Polynomials With Linear Structure and Maiorana–McFarland Construction

Pascale Charpin and Sumanta Sarkar

***Abstract*—In this paper, we study permutation polynomials over the finite fields that have linear structures. We present some results on such a permutation which transforms a hyperplane to another hyperplane. We fully characterize the bilinear polynomial with linear structure. The most important result of this paper is to show the relation between a Maiorana–McFarland function with an affine derivative and a polynomial with a linear structure. Moreover, we highlight this result in the context of resilient functions which are based on Maiorana–McFarland construction.**

***Index Terms*—Bent function, bilinear permutation, linear structure, linear space, Maiorana–McFarland function, permutation polynomial, resilient function.**

I. Introduction

LET $\mathcal{R}(r,n)$ denote the r-th order Reed-Muller code of length 2^n, which is basically the set of all n-variable Boolean functions having degree at most r. Bent functions with affine derivatives, i.e., derivatives in $\mathcal{R}(1,n)$, have been studied in [13] and (extensively) in [6]. In [13], Hou proved that all the 8-variable cubic bent functions have at least one affine derivative. However, the existence of 6-variable cubic bent functions which have no affine derivative was known [20]. So Hou raised the following question: for which dimensions do there exist cubic bent functions which have no affine derivative? This question was resolved in [6] by Canteaut and Charpin. They presented a class of cubic Maiorana–McFarland bent functions which have no affine derivative. They actually proved that for all $n \geq 6$, there exists an n-variable bent function which has no affine derivative if and only if $n \neq 8$. They also showed that if a bent function has an affine derivative then its dual also has an affine derivative. In this paper, we focus on the characterization of Maiorana–McFarland Boolean functions with affine derivatives. We show that such a function is defined by the existence of a polynomial with a linear structure. This result leads us to study permutation polynomials over finite fields with linear structures. In a more general context, we have in mind the characterization of permutations which have derivatives with low degree, notably when they are involved in some cryptosystems.

Linear structures have been studied in [16], [12], [8], [9]. In [16], Lai characterized the Boolean functions which admit linear structures. Dubuc [12] termed these functions as "weakly degenerate functions". Further Dubuc also characterized linear structures in terms of the Fourier transform. In [8], Charpin and Kyureghyan studied the polynomials of the form $F(x) = G(x) + \gamma \mathrm{Tr}(H(x))$, over $\mathbb{F}_{2^n}$, which are permutations. They showed that the considered problem is related to finding Boolean functions with linear structures and then presented some classes of permutation polynomials, by using Boolean functions which have linear structures. This was generalized in [9], where $F(x) \in \mathbb{F}_{p^n}[x]$, p is any prime number. In this paper we contribute some interesting results on the permutations with linear structure.

The paper is organized as follows. After some preliminaries, our aim in Section III is to propose a representation of permutations which have linear structures. Notably we prove that such a permutation provides a set of permutations which transform a hyperplane to another hyperplane (Theorem 3). These permutations have at least one affine component.

The problem of the existence of linear structures is developed in Section IV. After basic results, we fully characterize the so-called *bilinear polynomials* which have linear structures, proving that they cannot be bijective (Corollary 2). Further, we present a class of permutation polynomials which have linear structures. We prove that such polynomial can be of any even degree d, with $2 \leq d \leq n-1$ for odd n (Proposition 5). We study Maiorana–McFarland functions in Section V. By Theorem 7, we explain the relation between affine derivatives of such a function and a polynomial with linear structure. Later we present some constructions of Maiorana–McFarland bent functions for both cases: with affine derivatives and without affine derivatives. In Section VI, we indicate that Theorem 7 holds (in another form) when some resilient functions are considered.

II. Preliminaries

Let $\mathbb{F}_{2^n}$ be the finite field of 2^n elements. For any set E, the subset of nonzero elements of E is denoted by E^*. Any polynomial $F(X) \in \mathbb{F}_{2^n}[X]$ defines a function

$$\begin{aligned} F: \quad & \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \\ & x \mapsto F(x) \end{aligned}$$

which is called the *associated function of* $F(X)$. Recall that any function of a finite field into itself is given by a polynomial. Throughout the paper, we identify a polynomial with its associated function. In particular, a *permutation* polynomial over $\mathbb{F}_{2^n}$ defines a bijective function from $\mathbb{F}_{2^n}$ to itself.

Manuscript received January 25, 2010; revised October 18, 2010; accepted December 21, 2010. Date of current version May 25, 2011.

The authors are with SECRET Project-Team-INRIA Paris-Rocquencourt, 78153 Le Chesnay Cedex, France (e-mail: pascale.charpin@inria.fr; sumanta.sarkar@inria.fr).

Communicated by N. Yu, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2011.2133690

On the other hand, a so-called *linearized polynomial* has the following form:

$$L(X) = \sum_{k=1}^{n-1} c_k X^{2^k}, c_k \in \mathbb{F}_{2^n} \tag{1}$$

where at least one c_k is nonzero. Such a polynomial defines a *linear function* $x \mapsto L(x)$ over $\mathbb{F}_{2^n}$.

In this paper, the *weight* of an integer is the Hamming weight of the 2-adic expression of the integer. The *degree* of a polynomial $F(x)$ defined over $\mathbb{F}_{2^n}$ is the maximum of the weights of the exponents of x in $F(x)$. For instance $L(x)$, which is defined by (1) above, is always of degree 1.

Definition 1: Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. For $a \in \mathbb{F}_{2^n}$, the function $D_a F$ given by

$$D_a F(x) = F(x) + F(x+a), \text{ for all } x \in \mathbb{F}_{2^n}$$

is called the *derivative of F in the direction of a*. Further, $a \in \mathbb{F}_{2^n}^*$ is said to be a *linear structure* of F if the function $D_a F$ is constant.

By definition, it is clear that if $a \in \mathbb{F}_{2^n}$ is a linear structure of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ then

$$F(x) + F(x+a) = F(0) + F(a), \text{ for all } x \in \mathbb{F}_{2^n}. \tag{2}$$

If $F(0) + F(a) = c$ for some $c \in \mathbb{F}_{2^m}$, then a is called *c-linear structure*. It is clear that by adding 0 to the set of linear structures of F, we get a vector subspace of $\mathbb{F}_{2^n}$. It is called the *linear space* of F.

For any k dividing n, the function $Tr_k^n : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^k}$ is defined as

$$Tr_k^n(x) = x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{k(n/k-1)}}, x \in \mathbb{F}_{2^n}.$$

It will be denoted by $Tr(x)$ when $k = 1$. From now on, we will only consider functions from $\mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ for the cases $m = n$ and $m = 1$ (i.e., Boolean function).

All Boolean functions assuming a linear structure have been characterized by Lai [16]. In [9], Charpin and Kyureghyan have done the characterization for the functions of univariate variables from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ of the form $Tr(R(x))$, where $R(x)$ is a function over $\mathbb{F}_{p^n}$ (where p is any prime number). More generally, one can find the following result in [16] with another terminology. We give our proof for clarity, using the method proposed in [9].

