaces of f and g.

Theorem 4.5 *Let $h(\mathbf{x}, \mathbf{y}) := f(\mathbf{x}) \oplus g(\mathbf{y})$, for $\mathbf{x} \in \mathbb{F}_2^n$ and $\mathbf{y} \in \mathbb{F}_2^m$.*

1. *If $V \in \mathcal{RMS}(f)$ and $W \in \mathcal{RMS}(g)$, then $V \times W \in \mathcal{RMS}(h)$.*
2. *For any $U \in \mathcal{RMS}(h)$ there exist $V \in \mathcal{RMS}(f)$ and $W \in \mathcal{RMS}(g)$, such that $U \subseteq V \times W$.*
3. $\text{r-ind}(h) \le \text{r-ind}(f) + \text{r-ind}(g)$.

Proof *1.* Let $U = V \times W$. Since $V \in \mathcal{RMS}(f)$ and $W \in \mathcal{RMS}(g)$, then for all $\mathbf{v}_1, \mathbf{v}_2 \in V$ holds $D_{\mathbf{v}_1,\mathbf{v}_2} f = c_{\mathbf{v}_1,\mathbf{v}_2}$ and for all $\mathbf{w}_1, \mathbf{w}_2 \in W$ holds $D_{\mathbf{w}_1,\mathbf{w}_2} g = c_{\mathbf{w}_1,\mathbf{w}_2}$, where $c_{\mathbf{v}_1,\mathbf{v}_2}$ and $c_{\mathbf{w}_1,\mathbf{w}_2}$ are some constants. In this way, for all pairs $\mathbf{u}_1 = (\mathbf{v}_1, \mathbf{w}_1)$ and $\mathbf{u}_2 = (\mathbf{v}_2, \mathbf{w}_2)$ holds $D_{\mathbf{u}_1,\mathbf{u}_2} h = D_{\mathbf{v}_1,\mathbf{v}_2} f \oplus D_{\mathbf{w}_1,\mathbf{w}_2} g = c_{\mathbf{v}_1,\mathbf{v}_2} \oplus c_{\mathbf{w}_1,\mathbf{w}_2}$ and, hence, $U \in \mathcal{RMS}(h)$.

2. Recall that any vector $\mathbf{v} \in \mathbb{F}_2^{n+m}$ is identified with a pair $(\mathbf{v}_\mathbf{x}, \mathbf{v}_\mathbf{y})$, where $\mathbf{v}_\mathbf{x} \in \mathbb{F}_2^n$ and $\mathbf{v}_\mathbf{y} \in \mathbb{F}_2^m$. We define two vector subspaces $V \subseteq \mathbb{F}_2^n$ and $W \subseteq \mathbb{F}_2^m$ as follows:

$$V = \mathrm{span}(\{\mathbf{u}_\mathbf{x} \colon \mathbf{u} \in U\}) \text{ and } W = \mathrm{span}(\{\mathbf{u}_y \colon \mathbf{u} \in U\}).$$

We will show, that $V \in \mathcal{RMS}(f)$ and $W \in \mathcal{RMS}(g)$. We define two functions $f', g'\colon \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ as $f'(\mathbf{x}, \mathbf{y}) := f(\mathbf{x})$ for all $\mathbf{y} \in \mathbb{F}_2^m$ and $g'(\mathbf{x}, \mathbf{y}) := g(\mathbf{y})$ for all $\mathbf{x} \in \mathbb{F}_2^n$. Since $U \in \mathcal{RMS}(h)$, then for all $\mathbf{u}_1, \mathbf{u}_2 \in U$ the equality

$$D_{\mathbf{u}_1,\mathbf{u}_2} h(\mathbf{x}, \mathbf{y}) = D_{\mathbf{u}_1,\mathbf{u}_2} f'(\mathbf{x}, \mathbf{y}) \oplus D_{\mathbf{u}_1,\mathbf{u}_2} g'(\mathbf{x}, \mathbf{y}) = c_{\mathbf{u}_1,\mathbf{u}_2} \tag{4.1}$$

