Homogeneous cubic bent functions without affine derivatives outside the completed Maiorana-McFarland class

Alexandr A. Polujan and Alexander Pott

Otto-von-Guericke-Universität, Universitätsplatz 2, 39106, Magdeburg, Germany
{alexandr.polujan,alexander.pott}@ovgu.de

Abstract. In this paper we prove the existence of bent functions which have simultaneously the following properties: cubic, homogeneous, no affine derivatives and not in the completed Maiorana-McFarland class. We also show, that in opposite to the cases of 6 and 8 variables the original Maiorana-McFarland construction does not describe the whole class of cubic bent functions in n variables for all $n \geq 16$.

Keywords: Homogeneous cubic bent functions · Affine derivatives · Extended-affine equivalence · Completed Maiorana-McFarland class.

1 Introduction

Homogeneous cubic bent functions [11] and cubic bent functions without affine derivatives [9] have been intensively studied in the last two decades, partly because of their application in cryptography [10, 13]. Several infinite families of such functions were constructed, however all of them belong to the completed Maiorana-McFarland class $\mathcal{M}^{\#}$ [2, 10, 13], what may be considered as a cryptographic weakness of these functions [4, p. 396].

In this paper we prove that cubic bent functions in n variables, which possess both properties (homogeneity and having no affine derivatives), exist for all $n \geq 50$ and, moreover, do not belong to $\mathcal{M}^{\#}$. Our solution strategy consists of two steps. Firstly, we analyse lost[1] examples of homogeneous cubic bent functions in $n = 10$, 12 variables, constructed by Charnes et al. in [6, p. 149]. We show, that some of these functions are outside the $\mathcal{M}^{\#}$ class and do not have affine derivatives. Secondly, in order to extend these functions to an infinite family, we introduce a new sufficient condition on bent functions f and g, such that the direct sum $f \oplus g$ is outside $\mathcal{M}^{\#}$. Finally, since the direct sum $f \oplus g$ trivially preserves homogeneity and non-affinity of derivatives of functions f and g, it is enough to check, whether the analysed functions satisfy the new sufficient condition and hence are extendible to an infinite family of functions outside the $\mathcal{M}^{\#}$ class.

The paper is organized in the following way. In Section 1.1, some basic notions and background on Boolean functions are introduced. In Section 1.2 we

[1] Since they are not available online any more.

describe an algorithm, which checks, whether a given Boolean function belongs to the $\mathcal{M}^{\#}_{r,s}$ class; this is a generalization of the completed Maiorana-McFarland class $\mathcal{M}^{\#}$. In Section 2 we provide our main theoretical results. For a Boolean function f we introduce relaxed $\mathcal{M}$-subspaces as vector subspaces U by the property, that second-order derivatives $D_{\mathbf{a},\mathbf{b}}f$ are constants for all two-dimensional vector subspaces $\langle \mathbf{a}, \mathbf{b} \rangle$ of U. Subsequently, we deduce some properties of these subspaces and explain how one can construct them algorithmically. Finally, we prove that the direct sum $f \oplus g$ of bent functions f and g is outside $\mathcal{M}^{\#}$, provided relaxed $\mathcal{M}$-subspaces of functions f and g are "small enough". In Section 3 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 and (or) do not have affine derivatives. 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 $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ are called *Boolean functions* in n variables. A Boolean function on $\mathbb{F}_2^n$ can be uniquely expressed as a polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1 \oplus x_1^2, \ldots, x_n \oplus x_n^2)$. This representation is called the *algebraic normal form* (denoted further as *ANF*), that is,

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

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 *algebraic degree* of a Boolean function f, denoted by $\deg(f)$, is the algebraic degree of its ANF. Further we will be interested in *homogeneous cubic* functions, i.e. functions whose ANF contains monomials of degree three only.

With a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ one can associate the following two mappings: $D_{\mathbf{a}}f(\mathbf{x}) := f(\mathbf{x} \oplus \mathbf{a}) \oplus f(\mathbf{x})$, which is called the *first-order derivative* of f, and $D_{\mathbf{a},\mathbf{b}}f(\mathbf{x}) := D_{\mathbf{b}}(D_{\mathbf{a}}f)(\mathbf{x}) = f(\mathbf{x} \oplus \mathbf{a} \oplus \mathbf{b}) \oplus f(\mathbf{x} \oplus \mathbf{a}) \oplus f(\mathbf{x} \oplus \mathbf{b}) \oplus f(\mathbf{x})$, which is called the *second-order derivative* of f.

