Decomposing Bent Functions

Anne Canteaut and Pascale Charpin

***Abstract*—In a recent paper [1], it is shown that the restrictions of bent functions to subspaces of codimension 1 and 2 are highly nonlinear. Here, we present an extensive study of the restrictions of bent functions to affine subspaces. We propose several methods which are mainly based on properties of the derivatives and of the dual of a given bent function. We solve an open problem due to Hou [2]. We especially describe the connection, for a bent function, between the Fourier spectra of its restrictions and the decompositions of its dual. Most notably, we show that the Fourier spectra of the restrictions of a bent function to the subspaces of codimension 2 can be explicitly derived from the Hamming weights of the second derivatives of the dual function. The last part of the paper is devoted to some infinite classes of bent functions which cannot be decomposed into four bent functions.**

***Index Terms*—Bent functions, Boolean functions, derivatives of Boolean functions, Reed–Muller codes, restrictions of Boolean functions.**

I. Introduction

BENT functions are the most famous Boolean functions since they achieve the upper bound on nonlinearity. In other words, bent functions provide cosets of the Reed–Muller code of length 2^m (m even) and order one whose minimum Hamming weight corresponds to the covering radius of this Reed–Muller code. As exceptional objects, bent functions are related to combinatorial problems such as *difference sets* or with cryptographic criteria such as *perfect nonlinearity* [3]. When effective constructions are considered, there are two main classes of bent functions, the *Maiorana–McFarland* class and the *partial spreads* class (respectively denoted by $\mathcal{M}$ and $\mathcal{PS}$). In his thesis, Dillon [6] introduced the second class and he gave a lot of important properties characterizing bent functions. Two new classes, which can be considered as derivatives of some functions of $\mathcal{M}$ were later introduced by Carlet [4]. Dobbertin also gave a construction of bent functions which leads to some elements of $\mathcal{M}$ and of $\mathcal{PS}$ as extremal cases [5]. However, the problem of the classification of bent function remains open.

In this paper, we present a set of properties and tools for the study of the restrictions of any bent function to any subspace. Dillon's work [6] and recent papers of Carlet are here our main references. On the one hand, we want to consider the general problem of iterative constructions of bent functions. On the other hand, our interest is for other functions (of any number of variables) which can be built by means of the exceptional properties of bent functions.

Manuscript received August 23, 2001; revised March 12, 2003. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Lausanne, Switzerland, June/July 2002.

The authors are with the INRIA–Projet CODES, 78153 Le Chesnay Cedex, France (e-mail: Anne.Canteaut@inria.fr; Pascale.Charpin@inria.fr).

Communicated by A. M. Klapper, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2003.814476

The paper is organized as follows. The main definitions and basic properties are given in Section II. Most of these properties are usually known; they are proven for clarity. In Section III, we investigate the links between the derivatives of a bent function and those of its dual. This leads to a general property on the restrictions of the derivatives of a bent function to hyperplanes. Section IV focuses on bent functions which have at least one affine derivative. We point out that this property is invariant by duality. Moreover, we solve an open problem due to Hou [2]: we prove that for any even $m \geq 6$, $m \neq 8$, there exist cubic bent functions of m variables which have no affine derivatives. Section V is devoted to the fundamental properties of the restrictions of any bent function f and of its dual $\tilde{f}$ to some subspaces. Our main result is given by Theorem 6: we show that the Fourier spectra of the restrictions of f to a subspace V and to its cosets are related to the derivative of $\tilde{f}$ with respect to the dual space $V^\perp$. Section VI is then dedicated to the previous relationship when a subspace V of codimension 2 is considered. We give an explicit expression of the Fourier spectra of the restrictions of f to V and to its cosets as a function of the weight of the second derivative of $\tilde{f}$ with respect to $V^\perp$. Most notably, we prove that the restrictions of f to V and to its cosets are bent if and only if the derivative of $\tilde{f}$ with respect to $V^\perp$ is constant and equal to 1. Finally, Section VII focuses on the decompositions into four functions of some bent functions which belong to family $\mathcal{PS}^-$ or to class $\mathcal{M}$. For both classes, we exhibit infinite families of bent functions which cannot be decomposed into four bent functions. Our constructions are related to other works concerning the weight enumerators of some cyclic codes and the so-called *almost bent* functions.

II. Preliminaries

A. Notation

We denote by $\boldsymbol{F}_q$ the finite field with q elements. The *weight* of a binary vector $a = (a_1, \ldots, a_n) \in \boldsymbol{F}_2^n$ is the Hamming weight

$$\mathrm{wt}\,(a) = \sum_{i=1}^{n} a_i.$$

A *Boolean function of m variables* is a function from $\boldsymbol{F}_2^m$ into $\boldsymbol{F}_2$, and we denote by $\mathcal{B}_m$ the set of all Boolean functions of m variables. Any $f \in \mathcal{B}_m$ can be expressed as a polynomial, called its *algebraic normal form*

$$f(x_1, \ldots, x_m) = \sum_{u \in \boldsymbol{F}_2^m} \lambda_u \left(\prod_{i=1}^{m} x_i^{u_i} \right), \qquad \lambda_u \in \boldsymbol{F}_2.$$

The *degree* of f, denoted by $\deg(f)$, is the maximal value of $\mathrm{wt}(u)$ such that $\lambda_u \neq 0$.

Any Boolean function in $\mathcal{B}_m$ can also be identified with the codeword of length 2^m consisting of all values $f(x)$, $x \in \boldsymbol{F}_2^m$. This representation is unique only up to an ordering of $\boldsymbol{F}_2^m$. The *Reed–Muller code* of length 2^m and order r, $0 \leq r \leq m$, denoted by $R(r, m)$, is then the linear code composed of the vectors corresponding to all Boolean functions in $\mathcal{B}_m$ of degree less than or equal to r.

The usual dot product between two vectors x and y is denoted by $x \cdot y$. We denote by $V^\perp$ the dual of a subspace $V \subset \boldsymbol{F}_2^m$ relatively to the usual scalar product

$$V^\perp = \{x \in \boldsymbol{F}_2^m \,|\, \forall y \in V,\, x \cdot y = 0\}.$$

For any $\alpha \in \boldsymbol{F}_2^m$, φ_α is the linear function in $\mathcal{B}_m$: $x \mapsto \alpha \cdot x$. In some particular cases (Sections IV and VII-B) we will use another dot product (and, thus, another representation for the linear functions).

For any $f \in \mathcal{B}_m$, we denote by $\mathcal{F}(f)$ the following value related to the Fourier (or Walsh) transform of f:

$$\mathcal{F}(f) = \sum_{x \in \boldsymbol{F}_2^m} (-1)^{f(x)} = 2^m - 2\mathrm{wt}\,(f)$$

where $\mathrm{wt}\,(f)$ is the Hamming weight of f, i.e., the number of $x \in \boldsymbol{F}_2^m$ such that $f(x) = 1$. A function f is said to be *balanced* if $\mathcal{F}(f) = 0$.

Definition 1: The *Fourier spectrum* of a function $f \in \mathcal{B}_m$ is the multiset

$$\{\mathcal{F}(f + \varphi_\alpha),\, \alpha \in \boldsymbol{F}_2^m\}.$$

The *extended Fourier spectrum* of f is the multiset

$$\{\mathcal{F}(f + \varphi_\alpha + \varepsilon),\, \alpha \in \boldsymbol{F}_2^m,\, \varepsilon \in \boldsymbol{F}_2\}.$$

The values of the extended Fourier spectrum are symmetric with respect to 0 since $\mathcal{F}(f + \varphi_\alpha + 1) = -\mathcal{F}(f + \varphi_\alpha)$.

Note that we are not only interested in the values appearing in these spectra, but also in the number of times they occur.

Definition 2: The *nonlinearity* of a function $f \in \mathcal{B}_m$ is the Hamming distance between f and the set of affine functions. It is given by

$$2^{m-1} - \frac{1}{2}\mathcal{L}(f), \qquad \mathcal{L}(f) = \max_{\alpha \in \boldsymbol{F}_2^m} |\mathcal{F}(f + \varphi_\alpha)|.$$

The nonlinearity of f is then the minimum Hamming weight of the coset $f + R(1, m)$. When m is even, it is known that the maximal value of this weight is $2^{m-1} - 2^{m/2-1}$ and that the extended Fourier spectrum of the functions having maximal nonlinearity is unique [7].

Definition 3: A Boolean function $f \in \mathcal{B}_m$, m even, is said to be *bent* when its nonlinearity is equal to $2^{m-1} - 2^{m/2-1}$. The extended Fourier spectrum of such a function consists of two values, $\pm 2^{m/2}$.

The Fourier spectrum of a Boolean function $f \in \mathcal{B}_m$ is strongly related to the properties of its derivatives. For any $a \in \boldsymbol{F}_2^m$, the *derivative of f with respect to a* is the function $D_a f \in \mathcal{B}_m$ defined by

$$D_a f(x) = f(x + a) + f(x).$$

For instance, it is well known that f is bent if and only if all its derivatives $D_a f$, $a \neq 0$ are balanced. The *linear space* of a Boolean function f is the subspace of those a such that $D_a f$ is a constant function. Such a nonzero a is said to be a *linear structure* for f.

Let E be any subset of $\boldsymbol{F}_2^m$. We denote by ϕ_E the Boolean function in $\mathcal{B}_m$ whose value on x is 1 if and only if $x \in E$; it is called *the indicator of E*.

For any two functions f and g in $\mathcal{B}_m$, the function fg corresponds to the usual product in $\mathcal{B}_m$: $fg(x) = 1$ if and only if $f(x) = g(x) = 1$. For any $f \in \mathcal{B}_m$, the function $f\phi_E$ is called *the restriction of f to E*. Note that $f\phi_E(x) = 1$ if and only if $f(x) = 1$ and $x \in E$. When V is a k-dimensional linear subspace of $\boldsymbol{F}_2^m$, the restriction of f to V, $f\phi_V$, can obviously be identified with a function of k variables. Similarly, for any coset $a + V$ of V, we identify $f\phi_{a+V}$ with $h \in \mathcal{B}_k$ as follows: $h(x) = f(x + a)$, $x \in V$. Note that the function $h \in \mathcal{B}_k$ associated with $f\phi_{a+V}$ is defined up to a translation $x \mapsto x + v$, $v \in V$. But all properties studied in the paper are invariant under translations.

Note: For any subspace V of dimension k, any basis of V can be completed providing a basis of $\boldsymbol{F}_2^m$. So $V \times W = \boldsymbol{F}_2^m$; the cosets of V are the flats $a + V$, a describing W.

Definition 4: Let $f \in \mathcal{B}_m$ and let V be a linear subspace of $\boldsymbol{F}_2^m$ of dimension k. The *decomposition of f with respect to V* is the sequence $\{f\phi_{a+V},\, a \in W\}$ where $V \times W = \boldsymbol{F}_2^m$ and all $f\phi_{a+V}$ are considered as Boolean functions in $\mathcal{B}_k$.

B. Main Formulas on the Restrictions

The following formulas will be intensively used in this paper. They are usually known but we give the proofs for clarity.

Proposition 1: Let $f \in \mathcal{B}_m$ and let V be a subspace of $\boldsymbol{F}_2^m$ of dimension k. Then

$$\sum_{v \in V^\perp} \mathcal{F}(f + \varphi_v) = 2^{m-k}\mathcal{F}(f\phi_V), \tag{1}$$

where the function ϕ_V is the indicator of V.

Moreover, for any $a \neq 0$, let $f \circ \tau_a$ be the Boolean function in $\mathcal{B}_m$ defined by $f \circ \tau_a(x) = f(x + a)$. Then

$$\sum_{v \in V^\perp} \mathcal{F}(f \circ \tau_a + \varphi_v) = 2^{m-k}\mathcal{F}(f\phi_{a+V}). \tag{2}$$

Proof: Recall that $\varphi_v(x) = x \cdot v$

$$\begin{aligned}\sum_{v \in V^\perp} \mathcal{F}(f + \varphi_v) &= \sum_{v \in V^\perp} \sum_{x \in \boldsymbol{F}_2^m} (-1)^{f(x) + \varphi_v(x)} \\ &= \sum_{x \in \boldsymbol{F}_2^m} (-1)^{f(x)} \sum_{v \in V^\perp} (-1)^{x \cdot v}.\end{aligned}$$

But $\sum_{v\in V^\perp}(-1)^{x\cdot v}=0$ unless $x\in V$; in this case, the sum is equal to 2^{m-k}. So

$$\sum_{v\in V^\perp}\mathcal{F}(f+\varphi_v)=2^{m-k}\sum_{x\in V}(-1)^{f(x)}=2^{m-k}\mathcal{F}(f\phi_V).$$

The second equation is obviously deduced, since $(f\circ\tau_a)\phi_V$ is exactly the restriction of f to the coset $a+V$. □

Formula (2) can be interpreted in several ways:

- it means that (1) holds up to any translation τ_a (note that many properties of a Boolean function are invariant under translation);
- formula (2) also provides an explicit relation between the Fourier spectrum of f and the weights of all its restrictions $f\phi_{a+V}$: for any $a\in\boldsymbol{F}_2^m$, we have

$$\sum_{v\in V^\perp}(-1)^{a\cdot v}\mathcal{F}(f+\varphi_v)=2^{m-k}\mathcal{F}(f\phi_{a+V}),$$

since

$$\mathcal{F}(f\circ\tau_a+\varphi_v)=\sum_{x\in\boldsymbol{F}_2^m}(-1)^{f(x+a)+x\cdot v}=(-1)^{a\cdot v}\mathcal{F}(f+\varphi_v).$$

The weights of the restrictions of f to V and to its cosets are also related to the Fourier spectrum of f by the following formula, which is proved in [1, Theorem V.1].

Proposition 2: Let $f\in\mathcal{B}_m$ and let V be a subspace of $\boldsymbol{F}_2^m$ of dimension k. Let W be such that $V\times W=\boldsymbol{F}_2^m$. Then

$$\sum_{v\in V^\perp}\mathcal{F}^2(f+\varphi_v)=2^{m-k}\sum_{a\in W}\mathcal{F}^2(f\phi_{a+V}).$$

Most notably, if f is a bent function

$$\sum_{a\in W}\mathcal{F}^2(f\phi_{a+V})=2^m.$$

C. The Dual Function

Since its Fourier transform takes two values only, any bent function has a *dual*.

