On cubic-like bent Boolean functions

Claude Carlet and Irene Villa

Universities of Bergen, Norway, and Paris 8 (LAGA), France;

Universities of Trento, Italy, and Bergen, Norway.

E-mail: claude.carlet@gmail.com; irene1villa@gmail.com

Abstract

Cubic bent Boolean functions (i.e. bent functions of algebraic degree at most 3) have the property that, for every nonzero element a of $\mathbb{F}_2^n$, the derivative $D_af(x) = f(x) + f(x + a)$ of f admits at least one derivative $D_bD_af(x) = f(x) + f(x + a) + f(x + b) + f(x + a + b)$ that is equal to constant function 1. We study the general class of those Boolean functions having this property, which we call cubic-like bent. We study the properties of such functions and the structure of their constant second-order derivatives. We characterize them by means of their Walsh transform (that is, by their duals), by the Walsh transform of their derivatives and by other means. We study them within the Maiorana-McFarland class of bent functions, providing characterizations and constructions and showing the existence of cubic-like bent functions of any algebraic degree between 2 and $\frac{n}{2}$.

Keywords: Boolean functions; Bent functions; cubic functions; EA-equivalence

MSC: 06E30, 94A60, 11T71

1 Introduction

Bent functions are fascinating mathematical objects playing important roles in combinatorics, finite fields, error correcting codes, cryptography and sequences for telecommunications. Their classification seems out of reach (only quadratic bent functions are all known and classified under affine equivalence; for $k = 3, \ldots, \frac{n}{2}$, the structure of the bent functions of algebraic degree k is completely unknown) and their study consists then in investigating their properties, constructing classes of bent functions, studying superclasses such as those of partially bent and plateaued functions, and subclasses (with the hope that eventually, the classification of such sub-classes could be achieved). Bent functions can be defined as those Boolean functions whose derivatives $D_af(x) = f(x) + f(x + a)$, $a \neq 0$, are balanced. They are also those Boolean functions in even numbers of variables that lie at maximum Hamming distance $2^{n-1} - 2^{\frac{n}{2}-1}$ from affine Boolean functions.

Cubic functions are those Boolean functions whose algebraic normal form has degree at most 3. Their derivatives, which have then algebraic degree at most 2, are balanced if and only if they admit at least one derivative $D_bD_af(x) = D_aD_bf(x)$ that is equal to the constant function 1 (see e.g. [7]).

In this work we study the general class of those Boolean functions, that we call *cubic-like bent*, whose derivatives D_af, $a \neq 0$, all admit at least one derivative equal to constant function 1. Cubic-like bent functions are bent. We shall study the properties of cubic-like bent functions, study them within a classical class of bent functions, namely the Maiorana-McFarland class, provide construction methods for cubic-like bent functions, and show that, regardless of the restrictive condition in this newly introduced property, there are such functions of any (admissible) degree.

This work is organised as follows. After preliminaries in Section 2, we define cubic-like bent functions in Section 3, providing some basic characterizations and showing the EA-invariance of the notion. In Section 4 we study this property by means of the number of constant second-order derivatives. Section 5 investigates the dual of a cubic-like bent map and presents different characterizations of the studied property by means of the Walsh transform of the function (and hence, by means of the dual of the function), of the Walsh transform of its derivatives and of the convolutional product between the Walsh transforms of the function and of its derivatives. Section 6 studies the cubic-like bent property for functions belonging to the Maiorana-McFarland class (where we find cubic-like bent functions of any degree between 2 and $\frac{n}{2}$). At last, Section 7 presents some computational results.

2 Preliminaries

Let $\mathbb{F}_2$ be the finite field with two elements and, for n a positive integer, let $\mathbb{F}_2^n$ be the vector space of dimension n over $\mathbb{F}_2$. With e_i, for $1 \leq i \leq n$, we refer to the i-th vector in the canonical basis of $\mathbb{F}_2^n$, that is, the vector in $\mathbb{F}_2^n$ that has the i-th entrance equal to 1 and all the others equal to zero.
A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, where m is a positive integer too, is called an (n,m)-function, and if we do not want to specify the values of n and m, we call it a *vectorial Boolean function* or more simply a *vectorial function*. When $m = 1$, a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called an *n-variable Boolean function*. Its Hamming weight equals the size of its support: $w_H(f) = |supp(f)|$, where $supp(f) = \{x \in \mathbb{F}_2^n;\ f(x) = 1\}$ (and the Hamming distance between two functions equals the Hamming weight of their sum). The *linear kernel* of a Boolean function (or of a vectorial function) f equals the set of all $a \in \mathbb{F}_2^n$ such that the *derivative* $D_af(x) = f(x) + f(x + a)$ is constant. The *0-linear kernel* equals the set of all $a \in \mathbb{F}_2^n$ such that the *derivative* $D_af(x) = f(x) + f(x + a)$ equals the 0 function. Both are vector spaces over $\mathbb{F}_2$ since, for every a and b, we have $D_af(x) + D_bf(x) = D_{a+b}f(x + a)$. The 0-linear kernel of a Boolean function

either is a hyperplane of the linear kernel or equals the whole linear kernel.

A Boolean function f admits a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called its algebraic normal form (ANF):

$$f(x) = f(x_1, \ldots, x_n) = \bigoplus_{I \subseteq [n]} a_I \prod_{i \in I} x_i, \ a_I \in \mathbb{F}_2,$$

where $[n]$ is the set $\{1, \ldots, n\}$. The monomial $\prod_{i \in I} x_i$ is a term of f whenever $a_I \neq 0$, that is, $a_I = 1$. The algebraic degree of f, denoted by $\deg(f)$, is the maximal value in the set $\{|I| : I \subseteq [n] \ s.t. \ a_I \neq 0\}$. A function f has algebraic degree n if and only if it has an odd Hamming weight and it is affine if it has algebraic degree at most 1 (and linear if in addition it satisfies $f(0) = 0$). We call quadratic (resp. cubic) the Boolean functions of algebraic degree at most 2 (resp. at most 3). A Boolean function is called balanced if its output is equally distributed over 0's and 1's. A quadratic function f is balanced if and only if at least one of its derivatives $D_a f(x)$ equals constant function 1, see [7, Proposition 55 and foll.]. For a non-quadratic function f, this latter condition is sufficient (but no more necessary) for f to be balanced. Indeed, if f admits a derivative equal to constant function 1, then there exists $a \in \mathbb{F}_2^n$ and a set $V \subset \mathbb{F}_2^n$, $|V| = 2^{n-1}$ such that $V \cup (V + a) = \mathbb{F}_2^n$ and $(f(v), f(v + a)) = (1, 0)$ for every $v \in V$. Two n-variable Boolean functions f and g are called *extended affine equivalent* (shortly *EA-equivalent*) if there exist a linear automorphism $L(x)$ of $\mathbb{F}_2^n$, an affine n-variable Boolean function $\ell(x)$ and an element d of $\mathbb{F}_2^n$ such that:

$$g(x) = f(L(x) + d) + \ell(x). \tag{1}$$

In this case, we write $f \overset{\text{EA}}{\sim} g$. If in (1), we have $\ell = 0$, then f and g are called *affine equivalent* ($f \overset{\text{aff}}{\sim} g$) and if additionally $d = 0$, they are called *linearly equivalent*.

The Walsh transform of f is defined as $W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + x \cdot u}$ with $u \in \mathbb{F}_2^n$, where "$\cdot$" is some inner product in $\mathbb{F}_2^n$. It equals the Fourier transform of the so-called *sign function* $(-1)^{f(x)}$ where the Fourier transform of a function $\varphi : \mathbb{F}_2^n \to \mathbb{Z}$ equals $\widehat{\varphi}(u) = \sum_{x \in \mathbb{F}_2^n} \varphi(x)(-1)^{x \cdot u}$. We shall use the so-called inverse Walsh transform formula:

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

We denote by $\mathcal{F}(f)$ the value at 0 of the Walsh transform: $\mathcal{F}(f) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)}$. A function f is therefore balanced if and only if $\mathcal{F}(f) = 0$.

Note that $\mathbb{F}_2^n$ can be endowed with the structure of the field $\mathbb{F}_{2^n}$ and an inner product is then $x \cdot y = tr(xy)$, where tr is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$: $tr(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$ (see more in [7]).

The mentioned notions can be extended to the case of vectorial Boolean functions. Indeed, an (n, m)-function F can be seen as the concatenation of m Boolean functions (in n variables) $f_1, \ldots, f_m$, called the coordinate functions of F, and having the same input: $F(x) = (f_1(x), \ldots, f_m(x))$. The algebraic degree of F is then the maximal algebraic degree of its coordinate functions and the Walsh transform is defined as $W_F(u,v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + x \cdot u}$ with $u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m$.

This work is mainly devoted to the study of bent Boolean functions. In the following, we report the definition and some important properties related to these functions. An n-variable Boolean function f is called bent if and only if one of the following equivalent conditions holds ([7]):

1. for any nonzero $a \in \mathbb{F}_2^n$, the derivative $D_a f(x) = f(x+a) + f(x)$ is balanced;

2. f lies at maximal Hamming distance $2^{n-1} - 2^{\frac{n}{2}-1}$ from affine Boolean functions;

3. the Walsh transform W_f takes all its values in $\{-2^{\frac{n}{2}}, 2^{\frac{n}{2}}\}$.

Clearly, bent functions exist only for even values of n and they cannot be balanced. Moreover, a bent Boolean function in $n > 2$ variables has algebraic degree at most $\frac{n}{2}$, see [15]. All quadratic bent functions are known: they are the Boolean functions that are EA-equivalent to the function $x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$. Algebraic degree 2 is the only one for which such classification is known. In particular, the structure of cubic bent functions is widely unknown. Given a bent Boolean function f, its dual function, denoted by $\tilde{f}$, is the Boolean function that satisfies, for $u \in \mathbb{F}_2^n$, $2^{n/2}(-1)^{\tilde{f}(u)} = W_f(u)$. The function $\tilde{f}$ is also bent and its dual is f itself [12, 15]. The mapping $f \mapsto \tilde{f}$ preserves the Hamming distance between bent functions (see [7]). Using the dual for studying some kinds of bent functions is often very efficient, but not always as we shall see.

3 Definition and first observations on cubic-like bentness

For a cubic bent Boolean function, every (nonzero) derivative is a balanced quadratic function, and we know that any balanced quadratic function has at least one derivative equal to the constant function 1 (see *e.g.* [7]). Therefore we introduce the following definition.

Definition 1. *A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is* cubic-like bent *if, for every nonzero $a \in \mathbb{F}_2^n$, there exists $b \in \mathbb{F}_2^n$ such that the second-order derivative:*

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

equals the constant function 1. In this case, we write $D_a D_b f = 1$.

Proposition 1. *If f is a cubic bent function then f is cubic-like bent. On the other side, if f is cubic-like bent, then it is bent.*

Proof. The first implication is proved above. The second one comes from the fact that, for every nonzero $a \in \mathbb{F}_2^n$, the derivative $D_a f$ is balanced, hence the function is bent. $\square$

Remark 1. *The non-zero vector b in Definition 1 belongs to the linear kernel of $D_a f$. More precisely, it belongs to the complement of the 0-linear kernel of $D_a f$ in the linear kernel of $D_a f$; and the condition of Definition 1 is equivalent to saying that, for every nonzero a, the linear kernel of $D_a f$ and its 0-linear kernel are different.*
Proposition 1 implies that if f is cubic-like bent, then its number of variables is even.

3.1 Invariance of the notion with respect to EA equivalence and related properties

Proposition 2. *The* cubic-like bentness *property is EA-invariant.*

Proof. Assume f and g are two EA-equivalent n-variable Boolean functions, hence $g(x) = f(L(x) + d) + \ell(x)$ as in (1). For $a, b \in \mathbb{F}_2^n$ we have

$$\begin{aligned} D_a D_b g(x) = & g(x + a + b) + g(x + a) + g(x + b) + g(x) \\ = & f(L(x + a + b) + d) + f(L(x + a) + d) + f(L(x + b) + d) + f(L(x) + d) \\ = & D_{L(a)} D_{L(b)} f(L(x) + d). \end{aligned}$$

Since L is an automorphism, the invariance is proved. $\square$

Remark 2. *Recall that a Boolean function is bent if and only if, for every $x \in \mathbb{F}_2^n$, we have $\sum_{a,b\in\mathbb{F}_2^n} (-1)^{D_a D_b f(x)} = 2^n$ (see [11]), that is,*

$$\sum_{a,b\in\mathbb{F}_2^n, a\neq 0} (-1)^{D_a D_b f(x)} = 0.$$

Let us see how this property is satisfied by cubic-like bent functions. For every $a \neq 0$, let b_a be such that $D_a D_{b_a} f = 1$, we have then that $D_a D_{b+b_a} f(x) = D_a D_b f(x) + 1$, for every $b \in \mathbb{F}_2^n$, and then $(-1)^{D_a D_b f(x)} + (-1)^{D_a D_{b+b_a} f(x)} = 0$, which makes that in the sum $\sum_{b\in\mathbb{F}_2^n} (-1)^{D_a D_b f(x)}$, the values cancel each others by pairs of a specific type. This implies that if g_a is a Boolean function such that $D_a D_{b_a} g_a$ equals the zero function, we have $\sum_{b\in\mathbb{F}_2^n} (-1)^{D_a D_b (f+g_a)(x)} = 0$.
For general bent Boolean functions f, we have, denoting $y = x+b$, that the sum $\sum_{b\in\mathbb{F}_2^n} (-1)^{D_a D_b f(x)}$ equals $\sum_{y\in\mathbb{F}_2^n} (-1)^{D_a f(x)+D_a f(y)} = (-1)^{D_a f(x)} \mathcal{F}(D_a f) = 0$, which makes that the sum $\sum_{b\in\mathbb{F}_2^n} (-1)^{D_a D_b f(x)}$ equals zero. It then also vanishes for each value $a \neq 0$, but in a less specific way, and the property above does not work anymore, in general.