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

Remark 1. It is well-known, that bent functions in n variables exist only for n even and of degree at most $n/2$, see [12].

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 exist 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 $\mathbf{x} \in \mathbb{F}_2^n$.

1.2 The completed general Maiorana-McFarland class of Boolean functions

The *general Maiorana-McFarland class* $\mathcal{M}_{r,s}$ of Boolean functions in $n = r + s$ variables [4, p. 354] is the set of Boolean functions of the form

$$f(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \phi(\mathbf{y}) \rangle_r \oplus g(\mathbf{y}),$$

where $\mathbf{x} \in \mathbb{F}_2^r$, $\mathbf{y} \in \mathbb{F}_2^s$, g is an arbitrary Boolean function on $\mathbb{F}_2^s$ and $\phi \colon \mathbb{F}_2^s \to \mathbb{F}_2^r$ is some mapping. A function f belongs to the *completed general 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 ϕ is a permutation [4, p. 325]. The completed version of $\mathcal{M}$ is denoted by $\mathcal{M}^{\#}$.

The characterization of the completed Maiorana-McFarland class $\mathcal{M}^{\#}$ of bent functions is given in [8, p. 102] and [3, Lemma 33]. In the case of the $\mathcal{M}_{r,s}^{\#}$ class, the proof is similar.

Proposition 1. *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 Proposition 1.

Definition 2. *We will call a subspace U an $\mathcal{M}$-subspace of a Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$, if for all $\mathbf{a}, \mathbf{b} \in U$ 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*

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

Remark 2. It is enough to consider $\mathbf{a}, \mathbf{b} \in U$, which form two-dimensional vector subspaces, since all second-order derivatives of the form $D_{\mathbf{a},\mathbf{a}}f, D_{\mathbf{a},\mathbf{0}}f$ and $D_{\mathbf{0},\mathbf{b}}f$ are equal to the zero function.

Definition 3. *The linearity index* $\mathrm{ind}(f)$ *of a Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ is is the maximal possible r, such that $f \in \mathcal{M}_{r,s}^{\#}$, see for details [14, p. 82]. 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. 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

$D_{\mathbf{a},\mathbf{b}}f(\mathbf{x}) = c_{\mathbf{0}}(\mathbf{a},\mathbf{b}) \oplus (a_3b_2 \oplus a_2b_3)x_1 \oplus (a_3b_1 \oplus a_1b_3)x_2 \oplus (a_2b_1 \oplus a_1b_2)x_3$, 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, by verifying, that on all of its two-dimensional vector subspaces given by generators $\mathbf{a}$ and $\mathbf{b}$ below, the corresponding second-order derivatives $D_{\mathbf{a},\mathbf{b}}f$ are constant zero:

$$\begin{pmatrix} 0&0&0&1&0&0 \\ 0&0&0&0&0&1 \end{pmatrix} \mapsto 0, \begin{pmatrix} 0&0&0&1&0&0 \\ 0&0&0&0&0&1 \end{pmatrix} \mapsto 0, \begin{pmatrix} 0&0&0&1&1&0 \\ 0&0&0&0&0&1 \end{pmatrix} \mapsto 0, \begin{pmatrix} 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \end{pmatrix} \mapsto 0,$$
$$\begin{pmatrix} 0&0&0&1&0&1 \\ 0&0&0&0&1&0 \end{pmatrix} \mapsto 0, \begin{pmatrix} 0&0&0&1&0&0 \\ 0&0&0&0&1&1 \end{pmatrix} \mapsto 0, \begin{pmatrix} 0&0&0&1&0&1 \\ 0&0&0&0&1&1 \end{pmatrix} \mapsto 0.$$

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.

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 $r \in \mathbb{N}, r \geq 2$.
Output: The collection $\mathcal{MS}_r(f)$.

1: **Construct** $\mathcal{MS}_2(f) := \{U = \langle \mathbf{a},\mathbf{b} \rangle : \dim(U) = 2 \text{ and } D_{\mathbf{a},\mathbf{b}}f = 0\}$.
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 $\tilde{\mathbf{u}} \notin U$, s.t. 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 3. Algorithm 1 can be used to compute the linearity index of a given function f in the following way: $\mathrm{ind}(f)$ is the smallest r, for which $\mathcal{MS}_r(f) = \varnothing$.