holds for all $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^{n+m}$. Let $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}_2^n$ and consider the following equalities

$$D_{\mathbf{u}_1,\mathbf{u}_2} f'(\mathbf{x}_1, \mathbf{y}) \oplus D_{\mathbf{u}_1,\mathbf{u}_2} g'(\mathbf{x}_1, \mathbf{y}) = c_{\mathbf{u}_1,\mathbf{u}_2} \tag{4.2}$$

$$D_{\mathbf{u}_1,\mathbf{u}_2} f'(\mathbf{x}_2, \mathbf{y}) \oplus D_{\mathbf{u}_1,\mathbf{u}_2} g'(\mathbf{x}_2, \mathbf{y}) = c_{\mathbf{u}_1,\mathbf{u}_2}, \tag{4.3}$$

which hold for any $\mathbf{y} \in \mathbb{F}_2^m$ due to (4.1). Adding Eqs. (4.2)–(4.3), one gets $D_{\mathbf{u}_1,\mathbf{u}_2} f'(\mathbf{x}_1, \mathbf{y}) = D_{\mathbf{u}_1,\mathbf{u}_2} f'(\mathbf{x}_2, \mathbf{y})$ since g' depends on the variable $\mathbf{x}$ "fictively". Now, since f' depends on the variable $\mathbf{y}$ "fictively", we get that for all $\mathbf{v}_1, \mathbf{v}_2 \in V$ the equality $D_{\mathbf{v}_1,\mathbf{v}_2} f(\mathbf{x}_1) = D_{\mathbf{v}_1,\mathbf{v}_2} f(\mathbf{x}_2)$ holds for all $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}_2^n$ and hence $D_{\mathbf{v}_1,\mathbf{v}_2} f = c_{\mathbf{v}_1,\mathbf{v}_2}$ (one can think about $\mathbf{v}_1$ and $\mathbf{v}_2$ as $(\mathbf{u}_1)_{\mathbf{x}}$ and $(\mathbf{u}_2)_{\mathbf{x}}$, respectively). Thus we have shown, that $V \in \mathcal{RMS}(f)$. Since f and g are interchangeable, we get $W \in \mathcal{RMS}(g)$. Clearly, $U \subseteq V \times W$ and by the previous statement we have $V \times W \in \mathcal{RMS}(h)$.

3. Let $U \in \mathcal{RMS}(h)$ and $\dim(U) = \text{r-ind}(h)$. By the previous statement there exist $V \in \mathcal{RMS}(f)$ and $W \in \mathcal{RMS}(g)$, such that $U \subseteq V \times W$. Now, using the following series of inequalities

$$\begin{aligned} \text{r-ind}(h) = \dim(U) &\leq \dim(V \times W) = \dim(V) + \dim(W) \\ &\leq \max_{V \in \mathcal{RMS}(f)} \dim(V) + \max_{W \in \mathcal{RMS}(g)} \dim(W) \\ &= \text{r-ind}(f) + \text{r-ind}(g). \end{aligned}$$

we complete the proof. □

The next corollary provides a sufficient condition on bent functions f and g for $f \oplus g$ being not in the $\mathcal{M}^\#$ class in terms of their relaxed $\mathcal{M}$-subspaces.

Corollary 4.6 *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and $g : \mathbb{F}_2^m \to \mathbb{F}_2$ be two Boolean bent functions. If f and g satisfy* r-ind$(f) < n/2$ *and* r-ind$(g) \leq m/2$, *then $f \oplus k \cdot g \notin \mathcal{M}^\#$ on $\mathbb{F}_2^{n+km}$ for all $k \in \mathbb{N}$.*

Remark 4.7 Throughout the paper we will call a Boolean function f on $\mathbb{F}_2^n$ *strongly extendable*, if r-ind$(f) < n/2$ and *weakly extendable*, if r-ind$(f) = n/2$. In this way, if one wants to extend a strongly extendable function f with Corollary 4.6, it is enough to take a weakly extendable function g, while for the extension of a weakly extendable function g one has to take a strongly extendable function f.