Definition 5: Let f be a bent function of m variables. The *dual function* of f, denoted by $\tilde{f}$, is the Boolean function of m variables defined by

$$\mathcal{F}(f+\varphi_v)=2^{m/2}(-1)^{\tilde{f}(v)},\qquad v\in\boldsymbol{F}_2^m.$$

The duality of bent functions was introduced by Dillon [6]. It is easy to see that $\tilde{\tilde{f}}=f$, implying that $\tilde{f}$ is bent as well.

The following proposition shows that the action of a translation on a bent function corresponds to the addition of a linear function to its dual.

Proposition 3: Let f be a bent function of m variables. For any $a\in\boldsymbol{F}_2^m$, $f\circ\tau_a$ denotes the bent function $x\longmapsto f(x+a)$. Then, the dual of $f+\varphi_a$ is $\tilde{f}\circ\tau_a$. So the dual of $f\circ\tau_a$ is $\tilde{f}+\varphi_a$.

Proof: The result is easily deduced from the definition. Indeed

$$\mathcal{F}((f+\varphi_a)+\varphi_v)=2^{m/2}(-1)^{\tilde{f}(a+v)}$$

for all v. Then, $\widetilde{f+\varphi_a}=\tilde{f}\circ\tau_a$. By applying this relation to $\tilde{f}$, we obtain that the dual of $f\circ\tau_a$ is $\tilde{f}+\varphi_a$. □

Therefore, there is a symmetry between two sets of bent functions: the functions $f\circ\tau_a$ obtained by translating f are related to the bent functions $\tilde{f}+\varphi_a$ involved in the Fourier spectrum of $\tilde{f}$. This correspondence will be investigated in the next sections, concerning the restrictions of f and of $\tilde{f}$. On the other hand, there are some properties which are not satisfied by both f and $\tilde{f}$. We will see such situations concerning the derivatives of bent functions. There are also properties of $\tilde{f}$ which cannot be easily deduced from properties of f. The main open problem is the exact degree of $\tilde{f}$ when the degree of f is known. It is easy to prove that both degrees are equal when f has degree 2 or $m/2$. Otherwise, there is only a bound on the degree of $\tilde{f}$ [8].

D. Restrictions of a Bent Function to a Subspace of Large Dimension

The properties of the restrictions of a bent function to a subspace of codimension 1 and 2 (and to its cosets) have been investigated in [1]. This study points out the major role played by the functions whose extended Fourier spectrum takes on exactly three values. Such a function is called *three valued*.

Definition 6: A Boolean function f is said to be *three valued* if its extended Fourier spectrum takes on exactly three values, 0, $\mathcal{L}(f)$, and $-\mathcal{L}(f)$.

It is well known that the extended Fourier spectrum of a three-valued function is completely determined by its nonlinearity (see, e.g., [9, Theorem 2]). Here, we improve this result since we give the Fourier spectrum of such a function (i.e., the signs of the values $\mathcal{F}(f+\varphi_u)$ are also considered). Note that the following proposition includes both three-valued and bent functions.

Proposition 4: Let f be a Boolean function of m variables such that its extended Fourier spectrum takes at most three values, 0, $\mathcal{L}(f)$, and $-\mathcal{L}(f)$. Then, $\mathcal{L}(f)=2^s$ for some $s\geq m/2$ and f has the following Fourier spectrum:

$\mathcal{F}(f+\varphi_u)$	number of $u\in\boldsymbol{F}_2^m$
0	2^m-2^{2m-2s}
2^s	$2^{2m-2s-1}+(-1)^{f(0)}2^{m-s-1}$
-2^s	$2^{2m-2s-1}-(-1)^{f(0)}2^{m-s-1}$

Moreover, $s=m/2$ if and only if f is bent.

Proof: Set

$$L=\#\{u\in\boldsymbol{F}_2^m,\ \mathcal{F}(f+\varphi_u)\neq 0\}.$$

Parseval's relation implies that

$$L\cdot\mathcal{L}^2(f)=2^{2m},\qquad\text{with } L\leq 2^m.$$

Thus, we have $\mathcal{L}(f) = 2^s$ and $L = 2^r$ with $2s + r = 2m$ and $r \leq m$. We then obtain that $\mathcal{L}(f) = 2^s$ with $s = (2m - r)/2$. Note that $s \geq m/2$, since $r \leq m$.

Let L_+ (resp., L_-) denote the number of $u \in \boldsymbol{F}_2^m$ such that $\mathcal{F}(f + \varphi_u) = +2^s$ (resp., -2^s). Formula (1) leads to

$$\begin{aligned}\sum_{v \in \boldsymbol{F}_2^m} \mathcal{F}(f + \varphi_v) &= 2^m(-1)^{f(0)} \\ &= 2^s(L_+ - L_-) \\ &= 2^s(2L_+ - 2^{2m-2s}).\end{aligned}$$

Hence,

$$L_+ = 2^{2m-2s-1} + (-1)^{f(0)}2^{m-s-1}$$

providing

$$L_- = 2^{2m-2s-1} - (-1)^{f(0)}2^{m-s-1}. \qquad \square$$

For our purpose, the three-valued functions which have the highest possible nonlinearity are of most interest.

Definitiion 7: A three-valued Boolean function in $\mathcal{B}_m$ is called *three valued almost optimal* if $\mathcal{L}(f) = 2^{(m+1)/2}$ when m is odd, and $\mathcal{L}(f) = 2^{m/2+1}$ when m is even.

The *partially bent functions*, introduced by Carlet [10], are notably studied in [1]. These functions are three valued and could be almost optimal. We will say that such a function is a *partially bent optimal* function. In this paper, such a function, with an odd number of variables, will appear several times. So we recall the equivalent definitions (see [1, Proposition II.6 and Corollary V.4]).

Proposition 5: Let m be an odd integer, $m \geq 5$, and let $f \in \mathcal{B}_m$. Then f is *partially-bent optimal* if and only if it satisfies one of the following equivalent properties:

- **(i)** there is $b \neq 0$ such that $D_a f$ is balanced unless $a \in \{0, b\}$ and $D_b f$ is constant;
- **(ii)** f is three valued almost optimal and there is $b \neq 0$ such that $D_b f$ is constant.

The degree of f, when it is partially bent optimal, cannot exceed $\frac{m-1}{2}$.

The links between bent functions and three-valued almost optimal functions are described in [1, Theorems V.3 and V.4]; what we present here is in a slightly different form.

Theorem 1: Let m be an even integer $m \geq 4$, and let f be a bent function of m variables. Let H be any subspace of $\boldsymbol{F}_2^m$ of codimension 1, and let $\overline{H}$ denote $\boldsymbol{F}_2^m \setminus H$. Then, $f\phi_H$ and $f\phi_{\overline{H}}$ are three-valued almost optimal functions of $(m-1)$ variables and for any $u \in \boldsymbol{F}_2^{m-1}$, we have

$$\mathcal{F}^2(f\phi_H + \varphi_u) \neq \mathcal{F}^2(f\phi_{\overline{H}} + \varphi_u)$$

i.e., $\mathcal{F}^2(f\phi_H + \varphi_u) = 2^m$ if and only if $\mathcal{F}^2(f\phi_{\overline{H}} + \varphi_u) = 0$.

Theorem 2: Let m be an even integer $m \geq 4$, and let f be a bent function of m variables. Let V be any linear subspace $V \subset \boldsymbol{F}_2^m$ of codimension 2 and let $(f\phi_{a+V},\ a \in W)$ denote the decomposition of f with respect to V, with $W \times V = \boldsymbol{F}_2^m$.

Then, all the $f\phi_{a+V}$, $a \in W$, have the same extended Fourier spectrum: either all the $f\phi_{a+V}$ are bent, all the $f\phi_{a+V}$ are three valued almost optimal, or the $f\phi_{a+V}$ have the same extended Fourier spectrum with five values 0, $\pm 2^{(m-2)/2}$, $\pm 2^{m/2}$.

III. Links Between the Derivatives of a Bent Function and the Derivatives of its Dual

By definition, a bent function and its dual are related by their Fourier spectra. But the duality actually provides a closer link between a bent function and its dual. The next proposition shows that, in a certain sense, the Fourier spectrum of any derivative of a bent function f is linked with the values of the Fourier transforms of the derivatives of $\tilde{f}$. This is deduced from a simple observation. Note that for any fixed a we have for all u

$$\begin{aligned}\mathcal{F}(f + \varphi_{a+u})\mathcal{F}(f + \varphi_u) &= 2^m(-1)^{\tilde{f}(a+u)+\tilde{f}(u)} \\ &= 2^m(-1)^{D_a\tilde{f}(u)}. \qquad (3)\end{aligned}$$

This shows that the function $D_a\tilde{f}(u) = 1$ as many times as

$$\mathcal{F}(f + \varphi_{a+u}) = -\mathcal{F}(f + \varphi_u).$$

And this holds exactly 2^{m-1} times, since $D_a\tilde{f}(u)$ is balanced.

Proposition 6: Let f be a bent function of m variables and $\tilde{f}$ be its dual. Then, for any $a,\ b \in \boldsymbol{F}_2^m$, we have

$$\mathcal{F}\left(D_a\tilde{f} + \varphi_b\right) = \mathcal{F}(D_b f + \varphi_a).$$

Proof: We simply check the formula, by using (3): $\mathcal{F}(D_a\tilde{f} + \varphi_b)$ is equal to

$$\begin{aligned}&\sum_{u \in \boldsymbol{F}_2^m} (-1)^{D_a\tilde{f}(u)}(-1)^{b\cdot u} \\ &= 2^{-m} \sum_{u \in \boldsymbol{F}_2^m} \mathcal{F}(f + \varphi_{a+u})\mathcal{F}(f + \varphi_u)(-1)^{b\cdot u} \\ &= 2^{-m} \sum_{u \in \boldsymbol{F}_2^m} \sum_{x,\, y \in \boldsymbol{F}_2^m} (-1)^{f(x)+(a+u)\cdot x}(-1)^{f(y)+u\cdot y}(-1)^{b\cdot u} \\ &= 2^{-m} \sum_{x,\, y \in \boldsymbol{F}_2^m} (-1)^{f(x)+f(y)+a\cdot x} \sum_{u \in \boldsymbol{F}_2^m} (-1)^{u\cdot(x+y+b)} \\ &= \sum_{x \in \boldsymbol{F}_2^m} (-1)^{f(x)+f(x+b)+a\cdot x} \\ &= \mathcal{F}(D_b f + \varphi_a). \qquad \square\end{aligned}$$

Moreover, by applying Parseval's relation to $D_a\tilde{f}$ and according to Proposition 6, we obtain

$$\sum_{b \in \boldsymbol{F}_2^m} \mathcal{F}^2(D_b f + \varphi_a) = \sum_{b \in \boldsymbol{F}_2^m} \mathcal{F}^2\left(D_a\tilde{f} + \varphi_b\right) = 2^{2m}. \quad (4)$$

Actually we have more, as we explain now.

Corollary 1: Let a be any nonzero element of $\boldsymbol{F}_2^m$ and denote by H_a the hyperplane $\{0,\ a\}^\perp$. Then for any bent function f with m variables, we have

$$\sum_{b \in H_a} \mathcal{F}^2(D_b f + \varphi_a) = \sum_{b \in H_a} \mathcal{F}^2\left(D_a\tilde{f} + \varphi_b\right) = 2^{2m}.$$

Moreover, for $b \notin H_a$

$$\mathcal{F}(D_b f + \varphi_a) = \mathcal{F}\left(D_a\tilde{f} + \varphi_b\right) = 0.$$

Proof: Let us set $a \neq 0$ and note that we have

$$\sum_{b \in H_a} \mathcal{F}^2\left(D_a\tilde{f} + \varphi_b\right) = 2^{2m}$$

because this holds for any function $g \in \mathcal{B}_m$ which has a linear structure a such that $D_a g = 0$. Indeed, for such a function g, we obtain (see [1, Remark V.1])

$$\sum_{b \in H_a} \mathcal{F}^2(g+\varphi_b) = 2^{m-1}(\mathcal{F}(D_0 g) + \mathcal{F}(D_a g)) = 2^{2m}$$

since $\mathcal{F}(D_a g) = 2^m$. Thus, we have, according to (4)

$$\sum_{b \notin H_a} \mathcal{F}^2\left(D_a \tilde{f} + \varphi_b\right) = \sum_{b \notin H_a} \mathcal{F}^2(D_b f + \varphi_a) = 0$$

completing the proof. □

Note that, by applying Proposition 1, we have for any b

$$\mathcal{F}(D_b f) + \mathcal{F}(D_b f + \varphi_a) = 2\mathcal{F}((D_b f)\phi_{H_a})$$

where $\mathcal{F}(D_b f) = 0$, for $b \neq 0$, since f is bent. According to Corollary 1, we obtain, for any any $b \notin H_a$

$$2\mathcal{F}((D_b f)\phi_{H_a}) = \mathcal{F}(D_b f + \varphi_a) = 0.$$

Thus, we have proved the following property of derivatives of bent functions.

Theorem 3: Let f be any bent function of m variables. Let H be any hyperplane of $\boldsymbol{F}_2^m$. Then, for any $b \notin H$, the derivative $D_b f$ is such that its restrictions to H and to $\boldsymbol{F}_2^m \backslash H$ are balanced.

IV. Bent Functions With Affine Derivatives

The previous relationship between the derivatives of a bent function and the derivatives of its dual is of most interest for the bent functions which have at least one affine derivative. We now prove that a bent function has an affine derivative if and only if its dual has an affine derivative.

Corollary 2: Let f be a bent function of m variables. Let a and b be two nonzero elements in $\boldsymbol{F}_2^m$ and $\varepsilon \in \boldsymbol{F}_2$. Then, the following properties are equivalent.

- **(i)** $D_b f = \varphi_a + \varepsilon$.
- **(ii)** $D_a \tilde{f} = \varphi_b + \varepsilon$.
- **(iii)** The function $f\phi_{H_a}$, considered as a function of $(m-1)$ variables, is partially bent optimal with linear space $\{0, b\}$, where H_a denotes the hyperplane $\{0, a\}^{\perp}$.