2 Relaxed $\mathcal{M}$-subspaces of Boolean functions

In this section we analyse $\mathcal{M}$-subspaces of the direct sum construction. Recall that the function $h\colon \mathbb{F}_2^{n+m} \to \mathbb{F}_2$, defined by $h(\mathbf{x},\mathbf{y}) := f(\mathbf{x}) \oplus g(\mathbf{y})$, is called the *direct sum* of f and g, where $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ and $g\colon \mathbb{F}_2^m \to \mathbb{F}_2$. In this way, we will identify $\mathbb{F}_2^{n+m}$ with $\mathbb{F}_2^n \otimes \mathbb{F}_2^m$ and hence any vector $\mathbf{v} \in \mathbb{F}_2^{n+m}$ is identified with 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 $\mathbf{a},\mathbf{b} \in U$ second-order derivatives $D_{\mathbf{a},\mathbf{b}}h = 0$. 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 definition.

Definition 4. *We will call a subspace U a relaxed $\mathcal{M}$-subspace of a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, if for all $\mathbf{a}, \mathbf{b} \in U$ 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 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 5. *For a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ its relaxed linearity index* $\text{r-ind}(f)$ *is defined by* $\text{r-ind}(f) := \max_{U \in \mathcal{RMS}(f)} \dim(U)$.

Example 2. Let $f\colon \mathbb{F}_2^6 \to \mathbb{F}_2$ be a function from Example 1. One can check, that 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 $D_{\mathbf{a},\mathbf{b}}f$ are constant zero or constant one for all $\mathbf{a}, \mathbf{b} \in U$, corresponding to two-dimensional vector subspaces:

$$\begin{pmatrix} 0&0&0&1&0&0\\ 0&0&0&0&1&1 \end{pmatrix} \mapsto 0, \begin{pmatrix} 0&1&0&0&0&1\\ 0&0&0&0&1&1 \end{pmatrix} \mapsto 1, \begin{pmatrix} 0&1&0&1&0&1\\ 0&0&0&0&1&1 \end{pmatrix} \mapsto 1, \begin{pmatrix} 0&1&0&0&0&1\\ 0&0&0&1&0&0 \end{pmatrix} \mapsto 0,$$
$$\begin{pmatrix} 0&1&0&0&1&0\\ 0&0&0&1&0&0 \end{pmatrix} \mapsto 0, \begin{pmatrix} 0&1&0&0&0&1\\ 0&0&0&1&1&1 \end{pmatrix} \mapsto 1, \begin{pmatrix} 0&1&0&0&1&0\\ 0&0&0&1&1&1 \end{pmatrix} \mapsto 1.$$

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

Proposition 2. *Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function and let $n = r + s$.*

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

Proof. 1. This follows from 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 $|\mathcal{RMS}_r(f)| = |\mathcal{RMS}_r(f')|$ and $|\mathcal{MS}_r(f)| = |\mathcal{MS}_r(f')|$. Since $\dim(U) = \dim(U')$, we have $\text{ind}(f) = \text{ind}(f')$ and $\text{r-ind}(f) = \text{r-ind}(f')$.
3. First, since $\mathcal{MS}(f) \subseteq \mathcal{RMS}(f)$ the inequality $\text{ind}(f) \leq \text{r-ind}(f)$ 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, constructed via the direct product of relaxed $\mathcal{M}$-subspaces of f and g.

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

Proof. 1. Let $U = V \otimes W$. 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:

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

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

$$D_{\mathbf{u}_1,\mathbf{u}_2} h(\mathbf{x}, \mathbf{y}) = D_{\mathbf{u}_1,\mathbf{u}_2} f'(\mathbf{x}, \mathbf{y}) \oplus D_{\mathbf{u}_1,\mathbf{u}_2} g'(\mathbf{x}, \mathbf{y}) = c_{\mathbf{u}_1,\mathbf{u}_2} \tag{1}$$

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

$$D_{\mathbf{u}_1,\mathbf{u}_2} f'(\mathbf{x}_1, \mathbf{y}) \oplus D_{\mathbf{u}_1,\mathbf{u}_2} g'(\mathbf{x}_1, \mathbf{y}) = c_{\mathbf{u}_1,\mathbf{u}_2} \tag{2}$$

$$D_{\mathbf{u}_1,\mathbf{u}_2} f'(\mathbf{x}_2, \mathbf{y}) \oplus D_{\mathbf{u}_1,\mathbf{u}_2} g'(\mathbf{x}_2, \mathbf{y}) = c_{\mathbf{u}_1,\mathbf{u}_2}, \tag{3}$$

which hold for any $\mathbf{y} \in \mathbb{F}_2^m$ due to (1). Adding equation (2) to (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 $f'(\mathbf{x}, \mathbf{y})$ 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, $U \subseteq V \otimes W$ and by the previous statement we have $V \otimes W \in \mathcal{RMS}(h)$.
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 $U \subseteq V \otimes W$. Now, using the following series of inequalities

