HAL
archives-ouvertes.fr

Crooked functions

Pascale Charpin

▶ **To cite this version:**

Pascale Charpin. Crooked functions. Finite Fields, 2020. hal-02969132

HAL Id: hal-02969132
https://hal.inria.fr/hal-02969132

Submitted on 16 Oct 2020

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.

Pascale Charpin

Crooked functions

Abstract: Crooked permutations were introduced twenty years ago since they allow to construct interesting objects in graph theory. The field of applications was extended later. Crooked functions, bijective or not, correspond to APN functions and to some optimal codes. We adopt an unified presentation of crooked functions, explaining the connection with partially-bent functions. We then complete some known results and derive new properties. For instance, we observe that crooked functions allow to construct sets of bent functions and define some permutations.

Keywords: Vectorial function, Boolean function, derivative, differential set, plateaued function, partially-bent functions, bent functions, APN function, AB 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]. Such a function has been defined from V to W, two n-dimensional vector spaces over $\mathbb{F}_2$, by the following property: the image set of any of its derivatives is the complement of a hyperplane. This characterization implies that a crooked function is bijective, and allows, in particular, to construct distance regular graphs. Later, several authors have developed this work, and have generalised the previous definition. They notably related the crooked functions with several optimal objects, which have applications both to cryptography and coding theory [12, 13].

This paper is a survey on crooked functions, including several new results. We recall what is known about crooked functions presently. We introduce another appproach to study crooked functions by starting from the so-called *partially-bent* functions, and present some new results.

After preliminaries, we propose a brief survey on the (few) papers considering crooked functions. To our knowledge, the list of references includes all such papers. Section 4 is devoted to the structure of crooked functions. We begin by proving a link between partially-bent functions and crooked functions. We later differentiate the two cases: odd and even number of variables. The odd case was mainly treated in the first papers, since in this case, crooked functions could be permutations. In

Pascale Charpin, INRIA, 2 rue Simone Iff, Paris 75012

Sections 5 and 6, we show how to construct, respectively, a set of bent functions and a set of permutations, using the nice structure of a crooked function. We conclude by the main conjecture about the existence of crooked functions.

2 Definitions, basic properties

Thoughout this paper, $|E|$ denotes the cardinality of the set E, and $E^* = E \setminus \{0\}$. Let F be a mapping, from the finite field $\mathbb{F}_{2^n}$ to itself. Such a function is called *a vectorial function*, while a function f, from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is, as usually, a *Boolean function*. We denote by $\mathcal{I}m(\xi)$ the image set of any function ξ.

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

$$F(x) \ + \ F(x+a) \ = c, \quad a, c \in \mathbb{F}_{2^n} \ , \ a \neq 0 \ , \tag{1}$$

have zero or two solutions in $\mathbb{F}_{2^n}$, say x and $x+a$. Throughout this paper, we use U to denote a subfield of $\mathbb{F}_{2^n}$, usually $\mathbb{F}_{2^n}$ or $\mathbb{F}_2$. For $a \in \mathbb{F}_{2^n}^*$, the function from $\mathbb{F}_{2^n}$ to U, defined by

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

is called *derivative of* F, with respect to a. We call *differential set*, in point a, the image set of $D_a F$:

$$\mathcal{I}m(D_a F) = \{ \ F(x) + F(x+a) \mid x \in \ \mathbb{F}_{2^n} \}. \tag{2}$$

Clearly, when F is APN, we have for any $a \in \mathbb{F}_{2^n}^*$:

$$D_a F(x) = D_a F(x+a) = c, \text{ for some } c,$$

for only one pair $(x, x+a)$. This means that $D_a F$ is a 2-to-1 function. Thus, one can formulate the APN property as follows.

Proposition 1. *A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if and only if all its differential sets have cardinality 2^{n-1}.*

The 2^n, so-called, *components of* F are the Boolean functions

$$f_\lambda \ : \ x \ \longmapsto \ Tr(\lambda F(x)), \quad \lambda \in \mathbb{F}_{2^n},$$

where f_0 is the null function, by convention. They are linearly defined by means of the absolute trace on $\mathbb{F}_{2^n}$:

$$x \mapsto Tr(x) = x + x^2 + \ \ldots, \ x^{2^{n-1}}.$$

The dual $V^{\perp}$, of any subspace V of $\mathbb{F}_{2^n}$, is the subspace of those y such that $Tr(yx) = 0$, for all $x \in V$. The *Walsh transform* of a Boolean function f, is defined as

$$a \in \mathbb{F}_{2^n} \mapsto \mathcal{W}_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr(ax)}.$$

Recall the *Parseval's relation*:

$$\sum_{a \in \mathbb{F}_{2^n}} \big(\mathcal{W}_f(a)\big)^2 = 2^{2n}.$$

We will need the following result:

Lemma 1. [6, Lemma V.2] *Let f be a Boolean function over $\mathbb{F}_{2^n}$, and let V be a subspace of $\mathbb{F}_{2^n}$ of dimension k, $0 \leq k \leq n$. Then*

$$\sum_{v \in V} \big(\mathcal{W}_f(v)\big)^2 = 2^k \sum_{u \in V^{\perp}} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(x+u)}.$$

We now define particular APN functions, which exist for odd n only.