From the above remark, we have the following sufficient (but not necessary) condition:

Proposition 3. *Consider $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$. If f is cubic-like bent and g is a quadratic function such that, for every $a \neq 0$, the linear kernel of $D_a g$ includes that of $D_a f$ as a vector subspace and g is unbalanced, then $f + g$ is bent (and is more precisely cubic-like bent).*

Indeed, according to [7, Proposition 55], since $D_a g$ is unbalanced, we have that $D_a D_b g = 0$ for every b in the linear kernel of $D_a f$.
This leads to the following open question.

Question 1. *Given a cubic-like bent function f, do there exist non-affine quadratic functions g whose derivatives are unbalanced and have linear kernels including those of the derivatives of f in the same directions?*

Let us now show that cubic-like bent functions have a particular shape.

Proposition 4. *If f is a cubic-like bent function, then*

$$f(x_1, \ldots, x_n) \overset{\text{EA}}{\sim} x_1 x_2 + x_3 x_4 + h(x_1, \ldots, x_n),$$

with h such that none of its terms is a multiple of $x_1 x_2$ or $x_3 x_4$.

Proof. Consider $a = e_1$. Up to an EA-transformation, we can assume that for $b = e_2$ we have $D_a D_b f(x) = 1$. Hence we can write f as

$$f(x) = x_1 x_2 + x_1 g_1(\overline{x}^{\{1,2\}}) + x_2 g_2(\overline{x}^{\{1,2\}}) + g_3(\overline{x}^{\{1,2\}}),$$

where $\overline{x}^I$ denotes x deprived of its coordinates of indices $i \in I$. We can also assume that (the ANF of) g_1 and g_2 do not contain any constant or linear term (if x_1 is a term of f, then by applying the affine permutation $x_2 \to x_2 + 1$ the term disappears, similarly for the term x_2; notice that the other terms of g_1 and g_2 are not modified; and if $x_1 x_j$ is a term of f, then by applying the affine permutation $x_2 \to x_2 + x_j$ the term disappears, similarly for the term $x_2 x_j$; here again, the other terms of g_1 and g_2 are not modified).
Consider now $a = e_3$. We have $D_{e_3} f(x) = x_1 h_1(\overline{x}^{\{1,2,3\}}) + x_2 h_2(\overline{x}^{\{1,2,3\}}) + h_3(\overline{x}^{\{1,2,3\}})$, where h_1 and h_2 do not contain the constant term 1. Set $B = \{b \in \mathbb{F}_2^n;\ D_{e_3} D_b f = 1\}$. We show now that there exists at least an element $b \in B$ such that $b \neq e_1, e_2, e_1 + e_2$. By contradiction, assume that $B \subseteq \{e_1, e_2, e_1 + e_2\}$. Since $h_1, h_2 \neq 1$, we have that $e_1, e_2 \notin B$. If $e_1 + e_2 \in B$ then $h_1 + h_2 = 1$. This is not possible since both h_1 and h_2 do not contain the constant term 1. Therefore, there exists $b \notin \{e_1, e_2, e_1 + e_2\}$ such that $D_{e_3} D_b f = 1$, and up to an affine transformation[1], we can assume that $b = e_4$ and then $D_{e_3} D_{e_4} f = 1$ and so $f(x) = x_1 x_2 + x_3 x_4 + h(x_1, \ldots, x_n)$ as stated. □

We also obtain the following result, dealing with a secondary construction of bent functions called the direct sum. Since the notion of cubic-like bentness is EA-invariant, the result deals with what Dillon [12] called decomposable bent functions.

[1]Consider indeed an element $b = (b_1, \ldots, b_n) \in B$ (that is $D_{e_3} D_b f(x) = 1$). We have that b_i is not zero for some $i > 3$. Without loss of generality, assume $b_4 = 1$. Set T be a linear permutation such that $T(x_1) = x_1$, $T(x_2) = x_2$, $T(x_3) = x_3$ and $T(x_4) = \sum b_i x_i$. Then for $g = f \circ T$ we have $D_{e_1} D_{e_2} g = D_{e_3} D_{e_4} g = 1$. So $g(x) = x_1 x_2 + x_3 x_4 + h(x_1, \ldots, x_n)$ as stated.

Proposition 5. *Consider* $f : \mathbb{F}_2^{n+m} \to \mathbb{F}_2$ *such that*

$$f(x,y) \overset{\mathrm{EA}}{\sim} g(x) + h(y),$$

for $n, m > 1$*,* g *and* h *Boolean functions in* n *and* m *variables respectively. Then* f *is cubic-like bent if and only if* g *and* h *are cubic-like bent.*

Proof. Since the cubic-like bentness property is EA-invariant, we can assume without loss of generality that $f(x,y) = g(x) + h(y)$. To simplify the notation, we write an element $a \in \mathbb{F}_2^{n+m}$ as $a = (a_1, a_2)$ with $a_1 \in \mathbb{F}_2^n$ and $a_2 \in \mathbb{F}_2^m$. From the facts that for $a = (a_1, 0)$ we have $D_a f = D_{a_1} g$ and for $a = (0, a_2)$ we have $D_a f = D_{a_2} h$, we can easily deduce that if f is cubic-like bent, then also g and h are cubic-like bent. For the other implication, assume that g and h are cubic-like bent and take any nonzero $a = (a_1, a_2) \in \mathbb{F}_2^n$. If $a_1 = 0$ $(a_2 \neq 0)$, consider $b_2 \in \mathbb{F}_2^m$ such that $D_{a_2} D_{b_2} h = 1$ and set $b = (0, b_2)$. Then $D_a D_b f = 1$. If $a_1 \neq 0$, consider $b_1 \in \mathbb{F}_2^n$ such that $D_{a_1} D_{b_1} g = 1$ and set $b = (b_1, 0)$. Then we have that $D_a D_b f = 1$. From this we deduce the cubic-like bentness of f and we conclude the proof. $\square$

4 On the structure of those second-order derivatives that are constant

For a Boolean function f and $a \in \mathbb{F}_2^n$, consider the set

$$B_a = \{b \in \mathbb{F}_2^n;\ D_a D_b f = 1\}. \tag{2}$$

B_a being the difference between the linear kernel of $D_a f$ and its 0-linear kernel, then if it is not empty, it is an affine space (and not a vector space) and its direction equals the 0-linear kernel:

$$\overrightarrow{B_a} = \{b \in \mathbb{F}_2^n;\ D_a D_b f = 0\}. \tag{3}$$

Proposition 6. *Given an* n*-variable cubic-like bent function* f*, for any* $a \in \mathbb{F}_2^n$*,* $a \neq 0$*,* B_a *is an affine space whose direction equals* $\overrightarrow{B_a}$*.*

The union $B_a \cup \overrightarrow{B_a}$ equals the linear kernel of $D_a f$. Clearly, for any $a \neq 0$, $\{0, a\} \subseteq \overrightarrow{B_a}$.

The following relations can be easily verified.

- For $a, b \in \mathbb{F}_2^n \setminus \{0\}$, $b \in B_a$ if and only if $a \in B_b$.
- For $a, b \in \mathbb{F}_2^n \setminus \{0\}$, $b \in B_a$ if and only if $b + a \in B_a$.
- For every distinct nonzero a, a', we have that $B_a \cap B_{a'} \subseteq \overrightarrow{B_{a+a'}}$ since by addition we have that $D_a D_b f = 1$ and $D_{a'} D_b f = 1$ imply that $D_{a+a'} D_b f = 0$. Similarly, we have $\overrightarrow{B_a} \cap \overrightarrow{B_{a'}} \subseteq \overrightarrow{B_{a+a'}}$ and $B_a \cap \overrightarrow{B_{a'}} \subseteq B_{a+a'}$. Hence, we obtain that $B_a \cap B_{a'} = B_a \cap \overrightarrow{B_{a+a'}} = B_{a'} \cap \overrightarrow{B_{a+a'}}$, $\overrightarrow{B_a} \cap \overrightarrow{B_{a'}} \subseteq \overrightarrow{B_{a+a'}}$ and $B_a \cap \overrightarrow{B_{a'}} \subseteq B_{a+a'}$.

- Let us denote $A_{a,0} = \overrightarrow{B_a}$ and $A_{a,1} = B_a$, then we have that $A_{a,0}$ is a vector space for every $a \neq 0$, $A_{a,1}$ is a (distinct) coset of this vector space, and for every $u, v \in \mathbb{F}_2^n \times \mathbb{F}_2$ such that $u = (a, \epsilon)$, $v = (a', \epsilon')$, $a \neq a'$, we have $A_u \cap A_v = A_u \cap A_{u+v}$. Indeed, for instance, we have the inclusions $B_a \cap B_{a'} \subseteq B_a \cap \overrightarrow{B_{a+a'}}$ and $B_a \cap \overrightarrow{B_{a+a'}} \subseteq B_a \cap B_{a'}$.

Consider now the multi-set

$$\mathcal{B} = \{* |B_a| \,:\, a \in \mathbb{F}_2^n \setminus \{0\} *\}. \tag{4}$$

The function f is cubic-like bent if and only if $0 \notin \mathcal{B}$. Moreover we have that two EA-equivalent Boolean functions have the same multi-set $\mathcal{B}$.

We consider in the following some particular cases for the space B_a.

4.1 Case where B_a is a hyperplane for some a

Consider now the case where an n-variable cubic-like bent function f admits an element $a \neq 0$ such that $dim(\overrightarrow{B_a}) = n - 1$, hence such that $|B_a| = |\overrightarrow{B_a}| = 2^{n-1}$. So, the linear kernel $B_a \cup \overrightarrow{B_a}$ of $D_a f$ equals the whole space $\mathbb{F}_2^n$. This implies that the function $D_a f(x)$ is an affine (non constant) function. Note that, if we have another element a' that has the same property, the function $D_{a+a'} f(x) = D_a f(x) + D_{a'} f(x + a)$ is also affine; so, the set of elements a such that $a = 0$ or $dim(\overrightarrow{B_a}) = n - 1$ is a vector space. Let k be the dimension of this vector space; we have

$$|\{a \in \mathbb{F}_2^n;\ dim(\overrightarrow{B_a}) = n - 1\}| = 2^k - 1.$$

Up to a linear transformation, let $e_1, \ldots, e_k$ be in such set. We have therefore that $x_1, \ldots, x_k$ appear only in quadratic terms:

$$f(x) \overset{\text{aff}}{\sim} q(x_1, \ldots, x_n) + g(x_{k+1}, \ldots, x_n), \tag{5}$$

where q is a quadratic Boolean function in n variables and g is a Boolean function in $n - k$ variables. In order for f to be of algebraic degree greater than three, we need $k \leq n - 4$. Hence the following proposition is satisfied.

Proposition 7. *Given an n-variable cubic-like bent Boolean function f with* $\deg(f) > 3$*, consider be the multiset $\mathcal{B}$ defined in* (4)*. Then the multiplicity of 2^{n-1} in $\mathcal{B}$ is at most $2^{n-4} - 1$.*

If we consider the limit case with $k = n - 4$, we have the following result.

Proposition 8. *Consider an n-variable cubic-like bent Boolean function f of degree greater than 3. Assume that the multiset $\mathcal{B}$ defined in* (4) *contains the element 2^{n-1} with multiplicity $2^{n-4} - 1$. Then*

$$f(x) \overset{\text{EA}}{\sim} x_{n-3}x_{n-2}x_{n-1}x_n + \sum_{i=1}^{m} x_i x_{n-i+1},$$

where $m = n/2 \geq 4$.

The proof of this proposition is quite long and technical. It can be found at the end of this work, see Appendix A.

Remark 3. *The function in Proposition 8 belongs to the Maiorana-McFarland class (see Section 6 for more details). Indeed, denoting* $y = (x_m, \dots, x_3, x_2, x_n)$ *and* $z = (x_{m+1}, \dots, x_{n-2}, x_{n-1}, x_1)$ *we have* $f(x) \overset{\text{EA}}{\sim} y \cdot \pi(z)$ *with*

$$\pi(z) = \begin{bmatrix} x_{m+1} \\ \vdots \\ x_{n-2} \\ x_{n-1} \\ x_{n-3}x_{n-2}x_{n-1} + x_1 \end{bmatrix}.$$

4.2 Case where B_a is a pair for some a

The other limit case is when there exists an element $a \neq 0$ such that $B_a = \{b, a+b\}$. Without loss of generality, up to linear equivalence, let us assume that $a = e_n$ and $b = e_{n-1}$. Then we have that $D_{e_n} f(x) = x_{n-1} + g(x_1, \dots, x_{n-2})$, that is:

$$f(x) = x_n x_{n-1} + x_n \; g(x_1, \dots, x_{n-2}) + R(x_1, \dots, x_{n-1}).$$

Moreover we have that $D_u g(x)$ is never constant, for any $u \neq 0, e_n, e_{n-1}, e_n + e_{n-1}$ (since if $D_u g(x)$ is the constant 1, then $u \in B_a$, and if $D_u g(x)$ is the constant 0, then $u + b \in B_a$ and this contradicts the fact that $B_a = \{b, b+a\}$, where $a = e_n$ and $b = e_{n-1}$).

Computationally we looked unsuccessfully for such functions in dimension 8 when f is a Maiorana-McFarland map of degree greater than 3. Examples of such functions were found among cubic bent maps.