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

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 1. *Let* $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ *and* $g\colon \mathbb{F}_2^m \to \mathbb{F}_2$ *be two Boolean bent functions. If* f *and* g *satisfy* r-ind$(f) < n/2$ *and* r-ind$(g) \leq m/2$*, then* $f \oplus g \notin \mathcal{M}^{\#}$.

Remark 4. 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

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

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 the Algorithm 1 in the way already described in Remark 3.

3 Application to homogeneous cubic bent functions

First, we describe how one can compute, whether a given cubic function does not have affine derivatives.

Remark 5. If the function f is cubic, its derivatives are quadratic or affine. That means, for each $\mathbf{a} \in \mathbb{F}_2^n$ the first-order derivative $D_{\mathbf{a}}f$ can be represented as a quadratic form

$$D_{\mathbf{a}}f(\mathbf{x}) = \bigoplus_{1\leq i\leq j\leq n} c_{i,j}x_ix_j \oplus d = \mathbf{x}C\mathbf{x}^T \oplus d,$$

where $C = (c'_{i,j})_{1\leq i,j\leq n}$ is the *coefficient matrix* of the quadratic form, which is defined as $c'_{i,j} := c_{i,j}$ if $i \leq j$ and $c'_{i,j} := 0$ otherwise. The *rank* of a quadratic function f is defined as $\mathrm{rank}(f) := \mathrm{rank}_{\mathbb{F}_2}(C \oplus C^T)$. Finally, a cubic function f has no affine derivatives if and only if

$$\theta_0(f) := |\{\mathbf{a} \in \mathbb{F}_2^n\colon \mathbf{a} \neq \mathbf{0},\ \mathrm{rank}(D_{\mathbf{a}}f) = 0\}| = 0.$$

Using Remarks 3, 4 and 5 we checked, whether among the 200 functions in $n = 10$ variables and the 480 functions in $n = 12$ variables, constructed in [5, p. 149], there exist homogeneous cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$, which have relaxed linearity index less (or equal to) $n/2$. An example of such a function h_{10} in 10 variables with r-ind$(h_{10}) = 4$ is given in the Appendix. However, all homogeneous cubic bent functions in 12 variables, constructed in [5, p. 149] belong to the $\mathcal{M}^{\#}$ class. Nevertheless, among them we found a function h_{12} without affine derivatives and r-ind$(h_{12}) = 6$.

Since all cubic bent functions in 6 variables belong to $\mathcal{M}^{\#}$ [7, p. 37], one can expect to find only homogeneous cubic bent function without affine derivatives and relaxed linearity index equal to 3, but not outside $\mathcal{M}^{\#}$. Unfortunately, such

functions do not exist. However, we found a non-homogeneous cubic function f_6 without affine derivatives and relaxed linearity index equal to 3. Since all cubic bent functions in 8 variables are members of the $\mathcal{M}^{\#}$ class [1, p. 103] and have affine derivatives [9], we can only expect to have homogeneous cubic bent function with linearity index equal to 4. Such a function, denoted by h_8, is given in the Appendix.

Table 1. Linearity index ind$(\cdot)$, relaxed linearity index r-ind$(\cdot)$ and the number of affine derivatives $\theta_0(\cdot)$ for cubic bent functions f_6, h_8, h_{10}, h_{12}, given in the Appendix.

	f_6	h_8	h_{10}	h_{12}
ind$(\cdot)$	3	4	2	6
r-ind$(\cdot)$	3	4	4	6
$\theta_0(\cdot)$	0	1	0	0

Finally we give our main result about the existence of cubic bent functions outside $\mathcal{M}^{\#}$, having nice cryptographic properties.

