HAL open science

The crooked property

Pascale Charpin

To cite this version:

Pascale Charpin. The crooked property. 2020. hal-03091422v1

HAL Id: hal-03091422

https://inria.hal.science/hal-03091422v1

Preprint submitted on 31 Dec 2020 (v1), last revised 13 May 2022 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

The *Crooked* property

Pascale Charpin*

December 15, 2020

Abstract

Crooked permutations were introduced twenty years ago to construct interesting objects in graph theory. These functions, over $\mathbb{F}_{2^n}$ with odd n, are such that their derivatives have as image set a complement of a hyperplane. The field of applications was extended later, in particular to cryptography. However binary crooked functions are rare. It is still unknown if non quadratic crooked functions do exist. We extend the concept and propose to study the *crooked property* for any characteristic. A function F, from $\mathbb{F}_{p^n}$ to itself, satisfies this property if all its derivatives have as image set an affine subspace. We show that the partially-bent vectorial functions and the functions satisfying the crooked property are strongly related. We later focus on the components of these functions, establishing that the existence of linear structures is here decisive. We then propose a symbolic approach to identify the linear structures. We claim that this problem consists in solving a system of linear equations, and can often be seen as a combinatorial problem.

Keywords: Affine subspace, vectorial function, Boolean function, planar function, derivative, differential set, plateaued function, partially-bent functions, quadratic functions, bent functions, APN function, permutation.

1 Introduction

The *crooked functions* have been introduced by Bending and Fon-Der-Flaass in 1998, as combinatorial objects of great interest [1]. These

*INRIA-Paris, 2 rue Simone IFF, Paris 75012, FRANCE, pascale.charpin@inria.fr.

functions were defined in characteristic 2; they are bijective and their derivatives have as image set the complement of a hyperplane. The initial work on crooked functions was widely extended and discussed, always in characteristic two (see [20, 23, 25]). A survey of these works is proposed in [12].

In this paper, we study the vectorial functions whose derivatives have as image set an affine subspace. We will say that such a function satisfies *the crooked property*. Note that linear, quadratic and planar functions satisfy the crooked property. We consider functions from the finite field $\mathbb{F}_{p^n}$ of order p^n to itself, where p is any prime number.

An overall study about binary *vectorial plateaued functions* is due to Carlet in a recent paper [10]. For plateaued functions in odd characteristic, see [30] and references herein. We will highlight, in this paper, the strong connection between the functions satisfying the crooked property and a subclass of vectorial plateaued functions, namely the vectorial *partially-bent functions*. The partially-bent Boolean functions were introduced in [9]. The generalization to any characteristic is presented in [11].

Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, and let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, which is any component of F. When a derivative of f, in some direction a, is constant, we say that a is a *linear structure* of f. By definition, the crooked property implies that some components of F, have at least one linear structure, unless F is planar. We propose a symbolic approach to treat the existence of linear structures of components of F, which is valid for treating any function F. By this method, the study of a set of linear equations and of its solutions informs us about the (non)existence of linear structures. Also, we show that the problem can be viewed as a combinatorial problem, and then can be easily solved in some cases.

After preliminaries, we recall, in Section 3, the definition of binary crooked functions. We briefly explain that our terminology originates from the cryptanalysis of the hash function Maraca [8]. The crooked property is presented in Section 4, where some constructions are proposed. In the following section, we study the links between crooked property and partially-bentness. Section 6 is devoted to the study of linear structures of the components of any function over $\mathbb{F}_{p^n}$.

2 Preliminaries

Thoughout this paper, $||E||$ denotes the cardinality of the set E, and $E^* = E \setminus \{0\}$; $\mathcal{I}m(G)$ denotes the image set of any mapping G.

Let F be a mapping, from the finite field $\mathbb{F}_{p^n}$ to itself, where p is any prime number. Such a function is called *a vectorial function*, while a function f, from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is called a *p-ary Boolean function*. When $p = 2$, we say *a Boolean function*, as usually. We call *derivative of* F, with respect to a, the function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$:

$$x \mapsto D_aF(x) = F(x+a) - F(x),\ a \in \mathbb{F}_{2^n}^*.$$

The same terminology is used for the derivatives of p-ary Boolean functions. The image set of any D_aF is called a *differential set* of the vectorial function F, with respect to a:

$$\mathcal{I}m(D_aF) = \{\ F(x+a) - F(x) \mid x \in\ \mathbb{F}_{p^n}\}. \tag{1}$$

The p-ary Boolean functions

$$f_\lambda\ :\ x\ \mapsto\ Tr(\lambda F(x))\ ,\quad \lambda \in \mathbb{F}_{p^n},$$

are the p^n *component functions of* F, where f_0 is the null function (by convention). They are here defined by means of the absolute trace function, from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$:

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

The *Walsh transform* of any p-ary Boolean function f is the complex valued function defined by

$$\widehat{f}(a) = \sum_{x \in \mathbb{F}_{p^n}} \xi^{f(x) - Tr(ax)},\ a \in \mathbb{F}_{p^n},$$

where $\xi = e^{2\pi i/p}$. The *Walsh spectrum* of f is the set of all values of $\widehat{f}$. We denote by $|\widehat{f}(a)|$ the modulus of $\widehat{f}(a)$. Note that $\xi = -1$ for $p = 2$ and, in this case, $|\widehat{f}(a)|$ is the absolute value of $\widehat{f}(a)$. We will need the following properties of any function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$.

- f is *balanced* if it takes every value of $\mathbb{F}_p$ the same number of times, i.e. $\widehat{f}(0) = 0$.

- $a \in \mathbb{F}_{p^n}^*$ is a *linear structure* of f if

$$f(x+a) - f(x) = c \text{ for all } x, \text{ where } \ c \in \mathbb{F}_p.$$

  The set of such a is the *linear space* of f. By adding 0, it is a linear subspace of $\mathbb{F}_{p^n}$.

The function f is said to be *bent* when $|\widehat{f}(a)| = p^{n/2}$, for all a. It is called a *s-plateaued* function, $0 \leq s \leq n$, when $|\widehat{f}(a)| \in \{0, p^{n+s}\}$. Note that a bent function is 0-plateaued. The value $p^{(n+s)/2}$ is called the *amplitude* of f.

A *plateaued vectorial function* is a vectorial function whose components are plateaued p-ary Boolean functions. A vectorial function is said to be *plateaued with single amplitude* when all its components have the same amplitude.

A polynomial $F(X) \in \mathbb{F}_{p^n}[X]$ is called a *permutation polynomial* over $\mathbb{F}_{p^n}$, if the induced function, $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, is a permutation. The next property is well-known (see for instance [28, Theorem 7.7]).

Theorem 1 *Let F be a function from $\mathbb{F}_{p^n}$ to itself, with components f_λ. The function F is a permutation if and only if every f_λ is balanced.*

Throughout this paper, the hyperplanes of $\mathbb{F}_{p^n}$, appear as relevant objects, in several definitions and properties. The hyperplanes of $\mathbb{F}_{p^n}$, considered as $(n-1)$-dimensional vector-spaces, can be represented by the $p^n - 1$ subspaces:

$$H_\lambda = \{ \ y \mid Tr(\lambda y) = 0 \ \}, \ \lambda \in \mathbb{F}_{p^n}^*. \tag{2}$$

We now recall the definition of the *algebraic degree* of any polynomial of $\mathbb{F}_{p^n}[X]$, and then of any function over $\mathbb{F}_{p^n}$ that it induces.

Definition 1 *Let $k \in \mathbb{N}$, $0 \leq k \leq p^n - 2$. Define the p-ary expansion and the p-weight of k as, respectively,*

$$k = \sum_{i=0}^{n-1} k_i p^i \quad \textit{and} \quad w_p(k) = \sum_{i=0}^{n-1} k_i.$$

Let $P \in \mathbb{F}_{p^n}[x]$, $P(x) = \sum_{k=0}^{p^n-2} u_k x^k$. The algebraic degree $\deg(P)$ of P is the maximum value of $w_p(k)$, for those k such that $u_k \neq 0$. In particular, P is said to be affine when $\deg(P) = 1$ and quadratic when $\deg(P) = 2$.