5 Characterization by the Walsh transform

5.1 Characterization by the Walsh transform of the function and related condition on the dual function

We have $D_a D_b f(x) = 1$ if and only if $\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+a)+f(x+b)+f(x+a+b)} = -2^n$, that is, according to the inverse Walsh transform formula:

$$\sum_{x,u,v,w,t \in \mathbb{F}_2^n} W_f(u) W_f(v) W_f(w) W_f(t) (-1)^{u \cdot x + v \cdot (x+a) + w \cdot (x+b) + t \cdot (x+a+b)} = -2^{5n}.$$

Since $\sum_{x \in \mathbb{F}_2^n} (-1)^{(u+v+w+t) \cdot x}$ equals 0 if $u + v + w + t \neq 0$, the above equation corresponds to

$$\sum_{u,v,w \in \mathbb{F}_2^n} W_f(u) W_f(v) W_f(w) W_f(u+v+w) (-1)^{v \cdot a + w \cdot b + (u+v+w) \cdot (a+b)} = -2^{4n},$$

that is

$$\sum_{u,v,w\in\mathbb{F}_2^n} W_f(u)W_f(u+v)W_f(u+w)W_f(u+v+w)(-1)^{v\cdot b+w\cdot a} = -2^{4n}.$$

By applying the definition of dual of a bent function, we obtain the following result.

Proposition 9. *An n-variable bent function f is cubic-like bent if and only if, for every nonzero $a \in \mathbb{F}_2^n$, there exists $b \in \mathbb{F}_2^n$ such that:*

$$\sum_{u,v,w\in\mathbb{F}_2^n} (-1)^{D_v D_w \widetilde{f}(u)+v\cdot b+w\cdot a} = -2^{2n}. \tag{6}$$

Remark 4. *We observe then that the cubic-like bentness of a function is not equivalent to the cubic-like bentness of its dual (and then we have a second interesting subclass of bent functions, made of the duals of cubic-like bent functions). A simple example of a cubic-like bent function whose dual is not cubic-like bent is the function $(x,y) \in \mathbb{F}_{2^m}^2 = \mathbb{F}_2^{2m} \mapsto tr(xy^3) \in \mathbb{F}_2$, where tr is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$; the dual of this cubic bent function equals the function $(x,y) \in \mathbb{F}_{2^m}^2 \mapsto tr(xy^{-3}) = tr(xy^{2^m-4}) \in \mathbb{F}_{2^m}$ (see e.g. [7, Proposition 77]) and is not cubic-like bent, in general, since it does not satisfy the condition that we shall give in Proposition 14 (this can be checked for instance for $m = 5$).*

Open problem: determine all those cubic-like bent functions (resp. all those cubic bent functions) whose duals are cubic-like bent (resp. are cubic bent). Note that all quadratic bent functions have quadratic duals and belong then to these two classes.

According to (6), the cubic-like bentness condition is equivalent to the existence of an (n,n)-function ϕ such that $\phi(0) = 0$ and satisfying:

$$\sum_{a,u,v,w\in\mathbb{F}_2^n} (-1)^{D_v D_w \widetilde{f}(u)+v\cdot\phi(a)+w\cdot a} = -2^{2n}(2^n-2). \tag{7}$$

Therefore, we have the following.

Corollary 1. *An n-variable Boolean function is cubic-like bent if and only if there exists an (n,n)-function ϕ with $\phi(0) = 0$, satisfying:*

$$\sum_{v,w\in\mathbb{F}_2^n} \mathcal{F}(D_v D_w \widetilde{f})\, W_\phi(w,v) = -2^{2n}(2^n-2). \tag{8}$$

Of course, the cubic-like bentness condition is also equivalent to the existence of an (n,n)-function ϕ such that $\phi(0) = 0$, satisfying:

$$\sum_{a\in\mathbb{F}_2^n} \mathcal{F}(D_a D_{\phi(a)} f) = -2^n(2^n-2). \tag{9}$$

Remark 5. *For f and g affine equivalent cubic-like bent Boolean functions, their respective functions ϕ (ϕ_f and ϕ_g) can be taken linear equivalent. Indeed, if $f = g \circ A$, for $A(x) = L(x) + \epsilon$ an affine permutation of $\mathbb{F}_{2^n}$ (L linear), then $D_a D_{\phi_f(a)} f(x) = D_{L(a)} D_{L(\phi_f(a))} g(A(x))$ and ϕ_g can be taken equal to $L \circ \phi_f \circ L^{-1}$.*

Remark 6. *A natural particular case to be investigated is when ϕ is linear, since $W_\phi(w, v)$ equals then zero when $w \neq \phi^*(v)$. Relation (8) is then equivalent to:*

$$\sum_{v \in \mathbb{F}_2^n \setminus \{0\}} \mathcal{F}(D_v D_{\phi^*(v)} \widetilde{f}) = -2^n(2^n - 1),$$

that is, $\widetilde{f}$ would be also cubic-like bent. Unfortunately, ϕ linear is impossible: if $D_a D_{\phi(a)} f$ equals constant function 1 for every $a \neq 0$, then, for every x, the function $a \mapsto D_a D_{\phi(a)} f(x)$ equals the function $\delta_0(a) + 1$, where δ_0 is the Dirac or Kronecker symbol (i.e. the characteristic function of $\{0\}$) and the algebraic degree of the function $a \to D_a D_{\phi(a)} f(x) = f(x) + f(x+a) + f(x+\phi(a)) + f(x+a+\phi(a))$ equals then n, which is impossible for a function f of degree less than n. In fact, the algebraic degree of $f(x)+f(x+a)+f(x+\phi(a))+f(x+a+\phi(a))$ being bounded above by $\deg(f)\deg(\phi)$, and since we know from [15] that $\deg(f) \leq n/2$, we have $\deg(\phi) \geq 2$ and it is not clear whether ϕ can have algebraic degree 2.

5.2 Characterization by the Walsh transform of derivatives

Let us show that the characterization of Proposition 9 can be simplified. For every $v \in \mathbb{F}_2^n$, we have:

$$\begin{aligned} \sum_{u,w \in \mathbb{F}_2^n} (-1)^{D_v D_w \widetilde{f}(u) + v\cdot b + w\cdot a} &= \sum_{u,w \in \mathbb{F}_2^n} (-1)^{D_v \widetilde{f}(u) + D_v \widetilde{f}(u+w) + v\cdot b + w\cdot a} \\ &= \sum_{u,w \in \mathbb{F}_2^n} (-1)^{D_v \widetilde{f}(u) + D_v \widetilde{f}(w) + v\cdot b + (u+w)\cdot a} \\ &= (-1)^{v\cdot b} W^2_{D_v \widetilde{f}}(a). \end{aligned}$$

Hence, condition (6) writes :

$$\sum_{v \in \mathbb{F}_2^n} (-1)^{v\cdot b} W^2_{D_v \widetilde{f}}(a) = -2^{2n}. \tag{10}$$

Similarly, for every $w \in \mathbb{F}_2^n$, we have:

$$\sum_{u,v \in \mathbb{F}_2^n} (-1)^{D_v D_w \widetilde{f}(u) + v\cdot b + w\cdot a} = (-1)^{w\cdot a} W^2_{D_w \widetilde{f}}(b).$$

And condition (6) writes then:

$$\sum_{w \in \mathbb{F}_2^n} (-1)^{w\cdot a} W^2_{D_w \widetilde{f}}(b) = -2^{2n}. \tag{11}$$

Note that if $a = 0$ or $b = 0$ then $\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+f(x+a)+f(x+b)+f(x+a+b)} = 2^n$ and we have then, according to the same calculations: $\sum_{v\in\mathbb{F}_2^n}(-1)^{v\cdot b}W^2_{D_v\widetilde{f}}(a) = 2^{2n}$ and $\sum_{w\in\mathbb{F}_2^n}(-1)^{w\cdot a}W^2_{D_w\widetilde{f}}(b) = 2^{2n}$. Relations (10) and (11) are then equivalent with:

$$\sum_{v\in\mathbb{F}_2^n;v\cdot b=0} W^2_{D_v\widetilde{f}}(a) = 0, \tag{12}$$

and

$$\sum_{w\in\mathbb{F}_2^n;w\cdot a=0} W^2_{D_w\widetilde{f}}(b) = 0, \tag{13}$$

that is, $W_{D_v\widetilde{f}}(a) = 0$ for every $v \in \mathbb{F}_2^n$ such that $v \cdot b = 0$; and $W_{D_w\widetilde{f}}(b) = 0$ for every $w \in \mathbb{F}_2^n$ such that $w \cdot a = 0$.

In fact, Relations (12) and (13) can be directly shown without using Relation (6), and they provide necessary and sufficient conditions for f to be cubic-like bent: a Boolean function g is such that $D_bg = 1$ if and only if, for every $x \in \mathbb{F}_2^n$ we have $(-1)^{g(x+b)} = -(-1)^{g(x)}$, that is, by applying the Fourier transform (which is a bijective transformation), if $(-1)^{b\cdot u}W_g(u) = -W_g(u)$ for every $u \in \mathbb{F}_2^n$, that is, $W_g(u) = 0$ for every u such that $b \cdot u = 0$. Hence, given a Boolean function f, we have $D_aD_bf = 1$ if and only if $W_{D_af}(u) = 0$ for every u such that $b \cdot u = 0$. We have $W_{D_af}(u) = W_{D_u\widetilde{f}}(a)$ as proved in [5] (see also [7, Relation (6.4)]), and as can be easily checked. The condition for $D_aD_bf = 1$ is then that $W_{D_u\widetilde{f}}(a) = 0$ for every u such that $b \cdot u = 0$. It is equivalent to saying that the function $D_u\widetilde{f}(x) + a \cdot x$ is balanced for every u orthogonal to b. The same for the map $D_af(x) + u \cdot x$.

Proposition 10. *Given a Boolean function f, the following statements are equivalent:*

1. *f is cubic-like bent (for any $a \neq 0$ there exists b such that $D_aD_bf = 1$);*

2. *for any $a \neq 0$, there exists b such that $W_{D_af}(u) = 0$ (that is, $D_af(x)+u\cdot x$ is balanced) for every u orthogonal to b; in other words, the Walsh support of D_af is included in the complement of a linear hyperplane of $\mathbb{F}_2^n$;*

3. *for any $a \neq 0$, there exists b such that $W_{D_u\widetilde{f}}(a) = 0$ (that is, $D_u\widetilde{f}(x)+a\cdot x$ is balanced) for every u orthogonal to b; in other words, for every such u, the Walsh support of $D_u\widetilde{f}$ does not contain a.*

We see now better the difference between "f is cubic-like bent" and "$\widetilde{f}$ is cubic-like bent". In the former case, there exists a function ϕ such that, for every nonzero a, $W_{D_af}(u) = 0$ for every u orthogonal to $\phi(a)$, while in the latter case there exists a function ϕ such that, for every nonzero a, $W_{D_uf}(a) = 0$ for every u orthogonal to $\phi(a)$.

Remark 7. *It is also proved in [7] that $W_{D_af}(u) = 0$, that is, $D_af(x) + u \cdot x$ is balanced, for every u such that $a \cdot u = 1$. Hence, if f is cubic-like bent, the*

Walsh support of W_{D_af} is in fact included in the intersection of the complement of a linear hyperplane of $\mathbb{F}_2^n$ and the linear hyperplane of equation $a\cdot u = 0$; this intersection is an affine space of co-dimension 2 since it is the intersection of two affine hyperplanes with distinct directions $\{0,b\}^\perp$ and $\{0,a\}^\perp$ (indeed, b cannot equal a, since $D_aD_af = 0$).

Remark 8. *According to Proposition 10, a Boolean bent function f and its dual are both cubic-like bent if and only if, for every $a \neq 0$, there exist a linear hyperplane H_a and a linear hyperplane H'_a such that $W_{D_af}(u) = W_{D_{u'}f}(a) = 0$, for every $u \in H_a$ and every $u' \in H'_a$ (and also for every u, u' non-othogonal to a). Note that since $H_a \cap H'_a$ has dimension at least $n-2$, there is a vector space E_a of dimension at least $n-2$ such that $W_{D_af}(u) = W_{D_uf}(a) = 0$, for every $u \in E_a$.*

Remark 9. *Proposition 10 can be turned into a characterization by the Walsh transform of f itself. Indeed, $(-1)^{D_u\tilde{f}(x)+a\cdot x} = 2^{-n}W_f(x)W_f(x+u)(-1)^{a\cdot x}$ (by the definition of $\tilde{f}$).*
Note that we also have:

$$\begin{aligned}
W_{D_af}(u) =& \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+f(x+a)+u\cdot x}\\
=&2^{-2n} \sum_{x,v,w\in\mathbb{F}_2^n} W_f(v)W_f(w)(-1)^{(u+v+w)\cdot x+w\cdot a}\\
=&2^{-n} \sum_{v\in\mathbb{F}_2^n} W_f(v)W_f(u+v)(-1)^{(u+v)\cdot a}\\
=& \sum_{v\in\mathbb{F}_2^n} (-1)^{D_u\widetilde{f}(v)+(u+v)\cdot a}.
\end{aligned}$$

5.3 Characterization by the convolutional product of the Walsh transforms of the function and its derivatives

Instead of applying the Fourier transform to the equality $(-1)^{f(x)+f(x+a)} = -(-1)^{f(x+b)+f(x+a+b)}$ as above, we can apply it to the equality $(-1)^{f(x)} = -(-1)^{f(x+a+b)+f(x+a)+f(x+b)}$; we obtain that f is cubic-like bent if and only if, for every $a \neq 0$, there exists b such that:

$$\begin{aligned}
W_f(u) &= -\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x+a+b)+f(x+a)+f(x+b)+x\cdot u}\\
&= -\,2^{-3n}\sum_{x\in\mathbb{F}_2^n}\sum_{v,w,z\in\mathbb{F}_2^n} W_f(v)W_f(w)W_f(z)(-1)^{(v+w+z+u)\cdot x+w\cdot(a+b)+v\cdot a+z\cdot b}\\
&= -\,2^{-2n}\sum_{v,w\in\mathbb{F}_2^n} W_f(v)W_f(w)W_f(v+w+u)(-1)^{w\cdot a+v\cdot(a+b)+u\cdot b}\\
&= -\,2^{-n}\sum_{v\in\mathbb{F}_2^n} W_f(v)W_{D_af}(v+u)(-1)^{(v+u)\cdot b+u\cdot a}\\
&= -\,2^{-n}(-1)^{a\cdot u}\sum_{v\in\mathbb{F}_2^n} W_{D_af}(v)W_f(u+v)(-1)^{b\cdot v}.
\end{aligned}$$

The two last equalities come from the second part of Remark 9. We have therefore the following result.