Theorem 2. *On $\mathbb{F}_2^n$ there exist:*

1. *Cubic bent functions outside $\mathcal{M}^{\#}$ for all $n \geq 16$.*
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. We will prove only the last case, since it deals with the most interesting combination of properties and the rest of the cases can be shown in the same manner. First, we construct the following functions h_k in k variables for $k \in \{50, 52, 54, 56, 58\}$:

$$\begin{aligned}
h_{50} :=& h_{10} \oplus h_{10} \oplus h_{10} \oplus h_{10} \oplus h_{10},\\
h_{52} :=& h_{10} \oplus h_{10} \oplus h_{10} \oplus h_{10} \oplus h_{12},\\
h_{54} :=& h_{10} \oplus h_{10} \oplus h_{10} \oplus h_{12} \oplus h_{12},\\
h_{56} :=& h_{10} \oplus h_{10} \oplus h_{12} \oplus h_{12} \oplus h_{12},\\
h_{58} :=& h_{10} \oplus h_{12} \oplus h_{12} \oplus h_{12} \oplus h_{12}.
\end{aligned}$$

Let $h_n := h_k \oplus \left(\bigoplus_j h_{10}\right)$ be a function on $\mathbb{F}_2^n$, where $k \in \{50, 52, 54, 56, 58\}$. Clearly, for any even $n \geq 50$ the function h_n is homogeneous cubic bent [13, Theorem 2], does not have affine derivatives (otherwise one of the summands has) and is outside $\mathcal{M}^{\#}$, since functions h_{10} and h_{12} satisfy Corollary 1, see Table 1, and, hence, the relaxed linearity index of h_n is upper bounded by r-ind$(h_n) \leq 28 + 4j < n/2$. □

4 Conclusion

In this paper we proved the existence of homogeneous cubic bent functions without affine derivatives outside the $\mathcal{M}^{\#}$ class on $\mathbb{F}_2^n$ for all $n \geq 50$. However, since we do not have enough many good examples in small number of variables, some values of n are not covered. But we expect, that such bent functions exist for all even $n \geq 10$ and we leave this statement as a problem. Since our proof uses the direct sum construction and functions, some of them being members of $\mathcal{M}^{\#}$, what makes our solution not suitable for cryptographic purposes, we suggest to work on the following problem.

Problem 1. Construct homogeneous cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$ class not using the direct sum construction.

There are two main classes of Bent functions: the completed Maiorana-McFarland class $\mathcal{M}^{\#}$ of bent functions and the completed *partial spread class* $\mathcal{PS}^{\#}$ of bent functions, introduced by Dillon [8]. Since we have shown, that cubic bent functions with nice properties can be outside $\mathcal{M}^{\#}$, it is reasonable to ask, whether the cubic bent functions with the same properties can be outside $\mathcal{PS}^{\#}$. This problem seems way more difficult than the original one, solved in the paper, since unlike the $\mathcal{M}^{\#}$ class, the completed partial spread class $\mathcal{PS}^{\#}$ of bent functions does not have a nice algebraic description, which can be seen from the algebraic normal form of a Boolean function.

Problem 2. Construct homogeneous cubic bent functions without affine derivatives outside $\mathcal{PS}^{\#}$ class.

Appendix

Algebraic normal forms of cubic bent functions used in the paper. We abbreviated $0 \leq i \leq 9$ for the variable x_i, variables x_{10} and x_{11} are replaced by a and b respectively. The index below the function indicates the number of its variables. Homogeneous cubic bent functions h_8, h_{10} and h_{12} are taken from [6, p. 149].

f_6. $012 \oplus 034 \oplus 235 \oplus 05 \oplus 13 \oplus 24 \oplus 25 \oplus 34 \oplus 35$

h_8. $012 \oplus 013 \oplus 015 \oplus 017 \oplus 023 \oplus 025 \oplus 026 \oplus 045 \oplus 047 \oplus 057 \oplus 067 \oplus 126 \oplus 135 \oplus 136 \oplus 137 \oplus 146 \oplus 147 \oplus 167 \oplus 234 \oplus 235 \oplus 236 \oplus 245 \oplus 257 \oplus 267 \oplus 346 \oplus 356 \oplus 357 \oplus 567$

h_{10}. $015 \oplus 016 \oplus 017 \oplus 019 \oplus 023 \oplus 024 \oplus 026 \oplus 028 \oplus 029 \oplus 034 \oplus 035 \oplus 037 \oplus 038 \oplus 039 \oplus 046 \oplus 056 \oplus 057 \oplus 059 \oplus 068 \oplus 069 \oplus 089 \oplus 124 \oplus 127 \oplus 128 \oplus 129 \oplus 135 \oplus 136 \oplus 137 \oplus 145 \oplus 148 \oplus 156 \oplus 158 \oplus 159 \oplus 167 \oplus 169 \oplus 178 \oplus 179 \oplus 189 \oplus 236 \oplus 238 \oplus 245 \oplus 246 \oplus 247 \oplus 249 \oplus 257 \oplus 258 \oplus 269 \oplus 278 \oplus 279 \oplus 289 \oplus 346 \oplus 348 \oplus 349 \oplus 357 \oplus 359 \oplus 367 \oplus 368 \oplus 369 \oplus 379 \oplus 389 \oplus 457 \oplus 458 \oplus 459 \oplus 468 \oplus 469 \oplus 478 \oplus 479 \oplus 489 \oplus 567 \oplus 579 \oplus 589 \oplus 679$