Theorem 1: Let $F(x)$ be a function over the field $\mathbb{F}_{2^n}$ with degree at least 1. Then $F(x)$ has a linear structure if and only if there is a non-bijective linear function $L(x)$ over $\mathbb{F}_{2^n}$ such that

$$F(x) = G(L(x)) + L_1(x) \tag{3}$$

for some function $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and some linear function $L_1(x)$ over $\mathbb{F}_{2^n}$.

Proof: First, note that if F is an affine function then any $a \in \mathbb{F}_{2^n}{}^*$ is a linear structure of F. Indeed, in this case $F(x) = L_1(x) + c$ where L_1 is linear and $c \in \mathbb{F}_{2^n}$. So, for any $a \in \mathbb{F}_{2^n}$ we have $F(x) + F(x+a) = L_1(a)$ for all $x \in \mathbb{F}_{2^n}$. Therefore, (3) holds where G is the identity and $L(x) = c$ for all x.

From now on we assume that F has degree at least 2. Suppose that (3) holds for F. Since $L(x)$ is non-bijective, there exists $a \in \mathbb{F}_{2^n}^*$ such that $L(a) = 0$. Then we have

$$\begin{aligned} F(x) + F(x+a) &= G(L(x)) + L_1(x) \\ &\quad + G(L(x+a)) + L_1(x+a) \\ &= G(L(x)) + G(L(x) + L(a)) \\ &\quad + L_1(a) \\ &= G(L(x)) + G(L(x)) + L_1(a) \\ &= L_1(a), \text{ for all } x \in \mathbb{F}_{2^n}. \end{aligned}$$

Therefore, a is a linear structure of F.

Conversely, let $F(x)$ be a function over $\mathbb{F}_{2^n}$ having some linear structures. Denote by S the linear space of F. If k is its dimension then S is generated by a basis $\{a_1, \ldots, a_k\}$. We assume that a_i is a c_i-linear structure for every $i \in \{1, \ldots, k\}$. Therefore, for each $i \in \{1, \ldots, k\}$ we have

$$F(x) + F(x + a_i) = c_i, \text{ for all } x \in \mathbb{F}_{2^n}.$$

Also note that for any $(\delta_1, \ldots, \delta_k) \in \{0,1\}^k$, we have

$$F(x) + F\left(x + \sum_{i=1}^{k} \delta_i a_i\right) = \sum_{i=1}^{k} \delta_i c_i, \quad \forall x \in \mathbb{F}_{2^n}. \tag{4}$$

We extend the basis $\{a_1, \ldots, a_k\}$ of S to the basis $\{a_1, \ldots, a_k, a_{k+1}, \ldots, a_n\}$ of $\mathbb{F}_{2^n}$. First, we define a linear function L with the kernel S. Secondly we define another linear function L_1 by $L_1(a_i) = c_i$, for all $i \in \{1, \ldots, n\}$, where we choose $c_{k+1}, \ldots, c_n$ arbitrarily from $\mathbb{F}_{2^n}$. Now define $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ as

$$G(y) = \begin{cases} L_1(x) + F(x), & \text{if } y = L(x), \text{ for some} x \in \mathbb{F}_{2^n} \\ z_y, & \text{if } y \notin \text{Image}(L) \end{cases} \tag{5}$$

where z_y's are chosen arbitrarily from $\mathbb{F}_{2^n}$.

We show that G is well defined. Let $x_1, x_2 \in \mathbb{F}_{2^n}$ be such that $L(x_1) = L(x_2)$. Since $L(x_1 + x_2) = 0$, $x_2 = x_1 + \sum_{i=1}^{k} \delta_i a_i$, for some $(\delta_1, \ldots, \delta_k) \in \{0,1\}^k$. Then

$$\begin{aligned} L_1(x_2) + F(x_2) &= L_1\left(x_1 + \sum_{i=1}^{k} \delta_i a_i\right) \\ &\quad + F\left(x_1 + \sum_{i=1}^{k} \delta_i a_i\right) \\ &= L_1(x_1) + L_1\left(\sum_{i=1}^{k} \delta_i a_i\right) \\ &\quad + F(x_1) + \sum_{i=1}^{k} \delta_i c_i, \text{ by (4)} \\ &= L_1(x_1) + \sum_{i=1}^{k} \delta_i c_i + F(x_1) + \sum_{i=1}^{k} \delta_i c_i \\ &= L_1(x_1) + F(x_1). \end{aligned}$$

Therefore, $G(L(x_1)) = G(L(x_2))$, which justifies (5). Moreover we clearly defined G such that $F(x) = G(L(x)) + L_1(x)$ for all $x \in \mathbb{F}_{2^n}$, completing the proof. ∎

III. Permutations With Linear Structure

From Theorem 1, we have a precise expression of functions on $\mathbb{F}_{2^n}$ which have a linear structure. To have such an expression is difficult when we impose on such a function to be bijective. We want to exhibit specific properties of this kind of functions. First we discuss the following properties which are simply obtained.

Lemma 1: If F is a permutation of $\mathbb{F}_{2^n}$ then it cannot have a 0-linear structure.

Proof: If $a \in \mathbb{F}_{2^n}^*$ is a 0-linear structure of F then $F(x) = F(x+a)$, for all $x \in \mathbb{F}_{2^n}$, a contradiction. ∎

Lemma 2: Let F be a bijection over $\mathbb{F}_{2^n}$ and denote by F^{-1} the inverse function of F. Then, a is a b-linear structure of F if and only if b is an a-linear structure of F^{-1}.

Proof: By hypothesis, $F(x) + F(x+a) = b$ for all $x \in \mathbb{F}_{2^n}$. Thus, replacing $y = F(x)$, we have for all x or, equivalently, for all y:

$$\begin{aligned} F^{-1}(y) + F^{-1}(y+b) &= F^{-1}(F(x)) + F^{-1}(F(x)+b) \\ &= x + F^{-1}(F(x+a)) \\ &= x + x + a = a, \end{aligned}$$

completing the proof. ∎

If F is a permutation then $x \mapsto F(x)+c$ is also a permutation for any constant $c \in \mathbb{F}_{2^n}$. Moreover, both functions have the same linear space. Thus we can assume that $F(0) = 0$ without loss of generality. Recall that the hyperplanes of $\mathbb{F}_{2^n}$ can be described as the set of $2^n - 1$ subspaces of $\mathbb{F}_{2^n}$

$$H_\beta = \{y \,|\, Tr(\beta y) = 0\}, \beta \in \mathbb{F}_{2^n}^*. \tag{6}$$

Note that $Tr(\beta y) = 0$ is equivalent to $y \in \beta^{-1}H_1$. Thus, $H_\beta = H_\lambda$ is equivalent to $\lambda = \beta$. Also $Tr(\beta a) = 1$, i.e., $a \notin H_\beta$, for exactly 2^{n-1} such β. From now on, in this section, F is a permutation on $\mathbb{F}_{2^n}$ such that

$$F(0) = 0 \text{ and } F(x) + F(x+a) = F(a) \tag{7}$$

for all $x \in \mathbb{F}_{2^n}$, for some $a \neq 0$. To construct such a permutation F by using Theorem 1 is not immediate. However a direct construction is easy as we show now. Taking any $a \in \mathbb{F}_{2^n}^*$:

1) choose a hyperplane H_β such that $Tr(\beta a) = 1$ (i.e., $a \notin H_\beta$).
2) fix $F(0) = 0$, set $b = F(a)$ and $M = \mathbb{F}_{2^n} \setminus \{0, b\}$; set $H_\beta = \{x_1, \ldots, x_{2^{n-1}}\}$, with $x_1 = 0$.
3) for any i, from 2 to 2^{n-1}, consider the pair $(x_i, x_i + a)$, $x_i \in H_\beta$; choose $y_i = F(x_i)$ in M and set $F(x_i + a) = y_i + b$;
4) on each step i replace: $M := M \setminus \{y_i, y_i + b\}$.