Definition 1. *The function F is said to be an* almost bent *(AB) function if the numbers*

$$\mu_F(a, \lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda F(x)+ax)}, \tag{3}$$

are equal to 0 or $\pm 2^{\frac{n+1}{2}}$ only, when $a \in \mathbb{F}_{2^n}$ and $\lambda \in \mathbb{F}_{2^n}^*$.

Note that $\mu_F(a, \lambda) = \mathcal{W}_{f_\lambda}(a)$ for any fixed λ.

A Boolean function f, over $\mathbb{F}_{2^n}$, is said to be *bent* when $\mathcal{W}_f$ takes two values $\{\pm 2^{n/2}\}$ only, in particular n must be even then. It is said to be *s-plateaued* when $\mathcal{W}_f$ takes three values,

$$\{0, \pm 2^{(n+s)/2}\}, \text{ with } 1 \leq s \leq n-2 \text{ and } n+s \text{ even}.$$

By convention, a bent function is 0-plateaud. The value $2^{(n+s)/2}$ is the *amplitude* of f. A *plateaued vectorial function* is a vectorial function whose components are plateaued Boolean functions. It is said that F is *plateaued with single amplitude*, when all components of F have the same amplitude.

The *sum-of-square* indicator of f is defined by

$$\nu(f) = \sum_{a \in \mathbb{F}_{2^n}} \mathcal{W}^2_{D_a f}(0) = 2^{-n} \sum_{b \in \mathbb{F}_{2^n}} \mathcal{W}_f^4(b). \tag{4}$$

$\mathcal{W}_f(u)$	**number of** $u \in \mathbb{F}_{2^n}$
0	$2^n - 2^{n-s}$
$2^{(n+s)/2}$	$2^{n-s-1} + (-1)^{f(0)} 2^{(n-s)/2-1}$
$-2^{(n+s)/2}$	$2^{n-s-1} - (-1)^{f(0)} 2^{(n-s)/2-1}$

Table 1: Walsh spectrum of the Boolean s-plateaued function f

If f is s-plateaued then $\nu(f) = 2^{2n+s}$. Moreover, the vectorial function F is APN if and only if

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} \nu(f) = 2^{2n+1}(2^n - 1) \tag{5}$$

(see [2, Corollary 1]). A Boolean function f is said to be *balanced* if it takes the values 0 and 1 the same number of times. Recall a well-known result:

Theorem 1. *A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a permutation if and only if all its components f_λ, $\lambda \in \mathbb{F}_{2^n}^*$, are balanced.*

3 Brief record

We use our terminology, of the previous section, rather than of the initial works on crooked functions. The next definition was proposed by Bending and Fon-Der-Flaass in [1], twenty years ago.

Definition 2. *Let F be a function from $\mathbb{F}_{2^n}$ to itself. This function is called crooked if it satisfies the following three properties:*
(i) $F(0) = 0$*;*
(ii) $F(x) + F(y) + F(z) + F(x + y + z) \neq 0$*, for any three distinct x, y, z;*
(iii) $D_a F(x) + D_a F(y) + D_a F(z) \neq 0$*, for arbitrary x, y, z and any $a \neq 0$.*

This definition implies that such a function F is a bijection over $\mathbb{F}_{2^n}$, where n must be odd. Note that the condition (ii) means that F is APN (see (1)). Also, F is crooked if and only if any of its differential sets is a complement of a hyperplane. Further, other properties are studied, in [1], such as some relations of crooked permutations with bent functions of dimension $n - 1$, and with the so-called *Kerdock sets*.

Crooked permutations allow to construct some *distance regular graphs*. This was shown in [1], generalizing previous constructions. Later, van Dam and Fon-Der-Flaass proposed another construction, and then another generalisation (see, in particular, Thorem 3 of [12]). Conversely, Godsil and Roy have shown that crooked permutations can be fully characterized by Preparata codes of minimum distance 5. Similarly, some distance-regular graphs provide crooked permutations [15, Theorems 3,5].

Since the high interest for APN functions in cryptography and coding theory [10], the existence of crooked functions was later the core of the research on crooked functions. Kyureghyan proposed another definition of crooked functions, identifying all APN functions which are such that their differential sets are affine hyperplanes. She established the basic properties of such functions. She notably proved that the *monomial crooked* functions are quadratic [16, 17].

The APN quadratic functions are crooked. We do not know if crooked functions of higher algebraic degree do exist. This is a recurring question, about which only negative results have been obtained. An important result was obtained by Bierbrauer and Kyureghyan: *binomial crooked* functions are quadratic [4].

4 Structure of crooked functions

A hyperplane of $\mathbb{F}_{2^n}$ is an $(n-1)$-dimensional subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. For any hyperplane H there is a unique $\lambda \in \mathbb{F}_{2^n}^*$ such that

$$H = H_\lambda := \{\ y \in \mathbb{F}_{2^n} \mid Tr(\lambda y) = 0\ \}. \tag{6}$$

We will denote by $\overline{H_\lambda}$ the complement of H_λ. The dual of H_λ is obviously $H_\lambda^\perp = \{0, \lambda\}$.