We end this section by recalling the definition of some functions of great interest, namely *the planar functions.*

Definition 2 *Let p be an odd prime. A function F, from $\mathbb{F}_{p^n}$ to itself, is called a* planar function *if for every $a \in \mathbb{F}_{p^n}$, the function*

$$x \mapsto D_a F(x) = F(x+a) - F(x),$$

is a permutation over $\mathbb{F}_{p^n}$.

Example 1 $F : x \mapsto x^2$ *is planar for any n and any odd p.*

For our purpose, it is important to notice that *not quadratic planar functions do exist.* This was proved by Coulter and Matthews (1997):

Theorem 2 [18] *The following functions, say F from $\mathbb{F}_{p^n}$ to itself where p is odd,*

$$F(x) = x^{p^s+1} \text{ where } \frac{n}{\gcd(s,n)} \text{ is odd,} \tag{3}$$

and, with $p = 3$, $2 < k < n$, $\gcd(k, 2n) = 1$,

$$F(x) = x^d \quad \text{where } d = \frac{3^k+1}{2}, \tag{4}$$

are planar functions.

3 The binary case

Note that the case where $p = 2$ was longly explained in [12]. We first recall the definition of crooked functions, which was given for any value of n in [25].

Definition 3 *A function F, from $\mathbb{F}_{2^n}$ to itself, is called* crooked *when it is such that, for every $a \in \mathbb{F}_{2^n}^*$, its differential set*

$$S_a = \{\ F(x) + F(x+a) \mid x \in \ \mathbb{F}_{2^n}\},$$

is an affine hyperplane.

A mapping F over $\mathbb{F}_{2^n}$ is said to be an *almost perfect nonlinear (APN) mapping* if and only if all the equations

$$D_aF(x) = F(x) + F(x+a) = b, \quad a,\ b \in \mathbb{F}_{2^n}\ ,\ a \neq 0\ , \tag{5}$$

have either zero or two solutions in $\mathbb{F}_{2^n}$, say x and $x+a$. It is easy to check that, when F is APN, the function D_aF is 2-to-1, for any $a \neq 0$. Thus, one can express the APN property as follows.

Proposition 1 *Any mapping F over $\mathbb{F}_{2^n}$ is APN if and only if for all non zero $a \in \mathbb{F}_{2^n}$, the differential set of F, with respect to a, has cardinality 2^{n-1}. In particular, crooked functions are APN functions.*

More generally, it is well-known that the resistance of a cipher to *differential cryptanalysis* is quantified by its so-called *differential uniformity* [3, 31]. Hence, the following definitions were introduced:

$$\begin{aligned} \delta_F(a,b) &= ||\{\ x \in \mathbb{F}_{2^n}\ |\ D_aF(x) = b\ \}||, \\ \delta(F) &= \max_{a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}} \delta_F(a,b), \end{aligned} \tag{6}$$

where $\delta(F)$ is the differential uniformity of F

The terminology, that we introduce in the next section, is an extension of those stated by Canteaut and Naya-Plasencia in [8]. The authors have first introduced a new concept, as follows.

Definition 4 *Let F be a function from $\mathbb{F}_{2^n}$ to itself. For any $\beta \in \mathbb{F}_{2^n}^*$, the set of differences leading to β is defined by*

$$\mathcal{D}_F(\beta) = \{\ a \in \mathbb{F}_{2^n}\ |\ \beta \in \mathcal{I}m(D_aF)\ \},$$

and $\Delta(F) = \max_{\beta\in\mathbb{F}_{2^n}^*} ||\mathcal{D}_F(\beta)||$.

When F is a permutation, it was proved that $\mathcal{D}_F(\beta) = \mathcal{I}m(D_\beta F^{-1})$, where F^{-1} is the compositional inverse of F. Thus, the authors obtained the following result:

Theorem 3 [8, Theorem 2.6] *Let F be a permutation over $\mathbb{F}_{2^n}$. Then we have*

$$||\mathcal{D}_F(\beta)|| \geq \frac{2^n}{\delta(F)} \textit{for any } \beta \in \mathbb{F}_{2^n},$$

with equality if and only if $\delta_F(a,\beta) \in \{0, \delta(F)\}$ for all $a \in \mathbb{F}_{2^n}$.

Remark 1 *A function F, from $\mathbb{F}_{2^n}$ to itself, is said* differentially two-valued *when $\delta_F(a,\beta)$ takes two values only, which are 0 and $\delta(F)$, for all a,β. According to the theorem above, the permutation F satisfies*

$$\Delta(F) = \frac{2^n}{\delta(F)}$$

if and only if F is differentially two-valued*. The two-valued functions were studied in [4, 13].*

An attack against a hash function, named Maraca, was presented in [8], which exploits the fact that $\Delta(F)$ is high, where F is the underlying permutation. More precisely, the inverse of the permutation F, over $\mathbb{F}_{2^8}$, which is used in Maraca, is such the all its differential sets are contained in an affine subspace of codimension 3. Such a function is said to be *weakly crooked of codimension* 3.

Remark 2 *The authors of [8] ask to the existence of permutations over $\mathbb{F}_{2^n}$ whose, at least, one differential set is an affine subspace. Such functions of degree 2 do exist, so that this problem concerns permutations of higher degree. Note that a permutation can have a linear structure; moreover, it is easy to construct such permutations (see section III, in [16]). Thus, one can obtain permutations that have the following property: half of their differential sets are included in the same hyperplane [16, Theorem 3].*

If $\deg(F) > 2$ and $\deg(D_aF) \leq 1$, then a is a so-called fast-point of any component of F. See [32] for a recent work about faster points.

Problem 1 *Recall that nowadays, the existence of crooked functions over $\mathbb{F}_{2^n}$, which are not quadratic, remains an open problem.*

4 The crooked property

In this paper, we want to generalize the concept of *crookedness*. Our purpose is to extend the definition of crooked functions in order to include more classes of functions, whose definition sets are related with affine subspaces of $\mathbb{F}_{p^n}$. We are going to fix the terminology. Note that, without loss of generality, we always consider functions F such that $F(0) = 0$.

Definition 5 *A function F from $\mathbb{F}_{p^n}$ to itself, is said to have the* crooked property *if* all *their differential sets are affine subspaces of $\mathbb{F}_{p^n}$. Moreover:*

- *F is said to be* crooked of codimension k *when every differential set $\mathcal{I}m(D_aF)$, $a \in \mathbb{F}_{p^n}^*$, is a flat of codimension k, $0 \leq k \leq n$.*
- *F is said to be* crooked *when it is crooked of codimension* 1*, i.e., every differential set of F is an affine hyperplane.*
- *F is said to be* weakly crooked of codimension k *when every differential set $\mathcal{I}m(D_aF)$, $a \in \mathbb{F}_{p^n}^*$, is contained in an affine subspace of $\mathbb{F}_{p^n}$ of codimension at least k.*

The following results are simply derived from the definitions.

Proposition 2 *Linear functions are crooked of codimension n.*
Crooked functions of codimension 0 *are planar functions.*
When $p = 2$, crooked functions are APN.

The main question is the existence of functions, of any degree, which have the crooked property. The weakly crooked functions were introduced in [8], for $p = 2$, but it is easy to construct such a function for any p and any degree.

Example 2 *Let G be any function from $\mathbb{F}_{p^n}$ to itself, where $n = 2m$, and*

$$F(x) = (G(x))^{p^m} + G(x).$$

Clearly, $\mathcal{I}m(F)$ is included in $\mathbb{F}_{p^m}$ as well as any differential set of F. Thus F is weakly crooked of codimension m.

In the next proposition, we will use a planar function to construct a function which satisfies the crooked property. This is possible for odd p only. Note that in this kind of construction, F is such that its image set is included in (or equal to) a subspace of $\mathbb{F}_{p^n}$. So F is a very particular function.