At the end, for any pair $(F(x), F(x+a))$, one element will be in and the other outside of $F(H_\beta)$; by construction, F is a permutation satisfying (7). Now we are going to specify such F and its image by means of the hyperplanes of $\mathbb{F}_{2^n}$, after recalling a useful theorem.

Theorem 2: [8, Theorem 2] Let $G(x), H(x) \in \mathbb{F}_{2^n}[x], \gamma \in \mathbb{F}_{2^n}$ and $G(x)$ be a permutation polynomial. Then

$$F(x) = G(x) + \gamma \mathrm{Tr}(H(x))$$

is a permutation polynomial of $\mathbb{F}_{2^n}$ if and only if $H(x) = R(G(x))$, where $R(x) \in \mathbb{F}_{2^n}[x]$ and γ is a 0-linear structure of the Boolean function $Tr(R(x))$.

Theorem 3: Let F be a permutation on $\mathbb{F}_{2^n}$ with $F(0) = 0$. Assume that F has a linear structure $a \in \mathbb{F}_{2^n}^*$. Then, for any $\beta \in \mathbb{F}_{2^n}^*$ such that $Tr(\beta a) = 1$ and for any λ such that $Tr(\lambda F(a)) = 1$, there is a permutation $G_{\beta,\lambda}$ such that

$$G_{\beta,\lambda}(F(H_\beta)) = H_\lambda.$$

Moreover, setting $P_{\beta,\lambda} = G_{\beta,\lambda} \circ F$:

- a is a linear structure of the permutation $P_{\beta,\lambda}$;
- the derivatives of $P_{\beta,\lambda}$ satisfy:
  — if $b \in H_\beta$ then $P_{\beta,\lambda}(x) + P_{\beta,\lambda}(x+b) \in H_\lambda$ for all x;
  — if $b \notin H_\beta$ then $P_{\beta,\lambda}(x) + P_{\beta,\lambda}(x+b) \notin H_\lambda$ for all x.
- the Boolean function $x \mapsto \mathrm{Tr}(\lambda P_{\beta,\lambda}(x))$ is affine.

Proof: We assume that F is a permutation satisfying (7). Let $\beta, \lambda \in \mathbb{F}_{2^n}^*$ such that $Tr(\beta a) = 1$ and $Tr(\lambda F(a)) = 1$. Define

$$G_{\beta,\lambda} : y \longmapsto y + F(a) Tr(\beta F^{-1}(y) + \lambda y). \tag{8}$$

Let f be the Boolean function $f(y) = Tr(\beta F^{-1}(y) + \lambda y)$. The function $G_{\beta,\lambda}$ is a permutation if and only if $F(a)$ is a 0-linear structure of f (see Theorem 2). We compute the derivative of f with respect to $F(a)$:

$$\begin{aligned} f(y) + f(y + F(a)) &= \mathrm{Tr}(\beta(F^{-1}(y) + F^{-1}(y + F(a))) \\ &\quad + \lambda F(a)) \\ &= \mathrm{Tr}(\beta a + \lambda F(a)) = 1 + 1 = 0 \end{aligned}$$

since $F(a)$ is an a-linear structure of F^{-1} (see Lemma 2). Thus, we have proved that $G_{\beta,\lambda}$ is a permutation, for any pair (β, λ) as defined above. Now we examine the image set of the permutation $P_{\beta,\lambda} = G_{\beta,\lambda} \circ F$. We have, using (8):

$$P_{\beta,\lambda}(x) = F(x) + F(a) Tr(\beta x + \lambda F(x)). \tag{9}$$

Hence, for any $x \in H_\beta$

$$\begin{aligned} Tr(\lambda P_{\beta,\lambda}(x)) &= \mathrm{Tr}(\lambda F(x)) \\ &\quad + \mathrm{Tr}(\lambda F(a)) Tr(\beta x + \lambda F(x)) \\ &= \mathrm{Tr}(\lambda F(x) + \beta x + \lambda F(x)) = 0 \end{aligned}$$

since $Tr(\lambda F(a)) = 1$ and $Tr(\beta x) = 0$. Thus, $P_{\beta,\lambda}(x) \in H_\lambda$, for any $x \in H_\beta$, implying $P_{\beta,\lambda}(H_\beta) = H_\lambda$. Now we look at the derivatives of $P_{\beta,\lambda}$. First, using (7)

$$P_{\beta,\lambda}(x) + P_{\beta,\lambda}(x+a) = F(a) + F(a) Tr(\beta a + \lambda F(a)) = F(a)$$

for all $x \in \mathbb{F}_{2^n}$, since $Tr(\beta a) = \mathrm{Tr}(\lambda F(a)) = 1$. So a is an $F(a)$-linear structure of $P_{\beta,\lambda}$. More generally, since $P_{\beta,\lambda}(x) \in H_\lambda$ for any $x \in H_\beta$, we have for any $b \in \mathbb{F}_{2^n}^*$ using (9)

$$\begin{aligned} D_b P_{\beta,\lambda}(x) &= F(x) + F(x+b) \\ &\quad + F(a) Tr(\beta b + \lambda(F(x) + F(x+b))) \end{aligned}$$

for all x. Now, with $g_b(x) = Tr(\lambda D_b P_{\beta,\lambda}(x))$

$$\begin{aligned} g_b(x) &= \mathrm{Tr}(\lambda(F(x)+F(x+b))) \\ &\quad + \mathrm{Tr}(\lambda F(a))Tr(\beta b + \lambda(F(x)+F(x+b))) \\ &= \mathrm{Tr}(\lambda(F(x)+F(x+b))) \\ &\quad + \mathrm{Tr}(\beta b + \lambda(F(x)+F(x+b))), \\ &= \mathrm{Tr}(\beta b) \end{aligned}$$

since $Tr(\lambda F(a)) = 1$. We conclude

$$g_b(x) = \begin{cases} 0, \text{ if } b \in H_\beta \\ 1, \text{ if } b \notin H_\beta. \end{cases}$$

Note that besides this result we have also proved that any $b \in \mathbb{F}_{2^n}^*$ is a linear structure of the function $h(x) = \mathrm{Tr}(\lambda P_{\beta,\lambda}(x))$. Thus h is affine, completing the proof. ■

Remark 1: Let F be a permutation with a linear structure a. By Theorem 3 we proved that such an F is strongly related with permutations F' satisfying: there is (β, λ) such that

$$F'(H_\beta) = H_\lambda, \mathrm{Tr}(\beta a)Tr(\lambda F'(a)) = 1. \tag{10}$$

However, the converse is more complicated. There are permutations without linear structure which send one given hyperplane to another.