The next definition of *crooked* functions is due to Kyureghan [17]. The corpus of such functions includes the crooked permutations, but also a large variety of non-bijective crooked functions, especially in even dimension.

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.

We directly deduce from Proposition 1:

Claim 1. *Any crooked function is an APN function.*

Assuming that $S_a = H_\lambda$ or $\overline{H_\lambda}$, for some λ, we get

$$Tr\left(\lambda(D_aF(x))\right) = c, \text{ for all } x, \text{ where } c \in \mathbb{F}_2 \text{ is fixed.}$$

This means that the derivative of the component f_λ of F, in point a, is a constant function. In this case, a is said to be a *linear structure* of f_λ. The *linear space* of f_λ is the subspace, including $a = 0$, of its linear structures. We will see that crooked functions have always components with nonzero linear structures.

4.1 Crooked and partially-bent functions

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function of $\mathbb{F}_{2^n}$. Denote by N_d, the number of balanced derivatives of f, and by N_f, the size of the set $\{a|\mathcal{W}_f(a) = 0\}$. Partially-bent functions were introduced by Carlet in [9], as functions satisfying

$$(2^n - N_d)(2^n - N_f) = 2^n. \tag{7}$$

There is another characterization of partially-bent functions, which allows to determine their Walsh spectrum.

Theorem 2. [9, Theorem] *A Boolean function f is partially-bent if and only if its derivatives are either constant or balanced.*

This leads to the precise description of the Walsh spectrum of any partially-bent function. Note that bent functions are particular partially-bent functions, with $N_d = 2^n - 1$ and $N_f = 0$. Moreover, a partially-bent function is, in a certain sense, obtained by concatenating the same bent function, several times. (The next result is partly given by [9, Proposition 2]. See also [17, Theorem 1], which concerns crooked functions but, actually, holds for any partially-bent function. For the Walsh spectrum, see a proof in [7, Proposition 4].

Corollary 1. *Let f be a partially-bent Boolean function. Assume that f has a linear space V of dimension $s > 0$.*

Then f is an s-plateaued function, such that $n + s$ is even, and $\mathcal{W}_f$ takes three values, 0 and $\pm 2^{(n+s)/2}$. The Walsh spectrum of f is given in Table 1.

The definition of a partially-bent Boolean function can be extended to the one of a vectorial partially-bent function as follows.

Definition 4. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. The function F is said to be a partially-bent vectorial function if every component of F is partially-bent. In particular, when n is even, some components can be bent.*

Theorem 3. *Let F be a vectorial function over $\mathbb{F}_{2^n}$ with components f_λ. Set, for $a \in \mathbb{F}_{2^n}^*$,*

$$\Lambda_a = \{\ \lambda \in \mathbb{F}_{2^n}^* \mid D_a f_\lambda \text{ is constant } \} \cup \{0\},$$

and denote by $\ell(a)$ the dimension of Λ_a. Then we have:

- *Assume that F is partially-bent. Then the differential sets of F are affine subspaces. For any $a \in \mathbb{F}_{2^n}^*$, this subspace is of codimension $\ell(a)$, with $\ell(a) \geq 1$ and D_aF is a $2^{\ell(a)}$-to-1 function.*
- *The function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a crooked function if and only if F is partially-bent with $\ell(a) = 1$ for every non-zero a.*

Proof. Recall that $D_a f_\lambda(x) = Tr(\lambda D_a F(x))$, for all x. Obviously, Λ_a is a subspace of $\mathbb{F}_{2^n}$. Now, fixing a and x, we compute

$$\begin{aligned} B(a,x) &= \sum_{\lambda \in \mathbb{F}_{2^n}} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{D_a f_\lambda(x) + D_a f_\lambda(y)} \\ &= \sum_{y \in \mathbb{F}_{2^n}} \sum_{\lambda \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda(D_a F(x) + D_a F(y)))} \\ &= 2^n \times |\{\ y \mid D_a F(x) = D_a F(y)\}|. \end{aligned}$$

On the other hand, we set for any $\lambda \in \mathbb{F}_{2^n}^*$:

$$B(\lambda) = \sum_{y \in \mathbb{F}_{2^n}} (-1)^{D_a f_\lambda(x) + D_a f_\lambda(y)} = (-1)^{D_a f_\lambda(x)} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{D_a f_\lambda(y)}.$$

We first assume that F is partially bent. Note that $\ell(a) \geq 1$, since otherwise we would have that the Boolean function $D_a f_\lambda$ is balanced, for any $\lambda \in \mathbb{F}_{2^n}^*$, from Theorem 2. This is impossible since $D_a F$ cannot be a permutation (see Theorem 1).