Remark 4.8 For a given function f one can compute the relaxed linearity index r-ind(f) in the same way as the linearity index ind(f), but with only one change. Instead of the second-order derivative $D_{\mathbf{a},\mathbf{b}} f$, given by its ANF

$$D_{\mathbf{a},\mathbf{b}} f(\mathbf{x}) = \bigoplus_{\mathbf{v} \in \mathbb{F}_2^n} c_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) \left(\prod_{i=1}^{n} x_i^{v_i} \right),$$

where coefficients $c_{\mathbf{v}}$ depend on $\mathbf{a}$ and $\mathbf{b}$, one considers the *"relaxed" second-order derivative* $RD_{\mathbf{a},\mathbf{b}} f$, defined by $RD_{\mathbf{a},\mathbf{b}} f(\mathbf{x}) := D_{\mathbf{a},\mathbf{b}} f(\mathbf{x}) \oplus c_{\mathbf{0}}(\mathbf{a}, \mathbf{b})$ and use it as the input of Algorithm 1 in the way already described in Remark 1.7.

4.2 Application to homogeneous cubic bent functions without affine derivatives

In order to use Corollary 4.6 for the construction of cubic bent functions outside $\mathcal{M}^\#$, which can be homogeneous or have no affine derivatives, we need to find first such functions in a small number of variables and check, whether they are weakly or strongly extendable.

First we check, whether the equivalence classes of cubic bent functions in six [35, p. 303] and eight [3, p. 102] variables, contain functions with the mentioned properties. Since all cubic bent functions in 6 and 8 variables are members of the $\mathcal{M}^\#$ class, as it was shown in [10, p. 37] and [3, p. 103] respectively, the best what one expects to find is a weakly extendable cubic bent function. In this way:

Table 3 Extendable cubic bent functions in a small number of variables

# of variables, n	6	8	10	12
r-ind	3	4	4	6
Is homogeneous?	×	✓	✓	✓
Has no aff. derivatives?	✓	×	✓	✓
Example	R_3	h_1^8	h_4^{10}	h_5^{12}

- The only (up to equivalence) weakly extendable cubic bent function in 6 variables is the third Rothaus' function [35, p. 303], denoted here by R_3. It has no affine derivatives and is not equivalent to any homogeneous cubic bent function.
- An example of weakly extendable homogeneous cubic bent function in 8 variables is given by the function h_1^8. Like any other cubic bent function in eight variables, it has affine derivatives [20].

Now we analyze homogeneous cubic bent functions in 10 and 12 variables.

- An example of a strongly extendable cubic bent function in 10 variables is represented by the function h_4^{10}, which is simultaneously homogeneous and has no affine derivatives.
- Since all the mentioned functions in 12 variables belong to the $\mathcal{M}^\#$ class, they can not be strongly extendable. Nevertheless, among them we found a weakly extendable homogeneous function h_5^{12} without affine derivatives.

We summarize these data in Table 3 and list all the used functions in the Appendix.

Now we proceed to the proof of our main theorem: the series of existence results about cubic bent functions with nice cryptographic properties.

Theorem 4.9 *On $\mathbb{F}_2^n$ there exist:*

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

Proof In all the four cases the idea of the proof is the same: construct a strongly extendable Boolean function h_n in $n = 6i + 8j + 10k + 12l$ variables of the form

$$h_n := i \cdot R_3 \oplus j \cdot h_1^8 \oplus k \cdot h_4^{10} \oplus l \cdot h_5^{12} \tag{4.4}$$

and find the minimal value n_0, such that for all $n \geq n_0$ the function h_n inherits the properties of its components from Table 3. Since the only strongly extendable function is h_4^{10} in 10 variables, we require that in all the four cases below $k \neq 0$:

Case 1. Since the first case has nothing to do with homogeneity and having no affine derivatives, one can use all the components from Table 3. Clearly, the smallest value of n is $n_0 = 16$ and in order to cover the missing values of $n \in \{12, 14\}$, we construct a function h'_n of the form

$$h'_n(x_1, \ldots, x_n) := h_4^{10}(x_1, \ldots, x_{10}) \oplus Q_k(x_{11}, \ldots, x_n) \text{ with } k = n - 10.$$

Here $Q_k := f_{id,0}$ is the quadratic bent function in k variables, defined by the "standard" inner product on $\mathbb{F}_2^k$. Since for the quadratic bent function Q_k its relaxed linearity index r-ind$(Q_k) = k$, we can not use Corollary 4.6. However, by the second part of Theorem 4.5, one can verify, that $h'_n \notin \mathcal{M}^\#$, by showing, that none of the vector subspaces U of the form

$$\left\{U \subseteq V \times W \colon V \in \mathcal{RMS}\left(h_4^{10}\right), W \in \mathcal{RMS}(Q_k)\right\}$$

is an $\mathcal{M}$-subspace of the function h'_n.

Case 2. Since there are no weakly extendable homogeneous cubic bent functions in six variables, we can use only components $h_1^8, h_4^{10}, h_5^{12}$ in the Eq. (4.4). One can see, that the smallest value of n is $n_0 = 26$ and the missing values are in the set $\{14, 16, 24\}$.

Case 3. First, we observe that the direct sum of two functions has no affine derivatives, if and only if both of them have no affine derivatives. Hence, the only functions we can use are R_3, h_4^{10}, h_5^{12}. In this way, the smallest value of n is $n_0 = 26$ and the missing values are in the set $\{12, 14, 18, 24\}$.

Case 4. Finally, since the only extendable functions, which are simultaneously homogeneous and have no affine derivatives are h_4^{10} and h_5^{12}, we observe, that the smallest value of n is $n_0 = 50$ and the missing values of n are in the set $\{12, 14, 16, 18, 24, 26, 28, 36, 38, 48\}$, which completes the proof. □

5 Conclusion

In this paper we proved the existence of cubic bent functions outside the completed Maiorana-McFarland class $\mathcal{M}^\#$ on $\mathbb{F}_2^n$ for all $n \geq 10$ and showed that for almost all values of n these functions can simultaneously be homogeneous and have no affine derivatives. The reason, why some values of n are not covered by our proof is explained by the non-existence of examples with desired properties in 6 and 8 variables, which are necessary for the used recursive framework.

In general, we expect that homogeneous cubic bent functions without affine derivatives outside $\mathcal{M}^\#$ exist for all even $n \geq 10$ and we leave this as an open problem. Since our proof technique is based on the direct sum construction of functions, some of them being members of $\mathcal{M}^\#$, the functions constructed in such a way will presumably have bad cryptographic primitives (see [7, p. 330]). Thus, we suggest the following problem.

Open Problem 5.1 *Construct homogeneous cubic bent functions without affine derivatives outside the $\mathcal{M}^\#$ class without the use of the direct sum.*

The next problem, which we would like to address, is related to the normality of cubic bent functions. Recall that a Boolean function f on $\mathbb{F}_2^n$ is said to be normal (weakly normal), when it is constant (affine, but not constant) respectively, on some affine subspace U of $\mathbb{F}_2^n$ of dimension $\lceil n/2 \rceil$. In this case f is said to be normal (weakly normal) with respect to the flat U. It is well-known that all quadratic bent functions are normal. Moreover, one can also construct non-normal as well as non-weakly normal bent functions of all degrees $d \geq 4$, as it follows from [6, Fact 22]. At the same time all cubic bent functions in $n = 6$ variables are normal or weakly-normal, while for $n = 8$ they are proved to be normal [9].