Proposition 3 *Let G be any planar function from $\mathbb{F}_{p^n}$ to itself, where p is an odd prime. Let k be a proper divisor of n and*

$$F(x) = T_k^n(G(x)) = G(x) + (G(x))^{p^k} + \cdots + (G(x))^{p^{n-k}}.$$

Then F is crooked of codimension $n - k$.

Proof. First, $\mathcal{I}m(F)$ is included in $\mathbb{F}_{p^k}$, so that every differential set of F is included in $\mathbb{F}_{p^k}$ too. Consider $a \in \mathbb{F}_{p^n}^*$ and

$$D_aF(x) = T_k^n(G(x + a) - G(x)).$$

Since G is planar, the function $x \mapsto G(x+a) - G(x)$ is bijective, for any a. Thus, $\mathcal{I}m(D_aF)$ is the set of the values $T_k^n(y)$, $y \in \mathbb{F}_{p^n}$, which is exactly $\mathbb{F}_{p^k}$. $\diamond$

We will see, in the next section, that an important class of plateaued functions is such that every function satisfies the crooked property. To end this section, we want to recall the quadratic case. A quadratic polynomials is called a Dembowski-Ostrom (DO) polynomial, when each of its terms has algebraic degree 2.

Proposition 4 *Let F be any quadratic function, such that $F(0) = 0$:*

$$F(x) \;=\; \sum_{0 \le i \le j < n} u_{i,j} x^{p^i + p^j} + \sum_{i=1}^{n-1} v_i x^{p^i},\ u_{i,j} \in \mathbb{F}_{p^n},\ v_i \in \mathbb{F}_{p^n},$$

where at least one $u_{i,j}$, with $w_p(p^i + p^j) = 2$, is a nonzero. Then F satisfies the crooked property. In particular, if $F(x) = x^{p^i+p^j}$, with $i < j$, then F is either planar or crooked of codimension k, where $k = \gcd(n, j-i)$. When $i = j$ then F is planar.

Proof. For any $a \in \mathbb{F}_{p^n}^*$, set

$$L_a(x) = F(x+a) - F(x) - F(a) = \sum_{i<j} u_{i,j}(x^{p^i} a^{p^j} + a^{p^i} x^{p^j}).$$

Clearly, L_a is a linear function. Thus, the differential set of F in point a, is an affine subspace, whose codimension is the dimension of the kernel of L_a.

Assume that $F(x) = x^{p^i+p^j}$, with $i < j$. Then

$$L_a(x) = x^{p^i} a^{p^j} + a^{p^i} x^{p^j} = x^{p^i} a^{p^i} (a^{p^j - p^i} + x^{p^j - p^i}).$$

We get: $L_a(x) = 0$ if and only if either $x = 0$ or $x^{p^{j-i}-1} = -a^{p^{j-i}-1}$. Set $\ell = \gcd(n, j-i)$. If $p = 2$, the kernel of L_a has dimension ℓ, for any a, so that, $k = \ell$. When p is odd, the equation $(x/a)^{p^{j-i}-1} = -1$ has a solution if and only if n/ℓ is even. Clearly, this condition is independant from a and when it holds the dimension of the kernel of L_a equals ℓ for any a.

Note that $\gcd(n, j-i) = 1$, with $p = 2$, implies that F is APN. When $n/\gcd(n, j-i)$ is odd, with p odd, the functions L_a are bijective; so F is planar, as expected (see Theorem 2). $\diamond$

Remark 3 *Many problems about quadratic functions are still open. Note that to classify these functions in characteristice two, is the purpose of many works to identify the APN quadratic functions, which are the crooked functions of degree* 2 *(see for instance [5] and references herein). It was proved recently that a DO polynomial is planar if and only if it is* 2*-to-*1 *[19]. Quadratic planar functions which are not monomials do exist. For instance, some bilinear functions,*

$$x \mapsto L_1(x)L_2(x), \text{ where } L_1, L_2 \text{ are linear permutations},$$

are planar[26].

5 Partially-bent functions

In this section, we emphasize the importance of the *partially-bent functions* to study the functions which satisfy the crooked property. Let N_d be the *number of balanced derivatives* of the Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ and let

$$N_f = \#\{a | \widehat{f}(a) = 0\}$$

Partially-bent functions were introduced by Carlet in [9] as Boolean functions over $\mathbb{F}_{2^n}$ satisfying

$$(p^n - N_d)(p^n - N_f) = p^n, \quad \text{for} \quad p = 2. \tag{7}$$

More recently, Çeşmelioğlu, Meidl and Topuzoğlu have studied partially-bent functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, for any p, starting from another definition [11]. They proved that (7) holds for any p-ary Boolean function, which is partially-bent, for any p. They actually generalized [9, Theorem] as follows.

Theorem 4 [11, Theorem 1] *Let f be any function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, where p is any prime number. Then f is partially-bent if and only if its derivatives are either constant or balanced.*

Note that any p-ary Boolean function which has constant derivatives has, by definition, a linear space of dimension at least one. Thus we have this immediate property:

Corollary 1 *Let f be any function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, where p is any prime number, which is partially-bent. If its derivative in point a is not balanced, then a is a linear structure of f. The linear space of f is the set of such a.*

This leads to the precise description of the Walsh spectrum of any partially-bent function. The next result is partly given by [9, Proposition 2] for $p = 2$. See also [25, Theorem 1], which concerns binary crooked functions but holds for any partially-bent function.

Theorem 5 [11, Theorem 1] *Let f be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ with linear space V of dimension $s \geq 0$. Then f is partially bent if and only if it is s-plateaued.*

Thus, any partially-bent function f with linear space V has amplitude $p^{(n+s)/2}$, where s is the dimension of V. Note that for $p = 2$, we must have $n + s$ even. Moreover, in this case, f is either bent ($s = 0$), or three-valued, with values $\{0, \pm 2^{(n+s)/2}\}$ (see [7, Proposition 4]).

Now we are going to look at vectorial functions F which have partially-bent components. We will see that all these functions satisfy the crooked property.

Definition 6 *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. The function F is said to be a partially-bent vectorial function if each component of F is partially-bent.*

Theorem 6 *Let F be a partially-bent vectorial function over $\mathbb{F}_{p^n}$ with components f_λ, $\lambda \in \mathbb{F}_{p^n}^*$, such that $F(0) = 0$. Set for any $a \in \mathbb{F}_{p^n}^*$,*

$$\Lambda_a = \{ \ \lambda \in \mathbb{F}_{p^n}^* \mid D_a f_\lambda \text{ is constant } \} \cup \{0\}.$$

Then Λ_a is a subspace of $\mathbb{F}_{p^n}^*$ whose dimension $\ell(a)$ is strictly positive when $p = 2$. For odd p, $\ell(a) = 0$ if and only if the function $D_a F$ is a permutation.

Moreover, for any $a \in \mathbb{F}_{p^n}^*$ the image set of $D_a F$ is an affine subspace of dimension $n - \ell(a)$ and any function $D_a F$ is $p^{\ell(a)}$-to-1. Thus F satisfies the crooked property.

Proof. First recall that $D_a f_\lambda(x) = Tr(\lambda D_a F(x))$ so that Λ_a is clearly a subspace of $\mathbb{F}_{2^n}$. If $\ell(a) = 0$ then $D_a f_\lambda$ is balanced for any λ, *i.e.*, $D_a F$ is a permutation from Theorem 1. This is impossible when $p = 2$, because in this case $D_a F$ is a 2-to-1 function. Now, fixing a and x, we compute

$$\begin{aligned} B(a,x) &= \sum_{\lambda \in \mathbb{F}_{p^n}} \sum_{y \in \mathbb{F}_{p^n}} \xi^{D_a f_\lambda(x) - D_a f_\lambda(y)} \\ &= \sum_{y \in \mathbb{F}_{p^n}} \sum_{\lambda \in \mathbb{F}_{p^n}} \xi^{Tr(\lambda(D_a F(x) - D_a F(y))} \\ &= p^n \times \#\{ \ y \mid D_a F(x) = D_a F(y)\}. \end{aligned}$$

On the other hand, for any $\lambda \in \mathbb{F}_{p^n}^*$, we have

$$B(\lambda) = \sum_{y \in \mathbb{F}_{p^n}} \xi^{D_a f_\lambda(x) - D_a f_\lambda(y)} = \xi^{D_a f_\lambda(x)} \sum_{y \in \mathbb{F}_{p^n}} \xi^{-D_a f_\lambda(y)}.$$

Clearly, $B(\lambda) = 0$ if and only if $D_a f_\lambda$ is balanced. Assume that $D_a f_\lambda$ is not balanced and then is a constant function. In this case,

$$B(\lambda) = \xi^c p^n \xi^{-c} = p^n \text{ where } D_a f_\lambda(x) = c \text{ for all } x.$$

So we get $B(a, x) = p^{\ell(a)} p^n$, for all x, which shows that the number of y such that $D_a F(x) = D_a F(y)$ is not depending of x and equals to $p^{\ell(a)}$, *i.e.*, $D_a F$ is $p^{\ell(a)}$-to-1.