Clearly, $B(\lambda) = 0$ if and only if the function $D_a f_\lambda$ is balanced. If it is not balanced, then $\lambda \in \Lambda_a$, and this function is constantly equal to either 0 or 1. In both cases, we get $B(\lambda) = 2^n$. Hence, we get

$$B(a,x) = \sum_{\lambda \in \Lambda_a} B(\lambda) = 2^n 2^{\ell(a)}, \text{ for all } x,$$

implying that the number of y such that $D_a F(x) = D_a F(y)$ equals $2^{\ell(a)}$, *i.e.*, $D_a F$ is $2^{\ell(a)}$-to-1. Since $\mathcal{I}m(D_a F)$ is contained in an affine subspace of codimension $\ell(a)$, according to the definition of Λ_a, $\mathcal{I}m(D_a F)$ is equal to this affine subspace.

Now, we suppose that F is a crooked function. Consider any component f_λ of F. Let $a \in \mathbb{F}_{2^n}^*$ such that $D_a f_\lambda$ is not constant. Set $V = \mathcal{I}m(D_a F)$. Then we have that any x satisfies:

$$Tr(\lambda D_a F(x)) = 0 \text{ if and only if } x \in V \cap H_\lambda.$$

There are 2^{n-1} such x, since $D_a F$ is 2-to-1 and V is an affine hyperplane, which is neither H_λ nor its complement. Hence $D_a f_\lambda$ is balanced. We have proved that f_λ is partially-bent, completing the proof. □

Let F be any quadratic function:

$$F(x) \ = \sum_{0 \le i < j < n} u_{i,j} x^{2^i + 2^j} \ , \quad u_{i,j} \in \mathbb{F}_{2^n} \ .$$

The derivatives of F are affine functions, say L_a for any $a \in \mathbb{F}_{2^n}^*$. Thus, F is partially-bent; it is crooked if and only if every L_a is an affine function with kernel of dimension 1.

Corollary 2. *Any quadratic vectorial function is partially-bent. It is crooked if and only if it is APN.*

4.2 Crooked functions on $\mathbb{F}_{2^n}$, n odd

In this section, we study crooked functions of odd dimension, bijective or not. Theorem 4 (below) is the main result, describing the exceptional properties of such functions. These results are quite known, but were partially presented in several papers [13, 16, 17]. First, it is easy to describe the set of crooked permutations.

Lemma 2. *Let F be a crooked function such that $F(0) = 0$, with differential sets S_a. Let a and λ be such that S_a equals either H_λ or $\overline{H_\lambda}$, where H_λ is defined by (6). Then we have:*

$$S_a = \overline{H_\lambda} \iff Tr(\lambda F(a)) = 1.$$

Besides, F is a permutation if and only if $S_a = \overline{H_\lambda}$, for any such pair (λ, a). In this case, n is odd.

Proof. By hypothesis, we have $Tr(\lambda D_a F(x)) = c$ for all x, where $c \in \{0, 1\}$. In particular, $Tr(\lambda F(a)) = c$; further, $c = 0$ means that $\mathcal{I}m(D_a F) = H_\lambda$.

The function F is not bijective if and only if $F(x) = F(x+a)$, for some pair (x, a). Equivalently, there is (λ, a) such that $\mathcal{I}m(D_aF) = H_\lambda$, since 0 belongs to $\mathcal{I}m(D_aF)$.

When n is even, F cannot be a permutation, since it is an APN function, which is plateaued (see [2, Theorem 3]). □

When n is odd, a crooked function need not to be bijective, as we show by the next example.

Example 1. *Assume that n is odd. It is well-known that*

$$F \ : \ x \mapsto x^{2^t+1}, \quad \textit{with } \gcd(t, n) = 1,$$

is an AB permutation. So, it is a crooked permutation. Consider now the function $x \mapsto G(x) = x^{2^t+1}+x$, which is AB too, and then crooked. Since $G(0) = G(1) = 0$, G is not a permutation.

Definition 5. *A Boolean function is said to be near-bent if it is 1-plateaued, i.e., its Walsh transform takes the values 0 and $\pm 2^{(n+1)/2}$ only.*

Theorem 4. *Let n be odd, F be a crooked function over $\mathbb{F}_{2^n}$ with $F(0) = 0$. For every $a \in \mathbb{F}_{2^n}^*$, define $\lambda(a)$ as the unique element satisfying*

$$S_a = \beta + H_{\lambda(a)},$$

where $\beta \in \mathbb{F}_{2^n}$ is not unique. Then the following properties hold:

(i) *The differential sets S_a are pairwise distinct, which is equivalent to the statement that $a \mapsto \lambda(a)$ is bijective on $\mathbb{F}_{2^n}^*$.*

(ii) *Any component f_λ of F is a near-bent Boolean function with linear space of dimension 1, say $\{0, a\}$. When f_λ is balanced, its derivative in point a is equal to 1. This holds for any f_λ, when F is a permutation.*

(iii) *F is an AB function.*

Proof. Since F is crooked, it is partially-bent. Let f_λ, $\lambda \in \mathbb{F}_{2^n}^*$, be the components of F. Thus, for any λ and for any a, the derivative of f_λ, in point a, is either constant or balanced. Hence