Since the functions h_3^{10} and h_4^{10} do not belong to the completed Maiorana-McFarland class, they are good candidates to be checked for the normality. Based on our parallel implementation of [6, Algorithm 1] in `Mathematica` [39] we observe, that the function h_3^{10} is normal on the flat $48 \oplus \langle$g3, 8p, 4q, 2m, 1j$\rangle$ and the function h_4^{10} is normal on the flat $5 \oplus \langle$i5, 8h, 6n, 1g, f$\rangle$. Here we describe each binary vector of a flat by 32-base representation, using the following alphabet

$$0 \mapsto 0, \ldots, \mathrm{f} \mapsto 15, \mathrm{g} \mapsto 16, \ldots, \mathrm{v} \mapsto 31. \tag{5.1}$$

In this way, since one still has no examples of non-weakly normal cubic bent functions, it is reasonable to ask the following question.

Open Problem 5.2 *Do non-weakly normal cubic bent functions exist?*

Finally we list all the homogeneous cubic bent functions used in the paper.

Acknowledgements The authors would like to thank Pantelimon Stănică for providing homogeneous cubic bent functions from [8, p. 149] and anonymous referees for their detailed comments that largely improved the quality of the manuscript.

Appendix. Known inequivalent homogeneous cubic bent functions

We represent each homogeneous cubic bent function h_i^n in n variables by its binary characteristic vector $v_2(h_i^n)$ in the following way. We denote by $H^{n,3}(\mathbf{x})$ the list, containing all the monomials of degree 3 in n variables, ordered lexicographically, i.e. $H^{n,3}(\mathbf{x}) := (x_1x_2x_3, x_1x_2x_4, \ldots, x_{n-2}x_{n-1}x_n)$. The binary characteristic vector $v_2(h_i^n)$ of a function h_i^n is a vector of length $\binom{n}{3}$, containing 1 at the position k, if the monomial $H_k^{n,3}(\mathbf{x})$ is in the ANF of h_i^n, and 0 otherwise. Thus the ANF of h_i^n can be recovered from the $v_2(h_i^n)$ by:

$$h_i^n(\mathbf{x}) = v_2(h_i^n) \cdot H^{n,3}(\mathbf{x}) = \bigoplus_{1 \le i < j < k \le n} a_{ijk} x_i x_j x_k. \tag{5.2}$$

Due to the space limitations, we list in Table 4 the 32-base representations $v_{32}(h_i^n)$ of binary characteristic vectors $v_2(h_i^n)$, using the alphabet (5.1).

Example 5.3 The ANF of the homogeneous cubic bent function h_1^6 can be reconstructed from its 32-base characteristic vector $v_{32}(h_1^6)$ in the following way. First, one converts 32-base characteristic vector $v_{32}(h_1^6)$ to the binary $v_2(h_1^6)$

$$v_{32}(h_1^6) = \mathrm{tffu} \longleftrightarrow v_2(h_1^6) = (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$$

Table 4 The known homogeneous cubic bent functions in a small number of variables and their invariants

h_i^n	$v_{32}(h_i^n)$	$\mathrm{ind}(h_i^n)$	r-$\mathrm{ind}(h_i^n)$	$\dim(\mathbb{FP}_{h_i^n})$
h_1^6	tffu	3	4	3
h_1^8	an3pi8adifs	4	**4**	1
h_2^8	1mgao45k3fd2	4	5	2
h_1^{10}	2uehlgo3c005e9umaor7bi0s	5	5	1
h_2^{10}	vvh79pr9r377dvjjmjjmg594	5	5	1
h_3^{10}	iljgkiijc005e9umaor7bi0s	**4**	**4**	1
h_4^{10}	3nbrkdcktp5euatcfbbrevhk	**2**	**4**	**0**
h_1^{12}	9722929gkh0ic8ih93e010goi70002as005e01e0c4	6	**6**	2
h_2^{12}	dfajbadksl8qtaqldb2qkp0u51eli3g5lo62lh3e2i	6	**6**	2
h_3^{12}	rkiesir9j97na9n9qmql3g0oet93027l8g4q91qkpt	6	7	1
h_4^{12}	noaluan595bfhbf5mcql3g0oet93027l8g4q91qkpt	6	7	2
h_5^{12}	d42j82d0o18q8aq1c2oulp067seli1jhlo2olgpeqv	6	**6**	**0**
h_6^{12}	1e6pqufj5jt3tfrt002ca4jon34b8qbtg2saq1nk01	6	≥ 7	1
h_7^{12}	1e6pqufj5jt3tfrt002ca4jon369cq8si2t6qbn002	6	≥ 7	1