Proposition 11. *An n-variable Boolean function f is cubic-like bent if and only if, for every nonzero $a \in \mathbb{F}_2^n$, there exists $b \in \mathbb{F}_2^n$ such that for any $u \in \mathbb{F}_2^n$:*

$$W_f(u) = -2^{-n}(-1)^{a\cdot u}\sum_{v\in\mathbb{F}_2^n} W_{D_af}(v)W_f(u+v)(-1)^{b\cdot v}. \tag{14}$$

Remark 10. *Proposition 10 tells us that, for a cubic-like bent Boolean function f, we have $W_{D_af}(v) = 0$ whenever $v \cdot b = 0$. For such a function, Equation (14) also writes $W_f(u) = 2^{-n}(-1)^{a\cdot u}\sum_{v\in\mathbb{F}_2^n} W_{D_af}(v)W_f(u+v)$. But this latter equality is no more characteristic of cubic-like bent functions; actually, it is true for any Boolean function f, which is easily verified by taking $b = 0$ in the series of equalities above (with the sign "$-$" erased in front of them).*

Corollary 2. *A Boolean function f defined over $\mathbb{F}_2^n$ is cubic-like bent if and only if for every nonzero $a \in \mathbb{F}_2^n$ there is $b \in \mathbb{F}_2^n$ such that*

$$\sum_{v\in\mathbb{F}_2^n:v\cdot b=0} W_{D_af}(v)W_f(u+v) = 0, \text{ for any } u \in \mathbb{F}_2^n.$$

Proof. Since $W_f(u) = 2^{-n}(-1)^{a\cdot u}\sum_{v\in\mathbb{F}_2^n} W_{D_af}(v)W_f(u+v)$ is satisfied for a generic Boolean function, we obtain that the conditions in this corollary and Proposition 11 are equivalent. $\square$

6 On Maiorana-McFarland cubic-like bent functions

We have studied in Proposition 5 the secondary construction of cubic-like bent functions called direct sum. It does not provide yet new cubic-like bent functions

(that is, concretely, some that are non-cubic) since the direct sum of cubic functions is cubic. For providing new cubic-like bent functions, we need to revisit the classical primary constructions of bent functions. In this section, we study the simplest one, the Maiorana-McFarland construction (introduced in [13] and reported in [12]; see also [7, 10, 14]), which is known to provide a large number of bent functions and needs then to be considered. We shall see that it provides cubic-like bent functions that are non-cubic.
The principle of the construction is simple, but studying it in the framework of cubic-like bentness is a little technical. We shall then begin with a simpler subcase, which shall play in fact a specific role as we will see later.

6.1 Functions of the form $x \cdot \pi(y)$

We consider first the Maiorana-McFarland bent functions over $\mathbb{F}_2^{2m}$ of the form

$$f(x, y) = x \cdot \pi(y), \tag{15}$$

with $x, y \in \mathbb{F}_2^m$ and π a permutation of $\mathbb{F}_2^m$. We are interested in those π of algebraic degree larger than 2, for getting non-cubic functions f.
We know that (as for general Maiorana-McFarland functions that we shall study below) π being a permutation is a necessary and sufficient condition for $x \cdot \pi(y)$ to be bent, and the dual function of $x \cdot \pi(y)$ is $(x, y) \mapsto y \cdot \pi^{-1}(x)$, where π^{-1} is the compositional inverse of π.
Given a generic element $c \in \mathbb{F}_2^{2m}$, we use here and in the following the notation $c = (c_1, c_2)$ for $c_1, c_2 \in \mathbb{F}_2^m$. In this case we have, for $a = (a_1, a_2)$ and $b = (b_1, b_2)$,

$$\begin{aligned} D_a D_b f(x, y) =& (x + b_1 + a_1) \cdot \pi(y + b_2 + a_2) + (x + b_1) \cdot \pi(y + b_2) \\ &+ (x + a_1) \cdot \pi(y + a_2) + x \cdot \pi(y) \\ =& x \cdot [\pi(y + b_2 + a_2) + \pi(y + b_2) + \pi(y + a_2) + \pi(y)] \\ &+ a_1 \cdot [\pi(y + b_2 + a_2) + \pi(y + a_2)] + b_1 \cdot [\pi(y + b_2 + a_2) + \pi(y + b_2)] \\ =& x \cdot D_{a_2} D_{b_2} \pi(y) + a_1 \cdot D_{b_2} \pi(y + a_2) + b_1 \cdot D_{a_2} \pi(y + b_2). \end{aligned} \tag{16}$$

Therefore we deduce the following.

Lemma 1. *For m a positive integer, let π be a permutation of $\mathbb{F}_2^m$. A Maiorana-McFarland function of the form $x \cdot \pi(y)$ defined over $\mathbb{F}_2^{2m}$, with $x, y \in \mathbb{F}_2^m$, is cubic-like bent if and only if, for any nonzero $a = (a_1, a_2) \in \mathbb{F}_2^{2m}$, there exists an element $b = (b_1, b_2) \in \mathbb{F}_2^{2m}$ such that*

$$D_{a_2} D_{b_2} \pi(y) = 0 \text{ and } a_1 \cdot D_{b_2} \pi(y) + b_1 \cdot D_{a_2} \pi(y) = 1. \tag{17}$$

In fact, the condition simplifies:

Proposition 12. *Let π be a permutation of $\mathbb{F}_2^m$. The map $x \cdot \pi(y)$ described in Lemma 1 is cubic-like bent if and only if*

(i) for any nonzero $a_1 \in \mathbb{F}_2^m$, there exists $b_2 \in \mathbb{F}_2^m$ such that $a_1 \cdot D_{b_2} \pi(y) = 1$,

(ii) for any nonzero $a_2 \in \mathbb{F}_2^m$, there exists $b_1 \in \mathbb{F}_2^m$ such that $b_1 \cdot D_{a_2}\pi(y) = 1$.

This can be summarised in one condition:

(i) for any nonzero $\alpha \in \mathbb{F}_2^m$ there exist $\beta, \gamma \in \mathbb{F}_2^m$ such that $\beta \cdot D_\alpha \pi(y) = \alpha \cdot D_\gamma \pi(y) = 1$.*

Proof. Assume first that function $x \cdot \pi(y)$ satisfies (i) and (ii), and consider a generic nonzero element $a = (a_1, a_2) \in \mathbb{F}_2^{2m}$.
If $a_2 \neq 0$ then set $b = (b_1, 0)$ with b_1 such that $b_1 \cdot D_{a_2}\pi(y) = 1$; since $b_2 = 0$, Relation (17) is satisfied by b.
If $a_2 = 0$, set (for instance) $b = (0, b_2)$ with b_2 such that $a_1 \cdot D_{b_2}\pi(y) = 1$ (clearly a_1 is not zero); since $a_2 = 0$, Relation (17) is satisfied by b.
So we have that the function is cubic-like bent since it satisfies Lemma 1.
Assume now that the map is cubic-like bent. By considering Lemma 1 for nonzero elements of the form $(a_1, 0)$ and $(0, a_2)$, the property is verified. □

We observe the following.

Remark 11. *1. Condition (i) of Proposition 12 writes "for every $a_1 \neq 0$ there exists b_2 such that the function $D_{b_2}\pi$ takes all its values in the hyperplane of equation $a_1 \cdot y = 1$".*
2. If a function π satisfies Condition (ii) of Proposition 12, then it is a permutation since, for any nonzero a_2, $D_{a_2}\pi(y)$ cannot then vanish at any point.
3. According to Proposition 12, the first condition in (17) does not play a real role in the cubic-like bentness property of $x \cdot \pi(y)$ (because of the peculiarity of such function). However, as we will see in the next sections, permutations π such that this condition is satisfied for more than two elements (namely 0 and a_2) are good candidates for constructing cubic-like bent maps.

Remark 12. *Clearly, for any $a_1 \neq 0$, the set B_a (equal to $\{b \in \mathbb{F}_2^n;\ D_a D_b f = 1\}$) for $a = (a_1, 0)$ contains all the elements of the form (r, b_2) with any r over $\mathbb{F}_2^m$ and b_2 satisfying (i) in Proposition 12.*

6.1.1 Examples in dimension $n = 8$

Using the Magma Algebra package [2], we performed some experimental results (Section 7). We want to mention here some examples we found.

Computationally for $m = 4$ we found cases of functions $f(x, y) = x \cdot \pi(y)$ that are cubic-like bent and also of bent functions that are not cubic-like bent. For example for

$$\pi(y) = \begin{bmatrix} y_1 \\ y_2 \\ y_1 y_3 + y_4 \\ y_1 y_2 y_3 + y_2 y_4 + y_3 \end{bmatrix}$$

the map f is not cubic-like bent and $\mathcal{B} = \{*0^{32}, 4^{128}, 8^{84}, 32^8, 128^3*\}$.

Instead for

$$\pi(y) = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_1y_2y_3 + y_4 \end{bmatrix}, \begin{bmatrix} y_1y_2 + y_3 \\ y_1y_2 + y_1y_3 + y_2 \\ y_1y_2 + y_2y_3 + y_1 + y_2 \\ y_1y_2y_3 + y_4 \end{bmatrix}$$

both f's are cubic-like bent. In the first case we have $\mathcal{B} = \{*16^{240}, 128^{15}*\}$. In the second instead $\mathcal{B} = \{*4^{224}, 16^{16}, 32^{14}, 128*\}$.

6.1.2 Looking more in detail at the case where π is quadratic

Let us check how the characterization of Proposition 12 works when π is a quadratic permutation (in which case we know that $x \cdot \pi(y)$ is cubic-like bent, being cubic).
Since π is a quadratic permutation, then for every $a_2 \neq 0$, $D_{a_2}\pi$ takes all its values in an affine hyperplane which does not contain 0 (i.e., in the complement of a linear hyperplane) and Condition (ii) is straightforwardly satisfied. Condition (i) is that the linear hyperplanes outside which the derivatives $D_{b_2}\pi$ take their values can be taken distinct for distinct values of b_2. We state this property in the corollary below.
A particular case is when, for every $b_2 \neq 0$, the image set of $D_{b_2}\pi$ has size 2^{n-1} (that is, covers the whole affine hyperplane); π is then called almost perfect nonlinear (see e.g. [7]), and being a quadratic permutation, it is then a crooked function in the original meaning of this term given in [1] (note that since the introduction of this notion of crooked function, the existence of non-quadratic crooked functions is an open problem). The property that these linear hyperplanes are distinct for such crooked functions has been observed and is a direct consequence of the fact that the so-called associated function γ_π (see [8]) is a Maiorana-McFarland bent function as proved in [8], π being almost bent. It is related to the notion of ortho-derivative (term introduced in [4]).

Corollary 3. *For every nonzero integer m and every quadratic permutation π over $\mathbb{F}_2^m$, there exists a permutation $\phi : \mathbb{F}_2^m \setminus \{0\} \mapsto \mathbb{F}_2^m \setminus \{0\}$ such that, for every $b_2 \in \mathbb{F}_2^m \setminus \{0\}$, the image set of the derivative $D_{b_2}\pi$ is disjoint from the linear hyperplane $\{0, \phi(b_2)\}^\perp$.*

In fact, we shall see in the next subsection that this can be proved directly and that it extends to the so-called strongly plateaued permutations.

6.1.3 Case where π is strongly plateaued

Quadratic functions are a particular case of the so-called strongly plateaued functions [6, 7], which are those vectorial functions π whose components are partially-bent. In other words, a vectorial function π over $\mathbb{F}_2^m$ is strongly plateaued if, for every β, α in $\mathbb{F}_2^m$, the function $\beta \cdot D_\alpha\pi$ is either constant or balanced.
Strongly plateaued functions share with quadratic ones the fact that the image

set of any derivative $D_\alpha\pi$ is an affine space, as shown in [6, 7]. As we saw before, if π is a permutation, then, for $\alpha \neq 0$, this affine space does not contain 0 and Condition (ii) is then satisfied, since for every affine space A not containing 0, there exists a linear function which takes value 1 over A. Moreover, for every $\beta \neq 0$, we know that $\beta \cdot \pi$ is balanced and then we have $0 = \left(\sum_{x\in\mathbb{F}_2^m}(-1)^{\beta\cdot\pi(x)}\right)^2 = 2^m + \sum_{\alpha\neq 0}\left(\sum_{x\in\mathbb{F}_2^m}(-1)^{\beta\cdot D_\alpha\pi(x)}\right)$. Now, π being strongly plateaued, the function $\beta\cdot D_\alpha\pi$ is either zero (that is, $\sum_{x\in\mathbb{F}_2^m}(-1)^{\beta\cdot D_\alpha\pi(x)} = 2^m$) or equal to 1 (that is, $\sum_{x\in\mathbb{F}_2^m}(-1)^{\beta\cdot D_\alpha\pi(x)} = -2^m$) or balanced (that is, $\sum_{x\in\mathbb{F}_2^m}(-1)^{\beta\cdot D_\alpha\pi(x)} = 0$). There is then necessarily α such that $\beta\cdot D_\alpha\pi$ equals constant function 1. Hence Condition (i) is satisfied and we have the following result:

Proposition 13. *If π is a strongly plateaued permutation, then the Boolean function $x\cdot\pi(y)$ is cubic-like bent.*

Non-quadratic strongly plateaued (n,n)-permutations are known for every $n \geq 7$ (which provide then non-cubic functions in at least 14 variables, that are cubic-like bent), see [9].