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(x)+f_\lambda(x+a)} \in \{0, \pm 2^n\}.$$

For any fixed λ, there is at least one a, say $a(\lambda)$, such that D_af_λ is constant, since otherwise the function f_λ would be bent, which is impossible when n is odd. Thus,

we get the set of the $a(\lambda)$, whose size is at most 2^n-1. However, $a(\lambda)=a(\mu)=b$, for some $\mu\neq\lambda$, would mean the following: the Boolean functions

$$x\mapsto Tr(\lambda D_bF(x)) \text{ and } x\mapsto Tr(\mu D_bF(x))$$

are both constant. This would imply that S_b is of codimension at least 2, a contradiction. To each λ corresponds one and only one a, completing the proof of **(i)**.

We deduce that any component f_λ has only one nonzero linear structure, say a, *i.e.,* its linear space has dimension 1. Obviously, if f_λ is balanced, its derivative in point a is constantly equal to 1. When F is a permutation, all f_λ are balanced, completing the proof of **(ii)**.

From Corollary 1, every f_λ is near-bent, providing

$$\mathcal{W}_{f_\lambda}(a)\in\{\ 0,\ \pm 2^{(n+1)/2}\ \},\ \text{for all } a\in\mathbb{F}_{2^n}\ .$$

According to Definiton 1, F is an AB function, completing the proof. □

From Table 1, we know that the support of the Walsh spectrum of any near-bent Boolean function on $\mathbb{F}_{2^n}$ has size 2^{n-1}. It could be an affine subspace of codimension 1, as it holds for components of some crooked functions.

Proposition 2. *Let $F : \mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$, n odd, such that $F(0)=0$. Assuming that F is crooked, the set*

$$W_\lambda=\{\ a\in\mathbb{F}_{2^n}\mid \mathcal{W}_{f_\lambda}(a)=0\}$$

is an affine subspace of codimension 1, for all $\lambda\in\mathbb{F}_{2^n}^*$.

Conversely, assume that the sets W_λ are affine hyperplanes. In this case, if F is APN then F is crooked.

Proof. Assume that F is crooked and let $\lambda\in\mathbb{F}_{2^n}^*$. Since F is an AB function, f_λ is partially bent, with linear space $\{0,b\}$, for some nonzero b. Obviously, the function $g_a: x\mapsto f_\lambda(x)+Tr(ax)$ is partially bent too, with linear space $\{0,b\}$, for any $a\in\mathbb{F}_{2^n}$. We know that any partially-bent function is balanced if and only if it is not constant on its linear space (see [9, Proposition 2]). Thus, g_a is balanced if and only if

$$D_bg_a(x)=1,\quad \textit{i.e., } D_bf_\lambda(x)+Tr(ab)=1, \text{ for all } x.$$

Hence, we get $Tr(ab)=1+c$, $c\in\mathbb{F}_2$, since D_bf_λ is a constant function. We can suppose that $c=0$. Thus, g_a is balanced if and only if $Tr(ab)=1$, that is $a\in\overline{H_b}$. Thus

$$W_\lambda=\{\ a\in\mathbb{F}_{2^n}\mid Tr(ab)=1\}=\overline{H_b}.$$

Similarly, with $c = 1$ we obtain $W_\lambda = H_b$.

Conversely, suppose that W_λ is an affine subspace of codimension 1, say $u + H_b$, $u \in \mathbb{F}_{2^n}$, for some b. So, $H_b^\perp = \{0, b\}$ and we have from Lemma 1:

$$\sum_{a \in H_b} \mathcal{W}_{f_\lambda}(a)^2 = 2^{n-1} \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda D_0 F(x))} + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda D_b F(x))} \right).$$

By Parseval's relation, the sum above on the left is equal either to 0 or to 2^{2n}. We deduce that $D_b f_\lambda$ is a constant function. So, if $D_b F$ is 2-to-1, then $\mathcal{I}m(D_b F)$ is equal to either H_λ or $\overline{H_\lambda}$. □

4.3 Crooked functions on $\mathbb{F}_{2^n}$, n even

When n is even, crooked functions are partially-bent functions which have bent components. We recall this property below in Theorem 5.

Theorem 5. *Let F be a plateaued function over $\mathbb{F}_{2^n}$, with n even and $n > 4$. Let $2^{(t_\lambda+n)/2}$ be the amplitude of any component of F, namely of any f_λ, $\lambda \in \mathbb{F}_{2^n}^*$. Denote by B the number of bent components of F. Then F is APN if and only if*

$$B = \sum_{\lambda \in \mathbb{F}_{2^n}^*, t_\lambda > 0} (2^{t_\lambda} - 2). \tag{8}$$

This property holds, in particular, for crooked functions.

Consequently, B satisfies

$$\frac{2(2^n - 1)}{3} \leq B < 2^n - 2^{n/2}, \tag{9}$$

where the lower bound is reached if and only if $t_\lambda = 2$ for all non zero t_λ.

