New links between nonlinearity and differential uniformity

Pascale Charpin, Jie Peng

New links between nonlinearity and differential uniformity

Pascale Charpin* Jie Peng†

August 19, 2018

Abstract

In this paper some new links between the nonlinearity and differential uniformity of some large classes of functions are established. Differentially two-valued functions and quadratic functions are mainly treated. A lower bound for the nonlinearity of monomial δ-uniform permutations is obtained, for any δ, as well as an upper bound for differentially two-valued functions. Concerning quadratic functions, significant relations between nonlinearity and differential uniformity are exhibited. In particular, we show that the quadratic differentially 4-uniform permutations should be differentially two-valued and possess the best known nonlinearity.

Keywords: Vectorial Boolean function, quadratic function, nonlinearity, differential uniformity, differentially two-valued function.

1 Introduction

The first statistical attack proposed for breaking iterated block ciphers, namely the *differential cryptanalysis*, was proposed by Biham and Shamir in [2]. The security is quantified by the so-called *differential uniformity* of the substitution box (S-box), which can be represented by a function, say F,

*INRIA Paris, 2 rue Simone Iff, 75012, FRANCE. Email: Pascale.Charpin@inria.fr

†Mathematics and Science College of Shanghai Normal University, Shanghai, CHINA. Email: jpeng@shnu.edu.cn

over the finite field of order 2^n denoted $\mathbb{F}_{2^n}$. The Boolean functions used in block ciphers must have a high distance to the set of all affine functions to resist to the *linear cryptanalysis* [25]. This criteria is called the *nonlinearity*. In this context, the knowledge of nonlinearity and differential uniformity of large families of functions is useful. On the other hand such a study allows to exhibit specific objects or can be replaced in a theoretical research in algebraic coding theory or combinatorics. It seems difficult to establish precise relations between the differential uniformity and the nonlinearity of any function. The aim of this work is to exhibit such property.

In this paper, based on a result on the sum-of-square indicators of the components of any function over $\mathbb{F}_{2^n}$, we obtain a lower bound for the nonlinearity of monomial permutations and an upper bound for the nonlinearity of any differentially two-valued function, relating to their differential uniformity (Theorems 3 and 4). For quadratic functions, we put forward a new approach to establish links between the nonlinearity and differential uniformity by studying some relations between the subspaces related to these functions (Theorem 5). Some important results are then deduced. In particular, we show that the quadratic differentially 4-uniform permutations should be two-valued and possess the best known nonlinearity (Theorem 7).

The rest of the paper is organized as follows. The next section gives some definitions, notation, properties which will be used in all the paper. In Section 3, we establishes some new links between the nonlinearity and differential uniformity of power functions and differentially two-valued functions. In Section 4 we mainly concentrated on quadratic functions. Some interesting applications of the results for quadratic functions, based on previous results (notably [5, 7, 9, 11]), are given in Section 5. Finally, Section 6 concludes the paper.

2 Preliminaries

A mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is usually called an (n, m)-function or a *vectorial Boolean function*. There are two special and important cases with respect to m. One is $m = 1$, in this case we say F is an n-variable Boolean function and usually use small letter f instead, and let B_n be the set of all n-variable Boolean functions. The other case is $m = n$, in which we say that F is a function over $\mathbb{F}_{2^n}$. In this paper we are mainly concentrated on the latter case, but will use the representation of F by their *components functions*.

For any function F over $\mathbb{F}_{2^n}$, all the nonzero linear combinations of its coordinate functions are called the components of F. They are n-variable Boolean functions, which are represented as follows in this paper:

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

where Tr is the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. For any $a \in \mathbb{F}_{2^n}^*$, the function

$$D_aF : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ x \mapsto F(x+a)+F(x)$$

is called the *derivative of F in direction a.* For any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, we are interested by the cardinality of any set $(D_aF)^{-1}(b)$: set

$$\delta(a,b) = \#\{x \in \mathbb{F}_{2^n} \mid D_aF(x) = b\} \tag{1}$$

where $\#E$ denotes the cardinal of the set E. The *differential uniformity* δ of F is defined as

$$\delta = \max_{a \in \mathbb{F}_{2^n}^*,\ b \in \mathbb{F}_{2^n}} \delta(a,b). \tag{2}$$

We also say that F is *differentially δ-uniform.* It is clear that δ is a positive even integer. When $\delta = 2$, the possible smallest value, F is said to be *almost perfect nonlinear* (APN for short).