To identify the examples, used in the Proof of the Theorem 4.9, values are given in bold
Functions h_1^6 and h_1^8, h_2^8 describe up to equivalence all homogeneous functions in 6 and 8 variables, respectively. Functions h_3^{10} and h_1^{10} are the first and the second 10-variable functions from [27, p. 15]. Functions h_2^{10} and h_4^{10} are representatives of equivalence classes of functions, constructed in [8, p. 149]. Functions h_i^{12} for $1 \leq i \leq 5$ are representatives of equivalence classes of functions, constructed in [8, p. 149]. Functions h_6^{12} and h_7^{12} were constructed in Sect. 3.3

and according to (5.2) the ANF of h_1^6 is given by:

$$\begin{aligned} h_1^6(\mathbf{x}) := {} & x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_5 \oplus x_2x_3x_5 \oplus x_1x_4x_5 \\ & \oplus x_2x_4x_5 \oplus x_3x_4x_5 \oplus x_1x_3x_6 \oplus x_2x_3x_6 \oplus x_1x_4x_6 \oplus x_2x_4x_6 \\ & \oplus x_3x_4x_6 \oplus x_1x_5x_6 \oplus x_2x_5x_6 \oplus x_3x_5x_6. \end{aligned}$$

For each homogeneous cubic bent function $h_i^n \in \mathcal{M}^{\#}$ on $\mathbb{F}_2^n$ we list the collection $\mathcal{M}_{n/2}(h_i^n)$ as a $|\mathcal{M}_{n/2}(h_i^n)| \times n/2$ matrix in the following way. Each row of $\mathcal{M}_{n/2}(h_i^n)$ describes the Gauss-Jordan basis of an $\mathcal{M}$-subspace of h_i^n. Each element of a basis is given by 32-base number, which can be converted to the binary vector of length n in the same way as in Example 5.3. For instance, the first row of the matrix $\mathcal{MS}_6(h_3^{12})$ describes the GJB(U) of the $\mathcal{M}$-subspace U, given in (3.4).

- $\mathcal{MS}_5(h_1^{10}) = \begin{pmatrix} \text{o2 4l 2m 1j f} \end{pmatrix}$, $\mathcal{MS}_5(h_2^{10}) = \begin{pmatrix} \text{o0 60 12 o 5} \end{pmatrix}$;
- $\mathcal{MS}_6(h_1^{12}) = \begin{pmatrix} \text{22r 10m it 8e 66 17} \\ \text{20q 12o in af 4s 1p} \\ \text{21c 10d gs 9n 5r 2e} \\ \text{20b 11u gj 9t 47 33} \\ \text{20v 11k hh 9o 5f 3i} \end{pmatrix}$, $\mathcal{MS}_6(h_3^{12}) = \begin{pmatrix} \text{300 gg 88 44 22 11} \\ \text{21u 10v hh 99 55 33} \\ \text{20v 11u hh 99 55 33} \end{pmatrix}$,
  $\mathcal{MS}_6(h_5^{12}) = \begin{pmatrix} \text{300 gg 88 44 22 11} \end{pmatrix}$, $\mathcal{MS}_6(h_1^{12}) = \mathcal{MS}_6(h_2^{12})$, $\mathcal{MS}_6(h_3^{12}) = \mathcal{MS}_6(h_4^{12}) = \mathcal{MS}_6(h_6^{12}) = \mathcal{MS}_6(h_7^{12})$.