Proof:

(i) ⇔ (ii): Applying Proposition 6, for b such that $D_b f$ is affine ($D_b f = \varphi_a + \varepsilon$), it appears that

$$\mathcal{F}\left(D_a \tilde{f} + \varphi_b\right) = \mathcal{F}(D_b f + \varphi_a) = (-1)^{\varepsilon} 2^m.$$

This means that $D_a \tilde{f} = \varphi_b + \varepsilon$.

(i) ⇒ (iii): Note that $D_b f = \varphi_a + \varepsilon$ implies that $b \in H_a$; otherwise, $D_b D_b f = a \cdot b = 1$, a contradiction. Let $g = f\phi_{H_a}$. Then, for any $\alpha \in H_a$, we have $D_\alpha g = (D_\alpha f)\phi_{H_a}$. For $\alpha = b$, we obtain

$$D_b g = (\varphi_a + \varepsilon)\phi_{H_a} = \varepsilon$$

i.e., b is a linear structure of g. Since g is three valued almost optimal (Theorem 1), we deduce that g is partially bent optimal. Moreover, its linear space is exactly $\{0, b\}$ (see Proposition 5).

(iii) ⇒ (i): Suppose that b is a linear structure of g, i.e., $D_b g = \varepsilon$. Since $b \in H_a$, we have

$$(D_b f)\phi_{H_a} = D_b g = \varepsilon.$$

Moreover

$$\mathcal{F}(D_b f) = \mathcal{F}((D_b f)\phi_{H_a}) + \mathcal{F}((D_b f)\phi_{\overline{H}_a}) = 0$$

since $D_b f$ is balanced. Therefore, $(D_b f)\phi_{\overline{H}_a} = \varepsilon + 1$. This implies that $D_b f = \varphi_a + \varepsilon$. □

Hou proved in [2] that for $m = 8$ any cubic bent function in $\mathcal{B}_m$ has at least one derivative in $R(1, m)$. This property does not hold for $m = 6$ [7]. This observation leads to the following open question formulated by Hou [2]: for what values of m do there exist cubic bent functions of m variables which has no derivative in $R(1, m)$?

The following lemma enables us to completely solve this problem. In the remainder of this section, $\boldsymbol{F}_2^{\frac{m}{2}}$ is identified with the finite field with $2^{m/2}$ elements $\boldsymbol{F}_{2^{\frac{m}{2}}}$.

Lemma 1: Let $m = 2t$ be an even integer $m \geq 6$, and let i be an integer such that $1 \leq i < t$ and $\gcd(2^i + 1, 2^t - 1) = 1$. The cubic bent function of m variables defined by

$$\begin{aligned} f: \quad \boldsymbol{F}_{2^t} \times \boldsymbol{F}_{2^t} &\to \boldsymbol{F}_2 \\ (x, y) &\mapsto \mathrm{Tr}\,(xy^{2^i+1}) \end{aligned}$$

where Tr is the trace function from $\boldsymbol{F}_{2^t}$ to $\boldsymbol{F}_2$, has no derivative in $R(1, m)$.

Proof: The power function $x \mapsto x^{2^i+1}$ is a permutation of $\boldsymbol{F}_{2^t}$ since $\gcd(2^i + 1, 2^t - 1) = 1$. Then, it is well known that f is bent; it belongs to the family $\mathcal{M}$ and has degree 3 (see Section VII-B). We consider the derivative of such a function f in direction (a, b)

$$\begin{aligned} D_{(a,b)} f &= \mathrm{Tr}(xy^{2^i+1}) + \mathrm{Tr}((x+a)(y+b)^{2^i+1}) \\ &= \mathrm{Tr}\left(ay^{2^i+1} + (x+a)(by^{2^i} + b^{2^i}y + b^{2^i+1})\right). \end{aligned}$$

When $a \neq 0$, it is clear that $D_{(a,b)} f$ is quadratic, since $\mathrm{Tr}(ay^{2^i+1})$ cannot be constant. On the other hand, we have for every $b \neq 0$

$$D_{(0,b)} f = \mathrm{Tr}\left(x(by^{2^i} + b^{2^i}y + b^{2^i+1})\right).$$

Therefore, $D_{(0,b)} f$ is affine if and only if the function $y \mapsto by^{2^i} + b^{2^i}y + b^{2^i+1}$ is constant. This means that for any $y \in \boldsymbol{F}_{2^t}^*$

$$by^{2^i} + b^{2^i}y + b^{2^i+1} = b^{2^i+1}, \tag{5}$$

or equivalently

$$y^{2^i-1} = b^{2^i-1}.$$

It follows that yb^{-1} belongs to the subfield of $\boldsymbol{F}_{2^t}$ of order $2^{\gcd(i,t)}$. Therefore, the number of solutions y of (5) is exactly $2^{\gcd(i,t)} < 2^t$ because $i < t$. So such a function f is a cubic bent function which has no derivative in $R(1, m)$. □

Now, we use the previous infinite family of cubic bent functions for proving the following theorem.

Theorem 4: Let m be an even integer $m \geq 6$. There exists a cubic bent function of m variables which has no derivative in $R(1, m)$ if and only if $m \neq 8$.

Proof: Since all cubic bent functions of eight variables have a derivative in $R(1, 8)$ [2], we only need to exhibit a cubic bent function of m variables which has no derivative in $R(1, m)$ for any even $m \geq 6$, $m \neq 8$.

Let $m = 2t$. First, we prove that there exists an integer i such that $1 \leq i < t$ and $\gcd(2^i + 1, 2^t - 1) = 1$ if and only if t is not a power of 2. Recall that $\gcd(2^i + 1, 2^t - 1) = 1$ if and only if $\frac{t}{\gcd(i,t)}$ is odd. Then, if t is not a power of 2, we have $t = 2^r s$ where $r \geq 0$ and s is an odd integer $s \geq 3$. In that case, $i = 2^r$ satisfies the previous condition since $\frac{t}{\gcd(i,t)} = s$ is odd and $i < t$. We then deduce from Lemma 1 that there exists a cubic bent function of m variables which has no derivative in $R(1, m)$ when m is not a power of 2 .

Suppose now that $t = 2^r$ with $r \geq 3$ since $t \geq 3$ and $t \neq 4$. Let $t_1 = 2^{r-1} - 1$ and $t_2 = 2^{r-1} + 1$. Since $r \geq 3$, $t_2 > t_1 > 2$ and neither t_1 nor t_2 is a power of 2. Then, there exist two integers i_1 and i_2 such that

$$1 \leq i_1 < t_1, \qquad \gcd(2^{i_1} + 1, 2^{t_1} - 1) = 1$$

and

$$1 \leq i_2 < t_2, \qquad \gcd(2^{i_2} + 1, 2^{t_2} - 1) = 1.$$

Therefore, the following cubic function f of m variables is bent: for any $x = (x_1, y_1, x_2, y_2)$, $x \in \boldsymbol{F}_{2^{t_1}} \times \boldsymbol{F}_{2^{t_1}} \times \boldsymbol{F}_{2^{t_2}} \times \boldsymbol{F}_{2^{t_2}}$

$$f(x) = \mathrm{Tr}^{(t_1)}(x_1 y_1^{2^{i_1}+1}) + \mathrm{Tr}^{(t_2)}(x_2 y_2^{2^{i_2}+1})$$

where $\mathrm{Tr}^{(t_1)}$ (resp., $\mathrm{Tr}^{(t_2)}$) is the trace function from $\boldsymbol{F}_{2^{t_1}}$ (resp., $\boldsymbol{F}_{2^{t_2}}$) into $\boldsymbol{F}_2$ (see [6, Remark 6.2.16]). Moreover, Lemma 1 implies that f has no derivative in $R(1, m)$. □

V. Restrictions of a Bent Function and of its Dual to Subspaces

We now focus on the links between the restriction of a bent function to a subspace and the restrictions of its dual. Throughout this section, f is a bent function with dual $\tilde{f}$. The next theorem is a generalization of a remark of Dillon [6, Remark 6.2.14] and was proved by Carlet in [4, Lemma 1].

Theorem 5: Let f be a bent function of m variables and let V be any subspace of $\boldsymbol{F}_2^m$ of dimension k. Then

$$\mathcal{F}(f\phi_{V^\perp}) = 2^{m/2-k}\mathcal{F}\left(\tilde{f}\phi_V\right). \tag{6}$$

More generally, we have for any $a \in \boldsymbol{F}_2^m$

$$\mathcal{F}((f + \varphi_a)\phi_{V^\perp}) = 2^{m/2-k}\mathcal{F}\left(\tilde{f}\phi_{a+V}\right). \tag{7}$$

Proof: In accordance with Definition 5 and Proposition 1, we have

$$\begin{aligned}\sum_{v\in V} \mathcal{F}(f + \varphi_v) &= 2^{m/2}\sum_{v\in V}(-1)^{\tilde{f}(v)} \\ &= 2^k \mathcal{F}(f\phi_{V^\perp}) \\ &= 2^{m/2}\mathcal{F}\left(\tilde{f}\phi_V\right).\end{aligned}$$

Moreover, for any $a \in \boldsymbol{F}_2^m$

$$\begin{aligned}\sum_{v\in V} \mathcal{F}(f + \varphi_{a+v}) &= 2^{m/2}\sum_{v\in V}(-1)^{\tilde{f}(a+v)} \\ &= 2^k \mathcal{F}((f + \varphi_a)\phi_{V^\perp}) \\ &= 2^{m/2}\mathcal{F}\left(\tilde{f}\phi_{a+V}\right)\end{aligned}$$

since the restriction of the function $x \mapsto \tilde{f}(x + a)$ to V is the restriction of $\tilde{f}$ to the coset $a + V$. Note that when $a \in V$ we obtain the first formula again. □

Remark 1: Let V be a linear subspace of $\boldsymbol{F}_2^m$ of dimension k and let W be such that $V \times W = \boldsymbol{F}_2^m$. The Fourier spectrum of the $(m - k)$-variable function $f\phi_{V^\perp}$ corresponds to the set

$$\{\mathcal{F}((f + \varphi_u)\phi_{V^\perp}),\ u \in W\}.$$

This comes from the fact that, for any $(u_1, u_2) \in V \times W$ and for any $x \in V^\perp$

$$\varphi_{(u_1,u_2)}(x) = \varphi_{u_1}(x) + \varphi_{u_2}(x) = \varphi_{u_2}(x).$$

Therefore, $\varphi_{(u_1,u_2)}\phi_{V^\perp} = \varphi_{u_2}\phi_{V^\perp}$. In this context, the previous proposition means that the knowledge of the Fourier spectrum of $f\phi_{V^\perp}$ is equivalent to the knowledge of the weights of the restrictions $\tilde{f}\phi_{a+V}$, $a \in W$, where $(\tilde{f}\phi_{a+V},\ a \in W)$ is the decomposition of $\tilde{f}$ with respect to V.

Many properties can be directly deduced from Theorem 5. For instance, we have

- f is balanced on $V^\perp$ if and only if $\tilde{f}$ is balanced on V;
- $\mathcal{F}(f\phi_{V^\perp}) = \mathcal{F}(\tilde{f}\phi_V)$ for any V of dimension $m/2$. Most notably, the restriction of f to $V^\perp$ is constant if and only if the restriction of $\tilde{f}$ to V is constant too (and the constants take the same value in both cases). This property is related to the concept of *normality* [5], [11], [12] [1, Corollary V.3].

Corollary 3: Let f be a bent function of m variables. Let V be a linear subspace of $\boldsymbol{F}_2^m$ of dimension $k \geq m/2$ and let $(\tilde{f}\phi_{a+V},\ a \in W)$ denote the decomposition of $\tilde{f}$ with respect to V where $V \times W = \boldsymbol{F}_2^m$. Then f is constant on $V^\perp$ if and only if

$$\mathcal{F}\left(\tilde{f}\phi_V\right) = \mathcal{F}\left(\tilde{f}\right)$$

and

$$\mathcal{F}\left(\tilde{f}\phi_{a+V}\right) = 0, \qquad \forall\, a \in W \setminus \{0\}. \tag{8}$$

Proof: "f is constant on $V^\perp$" means that $\mathcal{F}(f\phi_{V^\perp}) = \pm 2^{m-k}$. From Theorem 5, f is constant on $V^\perp$ if and only if

$$\mathcal{F}\left(\tilde{f}\phi_V\right) = \pm 2^{m-k-m/2+k} = \pm 2^{m/2}.$$

By applying Proposition 2 to $\tilde{f}$, we deduce that

$$\begin{aligned}\sum_{a\in W} \mathcal{F}^2\left(\tilde{f}\phi_{a+V}\right) &= 2^m + \sum_{a\in W\setminus\{0\}} \mathcal{F}^2\left(\tilde{f}\phi_{a+V}\right) \\ &= 2^m.\end{aligned}$$

Therefore, $\mathcal{F}(\tilde{f}\phi_{a+V}) = 0$ for all nonzero a in W. This implies that

$$\mathcal{F}\left(\tilde{f}\right) = \sum_{a\in W} \mathcal{F}\left(\tilde{f}\phi_{a+V}\right) = \mathcal{F}\left(\tilde{f}\phi_V\right).$$

Conversely, if (8) is satisfied then $\mathcal{F}(\tilde{f}\phi_V) = \pm 2^{m/2}$ (since $\tilde{f}$ is bent) completing the proof. □

Now, we deduce some connections between constant kth derivatives of $\tilde{f}$ and the divisibility of the values occurring in the Fourier spectra of the restrictions of f.

Definition 8: Let V be a k-dimensional subspace of $\boldsymbol{F}_2^m$. The kth derivative of $f \in \mathcal{B}_m$ with respect to V is the function

$$D_V f = D_{a_1} D_{a_2} \cdots D_{a_k} f$$

where $(a_1, \ldots, a_k)$ is any basis of V.

Notation $D_V f$ is used for simplicity since the kth derivative of $f \in \mathcal{B}_m$ with respect to V does not depend on the choice of the basis of V. The following lemma, which corresponds to [1, Lemma III.1] with a different formulation, provides a relationship between the decomposition of a function with respect to a k-dimensional subspace and the corresponding kth derivative.