A function F over $\mathbb{F}_{2^n}$ is said *differentially two-valued* if $\delta(a,b)$ takes two values only. These values are known to be $\{0, 2^s\}$ for some positive integer s. Thus we will often say that F *is differentially two-valued* $\{0, 2^s\}$. A basic study of these functions has to be found in [3]. There are more general results in [20] such as the following which we will use later.

Corollary 1 [20, Corollary 6] *Let F be a differentially two-valued $\{0, 2^s\}$ function over $\mathbb{F}_{2^n}$. If s is even then n must be even too. In particular, F cannot be differentially 4-uniform when n is odd.*

Remark 1 *We proved in [20] that some properties of differentially two-valued functions hold for quadratic functions. These results reinforce [3, Conjecture 1], saying that differentially two-valued power functions are the quadratic and the so-called Kasami function. However note that APN functions and the inverse of differentially two-valued permutations are differentially two-valued too. Thus not all differentially two-valued functions are quadratic.*

For any $f \in B_n$, its *Walsh coefficients* are defined as

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+ax}, a \in \mathbb{F}_{2^n}.$$

The nonlinearity of f is denoted $nl(f)$ and computed as

$$nl(f) = 2^{n-1} - \frac{L(f)}{2} \quad \text{where} \quad L(f) = \max_{a \in \mathbb{F}_{2^n}} |W_f(a)|.$$

The function f is said to be *bent* when n is even and W_f takes two values $\{\pm 2^{n/2}\}$ only. It is said to be *plateaued* when either it is bent or W_f takes three values $\{0, \pm 2^{(n+s)/2}\}$, $1 \leq s \leq n$, where s is an integer such that $n+s$ is even. The value $2^{(n+s)/2}$ is called the *amplitude* of f. A *plateaued vectorial function* is a vectorial function whose components are plateaued Boolean functions. It is said *plateaued with single amplitude* when all its components have the same amplitude.

The *sum-of-square* indicator of $f \in B_n$ is defined by

$$\nu(f) = \sum_{a \in \mathbb{F}_{2^n}} W^2_{D_a f}(0) = 2^{-n} \sum_{b \in \mathbb{F}_{2^n}} W^4_f(b). \tag{3}$$

Recall that $\nu(f) \leq 2^n L^2(f)$ with equality if and only if f is plateaued, that is

$$L(f) = 2^{(n+s)/2} \text{ and } \nu(f) = 2^n L^2(f) = 2^{2n+s}, 1 \leq s \leq n. \tag{4}$$

We now consider any vectorial function F over $\mathbb{F}_{2^n}$ with components f_λ. The *Walsh transform* of the function F is defined as

$$W_F(\lambda, a) = W_{f_\lambda}(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda F(x)+ax)}, \ (\lambda, a) \in \mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n}. \tag{5}$$

The *Walsh spectrum* of F is the multiset consisting of integers $W_F(\lambda, a)$ with their multiplicities. The function F is said *almost bent* (AB) when $W_F(\lambda, a)$ takes only the three values $\{0, \pm 2^{(n+1)/2}\}$, so that n must be odd. The nonlinearity $NL(F)$ of F is defined as

$$NL(F) = 2^{n-1} - \frac{\mathcal{L}(F)}{2} \quad \text{where} \quad \mathcal{L}(F) = \max_{(\lambda,a) \in \mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n}} |W_F(\lambda, a)|.$$

For odd integers n, it has been proved that $NL(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$ [18], where the upper bound is achieved by the AB functions. While for even n,

the known maximum nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$, which is conjectured to be an upper bound [21].