6.1.4 Case where π is a power function

If π is a power permutation[2] $\pi(y) = y^d;\ y \in \mathbb{F}_{2^m};\ \gcd(d, 2^m-1) = 1$, then Condition (i) in Proposition 12 is satisfied for every a_1 if and only if it is satisfied for at least one nonzero a_1 (note that this is true thanks to the fact that π is a permutation; we can take for instance $a_1 = 1$), and Condition (ii) is satisfied for every a_2 if and only if it is satisfied for at least one nonzero a_2 (this is true independently of the fact that π is a permutation; we can take for instance $a_2 = 1$), and the two conditions are equivalent.

Proposition 14. *If π, viewed as a map over $\mathbb{F}_{2^m}$, is a power permutation, then the Boolean function $x\cdot\pi(y)$ is cubic-like bent if and only if there exists an element $\beta\in\mathbb{F}_{2^m}$ such that $\beta\cdot D_1\pi = 1$, that is, $tr(\beta D_1\pi(x)) = 1, \forall x$.*

This happens of course when π is quadratic, that is, up to linear equivalence, when $\pi(y) = y^{2^j+1}$, where $\frac{m}{\gcd(j,m)}$ is odd (this latter condition coming from the fact that $\gcd(2^j+1, 2^m-1) = \frac{\gcd(2^{2j}-1,2^m-1)}{\gcd(2^j-1,2^m-1)} = \frac{2^{\gcd(2j,m)}-1}{2^{\gcd(j,m)}-1}$). The question is to determine whether there are other power functions, up to equivalence, satisfying Proposition 14.

Remark 13. *In the case π is APN (that is, the image set of $D_1\pi$ has size 2^{m-1}; see more in e.g. [7]), the condition of Proposition 14 corresponds to saying that the image set of $D_1\pi$ is the complement of a linear hyperplane, as well, then, as the image set of any derivative of π. This means that π is crooked (see more in e.g. [7] as well). No non-quadratic crooked function is known. But if π is not taken APN, this leaves more freedom for finding such π.*

[2] Some authors call power functions the functions of the more general form ay^d; $a \neq 0$; we take here only $\pi(y) = y^d$ and this does not restrict the generality since, π being a permutation, function ay^d is linearly equivalent to π.

6.1.5 When π has a constant derivative

We shall see that, when π has a constant derivative, the cubic-like bentness of the function $x \cdot \pi(y)$ is equivalent to the cubic-like bentness of a Maiorana-McFarland function in less variables. Let us first recall how functions π having a constant derivative (also called a linear structure) can be simplified up to affine equivalence.

Assume that π is a permutation of $\mathbb{F}_2^m$ that admits a nonzero element α_0 for which $D_{\alpha_0}\pi(y)$ is constant, say, equals c. Recall that, since π is a permutation, c is nonzero. Up to an affine transformation, we can assume that $\alpha_0 = c = e_1$, so we have:

$$\pi(y) = \pi(y_1, \ldots, y_m) = \begin{bmatrix} y_1 + f(y_2, \ldots, y_m) \\ \bar{\pi}_1(y_2, \ldots, y_m) \\ \vdots \\ \bar{\pi}_{m-1}(y_2, \ldots, y_m) \end{bmatrix} = \begin{bmatrix} y_1 + f(y_2, \ldots, y_m) \\ \bar{\pi}(y_2, \ldots, y_m) \end{bmatrix}, \quad (18)$$

with f any Boolean function in $m-1$ variables and $\bar{\pi}$ a permutation of $\mathbb{F}_2^{m-1}$. In this case, the inverse equals:

$$\pi^{-1}(y) = \begin{bmatrix} y_1 + f \circ \bar{\pi}^{-1}(y_2, \ldots, y_m) \\ \bar{\pi}^{-1}(y_2, \ldots, y_m) \end{bmatrix}. \quad (19)$$

Proposition 15. *Assume that $\bar{\pi} = [\bar{\pi}_1, \ldots, \bar{\pi}_{m-1}]$ is a permutation of $\mathbb{F}_2^{m-1}$ and, for f any Boolean function in $m-1$ variables, consider the permutation over $\mathbb{F}_2^m$ of the form:*

$$\pi(y) = \pi(y_1, \ldots, y_m) = \begin{bmatrix} y_1 + f(y_2, \ldots, y_m) \\ \bar{\pi}_1(y_2, \ldots, y_m) \\ \vdots \\ \bar{\pi}_{m-1}(y_2, \ldots, y_m) \end{bmatrix}.$$

Then the map $x \cdot \pi(y)$ over $\mathbb{F}_2^m \times \mathbb{F}_2^m$ is cubic-like bent if and only if $\bar{x} \cdot \bar{\pi}(\bar{y})$, map over $\mathbb{F}_2^{m-1} \times \mathbb{F}_2^{m-1}$, is cubic-like bent.

Proof. Let us first assume that $\bar{x} \cdot \bar{\pi}(\bar{y})$ is cubic-like bent and prove that $x \cdot \pi(y)$ is cubic-like bent. From Proposition 12, we only need to show that for any nonzero $\alpha \in \mathbb{F}_2^m$, there are β, β' such that $\alpha \cdot D_\beta \pi(y) = \beta' \cdot D_\alpha \pi(y) = 1$.
Assume first that $\alpha = e_1$, then with $\beta = e_1$ we have $\alpha \cdot D_\beta \pi(y) = \beta \cdot D_\alpha \pi(y) = 1$. Assume now that $\alpha = (\alpha_1, \ldots, \alpha_m) \neq e_1$ and set $\bar{\alpha} = (\alpha_2, \ldots, \alpha_m)$. Clearly $\bar{\alpha}$ is nonzero. Then, since $\bar{x} \cdot \bar{\pi}(\bar{y})$ is cubic-like bent, there exist $\bar{\beta} \in \mathbb{F}_2^{m-1}$ such that $\bar{\alpha} \cdot D_{\bar{\beta}} \bar{\pi}(\bar{y}) = 1$ and $\bar{\beta}' \in \mathbb{F}_2^{m-1}$ such that $\bar{\beta}' \cdot D_{\bar{\alpha}} \bar{\pi}(\bar{y}) = 1$. Let $\beta' = (0, \bar{\beta}')$, then $\beta' \cdot D_\alpha \pi(y) = \bar{\beta}' \cdot D_{\bar{\alpha}} \bar{\pi}(y_2, \ldots, y_m) = 1$. Now for finding β such that $\alpha \cdot D_\beta \pi(y) = 1$, we need to separate into two cases. If α is such that $\alpha_1 = 1$, then with $\beta = e_1$ we have $\alpha \cdot D_\beta \pi(y) = 1$, and if $\alpha_1 = 0$, then with $\beta = (0, \bar{\beta})$ we have $\alpha \cdot D_\beta \pi(y) = 1$.
Conversely, let us assume that $\bar{x} \cdot \bar{\pi}(\bar{y})$ is not cubic-like bent (and prove that $x \cdot \pi(y)$ is not cubic-like bent):

- either there exists $\bar{\alpha} \neq 0$ such that for any $\bar{\beta}$, $\bar{\alpha} \cdot D_{\bar{\beta}}\bar{\pi}(\bar{y}) \neq 1$, then taking $\alpha = (0, \bar{\alpha})$, for any $\beta = (\beta_1, \bar{\beta})$, we have $\alpha \cdot D_\beta \pi(y) = \bar{\alpha} \cdot D_{\bar{\beta}}\bar{\pi}(\bar{y}) \neq 1$;

- or there exists $\bar{\alpha} \neq 0$ such that, for any $\bar{\beta}$, we have $\bar{\beta} \cdot D_{\bar{\alpha}}\bar{\pi}(\bar{y}) \neq 1$, then let $\alpha = (0, \bar{\alpha})$ and $\alpha' = (1, \bar{\alpha})$ and suppose that $\beta \cdot D_\alpha \pi(y) = 1$ and $\beta' \cdot D_{\alpha'}\pi(y) = 1$; this would imply $\beta_1 = \beta'_1 = 1$. So

$$\begin{aligned}
1 =& \beta \cdot D_\alpha \pi(y) = \bar{\beta} \cdot D_{\bar{\alpha}}\bar{\pi}(\bar{y}) + D_{\bar{\alpha}} f(\bar{y}) \\
1 =& \beta' \cdot D_{\alpha'}\pi(y) = \bar{\beta}' \cdot D_{\bar{\alpha}}\bar{\pi}(\bar{y}) + D_{\bar{\alpha}} f(\bar{y}) + 1 \\
1 =& (\bar{\beta} + \bar{\beta}') \cdot D_{\bar{\alpha}}\bar{\pi}(\bar{y})
\end{aligned}$$

  a contradiction.

This concludes the proof. □

Remark 14. *Proposition 15 provides a secondary construction (that can be applied recursively) of cubic-like bent functions*[3]*. It allows to obtain cubic-like bent functions of any algebraic degree up to $m = \frac{n}{2}$, since the Boolean function f can be taken of any algebraic degree at most $m - 1$.*
Moreover, Relation (19) shows that, if both $\bar{x} \cdot \bar{\pi}(\bar{y})$ and $\bar{y} \cdot \bar{\pi}^{-1}(\bar{x})$ are cubic-like bent, then not only $x \cdot \pi(y)$ is cubic-like bent but also $y \cdot \pi^{-1}(x)$, which is the dual of $x \cdot \pi(y)$. We have then also a recursive construction of cubic-like bent functions whose duals are cubic-like bent. Note that initial functions for this recursive construction are easily built: if $m = 3$, then π and π^{-1} being permutations, they are quadratic and $\bar{x} \cdot \bar{\pi}(\bar{y})$ and $\bar{y} \cdot \bar{\pi}^{-1}(\bar{x})$ are then both cubic-like bent (since they are cubic).

Remark 15. *What we observed with $m = 3$ is not true in higher dimensions, since there are in $\mathbb{F}_2^4$ many permutations π that do not generate cubic-like bent functions and whose duals do not either.*
This implies that for any $m \geq 5$ there exists a bent function $x \cdot \pi(y)$, with π as in (18) that it is not cubic-like bent and whose dual is not cubic-like bent.

6.1.6 When π is a Feistel permutation

A classical Feistel permutation is a function of the form $(X_L, X_R) \to (X_L + F(X_R), X_R)$, with $X_L \in \mathbb{F}_2^k$ and $X_R \in \mathbb{F}_2^{m-k}$ and where F is a mapping from $\mathbb{F}_2^{m-k}$ to $\mathbb{F}_2^k$. Such function is a permutation, being involutive. Many block ciphers (whose round functions must be permutations for allowing decryption and are better involutions to minimize the complexity of the encryption/decryption process) are built on this model, the most famous among these ciphers being of course the DES. Such structure of function can be generalized to:

$$(X_L, X_R) \to (X_L + F(X_R), \bar{\pi}(X_R)), \tag{20}$$

[3]There are many secondary constructions of bent functions, see e.g. [7], and it is good that some secondary constructions of cubic-like bent functions can be exhibited too.

where $\bar{\pi}$ is a permutation of $\mathbb{F}_2^{n-k}$, and we shall call *Feistel permutations* such more general functions (which are clearly bijective but are no more involutive, in general - involutivity is not a property having as much importance in our case as in the design of block ciphers). The permutation presented in Proposition 15 corresponds to the case $k = 1$.

The fact that a permutation is, up to affine equivalence, a Feistel permutation as in (20), is equivalent to the fact that its linear kernel has dimension at least k. Indeed, up to affine equivalence, we may assume that the linear kernel includes $\mathbb{F}_2^k \times \{0\}$, and denoting $x_L = (x_1, \dots, x_k)$ and $x_R = (x_{k+1}, \dots, x_n)$, a permutation π has such property if and only if $\pi(x) = \pi_1(x_L) + \pi_2(x_R)$, where π_1 is a linear injective function from $\mathbb{F}_2^k$ to $\mathbb{F}_2^n$ and π_2 is a function from $\mathbb{F}_2^{n-k}$ to $\mathbb{F}_2^n$, and up to affine equivalence, we may assume that π_1 is the identity. This means that the linear kernel of a permutation π has dimension at least k if and only if π is affine equivalent to a function of the form (20) and the bijectivity of $\bar{\pi}$ is clearly then necessary and sufficient.
In a more practical way, starting from a permutation having a linear kernel of dimension at least $k > 0$, we saw already that we can consider

$$\pi(y) = \begin{bmatrix} y_1 + f(y_2, \dots, y_m) \\ \pi_1(y_2, \dots, y_m) \end{bmatrix},$$

up to affine equivalence, and we can continue without loss of generality, assuming that $D_{e_2}\pi(y)$ is constant. Clearly, $D_{e_2}\pi(y) \neq e_1$, otherwise $D_{e_1+e_2}\pi(y) = 0$ and this is not possible since π is a permutation. Therefore we have also that $\bar{\pi}$ must admit a constant derivative and, up to affine equivalence, we can assume

$$\pi(y) = \begin{bmatrix} y_1 + f(y_2, y_3, \dots, y_m) \\ \pi_1(y_2, y_3, \dots, y_m) \end{bmatrix} = \begin{bmatrix} y_1 + f_1(y_3, \dots, y_m) \\ y_2 + f_2(y_3, \dots, y_m) \\ \pi_2(y_3, \dots, y_m) \end{bmatrix}. \qquad (21)$$

Iterating this method, if the dimension of the linear kernel of π is at least $k > 0$, we obtain a permutation in the Feistel form

$$\pi(y) = \pi(Y_1, Y_2) = \begin{bmatrix} Y_1 + F(Y_2) \\ \bar{\pi}(Y_2) \end{bmatrix}, \qquad (22)$$

with $\bar{\pi}$ a permutation of $\mathbb{F}_2^{m-k}$, for $k \leq m$, F a $(m-k, k)$-Boolean function, and where we write a generic element y of $\mathbb{F}_2^m$ as $y = (Y_1, Y_2)$ with $Y_1 \in \mathbb{F}_2^k$ and $Y_2 \in \mathbb{F}_2^{m-k}$. Moreover, notice that Proposition 15 can be iteratively applied to permutations as in (22). Indeed, by applying the proposition to (21) we have that $x \cdot \pi(y) = (x_1, \dots, x_m) \cdot \pi(y_1, \dots, y_m)$ is cubic-like bent if and only if $(x_2, \dots, x_m) \cdot \pi_1(y_2, \dots, y_m)$ is cubic-like bent if and only if $(x_3, \dots, x_m) \cdot \pi_2(y_3, \dots, y_m)$ is cubic-like bent. Therefore we can state the following result.