Lemma 2: Let f be a Boolean function with m variables. Let V be a linear subspace of $\boldsymbol{F}_2^m$ of dimension k and let $(f\phi_{a+V}, a \in W)$ denote the decomposition of f with respect to V, where $V \times W = \boldsymbol{F}_2^m$. Then

$$\mathrm{wt}(D_V f) = 2^k \#\{a \in W | \mathrm{wt}(f\phi_{a+V}) \text{ is odd}\}.$$

Proof: By definition, we have for any $x \in \boldsymbol{F}_2^m$

$$D_V f(x) = \sum_{v \in V} f(x+v)$$

where the preceding sum is an addition modulo 2. This relation implies that, for any $x \in \boldsymbol{F}_2^m$ and for any $v \in V$, $D_V f(x+v) = D_V f(x)$. Moreover, for any $a \in W$, we have

$$D_V f(a) = \sum_{v \in V} f(a+v) = \mathrm{wt}(f\phi_{a+V}) \bmod 2.$$

Therefore, we deduce

$$\begin{aligned}\mathrm{wt}(D_V f) &= 2^k \#\{a \in W,\, D_V f(a) = 1\} \\ &= 2^k \#\{a \in W,\, \mathrm{wt}(f\phi_{a+V}) \text{ is odd}\}.\end{aligned}$$ □

Theorem 6: Let f be a bent function of m variables and let V be a linear subspace of $\boldsymbol{F}_2^m$ of dimension $k \le m/2$. Then

- **(i)** $D_V \tilde{f} = 1$ if and only if the values occurring in the Fourier spectrum of $f\phi_{V^\perp}$ are of the form $\pm 2^{m/2-k+1}\lambda$ where λ is an odd integer which belongs to the interval $[1, 2^{k-1} - 1]$;
- **(ii)** $D_V \tilde{f} = 0$ if and only if the values occurring in the Fourier spectrum of $f\phi_{V^\perp}$ are of the form $\pm 2^{m/2-k+2}\lambda$ where λ is some integer which belongs to the interval $[0, 2^{k-2}]$.

Proof: Let $(\tilde{f}\phi_{a+V}, a \in W)$ denote the decomposition of $\tilde{f}$ with respect to V, where $V \times W = \boldsymbol{F}_2^m$. The previous lemma implies that

- $D_V \tilde{f} = 1$ if and only if $\mathrm{wt}(\tilde{f}\phi_{a+V})$ is odd for any $a \in W$;
- $D_V \tilde{f} = 0$ if and only if $\mathrm{wt}(\tilde{f}\phi_{a+V})$ is even for any $a \in W$.

Since $\mathcal{F}(\tilde{f}\phi_{a+V}) = 2^k - 2\mathrm{wt}(\tilde{f}\phi_{a+V})$, $\mathrm{wt}(\tilde{f}\phi_{a+V})$ is odd if and only if the value $\mathcal{F}(\tilde{f}\phi_{a+V})/2$ is odd. Note that $\tilde{f}\phi_{a+V}$ is a function in $\mathcal{B}_k$; thus, the value $|\mathcal{F}(\tilde{f}\phi_{a+V})|$ lies in the interval $[0, 2^k]$.

Therefore, we have $D_V \tilde{f} = 1$ if and only if $\mathcal{F}(\tilde{f}\phi_{a+V}) = \pm 2\lambda_a$ where λ_a is an odd integer and λ_a is in $[1, 2^{k-1} - 1]$, for all $a \in W$. According to (7), we obtain for every $a \in W$

$$\mathcal{F}((f + \varphi_a)\phi_{V^\perp}) = \pm 2^{m/2-k+1}\lambda_a.$$

This provides the complete Fourier spectrum of $f\phi_{V^\perp}$ according to Remark 1.

Similarly, $D_V \tilde{f} = 0$ if and only if $\mathcal{F}(\tilde{f}\phi_{a+V}) = \pm 4\lambda_a$, for all $a \in W$, where λ_a is an integer in $[0, 2^{k-2}]$. Hence,

$$\mathcal{F}((f + \varphi_a)\phi_{V^\perp}) = \pm 2^{m/2-k+2}\lambda_a.$$ □

Suppose that $\tilde{f}$ is of degree k. Then there is at least one V of dimension k such that $D_V \tilde{f} = 1$. This is a consequence of the definition of Reed–Muller codes (see [1, Proposition III.1]). Consider the function $g = f\phi_{V^\perp}$ of $m - k$ variables. From Theorem 6, g is such that its Fourier spectrum does not contain 0—i.e., there is no balanced function in the spectrum of g. Note that such a subspace V can be easily determined by using, for instance, the algebraic normal form of $\tilde{f}$. We have proved the following property.

Proposition 7: Let $f \in \mathcal{B}_m$ be a bent function such that its dual $\tilde{f}$ has degree k. Then there is a subspace V of $\boldsymbol{F}_2^m$ of dimension k such that the function $g = f\phi_{V^\perp}$, viewed as a Boolean function in $\mathcal{B}_{m-k}$, satisfies the following: for all u in $\boldsymbol{F}_2^{m-k}$ the function $g + \varphi_u$ is not balanced.

Example 1: Let f be a bent function with m variables $m \ge 6$, such that $\tilde{f}$ is of degree 3 and let $V = \langle e_1, e_2, e_3 \rangle$ such that $D_{e_1} D_{e_2} D_{e_3} \tilde{f} = 1$. Then $V^\perp$ has codimension 3 and the function $g = f\phi_{V^\perp}$ is a function of $m-3$ variables. According to Theorem 6, the values occurring in the Fourier spectrum of g are of the form

$$\pm 2^{m/2-2}\lambda, \qquad \lambda \in \{1, 3\}.$$

Moreover, both values of λ appear, since the only functions whose extended Fourier spectrum takes two values are the bent functions (g cannot be bent because it depends on an odd number of variables). The extended Fourier spectrum of g is then completely determined. Indeed, setting

$$N_1 = \#\{u, |\mathcal{F}(g + \varphi_u)| = 2^{m/2-2}\}$$

and

$$N_3 = \#\{u, |\mathcal{F}(g + \varphi_u)| = 3 \cdot 2^{m/2-2}\}$$

we have

$$\begin{aligned}\sum_{u \in \boldsymbol{F}_2^{m-3}} \mathcal{F}^2(g + \varphi_u) &= 2^{m-4}(N_1 + 9N_3) \\ &= 2^{m-4}(2^{m-3} + 8N_3) \\ &= 2^{2(m-3)}.\end{aligned}$$

Therefore, we have

$\lvert\mathcal{F}(g+\varphi_u)\rvert$	number of $u \in \boldsymbol{F}_2^{m-3}$
$2^{m/2-2}$	$2^{m-3} - 2^{m-6}$
$3 \cdot 2^{m/2-2}$	2^{m-6}

VI. Decompositions of a Bent Function Into Four Functions

Now, we focus on the restrictions of a bent function to subspaces of codimension 2. We first observe what Theorem 1 means when subspaces of codimension 1 are considered. Let H be such a subspace, f a bent function in $\mathcal{B}_m$, and $H^\perp = \{0, a\}$. Then, we have for any $u \in \boldsymbol{F}_2^m$

$$\mathcal{F}((f+\varphi_u)\phi_H) = 2^{m/2-1}\left((-1)^{\tilde{f}(u)} + (-1)^{\tilde{f}(u+a)}\right). \quad (9)$$

Moreover, we know from Theorem 1 that the restrictions of f to H and to $\boldsymbol{F}_2^m \setminus H$, say (f_1, f_2), are three valued almost optimal and satisfy: $\mathcal{F}^2(f_1+\xi) = 2^m$ if and only if $\mathcal{F}^2(f_2+\xi) = 0$, where ξ is any linear function in $\mathcal{B}_{m-1}$.

Let W be of codimension 1 such that $\boldsymbol{F}_2^m = \{0, a\} \times W$. According to Remark 1, the values of the Fourier spectrum of f_1 are

$$\mathcal{F}((f+\varphi_u)\phi_H), \qquad u \in W$$

and the decomposition of $\tilde{f}$ with respect to $\{0, a\}$ is

$$\left(\tilde{f}\phi_{u+\{0,a\}},\, u \in W\right).$$

By applying (9), it appears that for any $u \in W$

- **(i)** $\tilde{f}(u) \neq \tilde{f}(u+a)$ if and only if $\mathcal{F}(f_1+\varphi_u) = 0$—so $\mathcal{F}(f_2+\varphi_u) = (-1)^{\tilde{f}(u)}2^{m/2}$;
- **(ii)** $\tilde{f}(u) = \tilde{f}(u+a)$ if and only if $\mathcal{F}(f_1+\varphi_u) = (-1)^{\tilde{f}(u)}2^{m/2}$—in this case, $\mathcal{F}(f_2+\varphi_u) = 0$.

Note that the first case corresponds to the cosets $u+\{0, a\}$ on which $\tilde{f}$ has weight 1. This situation occurs exactly 2^{m-2} times because $D_a\tilde{f}$ is balanced (see Lemma 2).

Remark 2: The bent function $\tilde{f}$ is such that $D_a\tilde{f}$ is affine if and only if the union of the cosets $u+\{0, a\}$ corresponding to **(i)** is an affine hyperplane. The result of Hou [2] can be expressed as follows: when $m = 8$ and $\tilde{f}$ is cubic then this property holds for some H. We have proved that it is not true for other m (see Theorem 4).

Now, for the study of the decompositions into four functions we need to fix the terminology. Recall that the four functions involved in the decomposition of a bent function with respect to a subspace of codimension 2 have the same extended Fourier spectrum (cf. Theorem 2).

Definition 9: Let $f \in \mathcal{B}_m$. We call 4-*decomposition* of f a decomposition with respect to some subspace of codimension 2.

Let $(f_1, \ldots, f_4)$ be such a decomposition. We say that it is a *bent* 4-*decomposition* when all f_i are bent; when all f_i are three valued almost optimal, we say that it is a *three-valued almost optimal* 4-*decomposition* of f.

Theorem 7: Let f be a bent function of m variables, $m \geq 4$, and $\tilde{f}$ its dual. Let a and b be two nonzero distinct elements of $\boldsymbol{F}_2^m$, $V = \langle a, b\rangle^\perp$ and let us denote by $(f_1, \ldots, f_4)$ the 4-decomposition of f with respect to V. Then, all f_i, $1 \leq i \leq 4$ have the following Fourier spectrum:

$\lvert\mathcal{F}(f_i+\varphi_u)\rvert$	number of $u \in \boldsymbol{F}_2^{m-2}$
0	$3(2^{m-4} - 2^{-4}\lambda)$
$2^{(m-2)/2}$	$\lambda/4$
$2^{m/2}$	$2^{m-4} - 2^{-4}\lambda$

where $\lambda = \mathrm{wt}(D_aD_b\tilde{f})$.

Most notably, $(f_1, \ldots, f_4)$ is

- a bent 4-decomposition if and only if $D_aD_b\tilde{f} = 1$;
- a three-valued almost optimal 4-decomposition if and only if $D_aD_b\tilde{f} = 0$.

Proof: We know from Theorem 2 that all the f_i have the same Fourier spectrum. So we only consider $f_1 = f\phi_V$. Let $(\tilde{f}\phi_{u+\langle a,b\rangle},\, u \in W)$ be the decomposition of $\tilde{f}$ with respect to $\langle a, b\rangle$, where $\langle a, b\rangle \times W = \boldsymbol{F}_2^m$. The Fourier spectrum of f_1 consists of all $\mathcal{F}(f_1+\varphi_u\phi_V)$, $u \in W$. We denote by ξ_u the restriction of φ_u to V.

By applying Theorem 5 for $k = 2$, we obtain for all $u \in W$

$$\mathcal{F}(f_1+\xi_u) = 2^{m/2-2}\mathcal{F}\left(\tilde{f}\phi_{u+\langle a,b\rangle}\right). \quad (10)$$

Then, the right-hand term of (10) involves the weight of the restriction of $\tilde{f}$ on a coset of $\langle a, b\rangle$. Since $\tilde{f}\phi_{u+\langle a,b\rangle}$ is a function of two variables, its weight is

- either 2 implying $\mathcal{F}(f_1+\xi_u) = 0$;
- or in $\{0, 4\}$ implying $\mathcal{F}(f_1+\xi_u) = \pm 2^{m/2}$;
- or in $\{1, 3\}$ implying $\mathcal{F}(f_1+\xi_u) = \pm 2^{(m-2)/2}$.

We denote by L_1 the number of cosets of $\langle a, b\rangle$ which correspond to the values $\pm 2^{(m-2)/2}$ and by L_2 the number of cosets of $\langle a, b\rangle$ which correspond to the values $\pm 2^{m/2}$. Lemma 2 implies that

$$4L_1 = \mathrm{wt}(D_aD_b\tilde{f}).$$

Now, by using Parseval's formula, we get

$$\sum_{u\in W} \mathcal{F}^2(f_1+\xi_u) = 2^{2(m-2)} = 2^mL_2 + 2^{m-2}L_1$$

providing $L_2 = 2^{m-4} - 2^{-2}L_1$. Thereby, the number of cosets of $\langle a, b\rangle$ on which $\tilde{f}$ is balanced is equal to $2^{m-2} - L_1 - L_2$, that is,

$$3 \cdot 2^{m-4} - L_1(1 - 2^{-2}) = 3(2^{m-4} - 2^{-2}L_1).$$

Therefore, the Fourier spectrum of f_1 only depends on $\mathrm{wt}(D_aD_b\tilde{f})$. In particular, we obtain that f_1 is bent if and only if $\mathrm{wt}(D_aD_b\tilde{f}) = 2^m$, i.e., $D_aD_b\tilde{f} = 1$. Similarly, f_1 is three valued almost optimal if and only if $\mathrm{wt}(D_aD_b\tilde{f}) = 0$, i.e., $D_aD_b\tilde{f} = 0$. □

The previous theorem implies that for any bent function $f \in \mathcal{B}_m$ and any nonzero a and b, $a \neq b$, the weight of D_aD_bf is divisible by 2^4. This property can be directly deduced from the fact that the degree of f does not exceed $m/2$. It can be generalized as follows.

Proposition 8: Let $f \in \mathcal{B}_m$ be such that $\deg(f) \leq m/2$. Then, the weight of any kth derivative of f is divisible by 2^{k+2}.