In Table 1, we list the infinite families of differentially 4-uniform monomial permutations over $\mathbb{F}_{2^n}$ with the known maximum nonlinearity, which are currently known. It is conjectured that this table is complete [8], up to equivalence and including the compositional inverse of the functions. For multinomial functions satisfying the same properties see [9, 19, 33]. Such functions are rare and generally quadratic or derived from APN functions. Note that a monomial functions F, *i.e.,* $F(x) = x^d$, is currently called a *power function.*

	Functions	Condition	Ref.
Gold	x^{2^i+1}	$n=2k$, k is odd and $\gcd(n,i)=2$	[22]
Kasami	$x^{2^{2i}-2^i+1}$	$n=2k$, k is odd and $\gcd(n,i)=2$	[23]
Inverse	x^{-1} $(0^{-1}:=0)$	n is even	[27]
Bracken-Leander	$x^{2^{2m}+2^m+1}$	$n=4m$ and m is odd	[8]

Table 1: Known differentially 4-uniform power permutations over $\mathbb{F}_{2^{2k}}$ with best known nonlinearity

3 A general relation and some consequences

The following lemma gives some link between the differential uniformity of a function over $\mathbb{F}_{2^n}$ and the sum-of-square indicators of its components.

Lemma 1 *Let F be differentially δ-uniform over $\mathbb{F}_{2^n}$, with components f_λ, $\lambda \in \mathbb{F}_{2^n}^*$. Then*

$$(2^n-1)2^{2n+1} \leq \sum_{\lambda \in \mathbb{F}_{2^n}^*} \nu(f_\lambda) \leq (2^n-1)2^{2n}\delta,$$

where the lower bound is achieved if and only if F is APN, and the upper bound is achieved if and only if F is differentially two-valued.

Proof. The lower bound is obtained by [1, Corollary 1] as well as the case where equality holds.

The upper bound is computed by using (3). Recall the following formula due to Nyberg [28, p. 118](see formula (4) which is here rewritten in our context):

$$\sum_{\lambda\in\mathbb{F}_{2^n}} W^2_{D_a f_\lambda}(0) = 2^n \sum_{b\in\mathbb{F}_{2^n}} \delta^2(a,b).$$

Recall that $\sum_{b\in\mathbb{F}_{2^n}} \delta(a,b) = 2^n$. Thus we have

$$\begin{aligned}
\sum_{\lambda\in\mathbb{F}^*_{2^n}} \nu(f_\lambda) &= \sum_{\lambda\in\mathbb{F}^*_{2^n}} \sum_{a\in\mathbb{F}_{2^n}} W^2_{D_a f_\lambda}(0) \\
&= \sum_{a\in\mathbb{F}^*_{2^n}} \sum_{\lambda\in\mathbb{F}_{2^n}} W^2_{D_a f_\lambda}(0) \\
&= \sum_{a\in\mathbb{F}^*_{2^n}} 2^n \sum_{b\in\mathbb{F}_{2^n}} \delta^2(a,b) \\
&\leq \sum_{a\in\mathbb{F}^*_{2^n}} 2^n\delta \sum_{b\in\mathbb{F}_{2^n}} \delta(a,b) \\
&= (2^n-1)2^{2n}\delta.
\end{aligned}$$

Now suppose that equality holds. Using the inequality above, this is equivalent to

$$\sum_{a\in\mathbb{F}^*_{2^n}} 2^n \sum_{b\in\mathbb{F}_{2^n}} \delta(a,b)\,(\delta-\delta(a,b)) = 0,$$

which is possible if and only if $\delta(a,b) \in \{0,\delta\}$ for all a,b. ◇

Suppose that F is plateaued with single amplitude $2^{(n+s)/2}$; then $\nu(f_\lambda) = 2^{2n+s}$ for any λ (see Section 2). We deduce, from Lemma 1, that $2^{2n+s} \leq 2^{2n}\delta$ providing $2^s \leq \delta$ with equality when F is two-valued $\{0, 2^s\}$. Note that such functions F exist, which are two-valued and plateaued (see some quadratic functions later or [3, Theorem 2]).