Proposition 16. *Consider a Feistel permutation π as in* (22)*. Then the map $x \cdot \pi(y)$ over $\mathbb{F}_2^m \times \mathbb{F}_2^m$ is cubic-like bent if and only if the map $X_2 \cdot \bar{\pi}(Y_2)$ over $\mathbb{F}_2^{m-k} \times \mathbb{F}_2^{m-k}$, is cubic-like bent.*

6.2 Functions of the general form $x \cdot \pi(y) + g(y)$

The general construction for Maiorana-McFarland maps is

$$f(x, y) = x \cdot \pi(y) + g(y), \tag{23}$$

with π a permutation (which is again a necessary and sufficient condition for the bentness of the Maiorana-McFarland function) and $g : \mathbb{F}_2^m \to \mathbb{F}_2$. The dual of f is then the function $(x, y) \mapsto y \cdot \pi^{-1}(x) + g(\pi^{-1}(x))$. In this case we have

$$\begin{aligned}
D_a D_b f(x, y) = & (x + b_1 + a_1) \cdot \pi(y + b_2 + a_2) + g(y + b_2 + a_2) + x \cdot \pi(y) + g(y) \\
& + (x + a_1) \cdot \pi(y + a_2) + g(y) + (x + b_1) \cdot \pi(y + b_2) + g(y + b_2) \\
= & x \cdot [\pi(y + b_2 + a_2) + \pi(y + a_2) + \pi(y + b_2) + \pi(y)] \\
& + a_1 \cdot [\pi(y + b_2 + a_2) + \pi(y + a_2)] \\
& + b_1 \cdot [\pi(y + b_2 + a_2) + \pi(y + b_2)] \\
& + g(y + a_2 + b_2) + g(y + a_2) + g(y + b_2) + g(y) \\
= & x \cdot D_{a_2} D_{b_2} \pi(y) + a_1 \cdot D_{b_2} \pi(y + a_2) + b_1 \cdot D_{a_2} \pi(y + b_2) \\
& + D_{a_2} D_{b_2} g(y).
\end{aligned}$$

Therefore we can formulate the cubic-like bentness property, in the next lemma (which includes Lemma 1 as a particular case).

Lemma 2. *Consider a Boolean function f as in* (23)*. Then f is cubic-like bent if and only if, for any nonzero $a = (a_1, a_2) \in \mathbb{F}_2^{2m}$, there exists $b = (b_1, b_2) \in \mathbb{F}_2^{2m}$ such that the following two conditions are satisfied:*

1. $D_{a_2} D_{b_2} \pi(y) = 0$,
2. $a_1 \cdot D_{b_2} \pi(y) + b_1 \cdot D_{a_2} \pi(y) + D_{a_2} D_{b_2} g(y) = 1$.

Recall that we deduced Proposition 12 from Lemma 1 by considering the particular values of a of the forms $(a_1, 0)$ and $(0, a_2)$; the fact that Relation (17) was satisfied by some b for such nonzero values of a was sufficient for having it satisfied by some b for every nonzero a. In the case of Lemma 2, we still have that if (i) and (ii) of Proposition 12 are satisfied by π, then f in (23) is cubic-like bent: exactly the same first part of proof as in Proposition 12 applies to the new situation. Hence we can state in the next proposition that if $x \cdot \pi(y)$ satisfies the condition of Lemma 1 (for which it is sufficient that it does for these particular forms of a), then function $f(x, y) = x \cdot \pi(y) + g(y)$ does too (whatever is g). But the converse may not be true (see however Remark 16 below); indeed, for $a = (a_1, 0) \neq 0$, nothing changes, but for $a = (0, a_2) \neq 0$, Relation (17) writes "$D_{a_2} D_{b_2} \pi(y) = 0$ and $b_1 \cdot D_{a_2} \pi(y) + D_{a_2} D_{b_2} g(y) = 1$"; hence we may not have (ii) anymore, in the case there would not exist b satisfying Relation (17) and such that $b_2 = 0$. The converse becomes true if (ii) is assumed. We have then:

Proposition 17. *Consider a function $f(x, y) = x \cdot \pi(y) + g(y)$ as in* (23)*.*
If the map $h(x, y) = x \cdot \pi(y)$ as in (15) *is cubic-like bent (resp. if its dual is*

cubic-like bent), then also f is cubic-like bent (resp. its dual is cubic-like bent). Conversely, if f is cubic-like bent, then Permutation π satisfies Condition (i), that is, for any $a_1 \neq 0$ there exists b_2 such that $a_1 \cdot D_{b_2}\pi(y) = 1$, and if π also satisfies Condition (ii), that is, for every $a_2 \neq 0$, there exists among the elements b such that $D_a D_b f(x,y) = 1$, at least one that has the form $(b_1, 0)$, then also $x \cdot \pi(y)$ is cubic-like bent.

Remark 16. *Theoretically, there may exist cubic-like bent Maiorana-McFarland functions given by* (23) *whose part $x \cdot \pi(y)$ is not cubic-like bent. It would be interesting to find examples of such functions, and if possible a construction of an infinite class of them. However, all the cubic-like bent functions we found in our computer investigations satisfy Condition (ii) of Proposition 12, which may then be a necessary and sufficient condition. In dimension $n = 8$, we shall see in the paragraph before Subsection 7.1, that this is actually the case.*

Remark 17. *Thanks to Relation* (19)*, we know that, when π is a permutation of $\mathbb{F}_2^4$ of the form* (18)*, then for any Boolean function g, the map $x \cdot \pi(y) + g(y)$ is cubic-like bent and its dual is cubic-like bent.*

6.3 An infinite class of cubic-like bent functions having any algebraic degrees between 2 and $\frac{n}{2}$

Proposition 17 gives us another construction method for cubic-like bent functions of any degree up to m. Indeed, given $m \geq 3$, consider any cubic bent function $f(x,y) = x \cdot \pi(y)$ (that is indeed also cubic-like bent). For any m-variable Boolean function $g(y)$ the map $f(x,y) + g(y)$ is cubic-like bent. Since g can have degree up to m, we can construct a cubic-like bent function of any degree up to m.

7 Computational results on the Maiorana-McFarland construction

We report in this section some computational results obtained with the help of Magma Algebra package [2].

Mainly, the bent functions investigated are over $\mathbb{F}_2^8$ and a principal role is played by permutations over $\mathbb{F}_2^4$. Such permutations have been entirely classified up to affine equivalence: there are 302 such classes, see [3]. In the following we often refer to this list.

Consider the 8-variable Boolean functions of the form

$$f(x,y) = x \cdot \pi(y)$$

as in (15).

We obtain from Remark 14 that any permutation π of $\mathbb{F}_2^4$ that has a constant derivative generates a bent function $x \cdot \pi(y)$ that is cubic-like bent and which has a cubic-like bent dual. Indeed, if π has a constant derivative, up to an affine transformation we can display it as

$$\pi(y) = \begin{bmatrix} y_1 + f(y_2, y_3, y_4) \\ \bar{\pi}(y_2, y_3, y_4) \end{bmatrix},$$

where $\bar{\pi}$, being a permutation of $\mathbb{F}_2^3$, has degree at most 2. From Proposition 15 we deduce the statement.

Among the list of 302 permutations over $\mathbb{F}_2^4$, 10 are such that they admit a constant derivative. Referring to the numbering given in [3], they corresponds to no. 1, 258, 278, 293, 295, 297, 299, 300, 301, 302. Moreover, they are the only maps π such that $2 \notin \mathcal{V}_\pi$, where

$$\mathcal{V}_\pi = \mathcal{V} = \{* \, |\{b \in \mathbb{F}_2^m; \; D_a D_b \pi(y) = 0\}| : a \in \mathbb{F}_2^m \setminus \{0\} \, *\}.$$

Therefore, as stated above, all these permutations generate a cubic-like bent function, whose dual is also cubic-like bent.

Remark 18. *Notice that the fact that $2 \notin \mathcal{V}$ is not a necessary condition for the function $x \cdot \pi(y)$ to be cubic-like bent. The first part "$D_{a_2} D_{b_2} \pi(y) = 0$" in Condition (17) of Lemma 1 is trivially satisfied by $b_2 = 0$ or $b_2 = a_2$ and the second part "$a_1 \cdot D_{b_2} \pi(y) + b_1 \cdot D_{a_2} \pi(y) = 1$" does not exclude these two possibilities. This makes that all the values in $\mathcal{V}$ are at least 2 and it may happen that only these two values $b_2 = 0$ and $b_2 = a_2$ satisfy $D_{a_2} D_{b_2} \pi(y) = 0$ and then $2 \in \mathcal{V}$.*

Apart from these ten permutations, there are 263 permutations π in the list such that for every $a \neq 0$, the second-order derivative is constantly zero $D_a D_b \pi(x) = 0$ if and only if $b = 0$ or $b = a$. Hence such that $\mathcal{V} = \{*2^{15}*\}$. The remaining 29 permutations are displayed in Table 2 in Appendix B. Among them, there are two cases of cubic-like bent functions $x \cdot \pi(y)$ where $2 \in \mathcal{V}$. They correspond to no. 283 and 298. Moreover, also for these maps, their dual is cubic-like bent. Hence, in total, out of 302 permutations (up to affine equivalence), 12 permutations produce cubic-like bent functions with cubic-like bent duals.

Table 1 displays the results for the cases of f a cubic-like bent function in dimension 8, where we report also the multiset $\mathcal{D}eg$ of the algebraic degrees of the non-zero component functions and the multiset $\mathcal{B}$ as in (4). Notice that, as already stated in Subsection 4.2, in dimension 8 no Maiorana-McFarland cubic-like bent map is such that $2 \in \mathcal{B}$. From Proposition 17, we have that these 12 permutations generates also cubic-like bent maps of the form $f(x, y) = x \cdot \pi(y) + g(y)$, for any possible choice of the Boolean functions g, and the dual of f is also cubic-like bent.

The other permutations left do not satisfy either one or the other of the conditions of Proposition 12. This implies that, using Proposition 17, these permutations cannot generate any cubic-like bent map of the form $f(x, y) = x \cdot \pi(y) + g(y)$. So, also for the general Maiorana-McFarland construction, if

Table 1: Permutations π of $\mathbb{F}_2^4$ such that $x \cdot \pi(y)$ is cubic-like bent

no.	$\mathcal{D}eg$	$\mathcal{B}$	$\mathcal{V}$
1	$\{*1^{15}*\}$	$\{*128^{255}*\}$	$\{*16^{15}*\}$
258	$\{*1^7, 2^8*\}$	$\{*32^{224}, 128^{31}*\}$	$\{*8^{12}, 16^3*\}$
278	$\{*1^3, 2^4, 3^8*\}$	$\{*8^{192}, 16^{48}, 32^8, 128^7*\}$	$\{*4^{14}, 16*\}$
283	$\{*1^3, 3^{12}*\}$	$\{*4^{192}, 16^{60}, 128^3*\}$	$\{*2^{12}, 4^3*\}$
293,295	$\{*1, 2^{14}*\}$	$\{*8^{224}, 32^{28}, 128^3*\}$	$\{*4^{14}, 16*\}$
297	$\{*1^1, 2^6, 3^8*\}$	$\{*4^{128}, 8^{96}, 16^{16}, 32^{12}, 128^3*\}$	$\{*4^{14}, 16*\}$
298	$\{*1, 2^{14}*\}$	$\{*2^{128}, 32^{126}, 128*\}$	$\{*2^8, 8^7*\}$
299	$\{*1^7, 3^8*\}$	$\{*16^{240}, 128^{15}*\}$	$\{*4^{14}, 16*\}$
300	$\{*2^7, 3^8*\}$	$\{*4^{224}, 16^{16}, 32^{14}, 128*\}$	$\{*4^{14}, 16*\}$
301, 302	$\{*1^3, 2^{12}*\}$	$\{*8^{128}, 32^{120}, 128^7*\}$	$\{*4^8, 8^6, 16*\}$

a function f in dimension 8 is cubic-like bent, then also its dual is cubic-like bent. To be complete, we give in Tables 3 and 4, the results for these other functions, but since they are not cubic-like bent, we put these tables at the end of the paper, after the bibliography, see Appendix B. Although, it is interesting to notice that there are some functions $f(x, y) = x \cdot \pi(y)$ for which no non-zero second-order derivative equals the constant function 1. For example, the one generated from the permutation no. 20:

$$\pi_{20}(y) = \begin{bmatrix} y_1y_2 + y_1y_3y_4 + y_1y_4 + y_1 + y_2y_3 \\ y_1y_2y_4 + y_1y_3 + y_1y_4 + y_2y_3y_4 + y_2y_3 + y_2y_4 + y_2 + y_3y_4 \\ y_1y_2y_3 + y_1y_2y_4 + y_1y_3 + y_1y_4 + y_2y_4 + y_3 \\ y_1y_2y_3 + y_1y_2y_4 + y_1y_2 + y_1y_4 + y_2y_3y_4 + y_2y_3 + y_4 \end{bmatrix}.$$

7.1 When π over $\mathbb{F}_2^5$ has a constant derivative

We just saw that any permutation π in $\mathbb{F}_2^4$ that has a constant derivative generates a cubic-like bent function $x \cdot \pi(y)$.