Proof. Equality (8) has been proved in [11, Proposition 6], but may be computed by using (5). Indeed, since each f_λ is plateaued, we have $\nu(f_\lambda) = 2^{t_\lambda+2n}$, for any λ, and then:

$$A = \sum_{\lambda \in \mathbb{F}_{2^n}^*} \nu(f_\lambda) = 2^{2n} \sum_{\lambda \in \mathbb{F}_{2^n}^*} 2^{t_\lambda}.$$

According to (5), F is APN if and only if $A = 2^{2n+1}(2^n - 1)$, providing

$$B + \sum_{\lambda \in \mathbb{F}_{2^n}^*, t_\lambda > 0} 2^{t_\lambda} = 2(2^n - 1) = 2(B + N), \tag{10}$$

since $2^n - 1 = B + N$ with $N = |\{\lambda \mid t_\lambda > 0\}|$. Hence, the equality above is equivalent to (8). Note that $t_\lambda > 0$ implies $t_\lambda \geq 2$, since $n + t_\lambda$ must be even.

The lower bound of B, in (9), is known (see [2, Corollary 3]). The upper bound has been proved by [19, Theorem 3]. It cannot be reached here, since we must have $B \equiv 2 \pmod 4$, from (10). □

By the study of bent components, one understand precisely the difference between odd and even cases. Let F be a crooked function on $\mathbb{F}_{2^n}$, with components f_λ. We have seen that, when n is odd, there is a one to one correspondence $\lambda \mapsto a(\lambda)$, where $a(\lambda)$ is the unique linear structure of f_λ. When n is even, the linear space of f_λ has dimension s, where s is even. So, either f_λ is bent ($s = 0$) or $s \geq 2$. The number of hyperplanes involved in the structure of F is at most $(2^n - 1)/3$. For any a, there is one and only one λ such that $\mathcal{I}m(D_aF)$ is equal to H_λ or to $\overline{H_\lambda}$. But, the function D_af_λ is constant for any a belonging to the linear space of f_λ. There are at least three such nonzero a, when f_λ is not bent.

Proposition 3. *Let F be a crooked function on $\mathbb{F}_{2^n}$, n even, with components f_λ. For any $a \in \mathbb{F}_{2^n}^*$, there is a unique λ such that the derivative of f_λ, in point a, is a constant function.*

Conversely, any function f_λ is either bent or with linear space V of dimension $k \geq 2$.

Proof. By hypothesis, $\mathcal{I}m(D_aF)$ is an hyperplane H_λ, or the complement of H_λ, for any $a \in \mathbb{F}_{2^n}^*$. Hence $Tr(\lambda D_aF(x)) = c$, for all x, where $c \in \mathbb{F}_2$. Such a λ is unique, because otherwise $\mathcal{I}m(D_aF)$ would be an affine subspace of codimension 2.

Since F is a plateaued APN function, at least $2(2^n - 1)/3$ components of F are bent. Let f_λ be a non bent component. Its linear set has an even dimension, so this dimension must be greater than or equal to 2. □

5 Bent functions from crooked functions

In this section, we consider crooked functions over $\mathbb{F}_{2^n}$, where n is odd. The components of such a function are *near-bent* Boolean functions. Moreover, every component has (only) one derivative which is a constant function. (see Theorem 4). We will show that a set of $2^n - 1$ bent functions of $n + 1$ variables can be derived, using this strong property. Our main reference is the construction of Leander and McGuire [18], on the near-bent Boolean functions, that we apply to vectorial functions which are crooked. We first recall some facts which are more or less known, maybe not in this form.

Lemma 3. *Let f be a near-bent Boolean function over $\mathbb{F}_{2^n}$, where n is odd. Assume that $f(0) = 0$. Then* **(i)** *and* **(ii)** *are equivalent:*
(i) *f has a constant derivative in point $a \in \mathbb{F}_{2^n}^*$.*
(ii) *There exists a such that*

$$\{\ u \in \mathbb{F}_{2^n} \mid \mathcal{W}_f(u) = 0\ \} = \{\ u \in \mathbb{F}_{2^n} \mid Tr(ua) = 1 + f(a)\ \}.$$

Proof. Note that, f cannot have more than one linear structure, since it is near-bent. Assume that there is (a unique) a such that $D_a f(x) = c$, for all x, where $c \in \mathbb{F}_2$. Thus, $c = f(0) + f(a) = f(a)$. Now, we compute $\mathcal{W}_f(u)$:

$$\begin{aligned}\mathcal{W}_f(u) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+Tr(ux)} &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x+a)+Tr(u(x+a))} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(a)+Tr(u(x+a))} \\ &= (-1)^{f(a)+Tr(ua)}\ \mathcal{W}_f(u),\end{aligned}$$

since $f(x) + f(x + a) = f(a)$. Clearly, if u is such that $Tr(ua) + f(a) = 1$ then $\mathcal{W}_f(u) = 0$. But, there are 2^{n-1} such u, proving that **(ii)** holds.