Now, for any $\lambda \in \Lambda_a$, the image set of $D_a F$ is contained in the affine hyperplane $F(a) + H_\lambda$. Indeed, the function $Tr(\lambda D_a F)$ is constantly equal to some $c \in \mathbb{F}_p$ and $c = Tr(\lambda F(a))$ since $F(0) = 0$. Then $Im(D_a F)$ is contained in an affine subspace of dimension $n - \ell(a)$. It is equal to this affine subspace since $D_a F$ is $p^{\ell(a)}$-to-1. $\diamond$

A question naturally arises: is the sufficient condition, given in Theorem 6, also necessary? The answer is generally negative (see Corollary 3 below). However, this is the case for some classes of functions. Moreover, partial hypotheses lead to some constructions and other results. Notation is as in Theorem 6.

Theorem 7 *Let F be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ which satisfies the crooked property. Thus, for any $a \in \mathbb{F}_{p^n}^*$, $\mathcal{I}m(D_a F)$ is an affine subspace V_a of codimension ℓ_a. Then, there is a subspace of dimension ℓ_a as follows defined:*

$$\Lambda_a = \{ \ \lambda \in \mathbb{F}_{p^n} \mid Tr(\lambda D_a F(x)) = c, \ \forall \ x, \ \textit{where } c \in \mathbb{F}_p \ \}.$$

Moreover F is a partially-bent vectorial function if and only if for any nonzero a, the function $D_a F$ is p^{ℓ_a}-to-1.

When $\ell_a = 0$ for all a, p is odd and the function F is planar.

Proof. Let $a \in \mathbb{F}_{p^n}^*$. Note that $\ell_a = 0$ if and only if $\mathcal{I}m(D_a F) = \mathbb{F}_{p^n}$, implying that $D_a F$ is bijective. In this case, all components of $D_a F$ are balanced. When this property holds for any a then F is a planar function, a particular case of partially-bent vectorial function over $\mathbb{F}_{p^n}$, for odd p.

We now assume that $\mathcal{I}m(D_aF)$ is an affine subspace V_a of codimension $\ell_a > 0$. Thus, there exists $\lambda \in \mathbb{F}_{p^n}^*$ such that V_a is included in a coset of H_λ, providing

$$Tr(\lambda D_aF(x)) = c,\ c \in \mathbb{F}_p,\ \text{for all } x,$$

where $H_\lambda = \{\ x \mid Tr(\lambda x) = 0\ \}$ and $c = Tr(\lambda F(a))$. Set $U_a = V_a - F(a)$, which is therefore a subspace of $\mathbb{F}_{p^n}$ of codimension ℓ_a. And we have: $\lambda \in \Lambda_a$ if and only if

$$Tr(\lambda y) = 0,\ \text{for all } y \in U_a, \text{ where } y = x - F(a)\ ,$$

and x runs through V_a. This means that Λ_a is the dual of U_a, implying that Λ_a has dimension ℓ_a. If F is partially-bent then the function D_aF is p^{ℓ_a}-to-1, for any nonzero a, by applying Theorem 6. Conversely, we fix λ and consider any $b \in \mathbb{F}_{p^n}^*$ such that the function D_bf_λ is not constant. We have to prove that D_bf_λ is balanced.

Since F satisfies the crooked property, $\mathcal{I}m(D_bF)$ is an affine subspace V_b of codimension ℓ_b. This differential set cannot be included in any coset of H_λ. These cosets are as follows:

$$y_i + H_\lambda,\ 0 \le i \le p-1,\ \text{with } \dim\left(V_b \cap (y_i + H_\lambda)\right) = n - \ell_b - 1.$$

Thus, for any $y = D_bF(x)$ there is a unique i such that $y \in (y_i + H_\lambda)$, and we have

$$D_bf_\lambda(x) = Tr(\lambda y) = Tr(\lambda y_i) = c_i.$$

There are $p^{n-\ell_b-1}$ such y, and p^{ℓ_b} elements x such that $y = D_bF(x)$. Clearly, the c_i are two by two distinct, so that the set $\{c_0,\ \ldots,\ c_{p-1}\}$ equals $\mathbb{F}_p$. We can conclude that D_bf_λ takes every value of $\mathbb{F}_p$ the same number of times, *i.e.,* D_bf_λ is balanced. We have proved that f_λ is partially-bent, for any λ, completing the proof. $\diamond$

We get a necessary and sufficient condition,whenever we consider a class of functions F whose derivatives are p^ℓ-to-1, for some ℓ. Obviously, it is the case for binary crooked functions and for planar functions. This holds also for quadratic functions and for functions given by Proposition 3. For this last two cases, every D_aF is a p^{n-k}-to-1 function, where k is respectively the dimension of the image-set of D_aF, and a divisor of n.

Corollary 2 *Notation is as in Theorem 7. Assume that F satisfies the crooked property. Then, F is a vectorial partially-bent function when it satisfies one of the following property:*

- *$p = 2$ and F is a crooked function ($\ell_a = 1$ for all a);*
- *F is a planar function ($\ell_a = 0$ for all a);*
- *F is quadratic;*
- *F is among the functions given by Proposition 3.*

A functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ which is partially-bent is such that each of its components is s-plateaued (for some s). Thus the Walsh-transform of such component f_λ can be computed, thanks with the well-known formula:

$$|\widehat{f_\lambda}(a)|^2 = \sum_{b \in \mathbb{F}_{p^n}} \xi^{-Tr(ab)} \sum_{x \in \mathbb{F}_{p^n}} \xi^{D_b f_\lambda(x)},\ a \in \mathbb{F}_{p^n}. \tag{8}$$

Notably, $|\widehat{f_\lambda}(a)|^2 = p^n$, for all $\lambda \in \mathbb{F}_{p^n}^*$, when F is a planar function., *i.e.,* f_λ is bent, a well-known result. This is because every function $D_b f_\lambda$, $b \neq 0$, is balanced. The functions of the shape

$$F(x) = G(x) + \gamma Tr(H(x)),\ \gamma \in \mathbb{F}_{p^n}^*,\ G, H : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \tag{9}$$

have been widely studied, especially because they allow to define permutation classes [15, 17, 22, 27]. We will exhibit a subclass of such F where some functions are partially-bent.