This same argument is no more valid in dimension 5. Let us consider π a permutation of $\mathbb{F}_2^5$ with a constant derivative, containing therefore $\bar{\pi}$, permutation of $\mathbb{F}_2^4$. If we take $\bar{\pi}$ such that $\bar{x} \cdot \bar{\pi}(\bar{y})$ is not cubic-like bent, and we have plenty of such permutations, then $x \cdot \pi(y)$ is not cubic-like bent either. However, from computational results, we know that if $\bar{\pi}$ generates a cubic-like bent map, so does $\bar{\pi}^{-1}$. Hence if $x \cdot \pi(y)$ with a constant derivative is cubic-like bent, the dual $x \cdot \pi^{-1}(y)$ is also cubic-like bent.

When considering f of the general form

$$f(x, y) = x \cdot \pi(y) + g(y),$$

we already know that in dimension 8, any such function is cubic-like bent if and only if $x \cdot \pi(y)$ is cubic-like bent.

We know that π must satisfy the following property: for any $a_1 \neq 0$ there exists b_2 such that $a_1 \cdot D_{b_2}\pi(y) = 1$. Since π is of the form (18), the same property has to be satisfied by $\bar{\pi}$: for any $\bar{a}_1 \neq 0$ there exists $\bar{b}_2$ such that $\bar{a}_1 \cdot D_{\bar{b}_2}\pi(y) = 1$.

We know that, for $\bar{\pi}$ permutation of $\mathbb{F}_2^4$, this property is satisfied only by those permutations that generates cubic-like bent functions. Hence, in dimension 10, the bent function $f(x, y) = x \cdot \pi(y) + g(y)$, with π as in (18), is cubic-like bent if and only if $f(x, y) = x \cdot \pi(y)$ is cubic-like bent.

Conclusion

In this work, we studied those bent Boolean functions that share with cubic bent maps the property that each derivative in a nonzero direction has itself a derivative equal to constant function 1; we call such functions *cubic-like bent*. The idea was to identify an interesting sub-class of bent functions, and to understand better the behavior of its elements. We showed the invariance of the notion with respect to EA-equivalence, and provided characterizations by means of the Walsh transform.

We studied as a typical example Maiorana-McFarland functions, which allowed us to prove that cubic-like bent functions can have any degree between 2 and $\frac{n}{2}$. Proving that cubic-like bent maps exist that are not cubic was of course necessary for the interest of our study; finding such functions with any admissible degree strengthens it. Maiorana-McFarland cubic-like bent functions are not rare and this may be different for other classes than the Maiorana-McFarland class, for instance the $\mathcal{PS}_{ap}$ class. We also found examples of bent functions which are not cubic-like bent and do not have cubic-like bent duals. So, the class of cubic-like bent functions is a proper subclass of bent maps, and it is more general than the class of cubic bent functions. We studied some subclasses of Maiorana-McFarland cubic-like bent functions. We presented computational results which completely classify Maiorana-McFarland cubic-like bent functions in dimension 8 and partially in dimension 10. In dimension 8, most of the obtained maps belong to a specific class, the functions constructed from a permutation with a constant derivative.

We leave for a second paper the investigation of the cubic-like bent property for other well-known constructions of bent maps, which would take a too large number of additional pages and will need more work. It seems in particular that no $\mathcal{PS}_{ap}$ function can be cubic-like bent and if this is confirmed, it will show one more difference between Maiorana-McFarland and $\mathcal{PS}_{ap}$ classes, and an interesting property of the latter.

Future work will be to deduce new constructions of bent functions using the cubic-like bentness property. This seems very challenging.

Acknowledgement. We thank Lilya Budaghyan for interesting suggestions.

I. Villa was partially supported by the Research Council of Norway, grant no. 247742/070, and the Trond Mohn Stiftelse (TMS) Foundation.

References

[1] T. Bending, D. Fon-Der-Flaass. Crooked functions, bent functions and distance regular graphs. *Electron. J. Comb.* 5, Research paper 34 (electronic), 14 pages, 1998.

[2] W. Bosma, J. Cannon, C. Playoust. The Magma algebra system I: the user language, J. Symb. Comput. 24 (1997) 235–265.

[3] C. De Canniere. Analysis and Design of Symmetric Encryption Algorithms. PhD thesis (2007)

[4] A. Canteaut, A. Couvreur, L. Perrin. Recovering or testing extended-affine equivalence. To appear in *IEEE Transactions on Information Theory*, 2022.

[5] C. Carlet. On cryptographic propagation criteria for Boolean functions. *Information and Computation* 151, Academic Press pp. 32-56, 1999.

[6] C. Carlet. Boolean and vectorial plateaued functions, and APN functions. *IEEE Transactions on Information Theory* 61 (11), pp. 6272-6289, 2015.

[7] C. Carlet. Boolean Functions for Cryptography and Coding Theory. Monograph in *Cambridge University Press*, 562 pages, 2021.

[8] C. Carlet, P. Charpin, V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15 (2), pp. 125-156, 1998.

[9] C. Carlet, D. Davidova. On strongly plateaued functions. Preprint, 2022.

[10] C. Carlet, S. Mesnager. Four decades of research on bent functions. *Designs, Codes and Cryptography* 78(1), pp. 5-50, 2016.

[11] C. Carlet, E. Prouff. On plateaued functions and their constructions. *Proceedings of Fast Software Encryption 2003, Lecture notes in computer science* 2887, pp. 54-73, 2003.

[12] J. F. Dillon. Elementary Hadamard Difference sets. Ph. D. Thesis, Univ. of Maryland, 1974

[13] R. L. McFarland. A family of noncyclic difference sets. Journal of Combinatorial Theory, Series A 15, pp. 1–10, 1973.

[14] S. Mesnager. *Bent functions: fundamentals and results.* Springer, pp. 1-544, 2016.

[15] O. S. Rothaus. On "bent" functions. Journal of Combinatorial Theory, Series A 20.3 (1976): 300-305.

A Some proofs

Proof of Proposition 8 in Subsection 4.1.

Proof. Given Equation (5), we can consider

$$f(x) \overset{\text{aff}}{\sim} x_{n-3}x_{n-2}x_{n-1}x_n + q_3(x_{n-3}, x_{n-2}, x_{n-1}, x_n) + q(x_1, \dots, x_n),$$

where q_3 is a cubic map in four variables. In this proof, with abuse of notation, we keep indicating with g a Boolean function EA-equivalent to f, even if it is a different (but EA-equivalent) map.

By the action of an affine transformation, it is possible to cancel all the cubic terms in q_3. Indeed assume that $x_{n-2}x_{n-1}x_n$ appears in q_3, then with the transformation $x_{n-3} \to x_{n-3} + 1$ this cubic term disappears and the other cubic terms are not modified. By applying the same procedure for each cubic term in q_3, we obtain

$$f \overset{\text{aff}}{\sim} g = x_{n-3}x_{n-2}x_{n-1}x_n + \tilde{q}_2(x_1, \dots, x_n),$$

where $\tilde{q}_2$ is a quadratic map. Up to considering EA-equivalence, we can assume that $\tilde{q}_2$ is a DO polynomial, that is $\tilde{q}_2(x) = \sum_{i<j} b_{i,j}x_ix_j$. In the following we will write sometimes $b_{j,i}$ instead of $b_{i,j}$. Moreover, we will refer to the coefficients of the DO polynomial as $b_{i,j}$ even after applying a linear transformation. We have that $D_{e_n}g(x) = x_{n-3}x_{n-2}x_{n-1} + \sum_i b_{i,n}x_i$. From the cubic-like bentness property we have that $b_{i,n} \neq 0$ for at least one element $1 \leq i \leq n-4$. Without loss of generality let $b_{1,n} = 1$ and, by applying the transformation $x_1 \to x_1 + \sum_{i=2}^{n-1} b_{i,n}x_i$ we obtain an equivalent map

$$f \overset{\text{EA}}{\sim} g = x_{n-3}x_{n-2}x_{n-1}x_n + x_1x_n + \sum_{i=1}^{n-2}\sum_{j=i+1}^{n-1} b_{i,j}x_ix_j.$$

For the derivative in e_{n-1} we obtain $x_{n-3}x_{n-2}x_n + \sum_i b_{i,n-1}x_i$. Again, there exists an element $b_{i,n-1} \neq 0$ for $1 \leq i \leq n-4$. If the only possible element is for $i = 1$, then deriving in the direction of $a = e_n + e_{n-1}$ we obtain $D_a g(x) = x_{n-3}x_{n-2} + x_{n-3}x_{n-2}x_{n-1} + x_{n-3}x_{n-2}x_n + x_1 + x_1 + b_{n-3,n-1}x_{n-3} + b_{n-2,n-1}x_{n-2} = x_{n-3}x_{n-2}(1 + x_{n-1} + x_n) + b_{n-3,n-1}x_{n-3} + b_{n-2,n-1}x_{n-2}$. There is no element that satisfies the cubic-like bentness property for this specific derivative. Hence we can assume that $b_{2,n-1} = 1$ and with the transformation $x_2 \to b_{1,n-1}x_1 + x_2 + \sum_{i=3}^{n-2} b_{i,n-1}x_i$ we obtain an equivalent map $x_{n-3}x_{n-2}x_{n-1}x_n + x_1x_n + x_2x_{n-1} + \sum_{i,j=1}^{n-2} b_{i,j}x_ix_j$. By applying the same procedure for x_{n-2} and x_{n-3} we get

$$f(x) \overset{\text{EA}}{\sim} g = x_{n-3}x_{n-2}x_{n-1}x_n + \sum_{i=1}^{4} x_ix_{n-i+1} + \sum_{i,j=1}^{n-4} b_{i,j}x_ix_j.$$

Now, $D_{e_{n-4}}g(x) = \sum_{i=1}^{n-3} b_{i,n-4}x_i$. If $b_{i,n-4} \neq 0$ for a $5 \leq i \leq n-5$, then without loss of generality we assume $b_{5,n-4} = 1$ and applying a linear transformation, we obtain

$$f(x) \overset{\text{EA}}{\sim} g = x_{n-3}x_{n-2}x_{n-1}x_n + \sum_{i=1}^{5} x_i x_{n-i+1} + \sum_{i,j=1}^{n-5} b_{i,j} x_i x_j.$$

Assume instead that $D_{e_{n-4}} g(x) = \sum_{i=1}^{4} b_{i,n-4} x_i$, with at least one of the coefficient nonzero. Without loss of generality, assume that $b_{1,n-4} = 1$. Therefore we have that the derivative in the direction of $a = e_n + b_{2,n-4}e_{n-1} + b_{3,n-4}e_{n-2} + b_{4,n-4}e_{n-3} + e_{n-4}$ is $(x_n+1)(x_{n-1}+b_{2,n-4})(x_{n-2}+b_{3,n-4})(x_{n-3}+b_{4,n-4}) + x_n x_{n-1} x_{n-2} x_{n-3}$. By applying the transformation $(x_n, x_{n-1}, x_{n-2}, x_{n-3}) \to (x_n, x_{n-1} + b_{2,n-4}(x_n+1), x_{n-2} + b_{3,n-4}(x_n+1), x_{n-3} + b_{4,n-4}(x_n+1))$, we obtain $x_{n-1}x_{n-2}x_{n-3}$, which cannot be balanced. So we get to a contradiction.

The same procedure can be applied for each variable x_{n-t} for $t = 5, \dots, n/2 - 1$. Indeed, suppose we applied successfully the procedure for the variable x_{n-k-1}, for a $k \geq 5$, so $g = x_{n-3}x_{n-2}x_{n-1}x_n + \sum_{i=1}^{k} x_i x_{n-i+1} + \sum_{i,j=1}^{n-k} b_{i,j} x_i x_j$. The next step is to consider $a = e_{n-k}$ and compute the derivative. We have $D_a g(x) = \sum_{i=1}^{n-k-1} b_{i,n-k} x_i$. Using the same argument as before, we know that there exists $j \geq 5$ such that $b_{j,n-k} = 1$; and by applying a linear transformation, we can assume $D_a g(x) = \sum_{i=5}^{n-k-1} b_{i,n-k} x_i$. Suppose now that, for $j \geq k+1$ we have $b_{j,n-k} = 0$, so $D_a g(x) = \sum_{i=5}^{k} b_{i,n-k} x_i$. In this case, for $a' = e_{n-k} + b_{5,n-k}e_{n-4} + \ldots + b_{k,n-k}e_{n-k+1}$ we would obtain $D_{a'} g(x) = \sum_{i=5}^{k} b_{i,n-k} x_i + b_{5,n-k}x_5 + \ldots + b_{k,n-k}x_k = 0$. Therefore there must exist $j \geq k+1$ such that $b_{j,n-k} = 1$, without loss of generality let $b_{k+1,n-k} = 1$, and applying a linear transformation, we get to $g = x_{n-3}x_{n-2}x_{n-1}x_n + \sum_{i=1}^{k+1} x_i x_{n-i+1} + \sum_{i,j=1}^{n-k-1} b_{i,j} x_i x_j$.