Remark 2: We want to mention the link here with the so-called *crooked* functions which were introduced in [1], and more generally defined in [14]. A function F is crooked if the image of every derivative of F is an affine hyperplane. In this case F is a so-called *almost perfect nonlinear* (APN) function, i.e., all its derivatives are 2-to-1.

IV. Functions With(Out) Linear Structure

In this section, we exhibit an infinite class of permutations with linear structure. However, our purpose consists in a discussion on the existence of linear structures. We first indicate a basic result, whose proof is obvious because for an affine function its linear space equals $\mathbb{F}_{2^n}$.

Lemma 3: Let F be a function on $\mathbb{F}_{2^n}$. Then F has a linear structure, say $a \in \mathbb{F}_{2^n}^*$, if and only if a is a linear structure of $x \mapsto \lambda F(x) + L(x)$, for some $\lambda \in \mathbb{F}_{2^n}^*$ and some affine function L on $\mathbb{F}_{2^n}$.

Let i and j be two integers. We say that j *strictly covers* i if $i \neq j$ and, in the binary representation of i and j, every digit of i is less or equal to the corresponding digit of j. In this case we note $i \prec j$.

Theorem 4: Let $\alpha \in \mathbb{F}_{2^n}$. Let r and s be integers such that

$$1 \leq r, s \leq 2^n - 2.$$

Define the functions over $\mathbb{F}_{2^n}$

$$F(x) = \lambda(x^r + \alpha x^s) + L(x), \lambda \in \mathbb{F}_{2^n}^* \tag{11}$$

where L is any affine function. Then such a function F has no linear structure unless it is affine.

Proof: Thanks to Lemma 3, we have to study the function $F(x) = x^r + \alpha x^s$ only. If a is a linear structure of F then, using (2), we must have $D_a F(x) = a^r + \alpha a^s$. However,

$$\begin{aligned} D_a F(x) &= x^r + (x+a)^r + \alpha(x^s + (x+a)^s) \\ &= a^r + \alpha a^s + \sum_{0<\ell\prec r} a^{r-\ell}x^\ell + \alpha \sum_{0<\ell\prec s} a^{s-\ell}x^\ell. \end{aligned}$$

Then, we must have

$$\begin{aligned} P(x) &= \sum_{0<\ell\prec r} a^{r-\ell}x^\ell + \alpha \sum_{0<\ell\prec s} a^{s-\ell}x^\ell \\ &\equiv 0 \left(\mathrm{mod} x^{2^n} + x\right) \end{aligned} \tag{12}$$

which is impossible unless $P(x)$ is the null polynomial. Let $I_s = \{\ell \,|\, 0 < \ell \prec s\}$ and $I_r = \{\ell \,|\, 0 < \ell \prec r\}$; note that these sets can be empty.

If $I_s \neq I_r$, then $P(x)$ has at least one term corresponding to an exponent t of the form $a^k x^t$ with $k = r - t$ or $\alpha a^k x^t$ with $k = s - t$. Since $a \neq 0$ and $\alpha \neq 0$, it is impossible to have $P(x) = 0$ for all x. Note that this case happens notably for $\alpha = 0$ (i.e., when F is a monomial).

If $I_s = I_r \neq \emptyset$ then $r = s$ and F is a monomial. Finally $I_s = I_r = \emptyset$ is the only possibility, meaning that F is linear. ■

According to Theorem 1, we directly deduce:

Corollary 1: Let F be given by (11). Then F cannot be expressed in the form (3).

Note that the characterization of linear structures of a function F becomes difficult as soon as its expression includes more than two terms. We illustrate this fact by a simple example.

Example 1: The following F has 1 as linear structure

$$F(x) = x^{14} + x^{10} + x^{11} + x^7 + x^{13} + x^4 + x^5.$$

On the other hand, set $F(x) = x^{12} + x^5 + x^3$. Then F has no linear structure.

Next we summarize a few known results which characterize the so-called *component* (Boolean) functions of a permutation polynomial in terms of linear structures. Recall that a Boolean function f on $\mathbb{F}_{2^n}$ is said to be *balanced* when the set $\{x \,|\, f(x) = 1\}$ has cardinality 2^{n-1}.

Theorem 5: [18, Theorem 7.7] The function F over $\mathbb{F}_{2^n}$ is a permutation if and only if all its component functions

$$f_\lambda(x) = \mathrm{Tr}(\lambda F(x)), \lambda \in \mathbb{F}_{2^n}^*,$$

are balanced.

Note that if $F(x)$ is quadratic then the Boolean function $f_\lambda(x) = \mathrm{Tr}(\lambda F(x))$ is of degree at most 2 for all $\lambda \in \mathbb{F}_{2^n}^*$. The following result is currently known. A proof can be found in [5, Proposition A.1].

Proposition 1: Let f be a Boolean function of degree 2, then it is balanced if and only if there exists an element $a \in \mathbb{F}_{2^n}^*$ such that

$$D_a f(x) = 1, \text{ for all } x \in \mathbb{F}_{2^n}.$$

Combining Theorem 5 and Proposition 1, we get the following characterization of the quadratic permutation polynomials.

Theorem 6: Let $F(x)$ be any quadratic polynomial over $\mathbb{F}_{2^n}$. Then F is a permutation if and only if all its component functions $f_\lambda(x) = \mathrm{Tr}(\lambda F(x))$, $\lambda \in \mathbb{F}_{2^n}^*$, have a $1-$linear structure.

A. Bilinear Polynomials

The polynomials of the form $L_1(x)L_2(x)$, where $L_1(x)$ and $L_2(x)$ are two linear polynomials, are called *bilinear polynomials* [2], [17]. In [2], [17], some quadratic permutation polynomials have been identified in the class of bilinear polynomials of the form $xL(x)$. Below we characterize bilinear polynomials with linear structure.

Lemma 4: Let $L_1(x)L_2(x)$ be a bilinear polynomial. Then $a \in \mathbb{F}_{2^n}^*$ is a linear structure of $L_1(x)L_2(x)$ if and only if

$$L_2(a)L_1(x) + L_1(a)L_2(x) = 0, \text{ for all } x \in \mathbb{F}_{2^n}. \quad (13)$$

Proof: Using (2) we know that $a \in \mathbb{F}_{2^n}^*$ is a linear structure of $L_1(x)L_2(x)$ if and only if for all $x \in \mathbb{F}_{2^n}$

$$L_1(x)L_2(x) + L_1(x+a)L_2(x+a) = L_1(a)L_2(a). \quad (14)$$

Set $P(x) = D_a(L_1(x)L_2(x))$. We have

$$\begin{aligned} P(x) &= L_1(x)(L_2(x) + L_2(x+a)) + L_1(a)L_2(x+a) \\ &= L_2(a)L_1(x) + L_1(a)L_2(x) + L_1(a)L_2(a). \end{aligned}$$

Hence, (14) holds if and only if (13) holds, completing the proof. ∎

Note that by Theorem 6, we know that quadratic polynomials with linear structures exist, since quadratic permutations exist. For this special class of bilinear polynomials, we are able to give a complete result.