References

1. Bending T.D.: Bent functions, SDP designs and their automorphism groups. Ph.D. thesis, Queen Mary and Westfield College (1993).
2. Bosma W., Cannon J., Playoust C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**(3–4), 235–265 (1997). Computational algebra and number theory (London, 1993) https://doi.org/10.1006/jsco.1996.0125.
3. Braeken A.: Cryptographic properties of Boolean functions and S-boxes. Ph.D. thesis, Katholieke Universiteit Leuven (2006).
4. Canteaut A., Charpin P.: Decomposing bent functions. IEEE Trans. Information Theory **49**, 2004–2019 (2003). https://doi.org/10.1109/ISIT.2002.1023314.
5. Canteaut A., Charpin P., Kyureghyan G.M.: A new class of monomial bent functions. Finite Fields and Their Applications **14**(1), 221–241 (2008). https://doi.org/10.1016/j.ffa.2007.02.004.
6. Canteaut A., Daum M., Dobbertin H., Leander G.: Finding nonnormal bent functions. Discrete Applied Mathematics **154**(2), 202–218 (2006). https://doi.org/10.1016/j.dam.2005.03.027.
7. Carlet C.: Boolean functions for cryptography and error-correcting codes. In: Y. Crama, P.L. Hammer (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Encyclopedia of Mathematics and Its Applications, pp. 257–397. Cambridge University Press (2010). https://doi.org/10.1017/CBO9780511780448.011
8. Charnes C., Rötteler M., Beth T.: Homogeneous bent functions, invariants, and designs. Designs, Codes and Cryptography **26**(1), 139–154 (2002). https://doi.org/10.1023/A:1016509410000.
9. Charpin P.: Normal boolean functions. J. Complexity **20**(2–3), 245–265 (2004). https://doi.org/10.1016/j.jco.2003.08.010.
10. Dillon J.F.: A survey of bent functions. NSA Technical Journal Special Issue, pp. 191–215, (1972).
11. Dillon J.F.: Elementary Hadamard difference sets. Ph.D. thesis, University of Maryland (1974). https://doi.org/10.13016/M2MS3K194.
12. Ding C.: Codes from Difference Sets. World Scientific (2014). https://doi.org/10.1142/9283.
13. Ding C.: Designs from Linear Codes. World Scientific (2018). https://doi.org/10.1142/11101.
14. Dobbertin H., Leander G., Canteaut A., Carlet C., Felke P., Gaborit P.: Construction of bent functions via niho power functions. J. Comb. Theory, Ser. A **113**(5), 779–798 (2006). https://doi.org/10.1016/j.jcta.2005.07.009.
15. Duan M., Lai X., Yang M., Sun X., Zhu B.: Distinguishing properties of higher order derivatives of Boolean functions. Cryptology ePrint Archive, Report 2010/417 (2010).
16. Dukes P.J., Wilson R.M.: Linear algebra and designs. In: C.J. Colbourn, J.H. Dinitz (eds.) Handbook of Combinatorial Designs, 2 edn., pp. 783–791. Chapman & Hall/CRC Press, Boca Raton (2007). https://doi.org/10.1201/9781420010541
17. Edel Y., Pott A.: On designs and multiplier groups constructed from almost perfect nonlinear functions. In: Cryptography and Coding, 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15–17, 2009. Proceedings, pp. 383–401 (2009). https://doi.org/10.1007/978-3-642-10868-6_23.
18. Edel, Y., Pott, A.: On the equivalence of nonlinear functions. In: Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, pp. 87–103 (2009).
19. Gockenbach, M.S.: Finite-dimensional linear algebra. Discrete mathematics and its applications. CRC Press, Hoboken, NJ (2010). https://doi.org/10.1201/b18294
20. Hou X.: Cubic bent functions. Discrete Mathematics **189**(1), 149–161 (1998). https://doi.org/10.1016/S0012-365X(98)00008-9.
21. Kholosha, A., Pott, A.: Bent and related functions. In: G.L. Mullen, D. Panario (eds.) Handbook of Finite Fields, 1st edn., pp. 262–273. Chapman & Hall/CRC (2013). https://doi.org/10.1201/b15006
22. Lai, X.: Higher order derivatives and differential cryptanalysis. In: R.E. Blahut, D.J. Costello, U. Maurer, T. Mittelholzer (eds.) Communications and Cryptography: Two Sides of One Tapestry, pp. 227–233. Springer US, Boston, MA (1994). https://doi.org/10.1007/978-1-4615-2694-0_23
23. Langevin P., Leander G.: Counting all bent functions in dimension eight 99270589265934370305785861242880. Des. Codes Cryptography **59**(1–3), 193–205 (2011). https://doi.org/10.1007/s10623-010-9455-z.
24. Leander N.G.: Monomial bent functions. IEEE Trans. Information Theory **52**(2), 738–743 (2006). https://doi.org/10.1109/TIT.2005.862121.
25. MacWilliams F., Sloane N.: The Theory of Error-Correcting Codes, 2nd edn. North-holland Publishing Company, (1978).