Proof: Let $V \in \boldsymbol{F}_2^m$ be a linear subspace of dimension k, $k \geq 1$, and let W be such that $V \times W = \boldsymbol{F}_2^m$. Then, for any $x \in \boldsymbol{F}_2^m$ and any $v \in V$, we have $D_V f(x+v) = D_V f(x)$. Therefore, $\mathrm{wt}(D_V f) = 2^k \mathrm{wt}(g)$ where g denotes the restriction of $D_V f$ to W. Then, g is a Boolean function of $m-k$ variables and its degree cannot exceed the degree of $D_V f$, which is at most $\deg(f) - k \leq m/2 - k$. Using that $g \in R(m/2-k, m-k)$, we deduce that its weight is divisible by 2^ℓ with

$$\ell = \left\lfloor \frac{m-k-1}{\frac{m}{2}-k} \right\rfloor \geq 2$$

[13, p. 447], because $m - k - 1 \geq 2(\frac{m}{2} - k)$. □

When f is quadratic, its dual is quadratic as well. Moreover, all second derivatives of f are constant. So, *if f is bent and quadratic, any 4-decomposition of f is either bent or three valued almost optimal*. This property becomes more complicated for higher degrees. The following corollaries are devoted to those f which have a cubic dual.

Corollary 4: Let f be a bent function with m variables, $m \geq 4$, such that $\tilde{f}$ has degree 3. Let a and b be two nonzero distinct elements of $\boldsymbol{F}_2^m$, $V = \langle a, b\rangle^\perp$ and let us denote by $(f_1, \ldots, f_4)$ the 4-decomposition of f with respect to V. Then, one of the following three situations occurs:

- $(f_1, \ldots, f_4)$ is a bent 4-decomposition if and only if $D_a D_b \tilde{f} = 1$;
- $(f_1, \ldots, f_4)$ is a three-valued almost optimal 4-decomposition if and only if $D_a D_b \tilde{f} = 0$;
- all f_i have the following Fourier spectrum:

$\lvert\mathcal{F}(f_i + \varphi_u)\rvert$	number of $u \in \boldsymbol{F}_2^{m-2}$
0	$3 \cdot 2^{m-5}$
$2^{(m-2)/2}$	2^{m-3}
$2^{m/2}$	2^{m-5}

if and only if $D_a D_b \tilde{f}$ is not constant.

Proof: The result is directly deduced from Theorem 7, since any second derivative $D_a D_b \tilde{f}$ is either constant or balanced, when $\tilde{f}$ has degree 3. □

Moreover, we can prove that all the three situations which are described in the previous corollary occur.

Corollary 5: Let $f \in \mathcal{B}_m$ be a bent function such that $\tilde{f}$ is of degree 3. Then f has more than $(2^m - 1)/3$ bent 4-decomposition and at least one three-valued almost optimal 4-decomposition.

Proof: Since $\tilde{f}$ is cubic, it satisfies for any $a \neq 0$: $D_a \tilde{f}$ is balanced if and only if there is $b \in \boldsymbol{F}_2^m$ such that $D_b D_a \tilde{f} = 1$ (see [1, Proposition A.1]). Since $\tilde{f}$ is bent, each derivative of $\tilde{f}$ is balanced. Thus, for any $a \neq 0$, there is $b \neq a \neq 0$ such that the decomposition of f with respect to $\langle a, b\rangle^\perp$ is a bent 4-decomposition (from Theorem 7).

Now, we prove that $\tilde{f}$ has at least one null second derivative. We denote by $\mathcal{U}$ the set of all subspaces $\langle a, b\rangle$ of dimension 2 such that $D_b D_a \tilde{f} = 1$. Since a describes $\boldsymbol{F}_2^m$, then $\boldsymbol{F}_2^m = \bigcup_{U \in \mathcal{U}} U$ and the cardinality of $\mathcal{U}$ is minimal when any pair (U, U') of distinct elements of $\mathcal{U}$ satisfies $U \cap U' = \{0\}$. Suppose first that this situation occurs. In this case, the sets $U \setminus \{0\}$, $U \in \mathcal{U}$, form a partition of $\boldsymbol{F}_2^m \setminus \{0\}$. Therefore, $\mathcal{U}$ contains exactly $(2^m - 1)/3$ elements. According to Lemma 2, the weight of the function $\tilde{f}\phi_U$ is odd, for any $U \in \mathcal{U}$ (it is either 1 or 3). Assuming that $\tilde{f}(0) = 0$, we obtain

$$\mathrm{wt}(\tilde{f}) = \sum_{U \in \mathcal{U}} (1 + 2\varepsilon_U), \qquad \varepsilon_U \in \{0, 1\}$$

which implies

$$\mathrm{wt}(\tilde{f}) = \frac{2^m - 1}{3} + 2\lambda, \qquad 1 \leq \lambda \leq (2^m - 1)/3.$$

This means that the weight of $\tilde{f}$ is odd, which is impossible. We then deduce that there exists two distinct elements of $\mathcal{U}$ whose intersection differs from $\{0\}$. In other words, $\mathcal{U}$ contains $\langle a, b\rangle$ and $\langle a, e\rangle$ with $e \neq b$. Then

$$D_b D_a \tilde{f} + D_e D_a \tilde{f} = 0$$

which implies

$$D_a \tilde{f}(x+b) + D_a \tilde{f}(x+e) = 0$$

for all x. This is equivalent to saying that $D_{b+e} D_a \tilde{f}$ is the null function. We then deduce that there is at least one subspace $\langle a, c\rangle$ of codimension 2 such that $D_c D_a \tilde{f} = 0$. □

Remark 3: Corollary 5 can be generalized to the bent functions f which are such that all derivatives of $\tilde{f}$ are partially bent. However, we do not know if such functions exist when $\deg(\tilde{f}) > 3$. This is mentioned as an open problem in [1, Sec. II].

Finally, we point out that the weights of the second derivatives of the dual of a bent function $f \in \mathcal{B}_m$ also provide some information on the weight distribution of $f + R(2, m)$. Most notably, any three-valued almost optimal 4-decomposition of f leads to another bent function, lying in $f + R(2, m)$.

Theorem 8: Let f be a bent function of m variables $m \geq 4$, and $\tilde{f}$ its dual. Let a and b be two nonzero distinct elements of $\boldsymbol{F}_2^m$, $V = \langle a, b\rangle^\perp$. Then, the m-variable Boolean function $f + \phi_V$ is such that its Fourier spectrum satisfies

$\lvert\mathcal{F}(f + \phi_V + \varphi_u)\rvert$	0	$2^{m/2}$	$2^{m/2+1}$
number of $u \in \boldsymbol{F}_2^m$	$\frac{3}{4}\lambda$	$2^m - \lambda$	$\frac{1}{4}\lambda$

where $\lambda = \mathrm{wt}(D_a D_b \tilde{f})$. Most notably, we have

- $f + \phi_V$ is bent if and only if $D_a D_b \tilde{f} = 0$;
- $f + \phi_V$ is three-valued almost optimal if and only if $D_a D_b \tilde{f} = 1$.

Proof: Let W be such that $V \times W = \boldsymbol{F}_2^m$. For any $u \in \boldsymbol{F}_2^m$, the 4-decomposition of $f + \phi_V + \varphi_u$ with respect to V is related to the 4-decomposition of $f + \varphi_u$ as follows:

$$(f + \phi_V + \varphi_u)\phi_{a+V} = (f + \varphi_u)\phi_{a+V}$$

for all $a \in W \setminus \{0\}$, and

$$(f+\phi_V+\varphi_u)\phi_V = (f+\varphi_u)\phi_V + 1.$$

Therefore, we deduce that

$$\begin{aligned}\mathcal{F}(f+\phi_V+\varphi_u) &= \sum_{a\in W} \mathcal{F}((f+\phi_V+\varphi_u)\phi_{a+V}) \\ &= \mathcal{F}(f+\varphi_u) - 2\mathcal{F}((f+\varphi_u)\phi_V).\end{aligned}$$

From (7) in Theorem 5, we obtain

$$\begin{aligned}\mathcal{F}(f+\phi_V+\varphi_u) &= \mathcal{F}(f+\varphi_u) - 2^{\frac{m}{2}-1}\mathcal{F}\left(\tilde{f}\phi_{u+V^\perp}\right) \\ &= 2^{\frac{m}{2}-1}\left[(-2)^{\tilde{f}(u)} - \mathcal{F}\left(\tilde{f}\phi_{u+V^\perp}\right)\right].\end{aligned}$$

Since $V^\perp = \langle a, b\rangle$, the weight of $\tilde{f}\phi_{u+V^\perp}$ is

- either 2, implying that $\mathcal{F}(f+\phi_V+\varphi_u) = \pm 2^{\frac{m}{2}}$;
- or in $\{1, 3\}$, implying that $\mathcal{F}(f+\phi_V+\varphi_u)$ lies in $\{0, \pm 2^{\frac{m}{2}+1}\}$;
- or in $\{0, 4\}$, implying that $\tilde{f}\phi_{u+V^\perp}$ is constant and, thus, equal to $\tilde{f}(u)$. In this case, $\mathcal{F}(\tilde{f}\phi_{u+V^\perp}) = 4(-1)^{\tilde{f}(u)}$. Therefore, we have $\mathcal{F}(f+\phi_V+\varphi_u) = \pm 2^{\frac{m}{2}}$.

Let L_i denote the number of $u \in \boldsymbol{F}_2^m$ such that

$$|\mathcal{F}(f+\phi_V+\varphi_u)| = 2^{m/2}i$$

with $i \in \{0, 1, 2\}$. In accordance with Lemma 2, $\mathrm{wt}(D_aD_b\tilde{f})$, which is the cardinality of the set

$$\left\{u \in \boldsymbol{F}_2^m,\ \mathrm{wt}\left(\tilde{f}\phi_{u+V^\perp}\right) \text{ is odd}\right\}$$

is equal to L_0+L_2. Thus, $L_1 = 2^m - \lambda$, where $\lambda = \mathrm{wt}(D_aD_b\tilde{f})$.

By applying Parseval's relation to $f+\phi_V$, we obtain

$$2^{2m} = L_1 2^m + L_2 2^{m+2} = 2^{2m} - 2^m\lambda + L_2 2^{m+2}$$

implying $L_2 = \lambda/4$. Finally, we have

$$L_0 = 2^m - L_1 - L_2 = \frac{3}{4}\lambda. \qquad \square$$

By the previous theorem, we point out that $f+\phi_V$ is bent if and only if $D_{V^\perp}\tilde{f} = 0$. This result is related to the theorem of [4, p. 94].

VII. On Bent Functions Which do not Admit a 4-Bent Decomposition

When a bent function in $\mathcal{B}_m$ admits of a 4-bent decomposition, then it is related to some bent functions in $\mathcal{B}_{m-2}$. It is not the case for bent functions which do not admit a 4-bent decomposition. In this section, we give two examples of infinite classes of bent functions for which such a decomposition is not possible. We first define some notation.

We will use the *2-ary expansion* of any positive integer k which is

$$(k_0, \ldots, k_\ell),\ k_i \in \{0, 1\}, \qquad \text{where } k = \sum_{i=0}^{\ell} k_i 2^i,\ k_\ell = 1.$$

The Hamming weight of the 2-ary expansion of k is denoted by $\omega_2(k)$. Two integers k and k' can be related by a partial order, denoted by $\preceq$, which is, in fact, a relation on their 2-ary expansions

$$k' \preceq k \iff k'_i \le k_i, \quad \forall i.$$

Note that $k' \prec k$ means that k covers k' but is not equal to k'. Recall that, when we compute modulo 2, we have

$$(x+a)^k = \sum_{i \preceq k} x^i a^{k-i}. \tag{11}$$

A. Some Partial Spreads

Here, we identify any function in $\mathcal{B}_m$ with a function from the finite field $\boldsymbol{F}_{2^m}$ into $\boldsymbol{F}_2$. In this subsection, we focus on the class of Boolean functions of the form $g\colon x \longmapsto \mathrm{Tr}(\lambda x^k)$, where $\lambda \in \boldsymbol{F}_{2^t}$ and Tr is the trace function from $\boldsymbol{F}_{2^m}$ to $\boldsymbol{F}_2$

$$\mathrm{Tr}(u) = u + u^2 + \cdots + u^{2^{m-1}}.$$

For any k' in the 2-cyclotomic coset of k modulo (2^m-1), i.e., $k' \equiv 2^i k \bmod (2^m-1)$, $x \mapsto \mathrm{Tr}(\lambda x^{k'})$ obviously corresponds to g composed with a linear automorphism of $\boldsymbol{F}_{2^m}$. Therefore, we will assume that k is the smallest element of its cyclotomic coset. Note that such a function g could be constant only when there is some r dividing m such that

$$x^{2^r k} = x^k, \qquad \forall x \in \boldsymbol{F}_{2^m}$$

or equivalently

$$(2^r - 1)k \equiv 0 \bmod (2^m - 1).$$

From well-known properties of the Reed–Muller codes, the degree of such a function is equal to $\omega_2(k)$, the weight of the 2-ary expansion of k. Note that for any a in $\boldsymbol{F}_{2^m}$ we have

$$\begin{aligned}D_a g(x) &= \mathrm{Tr}[\lambda x^k + \lambda(x+a)^k] \\ &= \sum_{i \prec k} \mathrm{Tr}(\lambda x^i a^{k-i}).\end{aligned}$$

We know that the degree of $D_a g$ is less than or equal to $\omega_2(k) - 1$.

Now, we are interested in the values of the second derivatives of the functions $g\colon x \longmapsto \mathrm{Tr}(\lambda x^k)$. Let a and b in $\boldsymbol{F}_{2^m}$ be such that $a \neq b \neq 0$. Then, we have to study the polynomial

$$\mathrm{Tr}[\lambda(x^k + (x+a)^k + (x+b)^k + (x+a+b)^k)]$$

which is in fact

$$P(x) = \sum_{i \prec k} \mathrm{Tr}[\lambda(a^{k-i} + b^{k-i} + (a+b)^{k-i})x^i].$$

Whenever $i = k - 2^r$, for some r, we have

$$a^{k-i} + b^{k-i} + (a+b)^{k-i} = 0$$

as we expected since the degree of D_aD_bg is at most $\omega_2(k) - 2$. So

$$P(x) = \sum_{i \in I} \mathrm{Tr}[\lambda(a^{k-i} + b^{k-i} + (a+b)^{k-i})x^i] \tag{12}$$

where $I = \{i | i \prec k \text{ and } \omega_2(k-i) \neq 1\}$.