Proposition 5 *Let F be a function defined by (9) where G is a linear function over $\mathbb{F}_{p^n}$. Then, F is partially-bent if and only if the function $x \mapsto Tr(H(x))$ is partially-bent. It is especially the case when the function $x \mapsto Tr(H(x))$ is bent. In particular, this property holds when H is a planar function.*

Proof. Define the functions,

$$h_a :\ \mathbb{F}_{p^n} \to \mathbb{F}_p,\ h_a(x) = Tr\left(H(x+a) - H(x)\right),\ a \in \mathbb{F}_{p^n}^*.$$

We compute the derivatives of any component f_λ of F, $\lambda \in \mathbb{F}_{p^n}^*$. For any $a \in \mathbb{F}_{p^n}^*$:

$$\begin{aligned} D_a f_\lambda(x) &= Tr\left(\lambda D_a G(x) + Tr(\lambda\gamma) D_a H(x)\right) \\ &= Tr\left(\lambda G(a) + Tr(\lambda\gamma) D_a H(x)\right). \end{aligned}$$

If $Tr(\lambda\gamma) = 0$ then $D_a f_\lambda$ is constantly equal to $Tr\left(\lambda G(a)\right)$, for any a. Assume that $Tr(\lambda\gamma) = \nu$, with $\nu \in \mathbb{F}_p^*$. Then

$$D_a f_\lambda(x) = \nu Tr\left(H(x+a) - H(x)\right) + Tr\left(\lambda G(a)\right).$$

Therefore, we can conclude that F is partially-bent if only if the functions h_a are either constant or balanced, for all $a \in \mathbb{F}_{p^n}^*$. $\diamond$

Now, consider the derivatives of any function F defined by (9) where G is a linear. These derivatives satisfy, for any $a \neq 0$,

$$\mathcal{I}m(D_aF) = G(a) + \gamma E,\ E = \mathcal{I}m\left(h_a(x)\right).$$

Then, it appears that F can satisfy the crooked property, as we show by the following examples.
– If $p = 2$ then $\mathcal{I}m(D_aF) = G(a) + \gamma\mathbb{F}_2$, when we assume that h_a is not constant and γ does not belong to the image of G. Hence, F is crooked of codimension $n-1$.
– If p is odd then $\mathcal{I}m(D_aF) = G(a) + \gamma\mathbb{F}_p$, when we assume that $E = \mathbb{F}_p$ and $\gamma\mathbb{F}_p$ is not included in the image of G. Hence, F is crooked of codimension $n-1$.

It is clear that the functions F, which are defined above, are not necessarily partially-bent. Thus, we have proved the following result.

Corollary 3 *There are functions that satisfy the crooked property but are not partially-bent.*

Remark 4 *There is lack of constructions of vectorial partially-bent functions. It is interesting to notice that we have proposed such constructions, by Propositions 3 and 5. These constructions may seem obvious, but they are there to illustrate our purpose. We are sure that other constructions can be easily obtained. For instance, one could consider a generalization of the shape (9) as follows:*

$$F(x) = G(x) + \sum_{i\in I} \gamma_i Tr(H_i(x)),\ \gamma_i \in \mathbb{F}_{p^n}^*,\ G, H_i : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n},$$

for some I, especially when I has a small size.

6 Crooked property and linear structure

In this section, our purpose is to identify large classes of functions over $\mathbb{F}_{p^n}$ which cannot satisfy the crooked property. The existence of functions which satisfy the crooked property, is strongly connected

with the existence of linear structures of their components, which are Boolean p-ary functions. Definitions are given in Section 2.

The study of functions which have linear structures is an interesting problem in itself [14, 16, 21]. Note also the relation with the so-called *fast points* of Boolean functions [32], which characterize derivatives whose degree is lower than expected. Recall that, according to Theorem 6:

> If f does not satisfy the crooked property then it cannot be partially-bent.

We begin by explaining the link between functions with linear structures and crooked property.

Lemma 1 *Let F be a function, from $\mathbb{F}_{p^n}$ to itself, which satisfies the crooked property. The components of F are the functions*

$$f_\lambda : \ \mathbb{F}_{p^n} \to \mathbb{F}_p, \ f_\lambda(x) = Tr(\lambda F(x)), \ \lambda \in \mathbb{F}_{p^n}^*.$$

Then we have the following properties.

(i) *Let $a \in \mathbb{F}_{p^n}^*$ such that D_aF is bijective. Then, a cannot be a linear structure for f_λ, for any λ.*

(ii) *If F is planar then every f_λ has not any linear structure.*

(iii) *Let $a \in \mathbb{F}_{p^n}^*$ such that D_aF is not bijective. Then*

$$\exists \ \lambda \in \mathbb{F}_{p^n}^* \quad \text{such that } Tr(\lambda D_aF(x)) = c, \ \text{for all } x, \tag{10}$$

where $c \in \mathbb{F}_p$, i.e., a is a linear structure of f_λ.

Consequently, if F is not planar, there are some a such that (10) holds. In particular, (10) holds for any a when $p = 2$.

Proof. (i) and (ii): In this case, p is odd, and $\mathcal{I}m(D_aF) = \mathbb{F}_{p^n}$ for some a (case (i)) or for all a (case (ii)). If (10) holds for some λ, and for this a, then the dimension of $\mathcal{I}m(D_aF)$ is strictly less than n, a contradiction. When F is planar, any D_aF is bijective.
(iii): Here, the image set of D_aF is an affine subspace of $\mathbb{F}_{p^n}$ of dimension at most $n-1$. Then $\mathcal{I}m(D_aF)$ is included in a coset of an hyperplane H_λ, for some λ. This implies that $x \mapsto Tr(\lambda D_aF(x))$ is a constant function, so that a is a linear structure of $x \mapsto Tr(\lambda F(x))$. $\diamond$

6.1 Monomial functions

Recall that, for $p = 2$, Bierbrauer and Kyureghyan have proved that only quadratic binomials can be crooked [2]. Previously, Kyureghyan obtained the same result for monomials functions [24]. Moreover the existence of linear structures for the components of such a function was determined by the next theorem.

Theorem 8 [14, Theorem 5] *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $F(x) = x^d$, with $1 \leq d \leq p^n - 2$. Let $\lambda \in \mathbb{F}_{p^n}^*$ such that $f_\lambda(x) = Tr(\lambda x^d)$.*

Then, f_λ has a linear structure if and only if one of the following cases occurs:

- $d = p^j$, $0 \leq j \leq n-1$;
- $d = p^j(p^i + 1)$, $0 \leq i, j \leq n-1$, $i \notin \{0, n/2\}$.

This means that, according to Lemma 1, such a monomial function F cannot satisfy the crooked property, unless it is quadratic, linear or planar. Thus, the result of [24], about binary crooked monomials, can be generalized as follows.

Corollary 4 *Assume that F, defined as in Theorem 8, satisfies the crooked property. If F is not a planar function, then F is linear or quadratic.*

Remark 5 *The corpus of planar functions $F : x \mapsto x^d$ was described by Zieve as follows:* if F is a planar function over $\mathbb{F}_{p^n}$, where $p^n \geq (d-1)^4$ and p does not divide d then either (3) or (4) holds. *This was proved by [34, Theorem 1.1]. This property holds, in particular, for such F of small degree.*

6.2 A symbolic approach

Recall that the hyperplanes of $\mathbb{F}_{p^n}$, considered as $n-1$-dimensional vector-spaces, can be represented by the $p^n - 1$ subspaces:

$$H_\lambda = \{ \ y \mid Tr(\lambda y) = 0 \ \}, \ \lambda \in \mathbb{F}_{p^n}^*.$$

Let F be a function which satisfies the crooked property and is not planar. Thus, $\mathcal{I}m(D_aF)$ is included in a coset of some H_λ, whenever D_aF is not bijective. From Lemma 1, for any $a \in \mathbb{F}_{p^n}^*$ such that D_aF

is not bijective, there is $\lambda \in \mathbb{F}_{p^n}^*$ such that a is a linear structure of f_λ. That is, for $c \in \mathbb{F}_p$,

$$Tr(\lambda D_a F(x)) = c, \text{ for all } x.$$

Now, we are going, to transpose in our context, and generalize, a method of Li and Wang used in [29].