26. Mandal B., Gangopadhyay S., Stănică P.: Cubic Maiorana-McFarland bent functions with no affine derivative. International Journal of Computer Mathematics: Computer Systems Theory **2**(1), 14–27 (2017). https://doi.org/10.1080/23799927.2017.1304453.
27. Meng Q., Yang M., Zhang H., Cui J.: A novel algorithm enumerating bent functions. Cryptology ePrint Archive, Report 2004/274 (2004).
28. Mesnager S.: Several new infinite families of bent functions and their duals. IEEE Transactions on Information Theory **60**(7), 4397–4407 (2014). https://doi.org/10.1109/TIT.2014.2320974.
29. Newman M., Thompson R.C.: Matrices over rings of algebraic integers. Linear Algebra and its Applications **145**, 1–20 (1991). https://doi.org/10.1016/0024-3795(91)90284-4.
30. Polujan A.A., Pott A.: Homogeneous cubic bent functions without affine derivatives outside the completed Maiorana-McFarland class. In: Proceedings of the Eleventh International Workshop on Coding and Cryptography (2019).
31. Pott A.: Finite Geometry and Character Theory, vol. 1601. Lecture Notes in Mathematics Springer, Berlin (1995).
32. Pott A.: Almost perfect and planar functions. Des. Codes Cryptography **78**(1), 141–195 (2016). https://doi.org/10.1007/s10623-015-0151-x.
33. Preneel B.: Analysis and design of cryptographic hash functions. Ph.D. thesis, Katholieke Universiteit Leuven (1993).
34. Qu C., Seberry J., Pieprzyk J.: On the symmetric property of homogeneous Boolean functions. In: 4th Australasian Conference on Information Security and Privacy, pp. 26–35 (1999). https://doi.org/10.1007/3-540-48970-3_3.
35. Rothaus O.: On bent functions. J. Comb. Theory Ser. A **20**(3), 300–305 (1976). https://doi.org/10.1016/0097-3165(76)90024-8.
36. Seberry J., Xia T., Pieprzyk J.: Construction of cubic homogeneous Boolean bent functions. Australasian Journal of Combinatorics **22**, 233–245 (2000).
37. Weng G., Feng R., Qiu W.: On the ranks of bent functions. Finite Fields and Their Applications **13**(4), 1096–1116 (2007). https://doi.org/10.1016/j.ffa.2007.03.001.
38. Weng G., Feng R., Qiu W., Zheng Z.: The ranks of Maiorana-McFarland bent functions. Science in China Series A: Mathematics **51**(9), 1726–1731 (2008). https://doi.org/10.1007/s11425-007-0167-4.
39. Wolfram Research, Inc.: Mathematica, Version 11.2. Champaign, IL, (2017)
40. Yashchenko, V.V.: On the propagation criterion for Boolean functions and on bent functions. Probl. Peredachi Inf. 33(1), 75–86 (1997). In Russian.