Lemma 3: Let $m \ge 8$, m even, and consider the Boolean functions in $\mathcal{B}_m$ of the form

$$g\colon x \longmapsto \mathrm{Tr}(\lambda x^k), \qquad 15 \le k \le 2^{m/2} - 1$$

$\lambda \in \boldsymbol{F}_{2^m}^*$, where the weight of k satisfies $\omega_2(k) \ge 4$ and Tr is the trace function from $\boldsymbol{F}_{2^m}$ to $\boldsymbol{F}_2$.

If the 2-ary expansion of k, say $(k_0, \ldots, k_\ell)$, is such that $k_r = k_s = 1$ for some r and s, $0 < r < s < \ell$, with

$\gcd(s-r, m)=1$ then the function g is such that all its second derivatives are not constant.

Proof: We consider the polynomial $P(x)$ given by (12) and we are going to prove that this polynomial cannot be constant. Since $\mathrm{Tr}(u^2)=\mathrm{Tr}(u)$, then $P(x)$ can be expressed as follows:

$$P(x)=\mathrm{Tr}\left(\sum_{i\in I} u_i x^i\right), \qquad x\in \boldsymbol{F}_{2^m}$$

where u_i only depends on λ, a, and b and I consists of the smallest elements of the 2-cyclotomic cosets modulo 2^m-1 of all i which appear as exponents of x in (12).

This polynomial is of degree strictly less than 2^m-1. Moreover, we are sure that for any nonzero $i\in I$, the function $\mathrm{Tr}(u_i x^i)$ cannot be constant when $u_i\neq 0$. Indeed, $i<2^{m/2}-1$ implies that the cyclotomic coset of i has cardinality m: it is impossible to have $(2^r-1)i\equiv 0 \bmod (2^m-1)$ for some r dividing m, $r>1$.

Hence, $P(x)=0$, for all x, if and only if $u_i=0$ for all $i\in I$. On the other hand, $P(x)=1$ if and only if $P(x)+1=0$ for all x. This is equivalent to $u_i=0$ for all $i\neq 0$ and $\mathrm{Tr}(u_0)=1$.

In order to prove that at least one u_i, $i>0$, is not zero, we will choose an $i\in I$ such that $2^j i\geq k$ for all j, $1\leq j\leq m-1$. By hypothesis, the 2-ary expansion of k, $(k_0,\ldots,k_\ell)$, is such that: $k_0=k_\ell=1$, and there is a pair (r,s), $0<r<s<\ell$ with $\gcd(s-r,m)=1$, such that $k_r=k_s=1$. We take

$$\rho=k-2^s-2^r.$$

For instance, if $k=2^{m/2}-1$ then ρ could be chosen as follows:

$$\rho=(\underbrace{1,\ldots,1,0,0,1}_{m/2},\underbrace{0,\ldots,0}_{m/2})$$

with

$$k=(\underbrace{1,\ldots,1}_{m/2},\underbrace{0,\ldots,0}_{m/2}).$$

We have clearly $\omega_2(\rho)=\omega_2(k)-2$ and $\rho\prec k$. Moreover, since $\rho_\ell=\rho_0=1$, we have for all $j\neq 0$

$$2^j\rho \bmod (2^m-1)\geq 2^j+2^{(j+\ell)\bmod m}\geq k$$

because $k\leq 2^\ell-1$ and either j or $(j+\ell)\bmod m$ exceeds ℓ (since $\ell\leq m/2$). Then ρ is the leader of its cyclotomic coset ($\rho\in I$) and, therefore, it is the only one element of its cyclotomic coset appearing as a power of x in (12). This implies

$$\begin{aligned}u_\rho &= a^{k-\rho}+b^{k-\rho}+(a+b)^{k-\rho}\\ &= a^{2^s+2^r}+b^{2^s+2^r}+(a+b)^{2^s+2^r}\\ &= a^{2^s}b^{2^r}+b^{2^s}a^{2^r}\\ &= (ab)^{2^r}(a^{2^s-2^r}+b^{2^s-2^r})\\ &= (ab)^{2^r}(a^{2^{s-r}-1}+b^{2^{s-r}-1})^{2^r}.\end{aligned}$$

By hypothesis, $a\neq b\neq 0$. The equality $a^{2^{s-r}-1}=b^{2^{s-r}-1}$ would imply $(a/b)^{2^{s-r}-1}=1$ which is possible when $a=b$ only, since $\gcd(s-r,m)=1$. We conclude that $u_\rho\neq 0$. Therefore, P cannot be a constant polynomial, completing the proof. □

Note that other specific classes of functions $\mathrm{Tr}(\lambda x^k)$, corresponding to particular values of k, can be studied with similar methods. It seems complicated to treat the general problem; the next example illustrates this fact.

Example 2: Let m be even and $m\geq 8$. Let us consider the Boolean function in $\mathcal{B}_m$

$$g(x)=\mathrm{Tr}(x^k), \qquad \text{with } k=1+2^2+2^4+2^6. \tag{13}$$

Let $a\in \boldsymbol{F}_4$. By using (12) and the form of k, we obtain

$$D_aD_1g(x)=\sum_{i\in J}\mathrm{Tr}[(a^{k-i}+1+(a+1)^{k-i})x^i]$$

with $J=\{i\prec k,\ 2\leq \omega_2(k-i)\leq 4\}$. We first observe that

$$i\in J \quad\Longrightarrow\quad k-i\equiv \omega_2(k-i) \pmod 3$$

using that $2^{2\ell}\equiv 1 \bmod 3, \forall \ell$. Let $u_i=a^{k-i}+1+(a+1)^{k-i}$ $(i\in J)$. Since $a^3=1$, we have

- if $\omega_2(k-i)=2$ then $u_i=a^2+1+(a+1)^2=0$;
- if $\omega_2(k-i)=4$ then $u_i=a^4+1+(a+1)^4=0$;
- if $\omega_2(k-i)=3$ then $u_i=1$.

Therefore,

$$D_aD_1g(x)=\mathrm{Tr}[x+x^{2^2}+x^{2^4}+x^{2^6}]=0.$$

We have proved that *the Boolean functions defined by (13) have at least one constant second derivative.*

Now, we will point out that there is an infinite class of bent functions which satisfy the hypothesis of Lemma 3. These functions belong to the partial spread family, introduced by Dillon as *the class* $\mathcal{PS}$ [6, pp. 95–100]. We first recall the result of Dillon.

Theorem 9: Let $f\in\mathcal{B}_m$ with $m=2t$. Let

$$E_f=\{x\in \boldsymbol{F}_{2^m} | f(x)=1\}.$$

Let us denote by $\{E_i,\ i=1,\ 2\cdots N\}$ a set of subspaces of $\boldsymbol{F}_{2^m}$ of dimension t satisfying

$$i\neq j \quad\Rightarrow\quad E_i\cap E_j=\{0\}.$$

The function f is bent when it satisfies either **(i)** or **(ii)**. The bent functions which satisfy condition **(i)** (resp., **(ii)**) are said to be in the class $\mathcal{PS}^+$ (resp., $\mathcal{PS}^-$).

(i) $E_f=\bigcup_{i=1}^N E_i$ with $N=2^{t-1}+1$;

(ii) $E_f=\bigcup_{i=1}^N E_i^*$ with $N=2^{t-1}$.

Notation of Theorem 9 is preserved. Let α denote a primitive root of $\boldsymbol{F}_{2^m}$ with $m=2t$; by shifting the cyclic subgroup of $\boldsymbol{F}_{2^t}$ we obtain the sets $E_i^*=\alpha^i\boldsymbol{F}_{2^t}^*$, providing the partition

$$\boldsymbol{F}_{2^m}^*=\bigcup_{i=0}^{2^t} E_i^*.$$

Now, for all $x\in E_i^*$, $x=\alpha^i\beta$ with $\beta\in\boldsymbol{F}_{2^t}^*$, we have for any $\nu\in\boldsymbol{F}_{2^m}$

$$\begin{aligned}\mathrm{Tr}(\nu x^{2^t-1}) &= \mathrm{Tr}(\nu\alpha^{i(2^t-1)}\beta^{2^t-1})\\ &= \mathrm{Tr}(\nu\alpha^{i(2^t-1)}).\end{aligned}$$

Thus, the Boolean function $g\in\mathcal{B}_m$, $g(x)=\mathrm{Tr}(\nu x^{2^t-1})$, is constant on any E_i^* for any i (and is such that $g(0)=0$). This function is bent and belongs to $\mathcal{PS}^-$ if there are exactly 2^{t-1} exponents i in the interval $[0,2^t]$ such that $\mathrm{Tr}(\nu\alpha^{i(2^t-1)})=1$. This type of bent functions was introduced by Dillon who stated the

sufficient condition on ν which we explain now. Let $\gamma = \alpha^{2^t-1}$; then γ is a generator of the cyclic subgroup of order 2^t+1. Consider the set of binary codewords of length 2^t+1

$$w_\nu = (\mathrm{Tr}(\nu), \mathrm{Tr}(\nu\gamma), \ldots, \mathrm{Tr}(\nu\gamma^{2^t}))$$

where $\nu \in \boldsymbol{F}_{2^{2t}}$. These codewords form an *irreducible cyclic code* of length 2^t+1 and dimension $2t$. It appears that g is bent if and only if this code contains a codeword of weight 2^{t-1}.

Since 2^t+1 and 2^t-1 are relatively prime then $\nu = \lambda\gamma^j$ for some j and some $\lambda \in \boldsymbol{F}_{2^t}$. Hence, w_ν is a shift of w_λ, providing the same weight. The existence of $\lambda \in \boldsymbol{F}_{2^t}$, such that $\mathrm{wt}(w_\lambda) = 2^{t-1}$, for any t, was established by Lachaud and Wolfmann [14, Theorem 6.6].

Theorem 10: When a function g, defined as in Lemma 3, is bent then its dual $\tilde{g}$ admits neither a bent 4-decomposition nor a three-valued almost optimal 4-decomposition.

In particular, this property holds for the infinite class of bent functions of $\mathcal{B}_m$, $m = 2t$

$$g_m(x)\colon x \in \boldsymbol{F}_{2^m} \longmapsto \mathrm{Tr}(\lambda x^{2^t-1})$$

where $\lambda \in \boldsymbol{F}_{2^t}$ satisfies

$$\sum_{i=0}^{2^t} \mathrm{Tr}(\lambda\gamma^i) = 2^{t-1}$$

(where γ is a (2^t+1)th root of unity). Moreover, each g_m is equal to its dual. So g_m (as well as $\tilde{g}_m$) admits neither a bent 4-decomposition nor a three-valued almost-optimal 4-decomposition.

Proof: In accordance with Theorem 7, the first part of the theorem is immediately deduced from Lemma 3. The bent functions g_m, especially, satisfy Lemma 3.

Now, we focus on g_m. We have $E_{g_m} = \bigcup_{i\in I} E_i^*$ where

$$I = \{i,\, 0 \le i \le 2^t \text{ such that } \mathrm{Tr}(\lambda\alpha^{i(2^t-1)}) = 1\}.$$

Here, we use another scalar product, defining the linear functions as follows:

$$\psi_a\colon x \in \boldsymbol{F}_{2^m} \longmapsto \mathrm{Tr}(ax), \qquad a \in \boldsymbol{F}_{2^m}.$$

Then, the dual of g_m is defined in each a by

$$\mathcal{F}(g_m + \psi_a) = 2^t(-1)^{\tilde{g}_m(a)}.$$

We know that $E_{g_m} = \bigcup_{i\in I} E_i^*$ gives $E_{\tilde{g}_m} = \bigcup_{i\in I} (E_i^\perp)^*$ (from [6, Remark 6.3.10] or by applying Theorem 5). Moreover, we have here

$$\mathrm{Tr}\left((\alpha^i\beta)(\alpha^{2^t+1-i}\beta')\right) = \mathrm{Tr}(\alpha^{2^t+1}\beta\beta') = 0$$

for any β and β' in $\boldsymbol{F}_{2^t}$ (since $\alpha^{2^t+1} \in \boldsymbol{F}_{2^t}$). This shows that $E_i^\perp = E_{2^t+1-i}$. Thus, $E_{\tilde{g}_m} = \bigcup_{i\in I} E^*_{2^t+1-i}$. Now, taking in account that $\alpha^{i2^t(2^t-1)}\alpha^{i(2^t-1)} = 1$ we compute g_m on E_{2^t+1-i}

$$\begin{aligned}\mathrm{Tr}(\lambda\alpha^{(2^t+1-i)(2^t-1)}) &= \mathrm{Tr}(\lambda\alpha^{-i(2^t-1)}) \\ &= \mathrm{Tr}(\lambda\alpha^{i(2^t-1)}).\end{aligned}$$

Thus, $i \in I$ if and only if $(2^t+1-i) \in I$, providing that $E_{g_m} = E_{\tilde{g}_m}$. Therefore, the Boolean function $\tilde{g}_m$ is exactly the function g_m, completing the proof. □

Remark 4: The equality $\tilde{g}_m = g_m$ can be seen by using the description of codewords w_λ of the concerned irreducible code, given in [14, Proposition 6.5].

B. On Bent Functions of Family $\mathcal{M}$

This subsection is devoted to the 4-decompositions of the bent functions which belong to *family* $\mathcal{M}$ [6, pp. 89–95]. Here, we consider for $\mathcal{M}$ the completed version of the class introduced by Maiorana and McFarland [15]. In others words, we consider all functions which are affinely equivalent to the functions in the original family.

Now, we identify $\boldsymbol{F}_2^{2t}$ with $\boldsymbol{F}_2^t \times \boldsymbol{F}_2^t$, i.e., any element of $\boldsymbol{F}_2^{2t}$ is denoted by (x, y) with $x, y \in \boldsymbol{F}_2^t$.

Definition 10: Family $\mathcal{M}$ consists of all functions in $\mathcal{B}_{2t}$ which are affinely equivalent to

$$\begin{aligned}\boldsymbol{F}_2^t \times \boldsymbol{F}_2^t &\longrightarrow \boldsymbol{F}_2 \\ (x, y) &\longmapsto x \cdot \pi(y) + h(y)\end{aligned}$$

where π is any permutation on $\boldsymbol{F}_2^t$, h is any Boolean function in $\mathcal{B}_t$, and "$\cdot$" denotes any scalar product on $\boldsymbol{F}_2^t$. Any function in $\mathcal{M}$ is bent.

This class of bent function is characterized by the following property.