Lemma 2 *Let G be a function from $\mathbb{F}_{p^n}$ to itself and $c \in \mathbb{F}_p$.*

Then $Tr(G(x)) = c$ for all $x \in \mathbb{F}_{p^n}$ if and only if there exist a function R over $\mathbb{F}_{p^n}$ and $\gamma \in \mathbb{F}_{p^n}$ such that, for all x,

$$G(x) = (R(x))^p - R(x) + \gamma \pmod{x^{p^n} - x} \text{ where } Tr(\gamma) = c. \quad (11)$$

Proof. If (11) holds, we have obviously $Tr(G(x)) = Tr(\gamma) = c$, for all $x \in \mathbb{F}_{2^n}$. Now, we assume that $Tr(G(x)) = c$ for all $x \in \mathbb{F}_{p^n}$. So, for any fixed $y \in \mathbb{F}_{p^n}$ there is τ such that $G(y) = \tau^p - \tau + \gamma$ with $Tr(\gamma) = c$. Thus

$$g(\tau) = \tau^p - \tau + (\gamma - G(y)) = 0, \text{ where } Tr(\gamma - G(y)) = 0.$$

Since the polynomial $g(x) = x^p - x + a$, with $Tr(a) = 0$, is not irreducible, it has p distinct roots, say

$$(\tau,\ \tau + \xi_1, \ldots,\ \tau + \xi_{p-1}),\ \xi_i \in \mathbb{F}_p^*.$$

We set $R(y) = \tau$, for the corresponding y. We can choose a root τ which belongs to an hyperplane H_β such that $Tr(\beta) \neq 0$, providing $Tr(\beta\tau) = 0$ while for any i, we have $Tr(\beta\xi_i) \neq 0$. This uses that only one root is in H_β, since the ξ_i describe $\mathbb{F}_p^*$. Thus R is well-defined. $\diamond$

Lemma 3 *Let G be a function, from $\mathbb{F}_{p^n}$ to itself, such that*

$$Tr(G(x)) = c \text{ for all } x \in \mathbb{F}_{2^n}, \text{ where } c \in \mathbb{F}_p. \quad (12)$$

Equivalently, there is a polynomial P over $\mathbb{F}_{p^n}$, say

$$P(x) = \sum_{k \in \mathcal{I}} \rho_k x^k,$$

where $\mathcal{I}$ is a set of representatives of some p-cyclotomic cosets modulo $p^n - 1$, satisfying $Tr(G(x)) - c = Tr(P(x))$ for all x. Then, (12) holds if and only if $\rho_k = 0$ for all k.

Proof. We reduce $Tr(G(x))$ with the property $Tr(ax^{pk}) = Tr(a^{p^{n-1}}x^k)$. Moreover, we have $Tr(G(0)) = c$. Thus we get

$$Tr(G(x)) - Tr(G(0)) = Tr(P(x)) = 0, \text{ for all } x, \tag{13}$$

where $P(x) = \sum_{k\in\mathcal{I}} \rho_k x^k$, is the reduced polynomial obtained from G, proceeding as above, and $\mathcal{I}$ is a set of representatives of p-cyclotomic cosets modulo $p^n - 1$. Obviously, $\rho_k = 0$ for all k implies (12), and we are going to prove the reverse.

As in Lemma 2, we define $R(x) = \sum_k r_k x^k$, $0 \le k \le p^n - 2$, such that

$$P(x) = (R(x))^p - R(x) \pmod{x^{p^n} - x}.$$

Note that $\gamma = 0$, here. Then we have

$$P(x) = \sum_{k=0}^{p^n-2} (r_k^p x^{kp} - r_k x^k) = \sum_{k\in\mathcal{I}} \sum_{i=1}^{n} \left((r_{kp^{i-1}})^p - r_{kp^i}\right) x^{kp^i},$$

where $p^n \equiv 1$. Noticing that $\rho_k \neq 0$ if and only if $k \in \mathcal{I}$, we get, for $k \in I$:

$$\rho_k = (r_{kp^{n-1}})^p - r_k \text{ and } (r_{kp^{i-1}})^p - r_{kp^i} = 0 \text{ for } i = 1, \ldots, n-1, \tag{14}$$

which implies

$$(r_{kp^{n-1}})^p = (r_{kp^{n-2}})^{p^2} = \cdots = (r_{kp^2})^{p^{n-2}} = (r_{kp})^{p^{n-1}} = r_k,$$

so that $\rho_k = 0$. When we state (14), we suppose that the cyclotomic coset of k has size $s = n$. It is easy to see that $\rho_k = 0$ can be proved by the same way, when $s < n$, with $n = \ell s$. We have simply to consider the equations

$$\sum_{j=0}^{\ell-1} (r_{kp^{i+js-1}}^p - r_{kp^{i+js}}) = 0, \quad \text{for } i = 1, \ldots, s-1,$$

together with

$$\sum_{j=0}^{\ell-1} (r_{kp^{s(j+1)-1}}^p - r_{kp^{s(j+1)}}) = \rho_k.$$

◇

Now, we will use our previous results to express the existence of linear structures, for a component of any function F, from $\mathbb{F}_{p^n}$ to itself. We

consider a derivative D_aF of F, in point $a \in \mathbb{F}_{p^n}^*$, which satisfies (10): there is at least one $\lambda \in \mathbb{F}_{p^n}^*$ and $c \in \mathbb{F}_p$, such that $Tr(\lambda D_aF(x)) = c$, for all x. According to Lemma 3, we obtain the polynomial P_a, by reducing $Tr(\lambda D_aF(x))$. We get

$$\begin{aligned} P_a(x) &= \sum_{k \in \mathcal{I}} g_{a,k}(\lambda) x^k, \qquad (15) \\ \text{where } Tr(P_a(x)) &= Tr(\lambda D_aF(x)) - c = 0, \text{ for all } x. \end{aligned}$$

Here, the coefficients of P_a are the functions $g_{a,k} : \lambda \mapsto g_{a,k}(\lambda)$, over $\mathbb{F}_{p^n}$, and $\mathcal{I}$ is a set of representatives of cyclotomic cosets.

Theorem 9 *Notation is as above. The polynomial P_a is given by (15). Let F be a function over $\mathbb{F}_{p^n}$, with components f_λ. Assume that there is $a \in \mathbb{F}_{2^n}^*$, and $c \in \mathbb{F}_p$, such that a is a linear structure of f_λ, for some λ, i.e., $Tr(\lambda D_aF(x)) = c$, for all x. Then, the functions $g_{a,k}$ are linear functions of λ and satisfy:*

$$\textit{There is } \lambda \in \mathbb{F}_{p^n}^* \textit{ such that } \; g_{a,k}(\lambda) = 0 \textit{ for all } k. \qquad (16)$$

Proof. It is clear that the $g_{a,k}$ are linear, since P_a is obtained by means of this kind of transformation:

$$Tr\left(\lambda h_{a,p^ik} x^{p^ik}\right) = Tr\left((\lambda h_{a,p^ik})^{p^{n-i}} x^k\right),$$

where the h_{a,p^ik} are the coefficients of $D_aF(x)$. Further, by applying directly Lemma 3, The coefficients of P_a must be all equal to 0. This is exactly (16). ◇

Note that the previous theorem applies to any function F when one want to check if a point a is a linear structure of at least one f_λ. One obtain a negative answer by proving that no λ satisfies (16). Applying Lemma 1, we can derive from Theorem 9 the following property for components of functions which satisfy the crooked property.

Corollary 5 *Let F be a function over $\mathbb{F}_{p^n}$ which satisfies the crooked property. For any $a \in \mathbb{F}_{p^n}^*$, P_a is the reduced polynomial, which is obtained from $Tr(\lambda D_aF(x))$, as previously explained, with coefficients $g_{a,k}(\lambda)$ (see (15)). We assume that F is not planar.*

Then, for any $a \in \mathbb{F}_{p^n}^*$, such that D_aF is not bijective, there is $\lambda \in \mathbb{F}_{p^n}^*$ such that $g_{a,k}(\lambda) = 0$ for all k.

6.3 A combinatorial property: applications

Previous results lead us to consider the existence of linear structures as a combinatorial problem. Corollary 5 is most interesting in the binary case, since the functions D_aF are never bijective. Thus, we will begin by some results in characteristic two. In this section, we will need the following notation. Let s, t be integers in the range $[0, p^n - 1]$, and their p-adic expansions:

$$s = \sum_{i=0}^{n-1} s_i p^i, \quad t = \sum_{i=0}^{n-1} t_i p^i.$$

Then

$$s \prec t \quad \Leftrightarrow \quad s_i \leq t_i, \text{ for all } i, \text{ with } s \neq t; \tag{17}$$

$s \preceq t$ means that $s \prec t$ or $s = t$. For a better understanding of this section, recall that

$$x^s - (x+a)^s = \sum_{k \prec s} \binom{s}{k} x^k a^{s-k},$$

where

$$\binom{s}{k} \equiv \prod_{i=0}^{n-1} \binom{s_i}{k_i} \pmod{p}.$$

6.3.1 The binary case

We first present an example to explain our approach.