h_{12}. $024 \oplus 025 \oplus 027 \oplus 02a \oplus 038 \oplus 03a \oplus 046 \oplus 047 \oplus 049 \oplus 05a \oplus 068 \oplus 069 \oplus 06b \oplus 08a \oplus 08b \oplus 127 \oplus 129 \oplus 135 \oplus 136 \oplus 138 \oplus 13b \oplus 149 \oplus 14b \oplus 157 \oplus 158 \oplus 15a \oplus 16b \oplus 179 \oplus 17a \oplus 19b \oplus 234 \oplus 235 \oplus 239 \oplus 23a \oplus 23b \oplus 245 \oplus 247 \oplus 249 \oplus 24b \oplus 256 \oplus 257 \oplus 25a \oplus 279 \oplus 27a \oplus 28b \oplus 29a \oplus 29b \oplus 2ab \oplus 345 \oplus 346 \oplus 34a \oplus$

$34b \oplus 356 \oplus 358 \oplus 35a \oplus 367 \oplus 368 \oplus 36b \oplus 38a \oplus 38b \oplus 3ab \oplus 456 \oplus 457 \oplus 45b \oplus 467 \oplus 469 \oplus 46b \oplus 478 \oplus 479 \oplus 49b \oplus 567 \oplus 568 \oplus 578 \oplus 57a \oplus 589 \oplus 58a \oplus 678 \oplus 679 \oplus 689 \oplus 68b \oplus 69a \oplus 69b \oplus 789 \oplus 78a \oplus 79a \oplus 7ab \oplus 89a \oplus 89b \oplus 8ab \oplus 9ab$

Acknowledgements

The authors would like to thank Pantelimon Stănică for providing homogeneous cubic bent functions from [6, p. 149].

References

1. Braeken, A.: Cryptographic Properties of Boolean Functions and S-Boxes. Ph.D. thesis, Katholieke Universiteit Leuven, (2006)
2. Canteaut, A., Charpin, P.: Decomposing bent functions. IEEE Trans. Information Theory **49**, 2004–2019 (2003)
3. Canteaut, A., Daum, M., Dobbertin, H., Leander, G.: Finding nonnormal bent functions. Discrete Applied Mathematics **154**(2), 202–218 (2006)
4. Carlet, C.: Boolean Functions for Cryptography and Error-Correcting Codes, 257–397. Encyclopedia of Mathematics and its Applications, Cambridge University Press (2010)
5. Charnes, C., Dempwolff, U., Pieprzyk, J.: The eight variable homogeneous degree three bent functions. Journal of Discrete Algorithms **6**(1), 66–72 (2008)
6. Charnes, C., Rötteler, M., Beth, T.: Homogeneous bent functions, invariants, and designs. Designs, Codes and Cryptography **26**(1), 139–154 (2002)
7. Dillon, J.F.: A survey of bent functions. NSA Technical Journal, Special Issue, 191–215 (1972)
8. Dillon, J.F.: Elementary Hadamard difference sets. Ph.D. thesis, University of Maryland (1974)
9. Hou, X.-D.: Cubic bent functions. Discrete Mathematics **189**(1), 149–161 (1998)
10. 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)
11. Qu, C., Seberry, J., Pieprzyk, J.: On the symmetric property of homogeneous Boolean functions. ACISP'99, Proceedings, 26–35 (1999)
12. Rothaus, O.: On "bent" functions. Journal of Combinatorial Theory, Series A **20**(3), 300–305 (1976)
13. Seberry, J., Xia, T., Pieprzyk, J.: Construction of cubic homogeneous Boolean bent functions. Australasian Journal of Combinatorics **22**(1), 233–245 (2000)
14. Yashchenko, V.V.: On the propagation criterion for Boolean functions and on bent functions. Probl. Peredachi Inf. **33**(1), 75–86 (1997) (in Russian)