Now suppose that **(ii)** holds, for some a. Recall that

$$H_a = \{\ u \in \mathbb{F}_{2^n} \mid Tr(ua) = 0\ \} \text{ so that } H_a^{\perp} = \{0, a\}.$$

Thus, the set of those u such that $\mathcal{W}_f(u) = 0$ is either equal to the hyperplane H_a, or equal to its complement, according to either $f(a) = 1$ or $f(a) = 0$. So, we can apply Lemma 1:

$$\sum_{v\in H_a} \mathcal{W}_f(v)^2 = 2^{n-1}\left(\sum_{x\in\mathbb{F}_{2^n}} (-1)^0 + \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(x+a)}\right).$$

By hypothesis, this sum equals 0 if $f(a) = 1$ and 2^{2n} if $f(a) = 0$, since the Parseval's relation. This is possible only if $D_a f$ is a constant derivative of f. It is the only one such derivative, since f is near-bent. □

Lemma 4. *Let f be a near-bent Boolean function on $\mathbb{F}_{2^n}$ (n odd) such that $f(0) = 0$. Assume that f has a linear structure a. Let g be the function from $G = \mathbb{F}_{2^n} \times \mathbb{F}_2$ to $\mathbb{F}_2$:*

$$g(x, y) = (y + 1)f(x) + y\left(f(x) + Tr(a^{-1}x)\right) \tag{11}$$

Then g is a bent function of $n + 1$ variables.

Proof. For any u, we denote by f_u the Boolean function $x \mapsto f(x) + Tr(ux)$. Let $b = a^{-1}$. The restriction of g to $\mathbb{F}_{2^n}$ $(y = 0)$ and to its complement in G $(y = 1)$ are respectively f and f_b which are both near-bent Boolean functions. Moreover

$$D_a f(x) = f(a) \quad \text{and} \quad D_a f_b(x) = f(a) + Tr(ba) = f(a) + 1 = f_b(a),$$

since $Tr(ba) = Tr(1) = 1$. Let $u \in \mathbb{F}_{2^n}^*$. Applying Lemma 3, f_u is balanced if and only if $Tr(ua) = 1 + f(a)$ and f_{b+u} is balanced if and only if

$$Tr(a(u + b)) = 1 + f(a), \quad \text{providing } Tr(ua) = 1 + 1 + f(a) = f(a).$$

Thus f_u is balanced if and only if f_{b+u} is not balanced. This is equivalent to say that g is bent (see [6, Theorem V.3] or [18, Theorem 2]). □

Now, we consider a crooked function F, from $\mathbb{F}_{2^n}$ to itself. According to Theorem 4, we know that all components f_λ of F are near-bent with a (unique) constant derivative. This allows to derive a specific set of bent functions from any crooked function, in odd dimension.

Theorem 6. *Let F be a crooked function over $\mathbb{F}_{2^n}$ where n is odd, such that $F(0) = 0$. Denote by a_λ the linear structure of the component f_λ of F. Then we get a set $B(F)$ of $2^n - 1$ bent functions g_λ, each from $G = \mathbb{F}_{2^n} \times \mathbb{F}_2$ to $\mathbb{F}_2$:*

$$B(F) = \{\ g_\lambda(x, y) = (y + 1)f_\lambda(x) + y\left(f_\lambda(x) + Tr(a_\lambda^{-1}x)\right)\ \mid \lambda \in \mathbb{F}_{2^n}^*\ \}.$$

Proof. Since F is a crooked function, there is a bijective correspondence between the $\lambda \in \mathbb{F}_{2^n}^*$, and then the functions f_λ, and the linear structures a_λ of every f_λ. Thus, Lemma 4 applies for every λ, using a_λ^{-1}, providing $2^n - 1$ distinct bent functions. □

Remark 1. *The construction, given by Theorem 6, could be of interest regarding the problem of the existence of crooked functions. It would be useful to exhibit some properties of $B(F)$, or to construct other sets of bent functions. For instance, g_λ could have an higher degree, by replacing f_λ by another Boolean function, affinely equivalent to f_λ. The question is to know if such a set of bent functions does exist, for some degree greater than 2.*

Note that a set like $B(F)$ is not a subspace, but could generate a linear code with few weights.

To derive effectively bent functions from a given crooked function, it is necessary to have an expression of the linear structures a_λ. This is generally an open problem, even when F is a quadratic APN function.

Example 2. *Let $F(x) = x^{2^k+1}$, $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, n odd. It is well-known that F is crooked if and only if $\gcd(k, n) = 1$. For any $\lambda \in \mathbb{F}_{2^n}^*$, the unique linear structure of f_λ is $a_\lambda = \lambda^{-1/(2^k+1)}$. Thus, for any $\lambda \in \mathbb{F}_{2^n}^*$,*

$$g_\lambda(x, y) = (y + 1)Tr\left(\lambda x^{2^k+1}\right) + y\left(Tr(\lambda x^{2^k+1}) + Tr(\lambda^{1/(2^k+1)}x)\right),$$

is a bent function, $(x, y) \mapsto g_\lambda(x, y)$, from $\mathbb{F}_{2^n} \times \mathbb{F}_2$ to $\mathbb{F}_2$.