Example 3 *Let $p = 2$ and consider $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, where $n \geq 8$. Let $u, v \in \mathbb{F}_{2^n}^*$ and*

$$F(x) = x^7 + ux^{11} + vx^{13}.$$

For any $a \in \mathbb{F}_{2^n}^*$, we expand $G_a(x) = F(x+a) + F(x) + F(a)$ and then compute the reduced polynomial P_a, by $Tr(\lambda G_a(x)) = Tr(P_a(x))$. We get:

$$P_a(x) = g_{a,1}(\lambda)x + g_{a,3}(\lambda)x^3 + g_{a,5}(\lambda)x^5 + g_{a,9}(\lambda)x^9,$$

where the functions $g_{a,k} : \lambda \mapsto g_{a,k}(\lambda)$ are linear, and

$$Tr(\lambda(D_aF(x) + F(a))) = 0, \text{ for all } x \quad \Leftrightarrow \quad g_{a,k}(\lambda) = 0, \text{ for all } k.$$

Note that three 2-cyclotomic cosets appear, when we derive and then collect all elements s such that $s \prec \ell$ for some exponent ℓ of F. We write the functions $g_{a,k}$:

$$\begin{aligned} g_{a,1}(\lambda) &= \lambda(a^{12}v + a^{10}u + a^6) + \lambda^{2^{n-3}}(a^5v + a^3u)^{2^{n-3}}) \\ &+ \lambda^{2^{n-2}}(a^9v + a^3)^{2^{n-2}} + \lambda^{2^{n-1}}(a^9u + a^5)^{2^{n-1}}; \\ g_{a,3}(\lambda) &= \lambda(a^8u + a^4) + \lambda^{2^{n-2}}(av)^{2^{n-2}} + \lambda^{2^{n-1}}a^{2^{n-1}}; \\ g_{a,5}(\lambda) &= \lambda(a^8v + a^2) + \lambda^{2^{n-1}}(au)^{2^{n-1}}; \\ g_{a,9}(\lambda) &= \lambda(va^4 + ua^2). \end{aligned}$$

Here, the last equation provides the result. We choose a such that $a^2 \neq u/v$. Then, the only suitable solution is $\lambda = 0$. Hence, for any $a \notin \{0, (u/v)^{2^{n-1}}\}$ the components f_λ of F , $\lambda \neq 0$, cannot have a as linear structure. Thus F cannot have the crooked property. When $a = (u/v)^{2^{n-1}}$, we get $g_{a,9}(\lambda) = 0$ for any λ, showing that the Boolean functions $D_a f_\lambda$ have no term with exponent 9.

The previous example suggests a more general property. It is when one function $g_{a,k}$ is a monomial.

Corollary 6 *Let F be a polynomial over $\mathbb{F}_{2^n}$, $F(x) = \sum_{\ell=1}^{2^n-2} a_\ell x^\ell$. If there is an exponent ℓ, and k in the range $[1, 2^n - 2]$, such that $2^i k \not\prec \ell'$ for all exponent ℓ' and for any i, unless $i = 0$ and $\ell' = \ell$, then F cannot satisfy the crooked property. More precisely, each component of F has not any linear structure.*

Proof. For any $a \in \mathbb{F}_{2^n}^*$, we compute G_a and reduce it to obtain P_a:

$$P_a(x) = \sum_{k \in \mathcal{I}} g_{a,k}(\lambda) x^k \text{ where } Tr(P_a(x)) = Tr(\lambda G_a(x)) + c,\ c \in \{0, 1\},$$

and $\mathcal{I}$ is a set of representatives of some cyclotomic cosets. The hypothesis means that there is k, ℓ such that $k \prec \ell$ and $g_{a,k}(\lambda) = \lambda a^{\ell-k} a_\ell$. Thus $g_{a,k}(\lambda) = 0$ for $\lambda = 0$ only. $\diamond$

Actually, the problem becomes a combinatorial problem related to the exponents of any polynomial $F(x) = \sum_{\ell=1}^{2^n-2} a_\ell x^\ell$ over $\mathbb{F}_{2^n}$. We illustrate our purpose by the following result.

Proposition 6 *Let us define the polynomial over $\mathbb{F}_{2^n}$, with $n > 5$:*

$$F(x) = x^s + \sum_{\ell=1, \ell \neq s}^{2^n-2} a_\ell x^\ell,\ s = 2^k + 2^{k-1} - 1,\ 3 \leq k \leq n-2.$$

We assume that F is not a monomial and that all ℓ satisfy $w_2(\ell) < k$. Then F does not satisfy the crooked property.

Proof. We will prove that Corollary 6 applies. Let $t = s - 1$ so that $t \prec s$. Moreover $2^i t \not\prec s$ for all $i \not\equiv 0 \pmod{n}$. Indeed, if $i > 0$ is such that $2^i t < s$ then $i = n - 1$ is the only one solution for i. But, in this case we have:

$$s = 2^k + \sum_{j=0}^{k-2} 2^j \quad \text{and} \quad 2^{n-1}t = 2^{k-1} + \sum_{j=0}^{k-3} 2^j,$$

where it appears that $2^{n-1}t \not\prec s$. For $0 < i < n-1$, we get $2^i t > s$.

Now, take any exponent $\ell \neq s$. We have $w_2(t) = k - 1$ and $w_2(\ell) < k$. Thus, any u such that $u \prec \ell$ is such that $w_2(u) < k - 1$. It is impossible to have $2^i t \prec \ell$, for any i. $\diamond$

6.3.2 General case

In the binary case, we used the fact that one function $g_{a,k}$ has only one term, for some k. This can be observed, by the same way, for any function F over $\mathbb{F}_{p^n}$ and for any prime p. One can see this fact as another corollary of Theorem 9.

Corollary 7 *Let F be a function over $\mathbb{F}_{p^n}$. For any $a \in \mathbb{F}_{p^n}^*$, P_a is the reduced polynomial, which is obtained from $Tr(\lambda D_a F(x))$, as previously explained, with coefficients $g_{a,k}(\lambda)$ (see (15)).*

If $g_{a,k}(\lambda) = \lambda h(a)$ for some k, with $h(a) \neq 0$ for $a \in \mathbb{F}_{p^n}^*$, then F cannot satisfy the crooked property, unless it is a planar function. Moreover, any component f_λ cannot have any linear structure.

Proof. Assume that F satisfies the crooked property and is not planar. From Lemma 1, for any $a \in \mathbb{F}_{p^n}^*$ such that $D_a F$ is not bijective, there is λ such that a is a linear structure of f_λ. Thus we must have, for this pair (a, λ):

$$P_a(x) = \sum_{k \in \mathcal{I}} g_{a,k}(\lambda) x^k = 0 \text{ with } g_{a,k}(\lambda) = 0 \text{ for all } k,$$

applying Theorem 9. We suppose that there is k such that $g_{a,k}(\lambda) = \lambda h(a)$. Since $h(a) \neq 0$ for all a, any a cannot be a linear structure of any f_λ. $\diamond$

Example 4 *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ where p is odd and $n > 3$. Let*

$$F(x) = x^s + ux^t,\ u \in \mathbb{F}_{p^n}^*,\ s = 1 + p + p^2 \text{ and } t = 1 + 2p.$$

Set $A = \{\ \ell \mid \ell \prec s \text{ or } \ell \prec t\ \}$. We have

$$A = \{\ 1,\ p,\ p^2,\ 1+p,\ 1+p^2,\ p+p^2\ \} \cup \{\ 1,\ p,\ 1+p,\ 2p\ \}.$$

We compute $P_a(x)$ and obtain the $g_{a,k}$, with $k \in \mathcal{I}$ where

$$\mathcal{I} = \{\ 1,\ 1+p,\ 1+p^2, 2p\ \}.$$

Clearly, the functions $g_{a,k},\ k \in \{1+p^2, 2p\}$ have only one term, in particular $g_{a,1+p^2} = \lambda a^p$. Thus, F does not satisfy the crooked property. Any component of F cannot have any linear structure. Also, F cannot be partially -bent.