Proposition 9 [6, p. 102]: A bent function $f \in \mathcal{B}_{2t}$ belongs to family $\mathcal{M}$ if and only if there exists a t-dimensional subspace $V \subset \boldsymbol{F}_2^{2t}$ such that the derivative of f with respect to every two-dimensional subspace of V is identically zero.

Now, we focus on the pairs (α, β) such that the derivative of the dual of $f \in \mathcal{M}$ with respect to the two-dimensional subspace $\langle\alpha, \beta\rangle$ is constant. Note that the following result holds for any choice of the scalar product on $\boldsymbol{F}_2^t$.

Proposition 10: Let $m = 2t$ and let f be a bent function of m variables in family $\mathcal{M}$

$$\begin{aligned}f\colon \boldsymbol{F}_2^t \times \boldsymbol{F}_2^t &\longrightarrow \boldsymbol{F}_2 \\ (x, y) &\longmapsto x \cdot \pi(y) + h(y)\end{aligned}$$

where π is a permutation on $\boldsymbol{F}_2^t$ and h is a Boolean function in $\mathcal{B}_t$. We denote by σ the inverse of π and by $V \subset \boldsymbol{F}_2^m$ the t-dimensional subspace defined by $V = \{(0, y),\, y \in \boldsymbol{F}_2^t\}$.

Let $\alpha = (\alpha_1, \alpha_2)$ and $\beta = (\beta_1, \beta_2)$ be two nonzero distinct elements of $\boldsymbol{F}_2^m$. We have

- if $\langle\alpha, \beta\rangle \subset V$, then $D_\alpha D_\beta \tilde{f} = 0$;
- if $\langle\alpha, \beta\rangle \cap V = \{0, (0, \gamma)\}$ with $\gamma \neq 0$, then $D_\alpha D_\beta \tilde{f} = \varepsilon$ where $\varepsilon = \{0, 1\}$ if and only if the t-variable Boolean function

  $$\sigma_\gamma\colon x \mapsto \gamma \cdot \sigma(x)$$

  has a nonzero linear structure λ satisfying $D_\lambda\sigma_\gamma = \varepsilon$;
- if $\langle\alpha, \beta\rangle \cap V = \{0\}$, then $D_\alpha D_\beta \tilde{f} = \varepsilon$ where $\varepsilon = \{0, 1\}$ implies that

  $$\sigma(x + \alpha_1 + \beta_1) + \sigma(x + \alpha_1) + \sigma(x + \beta_1) + \sigma(x) = 0$$

  for all $x \in \boldsymbol{F}_2^t$.

Proof: The dual $\tilde{f}$ of f is defined by [6, p. 91]

$$\tilde{f}(x, y) = \sigma(x) \cdot y + h(\sigma(x)).$$

Therefore, the function $D_\alpha D_\beta \tilde{f}(x, y)$ is equal to

$$\begin{aligned}
&\tilde{f}(x+\alpha_1+\beta_1, y+\alpha_2+\beta_2) + \tilde{f}(x+\beta_1, y+\beta_2) \\
&\quad + \tilde{f}(x+\alpha_1, y+\alpha_2) + \tilde{f}(x, y) \\
&= \sigma(x+\alpha_1+\beta_1)\cdot(y+\alpha_2+\beta_2) + \sigma(x+\beta_1)\cdot(y+\beta_2) \\
&\quad + \sigma(x+\alpha_1)\cdot(y+\alpha_2) + \sigma(x)\cdot y + D_{\alpha_1}D_{\beta_1}h(\sigma(x)) \\
&= y\cdot(\sigma(x+\alpha_1+\beta_1) + \sigma(x+\beta_1) + \sigma(x+\alpha_1) + \sigma(x)) \\
&\quad + \alpha_2\cdot(\sigma(x+\alpha_1+\beta_1) + \sigma(x+\alpha_1)) \\
&\quad + \beta_2\cdot(\sigma(x+\alpha_1+\beta_1) + \sigma(x+\beta_1)) \\
&\quad + D_{\alpha_1}D_{\beta_1}h(\sigma(x)). \qquad (14)
\end{aligned}$$

It clearly appears that

$$D_{(0,\alpha_2)}D_{(0,\beta_2)}\tilde{f} = 0.$$

The condition $\langle \alpha, \beta\rangle \cap V = \{0, (0, \gamma)\}$ corresponds to one of the following three cases:

- $\alpha_1 = 0$: $D_\alpha D_\beta \tilde{f}(x, y) = \alpha_2 \cdot (\sigma(x+\beta_1) + \sigma(x))$;
- $\beta_1 = 0$: $D_\alpha D_\beta \tilde{f}(x, y) = \beta_2 \cdot (\sigma(x+\alpha_1) + \sigma(x))$;
- $\alpha_1 = \beta_1$: $D_\alpha D_\beta \tilde{f}(x, y) = (\alpha_2+\beta_2)\cdot(\sigma(x+\alpha_1)+\sigma(x))$.

Therefore, we obtain that

$$D_\alpha D_\beta \tilde{f}(x, y) = \gamma \cdot (\sigma(x+\lambda) + \sigma(x))$$

where $(0, \gamma)$ is the unique nonzero element in $V \cap \langle \alpha, \beta\rangle$ and λ is a nonzero element of $\boldsymbol{F}_2^t$. We have proved that, for such α and β, $D_\alpha D_\beta \tilde{f} = \varepsilon$ if and only if λ is a linear structure for the t-variable function σ_γ with $D_\lambda \sigma_\gamma = \varepsilon$.

We now assume that $\alpha_1 \neq \beta_1$ and both α_1 and β_1 differ from 0. The first term in (14) is the only one which depends on y. Hence, if $D_\alpha D_\beta \tilde{f}$ is constant, then this term vanishes, i.e.,

$$\sigma(x+\alpha_1+\beta_1) + \sigma(x+\beta_1) + \sigma(x+\alpha_1) + \sigma(x) = 0$$

for all $x \in \boldsymbol{F}_2^t$. □

We now exhibit an infinite class of bent functions in family $\mathcal{M}$ which admits no bent 4-decomposition. Recall that f admits a bent 4-decomposition if and only if there exist two nonzero distinct elements α and β in $\boldsymbol{F}_2^m$ such that $D_\alpha D_\beta \tilde{f} = 1$. From the previous proposition, it implies that σ satisfies one of the following properties.

(P1) There exist two nonzero distinct elements λ and γ in $\boldsymbol{F}_2^t$ such that for all $x \in \boldsymbol{F}_2^t$

$$\sigma(x+\lambda+\gamma) + \sigma(x+\lambda) + \sigma(x+\gamma) + \sigma(x) = 0.$$

(P2) There exist two nonzero elements λ and γ in $\boldsymbol{F}_2^t$ such that

$$\gamma \cdot (\sigma(x+\lambda) + \sigma(x)) = 1 \qquad \text{on } \boldsymbol{F}_2^t.$$

First, we show that Property **(P1)** is usually not satisfied when σ is a power permutation, i.e., $\sigma(x) = x^d$ where $\boldsymbol{F}_2^t$ is identified with the finite field with 2^t elements $\boldsymbol{F}_{2^t}$.

Lemma 4: Let $x \mapsto x^d$ be a power function over $\boldsymbol{F}_{2^t}$ with $\omega_2(d) \geq 2$. Then, there exist two nonzero distinct elements a and b in $\boldsymbol{F}_{2^t}$ such that for all $x \in \boldsymbol{F}_{2^t}$

$$(x+a+b)^d + (x+a)^d + (x+b)^d + x^d = 0 \qquad (15)$$

if and only if $d = 2^i + 2^j$ with $i < j$ and $\gcd(j-i, t) > 1$.

Proof: We consider two nonzero distinct elements a and b in $\boldsymbol{F}_{2^t}$ and set

$$P_d(x) = (x+a+b)^d + (x+a)^d + (x+b)^d + x^d.$$

Without loss of generality, we can assume that d is the smallest element in its 2-cyclotomic coset modulo $(2^t - 1)$. Indeed, $P_d(x)$ satisfies $P_{2d}(x) = (P_d(x))^2$.

By expanding the terms of $P_d(x)$, we obtain

$$P_d(x) = \sum_{\rho \preceq d} u_\rho x^{d-\rho}, \qquad u_\rho = (a+b)^\rho + a^\rho + b^\rho.$$

If we set $c = ab^{-1}$ we obtain a simpler expression

$$u_\rho = b^\rho v_\rho \quad \text{with} \quad v_\rho = (c+1)^\rho + c^\rho + 1.$$

The mapping $x \mapsto x^d$ satisfies (15) if and only if there is $c \in \boldsymbol{F}_{2^t}$, $c \notin \boldsymbol{F}_2$, such that $v_\rho = 0$ for all $\rho \preceq d$. We are going to prove that this is generally impossible.

If $\omega_2(d) \geq 3$, there is $\rho = 1 + 2^i + 2^j$, $0 < i < j$, such that $\rho \preceq d$. Then

$$\begin{aligned}
v_{2^i+1} &= (c+1)^{2^i+1} + c^{2^i+1} + 1 \\
&= c^{2^i} + c.
\end{aligned}$$

Thus, $v_{2^i+1} = 0$ if and only if $c \in \boldsymbol{F}_{2^i}$. Similarly, $v_{2^j+1} = c^{2^j} + c$. If $v_{2^j+1} = v_{2^i+1} = 0$ then $c^{1+2^i+2^j} = c^3$ and we obtain

$$v_\rho = (c+1)^3 + c^3 + 1 = c(c+1)$$

which vanishes for $c \in \boldsymbol{F}_2$ only, a contradiction. Thus, we have proved that d does not satisfy (15) when $\omega_2(d) \geq 3$.

When $\omega_2(d) = 2$, i.e., $d = 1 + 2^i$, there is c such that $v_{2^i+1} = 0$ if and only if $\gcd(i, t) > 1$, completing the proof. □

Open Problem: Characterize all nonquadratic permutations σ over $\boldsymbol{F}_2^t$ for which there exist two distinct nonzero elements a and b such that for all $x \in \boldsymbol{F}_2^t$

$$\sigma(x+a+b) + \sigma(x+a) + \sigma(x+b) + \sigma(x) = 0.$$

Now, we focus on some permutations σ which do not satisfy the previous property, and we determine whether $x \cdot \pi(y) + h(y)$ has a bent 4-decomposition, i.e., whether σ satisfies Property **(P2)**. Here, we choose for σ an *almost perfect nonlinear permutation* on $\boldsymbol{F}_2^t$ [16], [17]. A function σ over $\boldsymbol{F}_2^t$ is called almost perfect nonlinear (APN) if all equations

$$\sigma(x) + \sigma(x+a) = b, \qquad a \in \boldsymbol{F}_2^t,\ b \in \boldsymbol{F}_2^t,\ a \neq 0$$

have zero or two solutions in $\boldsymbol{F}_2^t$. Note that the inverse of an APN permutation is APN.

Proposition 11: Let $m = 2t$ be an even integer such that t is odd. Let π be an APN permutation on $\boldsymbol{F}_2^t$, and let σ denote the inverse permutation. Then, the m-variable bent function

$$\begin{aligned}
f: \boldsymbol{F}_2^t \times \boldsymbol{F}_2^t &\longrightarrow \boldsymbol{F}_2 \\
(x, y) &\longmapsto x \cdot \pi(y) + h(y)
\end{aligned}$$

where h is any Boolean function in $\mathcal{B}_t$, admits a decomposition into four bent functions if and only if there exists $\lambda \in \boldsymbol{F}_2^t$, $\lambda \neq 0$, such that the set $\{\sigma(x+\lambda)+\sigma(x),\, x \in \boldsymbol{F}_2^t\}$ is an affine hyperplane.

Proof: The bent function f admits a decomposition into four bent functions if and only if its dual $\tilde{f}$ has at least one second derivative which is constant and equal to 1. We now apply Proposition 10 with notation $V = \{(0, y),\, y \in \boldsymbol{F}_2^t\}$. If $D_\alpha D_\beta \tilde{f} = 1$ with $\langle \alpha, \beta\rangle \cap V = \{0\}$, then there exist two distinct elements a and b in $\boldsymbol{F}_2^t \setminus \{0\}$ such that for all $x \in \boldsymbol{F}_2^t$

$$\sigma(x)+\sigma(x+a)+\sigma(x+b)+\sigma(x+a+b)=0.$$

This situation cannot occur since σ is APN. Therefore, if $D_\alpha D_\beta \tilde{f} = 1$ then $\langle \alpha, \beta\rangle \cap V$ has cardinality 2. Moreover, we know from Proposition 10 that there exist two nonzero elements λ and γ in $\boldsymbol{F}_2^t$ such that

$$\gamma \cdot (\sigma(x+\lambda)+\sigma(x)) = 1, \qquad \text{for all } x \in \boldsymbol{F}_2^t.$$

Note that σ is an APN permutation if and only if the set

$$S_e = \{\sigma(x+e)+\sigma(x),\, x \in \boldsymbol{F}_2^t\}$$

has exactly 2^{t-1} elements for any $e \neq 0$. This comes from the definition: it is clear that S_e has at most a cardinality 2^{t-1}, since x and $x+e$ give the same values; the cardinality of S_e is exactly 2^{t-1} if and only if each equation $\sigma(x)+\sigma(x+e)=b$ has 0 or two solutions, i.e., σ is APN. Therefore, we have proved that if f admits a bent 4-decomposition, then there exists $\lambda \in \boldsymbol{F}_2^t$, $\lambda \neq 0$, such that S_λ is an affine hyperplane.

Conversely, if there exist two nonzero elements λ and γ such that the set $\{\sigma(x+\lambda)+\sigma(x),\, x \in \boldsymbol{F}_2^t\}$ is equal to the set $\{x \in \boldsymbol{F}_2^t,\, \varphi_\gamma(x) = 1\}$ then we have

$$D_{(0,\gamma)} D_{(\lambda,0)} \tilde{f}(x, y) = \gamma \cdot (\sigma(x+\lambda)+\sigma(x)) = 1.$$

Thus, f admits a bent 4-decomposition. □

Almost bent functions form a particular subclass of APN mappings over $\boldsymbol{F}_2^t$ for odd t. A function σ over $\boldsymbol{F}_2^t$ is called almost bent if any nonzero linear combination of its Boolean components, $x \mapsto b \cdot \sigma(x)$ for $b \neq 0$, is three-valued almost optimal [17], [18].