Proposition 2: Define the bilinear polynomial $F(x) = L_1(x)L_2(x)$. Assume that F is strictly bilinear, i.e., it is of degree 2.

Then, the linear structures of F are those $a \in \mathbb{F}_{2^n}^*$ such that $L_1(a) = L_2(a) = 0$. Consequently, if F is a permutation, it has no linear structure.

Proof: From Lemma 4, we know that $a \in \mathbb{F}_{2^n}^*$ is a linear structure of F if and only if (13) holds. Clearly, (13) holds when $L_1(a) = L_2(a) = 0$. In the case where $L_2(a) \neq 0$, we get

$$L_1(x) = \mu L_2(x), \mu = \frac{L_1(a)}{L_2(a)}, \text{ for all } x \in \mathbb{F}_{2^n}.$$

This leads to $F(x) = \mu(L_2(x))^2$, i.e., F is linear if $L_1(a) \neq 0$ and F is the null polynomial otherwise. On the other hand taking $L_1(a) \neq 0$ (at the beginning) we get a similar result and both cases contradict that F has degree 2.

So, if (13) holds then $L_2(a) = 0$ and, further, $L_1(a) = 0$. In this case, F cannot be a permutation since $F(a) = 0 = F(0)$, completing the proof. ∎

Thus, one can construct a bilinear polynomial with linear structure $a \in \mathbb{F}_{2^n}^*$ for any pair (L_1, L_2) of linear functions which have a as a common zero. Moreover, using Lemma 3, we obtain a more general result on the linear structures of quadratic polynomials.

Corollary 2: Let $F(x) = L_1(x)L_2(x) + L_3(x)$, where L_1 and L_2 are linear functions over $\mathbb{F}_{2^n}$ and L_3 is an affine function over $\mathbb{F}_{2^n}$. If L_1 or L_2 is bijective then F does not possess any linear structure.

Proof: If a is a linear structure of F then a is a linear structure of L_1L_2. From Proposition 2, this is possible if and only if $L_1(a) = L_2(a) = 0$. In this case, L_1 and L_2 are not bijective. ∎

So we have proved that any quadratic polynomial of the form

$$\sum_{i=1}^{n-1} \lambda_i x^{2^i+1} + \sum_{j=0}^{n-1} \mu_j x^{2^j}, \ \lambda_i \in \mathbb{F}_{2^n}, \mu_j \in \mathbb{F}_{2^n}$$

cannot have any linear structure.

Example 2: In [11], Dobbertin introduced a class of quadratic permutation polynomials as $x^{2^{m+1}+1} + x^3 + x$ over $\mathbb{F}_{2^{2m+1}}$. Since

$$x^{2^{m+1}+1} + x^3 + x = x\left(x^{2^{m+1}} + x^2\right) + x,$$

then using Corollary 2, it is clear that these permutations cannot have any linear structure.

B. A Class of Permutations With Linear Structure

In [8], a class of permutation polynomials was presented as follows.

Proposition 3: [8, Lemma 4] Let $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a linear 2-to-1 mapping with kernel $\{0, \alpha\}$ and $H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. If for some $\gamma \in \mathbb{F}_{2^n}$ the mapping

$$N(x) = L(x) + \gamma \mathrm{Tr}(H(x))$$

is a permutation of $\mathbb{F}_{2^n}$, then γ does not belong to the image set of L. Moreover, for such an element γ the mapping $N(x)$ is a permutation if and only if α is a 1-linear structure of $Tr(H(x))$.

Recall that the equation

$$x^2 + ax + b = 0, a \in \mathbb{F}_{2^n}^*$$

has no solution in $\mathbb{F}_{2^n}$ if and only if $Tr(b/a^2) \neq 0$.

Based on Proposition 3, we are able to construct quadratic permutation polynomials with linear structure. The next proposition is a particular case of [8, Theorem 6].

Proposition 4: Let n be odd and let i be an integer such that $1 \leq i \leq n-1$. Then the quadratic polynomial of the form

$$N(x) = x(x+1) + \gamma \mathrm{Tr}\left(x^{2^i+1}\right),$$

where $Tr(\gamma) \neq 0$, is a permutation polynomial over $\mathbb{F}_{2^n}$ with the linear structure 1.

Proof: Let $L(x) = x(x+1)$, then L is a 2-to-1 linear function with kernel $\{0,1\}$. Since $Tr(\gamma) \neq 0$, it is impossible to have $x^2 + x + \gamma = 0$. Hence, γ is not in the image set of L. Now, we have

$$Tr\left(x^{2^i+1} + (x+1)^{2^i+1}\right) = \mathrm{Tr}\left(x^{2^i} + x + 1\right) = \mathrm{Tr}(1) = 1$$

since n is odd, which shows that 1 is a 1-linear structure of $Tr(x^{2^i+1})$. Therefore, by Proposition 3, $N(x)$ is a permutation polynomial over $\mathbb{F}_{2^n}$.

Again, we have for any $x \in \mathbb{F}_{2^n}$

$$N(x) + N(x+1) = L(1) + \gamma \mathrm{Tr}(1) = 0 + \gamma = \gamma.$$

So, 1 is a linear structure of $N(x)$, completing the proof. ∎

Remark 3: It has been proved in [8] that for any integer s, $0 \leq s \leq 2^n - 2$, such that $s \notin \{2^i, 2^i + 2^j\}$ for all integers i and j, the Boolean function $x \mapsto \mathrm{Tr}(\delta x^s)$ can never have a linear structure (for any $\delta \in \mathbb{F}_{2^n}$). Therefore, one cannot construct any permutation polynomial having degree more than 2 and of the form

$$N(x) = L(x) + \gamma \mathrm{Tr}(x^s)$$

where $L(x)$ and γ are as given in Proposition 3.

Moreover, since $Tr(x^s)$ does not have a linear structure, $N(x) = L(x) + \gamma \mathrm{Tr}(x^s)$ does not have any linear structure too.

However, using Proposition 3 again, we are going to construct permutations of higher degree which have a linear structure. This construction is an example of an infinite class of higher degree permutations with a linear structure over $\mathbb{F}_{2^n}$ for odd n. There may be some other classes of higher degree permutations over $\mathbb{F}_{2^n}$ that have linear structures too.

Observe that if $H(x)$ has a linear structure a, then a is also a linear structure of $Tr(H(x))$. Moreover, if a is a 1-linear structure of $Tr(H(x))$, then

$$N(x) = x(x+a) + \gamma \mathrm{Tr}(H(x))$$

where $Tr(\gamma/a^2) \neq 0$, is a permutation polynomial with the linear structure a (see Proposition 3).