6 Permutations from crooked functions

Any crooked function allows to construct a set of permutations, via their derivatives.

Theorem 7. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, such that $F(0) = 0$. Assume that F is a crooked function. Define, for any $a \in \mathbb{F}_{2^n}^*$:*

$$x \mapsto G_a(x) = F(x) + F(x + a) + F(a).$$

Let us define:
- *$\lambda \in \mathbb{F}_{2^n}^*$, defining the hyperplane H_λ, which is the image set of G_a;*
- *β be such that $Tr(\lambda\beta) = 1$, i.e. $\beta \notin H_\lambda$;*
- *H_μ be any hyperplane such that $Tr(\mu a) = 1$, i.e., $a \notin H_\mu$.*

Then, the function

$$x \mapsto R_a(x) = G_a(x) + \beta Tr(\mu x)$$

is a permutation, such that $R_a(H_\mu) = H_\lambda$.

Proof. Let $x \neq y$ such that $R_a(x) = R_a(y)$. We get

$$G_a(x) + G_a(y) = \beta\left(Tr(\mu(x + y))\right).$$

If $Tr(\mu(x+y)) = 0$ then $G_a(x)+G_a(y) = 0$, which implies $y = x+a$, since G_a is 2-to-1 and $G_a(x) = G_a(x + a)$. In this case, we get $Tr(\mu(x + y)) = Tr(\mu a) = 0$, a contradiction.

Now suppose that $Tr(\mu(x + y)) = 1$. Hence $G_a(x) = G_a(y) + \beta$. But this is impossible, since $G_a(x)$ and $G_a(y)$ belong to H_λ while $\beta \notin H_\lambda$. Thus, we get again a contradiction and can conclude that R_a is a permutation.

By construction, $R_a(H_\mu) = H_\lambda$, since $Tr(\mu x) = 0$ for all $x \in H_\mu$ and $G_a(H_\mu) = H_\lambda$. Indeed, G_a is 2-to-1 and its image set is H_λ. For any pair $(x, x+a)$, we have $x \in H_\mu$ if and only if $x + a \in \overline{H_\mu}$ (with $G_a(x) = G_a(x + a)$). □

7 Comments to conclude

As a prelude of this conclusion, we want to recall the main conjecture concerning crooked functions:

Conjecture: Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a crooked function, as defined by Definition 3. Then F is quadratic or, in other terms, has algebraic degree 2.

By the two previous sections, we aim to exhibit specific constructions which are possible only with crooked functions. Our purpose is to open new ways to study the existence of crooked functions. We are convinced that other properties have to be found, increasing the knowledge on crooked functions, especially on the existence of such functions.

On the other hand, the quadratic functions form a corpus of great interest about which many problems remain open. In particular, we are still far from understanding the different structures of quadratic APN functions of even dimension. The determination of the number of bent components of such a function would be of great interest. Negative answers, concerning the APN property of quadratic vectorial functions, have been obtained, for instance in [2, 5]. In [3], a description of the corpus of binomial crooked functions is presented. As a conclusion, Bierbrauer has conjectured that, up to equivalence, no other binomial crooked functions exist.

Crooked functions of codimension k, $1 \leq k \leq n-1$, appeared during the cryptanalysis of a hash function, called MARACA [8]. Here, the differential sets are affine subspaces of same codimension. The authors of this cryptanalysis, Canteaut and Naya-Placienta, introduced the *crooked property*. They have shown that this property could make a cryptographic primitive very weak. We will explore, in a more general context, the *functions having the crooked property*, in a forthcoming work.

Acknowledgment: The author want to thank Gohar Kyureghyan for helpful comments and fruitful discussions.

References

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

[2] T.P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy. On almost perfect nonlinear functions. *IEEE Trans. Inform. Theory*, 52(9):4160–4170, September 2006.

[3] J. Bierbrauer, A family of crooked funcions, *Designs, Codes and Cryptography*, (2009) 50:235-241.

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

[5] E. Byrne and G. McGuire, On the non-existence of quadratic APN and crooked functions on finite fields, Proc. of the *Workshop on Coding and Cryptography*, WCC 2004, 316-324.

[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 Trans. Inform. 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. *Designs, Codes and Cryptography*, (3):135–145, 1993.

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

[11] 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.

[12] E.R. van Dam and D. Fon-Der-Flaass. Uniformly packed codes and more distance regular graphs from crooked functions. *J. Algebraic Combin.* 12 (2000), no. 2, 115?121. 94B05

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

[14] J.F. Dillon and G. McGuire, Near bent functions on a hyperplane, *Finite Fields Appl.*, 14 (2008), no. 3, 715???720.

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

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

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

[18] G. Leander and G. McGuire, Construction of bent functions from near-bent functions, *Journal of Combinatorial Theory*, Series A 116 (2009) 960???970.

[19] A. Pott, E. Pasalic, A. Muratovic-Ribic and S. Bajric, On the maximum number of bent component of vectorial functions, *IEEE Transactions on Information Theory*, Vol. 64, No. 1, January 2018, pp. 403-411.

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