Remark 5: The permutations σ over $\boldsymbol{F}_2^t$ such that all sets, for $a \in \boldsymbol{F}_2^t$ $(a \neq 0)$

$$S_a = \{\sigma(x+a)+\sigma(x),\, x \in \boldsymbol{F}_2^t\}$$

are affine hyperplanes have been introduced in [19] and they are called *crooked functions*. A part of the proof of the next lemma can be found in [20] (using another terminology). The only examples of crooked functions known at present have degree 2 [19, p. 8].

Lemma 5: Let t be an odd integer $t \geq 5$. Let σ be an APN function over $\boldsymbol{F}_2^t$ such that, for any nonzero $a \in \boldsymbol{F}_2^t$, the set

$$S_a = \{\sigma(x+a)+\sigma(x),\, x \in \boldsymbol{F}_2^t\}$$

is an affine hyperplane. Then, σ is almost bent and its degree cannot exceed $\frac{t-1}{2}$.

Proof: We denote by H_b the hyperplane $\{0, b\}^\perp$ and by $\overline{H}_b$ its complement. We first prove that all sets S_a, $a \neq 0$ are distinct: otherwise, there exists a and a' such that $S_a = S_{a'} = \overline{H}_b$ for some b. Then, for any $x \in \boldsymbol{F}_2^t$, $\sigma(x+a+a')+\sigma(x)$ is equal to

$$(\sigma(x+a+a')+\sigma(x+a))+(\sigma(x+a)+\sigma(x))$$

and belongs to H_b since it can be expressed as the sum of two elements in $\overline{H}_b$. Then, $S_{a+a'}$ cannot be an affine hyperplane since $S_{a+a'} \subset H_b$. Therefore, for any $b \in \boldsymbol{F}_2^t$, $b \neq 0$, there exists a unique $a \neq 0$ such that $S_a = \overline{H}_b$.

We now consider the linear combinations of the Boolean components of σ, i.e., the Boolean functions

$$\sigma_b \colon x \mapsto b \cdot \sigma(x).$$

For any $\alpha \in \boldsymbol{F}_2^t$, we have [10]

$$\mathcal{F}^2(\sigma_b + \varphi_\alpha) = \sum_{a \in \boldsymbol{F}_2^t} (-1)^{\alpha \cdot a} \mathcal{F}(D_a \sigma_b).$$

Since S_a is an affine hyperplane for $a \neq 0$, $D_a\sigma_b$ is either balanced or equal to 1. It is equal to 1 for the unique $a \neq 0$ such that $S_a = \overline{H}_b$. Therefore,

$$\mathcal{F}^2(\sigma_b + \varphi_\alpha) = 2^t \pm 2^t \in \{0,\, 2^{t+1}\}$$

i.e., all functions σ_b, $b \neq 0$, are three valued almost optimal (or equivalently σ is an almost-bent permutation). Moreover, all σ_b have a nonzero linear structure. We know that any three-valued almost-optimal function of t variables (with t odd and $t \geq 5$) having a linear structure is *partially bent* with degree less than or equal to $\frac{t-1}{2}$ (see Proposition 5). □

Now, we apply Proposition 11 in the case where π is an APN power permutation $\pi(x) = x^s$. Note that APN power permutations over $\boldsymbol{F}_{2^t}$ only exist for odd t (see [21], [22, Proposition 4]). In the sequel, $\boldsymbol{F}_2^t$ is identified with the finite field of order 2^t, $\boldsymbol{F}_{2^t}$, and the linear functions are the mappings $y \mapsto \mathrm{Tr}(by)$ on $\boldsymbol{F}_{2^t}$, where b describes $\boldsymbol{F}_{2^t}$ and Tr is the trace function from $\boldsymbol{F}_{2^t}$ to $\boldsymbol{F}_2$. The scalar product of two elements x and y then corresponds to $\mathrm{Tr}(xy)$.

Proposition 12: Let $m = 2t$ be an even integer such that t is odd and let Tr denote the trace function from $\boldsymbol{F}_{2^t}$ to $\boldsymbol{F}_2$. Let $x \mapsto x^s$ be an APN power permutation over $\boldsymbol{F}_{2^t}$ and let $x \mapsto x^d$ denote the inverse mapping. Then, the following properties are equivalent.

(i) The m-variable bent function

$$f(x, y) = \mathrm{Tr}(xy^s) + h(y)$$

where h is any Boolean function in $\mathcal{B}_t$, admits a decomposition into four bent functions.

(ii) The t-variable Boolean function

$$g \colon x \mapsto \mathrm{Tr}(x^d)$$

has a nonzero linear structure a such that $D_a g = 1$.

(iii) For any nonzero $a \in \boldsymbol{F}_{2^t}$, the set

$$S_a = \{(x+a)^d + x^d,\, x \in \boldsymbol{F}_{2^t}\}$$

is an affine hyperplane.

Moreover, each of these properties implies that $x \mapsto x^d$ is almost bent and that it has degree at most $\frac{t-1}{2}$, i.e., $\omega_2(d) \leq \frac{t-1}{2}$ for $t \geq 5$.

Proof: Let us denote by g_b the functions

$$g_b\colon x \longmapsto \mathrm{Tr}(bx^d), \qquad b \in \boldsymbol{F}_{2^t},\ b \neq 0.$$

According to Proposition 11, we know that f admits a decomposition into four bent functions if and only if there exists γ and λ in $\boldsymbol{F}_{2^t} \setminus \{0\}$ such that the set $\{(x+\lambda)^d + x^d,\ x \in \boldsymbol{F}_{2^t}\}$ is equal to the set $\{x \in \boldsymbol{F}_{2^t},\ \mathrm{Tr}(\gamma x) = 1\}$ (i.e., $D_\lambda g_\gamma = 1$). So **(ii)** implies **(i)**, and **(iii)** implies **(i)**.

Assume that **(i)** holds, i.e., that there exist two nonzero elements λ and γ such that $D_\lambda g_\gamma = 1$. Actually, any function g_b can be obtained from g_γ by *shifting* the codeword $(\mathrm{Tr}(\gamma x^d), x \in \boldsymbol{F}_{2^t})$. More precisely, if $b = c^d\gamma$ with $c \neq 0$, we have $g_b = \mathrm{Tr}(bx^d) = \mathrm{Tr}(\gamma(cx)^d)$. Then, we obtain for any $a \in \boldsymbol{F}_{2^t}$

$$\begin{aligned} D_a g_b(x) &= \mathrm{Tr}\left(\gamma(cx)^d + \gamma(cx+ca)^d\right) \\ &= D_{ca} g_\gamma(cx). \end{aligned}$$

Thus, for any $b \in \boldsymbol{F}_{2^t}$, $b \neq 0$, $D_a g_b = 1$ for $a = \lambda c^{-1} = \lambda(\gamma b^{-1})^s$. Moreover, the sets

$$S_a = \{(x+a)^d + x^d,\ x \in \boldsymbol{F}_{2^t}\}$$

are affine hyperplanes (since S_a has cardinality 2^{t-1} because $x \mapsto x^d$ is APN). We have proved that **(i)** implies **(ii)** and **(iii)**. Therefore, all three properties are equivalent. Moreover, it follows from Lemma 5 that **(iii)** implies that $x \mapsto x^d$ is almost bent and has degree at most $\frac{t-1}{2}$. □

Proposition 12 enables us to exhibit some bent functions in family $\mathcal{M}$ which admit no bent 4-decomposition. We only have to choose an APN power permutation $x \mapsto x^s$ over $\boldsymbol{F}_{2^t}$ which is not almost bent or whose degree exceeds $\frac{t-1}{2}$. As an example, the following corollary exhibits an infinite family of cubic bent functions in family $\mathcal{M}$ which admit no bent 4-decompositions. These functions are derived from the quadratic APN power permutations (defined by Gold exponents [23]). They exist for any m such that $m \equiv 2 \bmod 4$ and $m \geq 10$. Recall that we proved that, for any $m \leq 8$, any m-variable cubic bent function admits a decomposition into four bent functions (since its dual has degree 3).

Corollary 6: Let $m = 2t$ be an even integer such that t is odd and $t \geq 5$. Let h be any Boolean function in $\mathcal{B}_t$. The m-variable bent function

$$f(x, y) = \mathrm{Tr}(xy^{2^i+1}) + h(y)$$

where i is any integer such that $\gcd(i, t) = 1$ and $1 \leq i \leq \frac{t-1}{2}$, admits no decomposition into four bent functions.

Proof: The power function $x \mapsto x^{2^i+1}$ is an APN permutation [16], [23]. The previous proposition implies that if f admits a decomposition into four bent functions, then the function $x \mapsto x^d$ corresponding to the inverse of $x \mapsto x^{2^i+1}$ has degree at most $(t-1)/2$. But, it is known that the inverse of this power permutation has degree $(t+1)/2$ [16, Proposition 5] because

$$d = \sum_{k=0}^{\frac{t-1}{2}} 2^{2ik} \bmod (2^t - 1).$$ □

Other examples of bent functions in $\mathcal{M}$ which admit no bent 4-decomposition can be derived from APN power permutations which are not almost bent. Some examples are $x \mapsto x^d$ over $\boldsymbol{F}_{2^t}$ for $d = 2^{t-1} - 1$ [14], [16], and for $d = 2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$, where $t = 5i$ [24], [25]. Therefore, for $m = 2t$, t odd, and $t \geq 5$, the following m-variable bent functions in $\mathcal{M}$ admit no bent 4-decomposition:

$$f(x, y) = \mathrm{Tr}(xy^s) + h(y)$$

where h is any Boolean function in $\mathcal{B}_t$ and $s = 2^{t-1} - 1$ or $s = 2^{4i} - 1$ with $t = 5i$ (since $(2^{4i}-1)(2^{4i}+2^{3i}+2^{2i}+2^i-1) \equiv 2 \bmod (2^{5i} - 1)$).

VIII. Conclusion

Our study points out that the bent functions may differ on the properties of their 4-decompositions. For instance, any bent function whose dual has degree 3 admits a decomposition into four bent functions, whereas both families $\mathcal{M}$ and $\mathcal{PS}^-$ contain some bent functions which do not satisfy this property. In this context, it appears that the structure of a bent function highly depends on some properties of its dual, such as its degree and the Hamming weights of its second derivatives. Moreover, we have proved that the bent functions whose duals have a constant second derivative present some specificities. From any such bent function f, it is possible to derive some other bent functions. When $D_a D_b f = 1$, the restriction of f to $V = \langle a, b\rangle^\perp$ is a bent function, and when $D_a D_b f = 0$, the function $f + \phi_V$ is bent. However, determining the structures of the bent functions which are obtained this way from a known bent function remains an open problem.

Acknowledgment

The authors would like to thank Claude Carlet for helpful suggestions all along this work. Actually, this paper is based on several discussions with him concerning bent functions and the properties of their duals.

References

[1] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "On cryptographic properties of the cosets of $R(1, m)$," *IEEE Trans. Inform. Theory*, vol. 47, pp. 1494–1513, May 2001.

[2] X.-D. Hou, "Cubic bent functions," *Discr. Math.*, no. 189, pp. 149–161, 1998.

[3] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Advances in Cryptology—EUROCRYPT'89 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1990, vol. 434, pp. 549–562.

[4] C. Carlet, "Two new classes of bent functions," in *Advances in Cryptology—EUROCRYPT'93 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, vol. 765, pp. 77–101.

[5] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Fast Software Encryption (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, vol. 1008, pp. 61–74.

[6] J. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, Univ. Maryland, College Park, 1974.

[7] O. Rothaus, "On bent functions," *J. Combin. Theory Ser. A*, vol. 20, pp. 300–305, 1976.

[8] X.-D. Hou, "New constructions of bent functions," *J. Combin. Inform. System Sci.*, vol. 25, no. 1–4, pp. 173–189, 2000.

[9] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions," in *Advances in Cryptology—EUROCRYPT 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1807, pp. 507–522.

[10] C. Carlet, "Partially-bent functions," *Des. Codes Cryptogr.*, no. 3, pp. 135–145, 1993.
[11] M. Daum, H. Dobbertin, and G. Leander, "An algorithm for checking normality of Boolean functions," in *Proc. Int. Workshop on Coding and Cryptography—WCC 2003*, Versailles, France, Mar. 2003, pp. 133–142.
[12] A. Canteaut, M. Daum, H. Dobbertin, and G. Leander, "Normal and non normal bent functions," in *Proc. Int. Workshop on Coding and Cryptography—WCC 2003*, Versailles, France, Mar. 2003, pp. 91–100.
[13] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[14] G. Lachaud and J. Wolfmann, "The weights of the orthogonal of the extended quadratic binary Goppa codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 686–692, May 1990.
[15] R. L. McFarland, "A family of noncyclic difference sets," *J. Combin. Theory Ser. A*, vol. 15, pp. 1–10, 1973.
[16] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in Cryptology—EUROCRYPT'93 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1993, vol. 765, pp. 55–64.
[17] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Des. Codes Cryptogr.*, vol. 15, no. 2, pp. 125–156, 1998.
[18] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis," in *Advances in Cryptology—EUROCRYPT'94 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1995, vol. 950, pp. 356–365.
[19] T. Bending and D. F. der Flass, "Crooked functions, bent functions, and distance regular graphs," *Electron. J. Combin.*, vol. 5, no. 1, 1998, r34.
[20] E. van Dam and D. F. der Flass, "Codes, graphs, and schemes from nonlinear functions," Tilburg University, Tilburg, The Netherlands, Res. Memo. FEW 790, May 2000.
[21] P. Charpin, A. Tietäväinen, and V. Zinoviev, "On binary cyclic codes with minimum distance $d = 3$," *Probl. Inform. Transm.*, vol. 33, no. 4, pp. 287–296, 1997.
[22] A. Canteaut, "Differential cryptanalysis of Feistel ciphers and differentially uniform mappings," in *Proc. Selected Areas on Cryptography, SAC'97*, Ottawa, ON, Canada, 1997, pp. 172–184.
[23] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorrelation functions," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 154–156, Jan. 1968.
[24] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: A new class for n divisible by 5," preprint, 1999.
[25] A. Canteaut, P. Charpin, and H. Dobbertin, "Weight divisibility of cyclic codes, highly nonlinear functions on GF(2^m) and crosscorrelation of maximum-length sequences," *SIAM J. Discr. Math.*, vol. 13, no. 1, pp. 105–138, 2000.