Lemma 5: Let s and i be two integers such that $1 \leq s \leq 2^n - 2$ and $0 \leq i \leq n-1$. Set

$$H(x) = x^s + x^{2^i}(x^s + (x+1)^s + 1).$$

Then for any i, $H(x) + H(x+1) = 1$, for all $x \in \mathbb{F}_{2^n}$.

Proof: We simply compute the derivative of H at the point 1 and for any i.

$$\begin{aligned} D_1 H(x) &= x^s + (x+1)^s \\ &\quad + x^{2^i}(x^s + (x+1)^s + 1) \\ &\quad + \left(x^{2^i} + 1\right)(x^s + (x+1)^s + 1) \\ &= x^s + (x+1)^s + (x^s + (x+1)^s + 1) \\ &= 1, \text{ for all } x. \end{aligned}$$

Thus 1 is a 1-linear structure of H. ∎

Proposition 5: Let n be odd, $n \geq 5$ and let k be an odd integer such that $1 \leq k \leq n-2$. Let

$$s = 1 + 2^{i_1} + \cdots + 2^{i_k}, 1 \leq i_1 < \cdots < i_k \leq n-2,$$

i.e., $3 \leq s \leq 2^{n-1} - 1$. Consider the function

$$N(x) = x(x+1) + \gamma \mathrm{Tr}(H(x))$$

where $H(x) = x^s + x^{2^{n-1}}(x^s + (x+1)^s + 1)$ and $\gamma \in \mathbb{F}_{2^n}^*$ satisfies $Tr(\gamma) = 1$.

Then $N(x)$ is a permutation of degree $k+1$ which has 1 as a γ-linear structure.

Proof: From Lemma 5 we know that 1 is a 1-linear structure of H. Hence, for all $x \in \mathbb{F}_{2^n}$

$$Tr(H(x)) + \mathrm{Tr}(H(x+1)) = \mathrm{Tr}(1) = 1.$$

According to Proposition 3, N is a permutation. Moreover

$$N(x) + N(x+1) = 0 + \gamma \mathrm{Tr}(H(x) + H(x+1)) = \gamma.$$

Now we look at the degree of N. We have clearly

$$H(x) = x^s + \sum_{r \neq 0, r \prec s} x^{r + 2^{n-1}}.$$

Note that in $H(x)$, the exponents s and $r + 2^{n-1}$, where $r = s - 2^i$ for some $i \in \{0, i_1, \ldots, i_k\}$, only have the maximum weight, i.e., $k+1$. In total, there are $k+2$ exponents of weight $k+1$. Among these $k+2$ exponents, if two exponents belong to the same cyclotomic coset, then they cancel each other in $Tr(H(x))$. Since k is odd and so is $k+2$, therefore, at least one exponent will not be canceled out in $Tr(H(x))$ by some other exponent. Thus, the degree of $Tr(H(x))$ is also equal to $k+1$ and hence the degree of $N(x)$ is equal to $k+1$ (the Hamming weight of s). ∎

V. Maiorana–McFarland Bent Functions Without Affine Derivative

In [13], Hou proved that all the 8-variable cubic Boolean bent functions have at least one derivative in $\mathcal{R}(1,n)$. In [6], Canteaut and Charpin presented a family of n-variables, $n \geq 6$ and $n \neq 8$ cubic bent functions which have no derivative in $\mathcal{R}(1,n)$. Those functions belong to the Maiorana–McFarland class which was extensively studied by Dillon [10, pp. 90–95]. This class is usually called the *class* $\mathcal{M}$ of bent functions. Using our previous results, we propose a more general approach.

Lemma 6: Let $n = 2t$. Let us consider a Boolean function f defined by

$$f : (x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \mapsto \mathrm{Tr}_1^t(x\pi(y) + h(y)) \qquad (15)$$

where π is a function over $\mathbb{F}_{2^t}$ and h is any function on $\mathbb{F}_{2^t}$. Then, f is a bent function if and only if π is a bijection. In this case, f is said to belong to the class $\mathcal{M}$ of bent functions.

Theorem 7: Let $n = 2t$. Let π be a function over $\mathbb{F}_{2^t}$ of degree ℓ, $1 < \ell \leq t-1$. Let f be a function given by (15) where the degree of h is less than or equal to 2. Then f has no affine derivative if and only if π does not have any linear structure.

In this case, if π is a bijection then f is a bent function without affine derivative.

Proof: Note that, since the degree of h is less than or equal to ℓ, the degree of f is exactly $\ell+1$. Take $a, b \in \mathbb{F}_{2^t}$. Then

$$\begin{aligned} D_{(a,b)}f(x,y) &= \mathrm{Tr}_1^t(x\pi(y) + (x+a)\pi(y+b) \\ &\quad + h(y) + h(y+b)) \\ &= \mathrm{Tr}_1^t(a\pi(y+b)) + \mathrm{Tr}_1^t(x(\pi(y) \\ &\quad + \pi(y+b)) + h(y) + h(y+b)). \end{aligned}$$

It is clear that the degree of $D_{(a,b)}f$ is at most ℓ. If $a \neq 0$, then the term $a\pi(y+b)$ asserts that $D_{(a,b)}f$ is of degree exactly ℓ. In this case, $D_{(a,b)}f$ is not affine.

Let us now investigate for the case $a = 0$. In this case, we have

$$\begin{aligned} D_{(0,b)}f(x,y) = \mathrm{Tr}_1^t(x(\pi(y) + \pi(y+b)) \\ +h(y) + h(y+b)). \end{aligned}$$

Since $\ell > 1$ and any derivative of h is affine or constant, $D_{(0,b)}f$ is affine if and only if the function $y \mapsto \pi(y) + \pi(y+b)$ is constant, i.e., b is a linear structure of π.

When π is a permutation, f is a bent function belonging to $\mathcal{M}$ (see Lemma 6). ∎

By Theorem 7, we are able to construct bent functions of any degree $d, 3 \leq d \leq t$, on $\mathbb{F}_{2^n}$ $(n = 2t)$ which have affine derivatives. For example, we obtain the following result directly from Proposition 5.

Corollary 3: Let $n = 2t$ with t odd. Let N be defined as in Proposition 5. Then $f(x,y) = \mathrm{Tr}_1^t(xN(y))$ is a bent function of degree $d = k+2$ whose derivative at the point 1 is affine.

On the other hand we can state some general results such as the following which generalizes [6, Lemma 1].

Corollary 4: Let $n = 2t$. Let r and s be integers such that $1 \leq r, s \leq 2^n - 2$. Let $\alpha \in \mathbb{F}_{2^n}$. Assume that $y \mapsto y^r$ has degree $\ell > 1$ and h is any function of degree at most 2. Then the function

$$f : (x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \mapsto \mathrm{Tr}_1^t(x(y^r + \alpha y^s) + h(y))$$

does not have any affine derivative. In particular, any function

$$f : (x,y) \mapsto \mathrm{Tr}_1^t\left(xy^{2^i+1}\right) \text{ with } \frac{t}{\gcd(t,i)} \text{ odd}$$

is a bent function without affine derivatives.