The previous example is very simple but in fact the property that is exploited there is usually satisfied by a number of monomials and binomials. In particular, a function over $\mathbb{F}_{p^n}$ having the following form does not generally satisfy the crooked property:

$$x^d + \sum_{i \in U} u_i x^i,\ w_p(i) < w_p(d),\ \text{for all } i \in U.$$

(see Proposition 6). However, the study of the set of representatives of cyclotomic cosets, denoted $\mathcal{I}$, which appear in the exponents of the function may reveal some interesting properties on the derivatives of this function. For instance, assume that $g_{a,k}(\lambda) = \lambda h(a)$ for some k, as in Corollary 7. If $h(a) = 0$ for $a \in \mathbb{F}_{p^n}^*$, then the components of $D_a F$ have no term with exponent k.

7 Conclusion

This paper follows the works on the binary crooked functions. Our aim is first of all to study a larger corpus, including all the functions over $\mathbb{F}_{p^n}$ whose differential sets are subspaces of $\mathbb{F}_{p^n}$. Clearly, these objects remain very specific, but the set of functions satisfying the crooked property contains classes of great interest. In particular, we have described in detail the relationship between these two properties: to satisfy the crooked property and to be partially-bent. More generally,

we hope that, by our approach, some properties concerning interesting objects will appear in another form.

To illustrate our purpose, we propose some constructions, which are easily obtained but suggest that other constructions are possible. Note that, although they were widely studied, many interesting problems remain open where plateaued functions are involved, while there are few constructions of vectorial plateaued functions.

Section 6 is devoted to the (large) class of functions which do not satisfy the crooked property. In fact we want to deal in general with the research of linear structures of components of any vectorial function. We have shown that, since the functions are in polynomial form, the study of the exponents of every term informs us, sometimes completely about the existence of linear structures.

References

[1] T. Bending and D. Fon der Flass. Crooked functions, bent functions, and distance regular graphs. *Electronic Journal of Combinatorics*, 5(1), 1998. R34.

[2] J. Bierbrauer and G. Kyureghyan, Crooked binomials, *Des. Codes Cryptogr.*, 46 (2008) 269-301.

[3] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems, *J. Cryptol.*, 4(1):3-72, 1991.

[4] C. Blondeau, A. Canteaut, and P. Charpin. Differential properties of power functions, *Int. J. Inform. and Coding Theory*, 1(2):149–170, 2010. Special Issue dedicated to Vera Pless.

[5] L. Budaghyan, M. Calderini and I. Villa. On equivalence between known families of quadratic APN functions, *Finite Fields Appl.*, to appear.

[6] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. On cryptographic properties of the cosets of $R(1, m)$. *IEEE Transactions on Information Theory*, 47(4):1494–1513, 2001.

[7] A. Canteaut, P. Charpin. Decomposing bent functions. *IEEE Transactions on Information Theory*, 49(8), pp. 2004-19, August 2003.

[8] A. Canteaut and M. Naya-Plasencia. Structural weaknesses of permutations with a low differential uniformility and generalized

crooked functions. In *Finite Fields: Theory and Applications - FQ9 - Contemporary Mathematics*, AMS, number 518, pp. 55-71, 2010.

[9] C. Carlet. Partially-bent functions. *Des. Codes Cryptogr.*, (3):135–145, 1993.

[10] C. Carlet, Boolean and Vectorial Plateaued Functions and APN Functions. *IEEE Transactions on Information Theory*, 61(11): 6272–6289, 2015.

[11] A. Çeşmelioğlu, W. Meidl and A. Topuzoğlu, Partially bent functions and their properties, *Applied Algebra and Number Theory*, pp. 22-38 Cambridge Univ. Press, Cambridge, 2014.

[12] P. Charpin, Crooked functions, In *Finite Fields Applications.* Berlin, Boston: De Gruyter, pp. 87–102.

[13] P. Charpin and J. Peng. Differential uniformity and the associated codes of cryptographic functions. *Advances in Mathematics of Communications*, AIMS, Special issue on *Applications of discrete mathematics in secure communication*, Subhamoy Maitra Ed., November 2019, 13(4): 579-600.

[14] P. Charpin and G. Kyureghyan, Monomial functions with linear structure and permutation polynomials, in: Finite Fields: Theory and Applications FQ9, in: *Contemp. Math.,* vol. 518, AMS, 2010, pp. 99–111.

[15] P. Charpin and G. Kyureghyan, When does $G(x) + \gamma Tr(H(x))$ permute $\mathbb{F}_{p^n}$? *Finite Fields Appl.*, 15 (2009), no. 5, pp. 615–632.

[16] P. Charpin and S. Sarkar. Polynomials with linear structure and Maiorana-McFarland construction. *IEEE Transactions on Information Theory*, 57(6):3796–3804, 2010.

[17] P. Charpin, G. Kyureghyan and V. Suder, Sparse permutations with low differential uniformity. *Finite Fields Appl.* 28 (2014), pp. 214–243.

[18] R.S. Coulter and R. Matthews, Planar functions and planes of the Lenz-Barlotti class II, *Des. Codes Cryptogr.*, vol. 10, pp. 165–185, 1997.

[19] R.S. Coulter and R. Matthews, On the number of distinct values of a class of functions over a finite field. *Finite Fields Appl.*, 17 (2011) 220–224.

[20] E.R. van Dam and D. Fon-Der-Flass. Codes, graphs, and schemes from nonlinear functions. *European J. Combin.* 24 (1) (2003) 85–98.

[21] S. Dubuc, Characterization of linear structures, *Des. Codes Cryptogr.* vol. 22, pp. 33–45, 2001.

[22] D. Gerike and G. Kyureghyan, Results on permutation polynomials of shape $x^t + \gamma Tr_{q^n/q}(x^d)$, *Combinatorics and Finite Fields*, pp. 67–78, Radon Ser. Comput. Appl. Math., 23, De Gruyter, Berlin, 2019.

[23] C. Godsil and A. Roy. Two characterization of crooked functions, *IEEE Trans. Inform. Theory* 54 (2008), no. 2, 864–866.

[24] G. Kyureghyan, The only crooked power functions are $x^{2^k+2^l}$, *European J. Combin.* 28 (2007) 1345–1350.

[25] G. Kyureghyan, Crooked maps in F_{2^n}, *Finite Fields Appl.* 13(3), pp. 713-726 (2007).

[26] G. Kyureghyan and F. Ozbudak, Plenarity of products of two linearized polynomials, *Finite Fields Appl.* 18(2012) 1076–1088.

[27] G. Kyureghyan and M. Zieve, Permutation polynomials of the form $X + \gamma Tr(X^k)$. *Contemporary developments in finite fields and applications*, 178?194, World Sci. Publ., Hackensack, NJ, 2016.

[28] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications,Cambridge: Cambridge University Press. (1996).

[29] Y. Li and M. Wang. On EA-equivalence of certain permutations to power mappings. *Des. Codes Cryptogr.*, 58(3):259–269, 2011.

[30] S. Mesnager, F. Ozbudak, A. Sinak and G. Cohen, On q-ary plateaued functions over F_q and their explicit characterizations functions, *European Journal of Combinatorics*, 63 (2017), 6139–6148.

[31] K. Nyberg, Differentially uniform mappings for cryptography, In *Advances in Cryptology–EUROCRYPT'93* LNCS, vol. 765, 55-64, Springer-Verlag, 1993.

[32] A. Salagean and F. Ozbudak, Counting Boolean functions with Faster Points, *Des. Codes Cryptogr.*, 88, 18671883 (2020).

[33] Y. Zheng and X. M. Zhang, On plateaued functions, *IEEE Trans. Inform. Theory*, 47(2001), No. 3, pp. 1215–1223.

[34] M.E. Zieve, Planar functions and perfect nonlinear monomials, *Des. Codes Cryptogr.*, (2015) 75:71–80.