Therefore, with the iteration of this procedure, the map obtained is of the form

$$f(x) \overset{\text{EA}}{\sim} g = x_{n-3}x_{n-2}x_{n-1}x_n + \sum_{i=1}^{n/2} x_i x_{n-i+1} + \sum_{i,j=1}^{n/2} b_{ij} x_i x_j.$$

For $i = 5, \dots, n/2$ we apply the linear transformation $x_{n-i+1} \to x_{n-i+1} + \sum_{j=1}^{n/2} b_{ij} x_j$, obtaining

$$f(x) \overset{\text{EA}}{\sim} g = x_{n-3}x_{n-2}x_{n-1}x_n + \sum_{i=1}^{n/2} x_i x_{n-i+1} + \sum_{i=1}^{3} \sum_{j=i+1}^{4} b_{ij} x_i x_j.$$

As last step, assume without loss of generality that $\beta = (b_{12}, b_{13}, b_{14}) = (\beta_1, \beta_2, \beta_3) \neq (0,0,0)$. Hence, the derivative in the direction of $a = e_1 + \beta \cdot (e_{n-1}, e_{n-2}, e_{n-3})$ is of the form

$$\begin{aligned} &x_n(\beta_1\beta_2\beta_3 + \beta_1 x_{n-2}x_{n-3} + \beta_2 x_{n-1}x_{n-3} + \beta_3 x_{n-1}x_{n-2} + \beta_1\beta_2 x_{n-3} \\ &\quad + \beta_1\beta_3 x_{n-2} + \beta_2\beta_3 x_{n-1} + 1). \end{aligned}$$

By analysing all possible cases, we have that no second-order derivative can be the constant function 1. Indeed,

- if $\beta = (100)$ then the derivative function equals $x_n(x_{n-2}x_{n-3} + 1)$;
- if $\beta = (110)$ we have $x_n(x_{n-2}x_{n-3}+x_{n-1}x_{n-3}+x_{n-3}+1) \overset{\text{EA}}{\sim} x_n(x_{n-2}x_{n-3}+1)$;
- if $\beta = (111)$ we have $x_n(x_{n-2}x_{n-3}+x_{n-1}x_{n-3}+x_{n-1}x_{n-2}+x_{n-3}+x_{n-2}+x_{n-1}) \overset{\text{EA}}{\sim} x_n(x_{n-2}x_{n-3} + 1)$.

Therefore we conclude the proof. $\square$

B Further computational results

We report here some tables with computational results, that were not listed in Section 7 because of lack of space.

Table 2: Permutations of $\mathbb{F}_2^4$ such that $2 \in \mathcal{V} \neq \{*2^{15}*\}$

no.	$\mathcal{D}eg$	$\mathcal{V}$
22, 294	$\{*1^3, 2^4, 3^8*\}$	$\{*2^8, 4^6, 8*\}$
39, 205, 283, 291	$\{*1^3, 3^{12}*\}$	$\{*2^{12}, 4^3*\}$
96, 165, 206, 274, 289	$\{*1, 2^6, 3^8*\}$	$\{*2^{12}, 4^3*\}$
112, 193, 202, 230,266, 268, 277, 284	$\{*1, 2^2, 3^{12}*\}$	$\{*2^{12}, 4^3*\}$
140, 174, 234, 237	$\{*2^3, 3^{12}*\}$	$\{*2^{12}, 4^3*\}$
231, 292	$\{*1, 2^6, 3^8*\}$	$\{*2^8, 4^6, 8*\}$
242, 281	$\{*2^7, 3^8*\}$	$\{*2^{12}, 4^3*\}$
290	$\{*1, 2^6, 3^8*\}$	$\{*2^{12}, 4^3*\}$
298	$\{*1, 2^{14}*\}$	$\{*2^8, 8^7*\}$

Table 3: Permutations π of $\mathbb{F}_2^4$ with $1 \in \mathcal{D}eg$ and $x \cdot \pi(y)$ not cubic-like bent

no.	$\mathcal{D}eg$	$\mathcal{B}$
7, 87, 135, 286	$\{*1, 3^{14}*\}$	$\{*0^{108}, 2^{128}, 4^{16}, 16^2, 128*\}$
10	$\{*1, 3^{14}*\}$	$\{*0^{18}, 2^{128}, 4^{96}, 16^{12}, 128*\}$
22	$\{*1^3, 2^4, 3^8*\}$	$\{*0^{12}, 4^{128}, 8^{72}, 16^{28}, 32^{12}, 128^3*\}$
39	$\{*1^3, 3^{12}*\}$	$\{*0^{12}, 4^{192}, 8^{24}, 16^{24}, 128^3*\}$
45, 46, 158, 159, 190	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{108}, 2^{96}, 4^{48}, 32^2, 128*\}$
51, 251	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{72}, 2^{96}, 4^{80}, 16^4, 32^2, 128*\}$
53	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{90}, 2^{96}, 4^{64}, 16^2, 32^2, 128*\}$
73	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{54}, 2^{96}, 4^{96}, 16^6, 32^2, 128*\}$
96, 289, 290	$\{*1, 2^6, 3^8*\}$	$\{*0^{72}, 2^{64}, 4^{72}, 8^{40}, 32^6, 128*\}$
107	$\{*1, 3^{14}*\}$	$\{*0^{72}, 2^{128}, 4^{48}, 16^6, 128*\}$
112	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{36}, 2^{128}, 4^{32}, 8^{40}, 16^{16}, 32^2, 128*\}$
113, 259	$\{*1, 3^{14}*\}$	$\{*0^{126}, 2^{128}, 128*\}$
122	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{74}, 2^{128}, 4^{48}, 16^2, 32^2, 128*\}$
125	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{72}, 2^{128}, 4^{32}, 8^{16}, 16^4, 32^2, 128*\}$
165	$\{*1, 2^6, 3^8*\}$	$\{*0^{46}, 2^{64}, 4^{112}, 8^{20}, 16^6, 32^6, 128*\}$
193	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{92}, 2^{96}, 4^{56}, 8^8, 32^2, 128*\}$
194, 288	$\{*1, 3^{14}*\}$	$\{*0^{90}, 2^{128}, 4^{32}, 16^4, 128*\}$
202	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{72}, 2^{96}, 4^{56}, 8^{24}, 16^4, 32^2, 128*\}$
205, 291	$\{*1^3, 3^{12}*\}$	$\{*0^{60}, 4^{192}, 128^3*\}$
206	$\{*1, 2^6, 3^8*\}$	$\{*0^{54}, 2^{48}, 4^{120}, 8^{20}, 16^6, 32^6, 128*\}$
230	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{82}, 2^{96}, 4^{56}, 8^{16}, 16^2, 32^2, 128*\}$
231	$\{*1, 2^6, 3^8*\}$	$\{*0^{12}, 2^{128}, 8^{88}, 16^{12}, 32^{14}, 128*\}$
266	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{56}, 2^{128}, 4^{40}, 8^{24}, 16^4, 32^2, 128*\}$
268	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{72}, 2^{128}, 4^{48}, 8^4, 32^2, 128*\}$
270, 273, 285	$\{*1, 3^{14}*\}$	$\{*0^{54}, 2^{128}, 4^{64}, 16^8, 128*\}$
274	$\{*1, 2^6, 3^8*\}$	$\{*0^{32}, 2^{128}, 4^{56}, 8^{32}, 32^6, 128*\}$
277	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{48}, 2^{128}, 4^{32}, 8^{40}, 16^4, 32^2, 128*\}$
282	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{92}, 2^{128}, 4^{32}, 32^2, 128*\}$
284	$\{*1, 2^2, 3^{12}*\}$	$\{*0^{46}, 2^{128}, 4^{48}, 8^{20}, 16^{10}, 32^2, 128*\}$
292	$\{*1, 2^6, 3^8*\}$	$\{*0^{40}, 2^{64}, 4^{112}, 8^{28}, 32^{10}, 128*\}$
294	$\{*1^3, 2^4, 3^8*\}$	$\{*0^{32}, 4^{128}, 8^{84}, 32^8, 128^3*\}$

Table 4: Permutations π of $\mathbb{F}_2^4$ with $1 \notin \mathcal{D}eg$ and $x \cdot \pi(y)$ not cubic-like bent

no.	$\mathcal{D}eg$	$\mathcal{B}$
2, 3, 4, 17, 26, 42, 54, 94, 108, 115, 119, 171, 176, 178, 181, 213	$\{*2, 3^{14}*\}$	$\{*0^{171}, 2^{80}, 16^3, 32*\}$
5, 30, 83, 103, 111, 142, 150, 191	$\{*2, 3^{14}*\}$	$\{*0^{187}, 2^{48}, 4^{16}, 16^3, 32*\}$
6, 69, 138, 201, 210, 272	$\{*2, 3^{14}*\}$	$\{*0^{204}, 2^{32}, 4^{16}, 16^2, 32*\}$
8, 15, 18, 31, 137, 169, 187, 207	$\{*2, 3^{14}*\}$	$\{*0^{153}, 2^{80}, 4^{16}, 16^5, 32*\}$
9, 12, 25, 34, 40, 41, 58, 64, 75,84, 98, 130, 141, 147, 156, 157,179, 182, 208, 209, 211, 215, 219, 228, 238, 248, 253,257	$\{*2, 3^{14}*\}$	$\{*0^{188}, 2^{64}, 16^2, 32*\}$
11, 44	$\{*2, 3^{14}*\}$	$\{*0^{119}, 2^{112}, 4^{16}, 16^7, 32*\}$
13, 162, 184, 195, 221, 260, 264, 271	$\{*2^3, 3^{12}*\}$	$\{*0^{138}, 2^{96}, 4^{16}, 16^2, 32^3*\}$
14, 19, 23, 33, 36, 50, 62, 63, 68,72, 81, 85, 88, 91, 97, 100, 124,131, 139, 143, 149, 153, 168, 173, 183, 198, 212, 218, 223, 229, 232, 233, 244, 250, 256	$\{*2, 3^{14}*\}$	$\{*0^{205}, 2^{48}, 16, 32*\}$
16, 35, 48, 59, 101, 110, 227, 243, 269	$\{*2, 3^{14}*\}$	$\{*0^{222}, 2^{32}, 32*\}$
20, 127, 128, 220, 241, 245, 247, 254, 267, 280, 296	$\{*3^{15}*\}$	$\{*0^{255}*\}$
21, 43, 92, 136, 175, 199, 216, 265	$\{*3^{15}*\}$	$\{*0^{187}, 2^{64}, 16^4*\}$
24, 47, 61, 66, 76, 77, 79, 93, 114, 123, 151, 185, 203	$\{*3^{15}*\}$	$\{*0^{204}, 2^{48}, 16^3*\}$
27, 29, 57, 80, 89, 95, 116, 120, 148, 240	$\{*2, 3^{14}*\}$	$\{*0^{154}, 2^{96}, 16^4, 32*\}$
28	$\{*2, 3^{14}*\}$	$\{*0^{136}, 2^{96}, 4^{16}, 16^6, 32*\}$
32, 38, 60, 65, 99, 105, 160, 163, 192, 214, 235, 287	$\{*3^{15}*\}$	$\{*0^{238}, 2^{16}, 16*\}$
37, 49, 55, 67, 104, 117, 118, 121, 129, 146, 152, 161, 166, 167, 170, 172, 189, 200, 217, 252, 261	$\{*3^{15}*\}$	$\{*0^{221}, 2^{32}, 16^2*\}$
56, 70, 86, 102, 204, 226, 239, 249, 255, 262, 275	$\{*2^3, 3^{12}*\}$	$\{*0^{172}, 2^{64}, 4^{16}, 32^3*\}$
52, 155	$\{*3^{15}*\}$	$\{*0^{170}, 2^{80}, 16^5*\}$
71	$\{*3^{15}*\}$	$\{*0^{136}, 2^{112}, 16^7*\}$
74, 133, 196	$\{*2, 3^{14}*\}$	$\{*0^{170}, 2^{64}, 4^{16}, 16^4, 32*\}$
78	$\{*3^{15}*\}$	$\{*0^{85}, 2^{160}, 16^{10}*\}$
82, 126, 186, 246	$\{*2^3, 3^{12}*\}$	$\{*0^{154}, 2^{64}, 4^{32}, 16^2, 32^3*\}$
90, 134, 144, 145, 188	$\{*2^3, 3^{12}*\}$	$\{*0^{155}, 2^{80}, 4^{16}, 16, 32^3*\}$
106, 109, 236, 263, 276	$\{*3^{15}*\}$	$\{*0^{153}, 2^{96}, 16^6*\}$
132	$\{*2, 3^{14}*\}$	$\{*0^{120}, 2^{128}, 16^6, 32*\}$
140	$\{*2^3, 3^{12}*\}$	$\{*0^{154}, 2^{32}, 4^{56}, 8^8, 16^2, 32^3*\}$
154, 222	$\{*2^3, 3^{12}*\}$	$\{*0^{137}, 2^{80}, 4^{32}, 16^3, 32^3*\}$
164, 225	$\{*2^3, 3^{12}*\}$	$\{*0^{120}, 2^{96}, 4^{32}, 16^4, 32^3*\}$
174	$\{*2^3, 3^{12}*\}$	$\{*0^{136}, 2^{48}, 4^{48}, 8^{16}, 16^4, 32^3*\}$
177, 197	$\{*2^3, 3^{12}*\}$	$\{*0^{122}, 2^{128}, 16^2, 32^3*\}$
224	$\{*2^7, 3^8*\}$	$\{*0^{72}, 2^{160}, 8^{16}, 32^7*\}$
180	$\{*2^7, 3^8*\}$	$\{*0^{119}, 2^{16}, 4^{112}, 16, 32^7*\}$
234	$\{*2^3, 3^{12}*\}$	$\{*0^{138}, 2^{64}, 4^{40}, 8^8, 16^2, 32^3*\}$
237	$\{*2^3, 3^{12}*\}$	$\{*0^{102}, 2^{96}, 4^{32}, 8^{12}, 16^{10}, 32^3*\}$
242	$\{*2^7, 3^8*\}$	$\{*0^{54}, 2^{144}, 4^{24}, 8^{20}, 16^6, 32^7*\}$
279	$\{*2^3, 3^{12}*\}$	$\{*0^{136}, 2^{96}, 8^{16}, 16^4, 32^3*\}$
281	$\{*2^7, 3^8*\}$	$\{*0^{136}, 4^{88}, 8^{24}, 32^7*\}$