Proof: By Theorem 7, we know that the function $y \mapsto y^r + \alpha y^s$ has no linear structure. Hence we can apply Theorem 7. In particular, we get the class of cubic bent functions without any affine derivative introduced in [6]. Note that 2^i+1 is coprime to 2^t-1 (i.e., $y \mapsto y^{2^i+1}$ is a permutation) if and only if $t/\gcd(t,i)$ is odd (see for instance [19, Lemma 11.1]). ∎

Theorem 7 also has a surprising consequence. By Hou's result [13], we know that all the cubic bent functions of 8 variables have at least one affine derivative. In particular this property holds for bent functions of the form (15) with $t = 4$ and where π is a permutation on $\mathbb{F}_{2^4}$. Thus we have:

Corollary 5: Any quadratic permutation over $\mathbb{F}_{2^4}$ has at least one linear structure.

Note that quadratic permutations over $\mathbb{F}_{2^4}$ do exist (see a simple example below). Corollary 5 leads us to suggest the following open problem.

Open Problem 1: How to define a family $\mathcal{P}$ of quadratic permutations each having a linear structure, satisfying (i) and (ii) stated below:

i) $\mathcal{P}$ contains permutations over $\mathbb{F}_{2^n}$ for n taking an infinite number of values;
ii) any quadratic permutation over $\mathbb{F}_{2^4}$ is contained in $\mathcal{P}$.

Example 3: It is easy to check that the function

$$x \mapsto x + Tr(x^3) \text{ over } \mathbb{F}_{2^4}$$

is a permutation, and its derivative at point 1 is

$$1 + Tr(x^2 + x + 1) = 1 + Tr(1) = 1.$$

In [6, Section IV], it was proved that a bent function has an affine derivative if and only if its dual has an affine derivative. The dual of a bent function f of the class $\mathcal{M}$ given by (15) is known to be as follows:

$$\tilde{f} : (x,y) \mapsto \mathrm{Tr}_1^t(y\pi^{-1}(x) + h(\pi^{-1}(x)))$$

(where π is a permutation). Let f be a bent function, defined as in Theorem 7. If π has no linear structure then f has no affine derivative. Thanks to Lemma 2, π^{-1} has no linear structure too; further $\tilde{f}$ has no affine derivative. So we prove, by another way, an instance of the result given in [6].

VI. Cryptographic Relevance

So far we have considered functions over the finite field $\mathbb{F}_{2^n}$. Let $\mathbb{F}_2^n$ denote the vector space of 2^n binary n-tuples. The vector space $\mathbb{F}_2^n$ can easily be identified to the field $\mathbb{F}_{2^n}$. This is done by choosing a basis $\{\alpha_1, \ldots, \alpha_n\}$ of the vector space $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then an element $x \in \mathbb{F}_{2^n}$ can be described as $\sum_{i=1}^n x_i\alpha_i$, i.e., we can identify x to the n-tuple

$$(x_1, \ldots, x_n) \in \mathbb{F}_2^n, x_i \in \mathbb{F}_2 \text{ for } i = 1 \ldots n.$$

The number of nonzero x_i's is the Hamming weight of x, denoted by $wt(x)$, and any Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is an n-variable Boolean function. The n-variable function f can be expressed as a sum of products of $x_1, x_2, \ldots, x_n$ as

$$f(x_1, \ldots, x_n) = \bigoplus_{u=(u_1,\ldots,u_n)\in\mathbb{F}_2^n} \Gamma_u \left(\prod x_i^{u_i}\right).$$

This representation is called the algebraic normal form (ANF) of f. The maximum value of $wt(u)$ such that $\Gamma_u \neq 0$ is called the *algebraic degree* of f. For example

$$f(x_1, x_2, x_3, x_4) = x_1 + x_2x_3 + x_2x_3x_4$$

is a 4-variable Boolean function with algebraic degree 3. The ANF representation of f is unique.

Let f be a Boolean function represented by a univariate polynomial $F(x)$ over $\mathbb{F}_{2^n}$. Using the relation $\sum_{i=1}^{n} x_i\alpha_i$, one can obtain the ANF of f. It can also be shown that the value of the degree of $F(x)$ as it was defined in Section II, is the same as the algebraic degree of f. Henceforth, we will only say *degree* instead of algebraic degree for any Boolean function defined over $\mathbb{F}_2^n$.

There are several cryptosystems in which Boolean functions are used. For instance, in some LFSR based stream ciphers, a Boolean function is used to combine the outputs of several LFSRs. For secure design purpose, it is required that the output of the Boolean function should not have correlation with a subset of input variables. Otherwise, one can mount the correlation attack [21] by exploiting the statistical dependence between the input variables and the output of the Boolean function. Therefore in order to resist this attack it is required that the Boolean function remains balanced if some input bits are kept constant. From this requirement, the concept of *resiliency* comes.

A Boolean function $g : \mathbb{F}_2^n \to \mathbb{F}_2$ is k-resilient if and only if

$$W_g(\lambda) = \sum_{z\in\mathbb{F}_2^n} (-1)^{f(z)+\lambda\cdot z} = 0$$

for all $\lambda \in \mathbb{F}_2^n$ such that $wt(\lambda) \le k$, where $\lambda \cdot z$ denotes the usual dot product over $\mathbb{F}_2^n$.

There are several constructions of resilien
t functions. There is one construction, introduced in [4, Proposition 4.2], which is quite similar to the Maiorana–McFarland construction of bent functions.

Proposition 6: [4] Let k be an integer such that $0 \le k \le n-r-2$. Let $G : \mathbb{F}_2^r \to \mathbb{F}_2^{n-r}$ be any function such that $wt(G(y)) \ge k+1$ for all $y \in \mathbb{F}_2^r$. Then the Boolean function

$$f : \mathbb{F}_2^{n-r} \times \mathbb{F}_2^r \to \mathbb{F}_2$$

given by

$$f(x,y) = \langle x, G(y)\rangle_{n-r} + H(y)$$

is a k-resilient function of n variables, where H is any function from $\mathbb{F}_2^r$ to $\mathbb{F}_2^{n-r}$ and $\langle\cdot,\cdot\rangle_{n-r}$ is the dot product on $\mathbb{F}_2^{n-r}$.

Using the multivariate representation, after identifying the field $\mathbb{F}_{2^n}$ to the vector space $\mathbb{F}_2^n$, any Maiorana–McFarland bent function given by (15) can easily be defined over $\mathbb{F}_2^t \times \mathbb{F}_2^t$. Note that for $x, y \in \mathbb{F}_{2^n}$, $\mathrm{Tr}_1^t(xy)$ is identified with the scalar product $\langle \bar{x}, \bar{y}\rangle_t$, where $\bar{x}$ and $\bar{y}$ are the vectors in $\mathbb{F}_2^n$ corresponding to x and y respectively. Then it is easy to note the similarity between the above mentioned construction of resilient functions and the construction of Maiorana–McFarland bent functions. Thus, Theorem 7 can easily be extended in the case of resilient functions as follows.

Theorem 8: Let $G : \mathbb{F}_2^r \to \mathbb{F}_2^{n-r}$ be any function of degree ℓ, $1 < \ell \le r-1$, such that $wt(G(x)) \ge k+1$ for all $x \in \mathbb{F}_2^r$. Then the k-resilient function of degree more than 2

$$f : \mathbb{F}_2^{n-r} \times \mathbb{F}_2^r \to \mathbb{F}_2 \text{ where } f(x,y) = \langle x \cdot G(y)\rangle_{n-r}$$

does not possess any affine derivative if and only if G does not have any linear structure.

Proof: We simply translate the proof of Theorem 7 in the context of vector space. Take $(a,b) \in \mathbb{F}_2^{n-r} \times \mathbb{F}_2^r$. Then

$$\begin{aligned} D_{(a,b)}f(x,y) &= \langle x \cdot G(y)\rangle_{n-r} \\ &\quad + \langle (x+a)\cdot G(y+b)\rangle_{n-r} \\ &= \langle a \cdot G(y+b)\rangle_{n-r} \\ &\quad + \langle x \cdot (G(y)+G(y+b))\rangle_{n-r}. \end{aligned}$$

It is clear that the degree of $D_{(a,b)}f$ is at most ℓ. If $a \neq 0$, then the term $a \cdot G(y+b)$ asserts that $D_{(a,b)}f$ is of degree exactly ℓ. In this case, $D_{(a,b)}f$ is not affine.

On the other hand, when $a = 0$, we get

$$D_{(0,b)}f(x,y) = \langle x \cdot (G(y)+G(y+b))\rangle_{n-r}.$$

Since $\ell > 1$, $D_{(0,b)}f$ is affine if and only if the function $y \mapsto G(y)+G(y+b)$ is constant, i.e., b is a linear structure of G. ■

VII. Conclusion

The most significant result of this paper is that we have characterized when Maiorana–McFarland functions have affine derivatives. More generally, this characterization holds for any Boolean function which is of Maiorana–McFarland type. In particular, such resilient functions which have affine derivative are characterized. However, if a Maiorana–McFarland function has an affine derivate, so far it is not clear how to use this fact to mount some attacks.

Lai [15] proposed higher order differential attack which works for vectorial Boolean functions with low degree derivatives. Therefore, it will be interesting to find some attacks on Boolean functions in general which have low degree derivatives. This kind of attack on resilient functions of the Maiorana–McFarland type may be an interesting special case.

Acknowledgment

The authors would like to thank the anonymous reviewers whose comments have improved this paper.

References

[1] T. Bending and D. Fon der Flass, "Crooked functions, bent functions, and distance regular graphs," *Electron. J. Combin.*, vol. 5, no. 1, 1998, R34.

[2] A. Blokhuis, R. S. Coulter, M. Henderson, and C. M. O'Keefe, "Permutations amongst the Dembowski-Ostrom polynomials," in *Finite Fields and Applications: Proc. 5th Int. Conf. Finite Fields and Applications*, 2001, pp. 37–42.

[3] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "Determining the nonlinearity of a new family of APN functions," in *Proc. AAECC*, 2007, vol. 4851, pp. 72–79, Lecture Notes in Computer Science, Springer-Verlag.

[4] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation-immune functions," in *Proc. CRYPTO*, 1992, vol. 576, pp. 86–100, Lecture Notes in Computer Science.

[5] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "On cryptographic properties of the cosets of $R(1,m)$," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1494–1513, Apr. 2001.

[6] A. Canteaut and P. Charpin, "Decomposing bent functions," *IEEE Trans. Inf. Theory*, vol. 49, no. 8, pp. 2004–2019, Aug. 2003.

[7] C. Carlet, "More on correlation-immune function and resilient functions over Galois field and Galois ring," in *Proc. EUROCRYPT*, 1997, vol. 1233, pp. 422–433, Lecture Notes in Computer Science, Springer-Verlag.

[8] P. Charpin and G. M. Kyureghyan, "On a class of permutation polynomials over $\mathbb{F}_{2^n}$," in *Proc. SETA*, 2008, vol. 5203, pp. 368–376, Lecture Notes in Computer Science.
[9] P. Charpin and G. M. Kyureghyan, "When does $G(x)+\gamma\, Tr(H(x))$ permute $\mathbb{F}_{2^n}$?," *Finite Fields and Their Applic.*, vol. 15, no. 5, pp. 615–632, 2011.
[10] J. Dillon, "Elementary Hadamard Difference Sets," Ph.D. dissertation, Univ. of Maryland, College Park, 1974.
[11] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1271–1275, Apr. 1999.
[12] S. Dubuc, "Characterization of linear structures," *Des. Codes Cryptog.*, vol. 22, pp. 33–45, 2001.
[13] X.-D. Hou, "Cubic bent functions," *Discrete Maths.*, vol. 189, pp. 149–161, 1998.
[14] G. Kyureghyan, "Crooked maps in F_{2^n}," *Finite Fields Appl.*, vol. 13, no. 3, pp. 713–726, 2007.
[15] X. Lai, "Higher order derivatives and differential cryptanalysis," in *Commun. and Cryptog.*. Norwell, MA: Kluwer, 1994, pp. 227–233.
[16] X. Lai, "Additive and linear structures of cryptographic functions," in *Proc. FSE*, 1995, vol. 1008, pp. 75–85, Lecture Notes in Computer Science.
[17] Y. Laigle-Chapuy, "A note on a class of quadratic permutations over F_{2^n}," in *Proc. AAECC 17*, 2007, vol. 4851, pp. 130–137, Lecture Notes in Computer Science.
[18] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and Its Applications*, 2nd ed. Cambridge, MA: Cambridge University Press, 1997, vol. 20.
[19] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Norwell, MA: Kluwer, 1987.
[20] O. S. Rothaus, "On bent functions," *J. Combin. Theory Ser. A*, vol. 20, pp. 300–305, 1976.
[21] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 5, pp. 776–780, 1984.

Pascale Charpin received the Ph.D. degree and the Doctorate in sciences (theoretical computer science) from the University of Paris VII, Paris, France, in 1982 and 1987, respectively.

She was with the Department of Mathematics, University of Limoges, Limoges, France, from 1973 to 1982, and the University of Paris VI from 1982 to 1989. She is currently Director of Research at INRIA (the French National Institute for Research in Computer Science), Rocquencourt, France. She was the Scientific Head of the group CODES (coding and cryptography) at this institute from 1995 to 2002. Her research interests include finite algebra, algorithmic, and applications to coding (error-correcting coding and cryptology).

Dr. Charpin served on the Editorial Board of the IEEE TRANSACTIONS ON COMPUTERS from 2000 to 2004 and currently serves on the Editorial Board of *Designs, Codes and Cryptography*.

Sumanta Sarkar received the Master's degree in mathematics from the University of North Bengal, West Bengal, India, in 2002 and the Ph.D. degree from Jadavpur University, West Bengal, in 2008 (after completing research at the Indian Statistical Institute, Kolkata, India).

Currently he is a Postdoctoral Researcher at INRIA Paris-Rocquencourt.