Proposition 1 *Let F be a function over $\mathbb{F}_{2^n}$ which is plateaued with single amplitude $2^{(n+s)/2}$ for some integer s such that $n+s$ is even. Then, the differential uniformity δ of $\mathbb{F}_{2^n}$ satisfies $\delta \geq 2^s$ with equality if and only if F is differentially two-valued.*

Thus we have, since δ is even,

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} \nu(f_\lambda) = \gamma(2^n-1)2^{2n+1} \tag{6}$$

where γ is a rational number such that $1 \leq \gamma \leq \delta/2$.

The number of bent components of vectorial functions over $\mathbb{F}_{2^n}$, n even, is an interesting issue. A general approach is proposed by [29, Theorem 3]. For APN functions, this number has been characterized for plateaued such functions [1, Corollary 3]. For differentially 4-uniform functions, the following result gives part of the answer.

Theorem 1 *Let n be even and let F be a differentially 4-uniform function over $\mathbb{F}_{2^n}$ such that all its components are plateaued. Let A be the number of bent components of F. Then there exists some rational number $1 < \gamma \leq 2$ depending on F, such that*

$$A \geq \frac{(4-2\gamma)(2^n-1)}{3},$$

providing that if F is not two-valued, i.e., $\gamma \neq 2$, then F has bent components.

Consequently, if F is not two-valued, then F is not a permutation. Moreover, for any linear function L over $\mathbb{F}_{2^n}$, $F+L$ is not a permutation.

In particular, any differentially 4-uniform quadratic permutation is two-valued.

Proof. Since F is differentially 4-uniform, the number γ defined by (6) satisfies $1 < \gamma \leq 2$. For any component f_λ of F we have

$$\nu(f_\lambda) \begin{cases} = 2^{2n} & \text{if } f_\lambda \text{ is bent,} \\ \geq 2^{2n+2} & \text{otherwise,} \end{cases}$$

since n is even and f_λ is plateaued (see Section 2). Therefore, there exists some integer B such that

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} \nu(f_\lambda) = \gamma(2^n-1)2^{2n+1} = A2^{2n} + B2^{2n+2}$$

with $A + B \geq 2^n - 1$. We get $2\gamma(2^n-1) = A + 4B$, and then

$$3A + 2\gamma(2^n-1) = 4A + 4B \geq 4(2^n-1),$$

which leads to $A \geq (4-2\gamma)(2^n-1)/3$. In particular, if F is not differentially two-valued, then $1 < \gamma < 2$, and thus $A > 0$.

It is well known that F is a permutation if and only if all its nonzero components are balanced. If F is not differentially two-valued, then F has a bent component, say f_μ, which is not balanced. Hence F cannot be a permutation. Moreover, for any linear function L, the component $(F+L)_\mu = f_\mu + Tr(\mu L)$ is also bent, which implies that $F + L$ is not a permutation. $\diamond$

To illustrate our previous result, we exhibit a function with bent components, by the next corollary. For our proof, we need a property of linear functions whose proof can be found in [7, Corollary 3.2].

Lemma 2 *Let L be a linear function over $\mathbb{F}_{2^n}$ as follows defined:*

$$L(x)=\sum_{i=0}^{d} l_i x^{2^{si}},\ l_i \in \mathbb{F}_{2^n} \text{ and } l_d \neq 0, \text{ where } \gcd(n,s)=1.$$

Then the kernel of L has dimension at most d.

Corollary 2 *Let $F(x) = x^{2^{2t}+1} + \beta x^{2^t+1}$ be a function over $\mathbb{F}_{2^n}$ where β is any nonzero element of $\mathbb{F}_{2^n}^*$ and $\gcd(n,t) = 1$. Then F is differentially 4-uniform and not two-valued. Consequently when n is even, F has bent components; thus $F + L$ cannot be a permutation for any linear function L.*

Proof. Since F is quadratic, it is plateaued (see Section 4 later). We compute the derivatives of F. For any $a \in \mathbb{F}_{2^n}^*$:

$$\begin{aligned} D_aF(x) &= x^{2^{2t}}a + a^{2^{2t}}x + \beta(x^{2^t}a + a^{2^t}x) + F(a) \\ &= ax^{2^t}(x^{2^{2t}-2^t} + \beta) + x(a^{2^{2t}} + \beta a^{2^t}) + F(a) \\ &= x^{2^{2t}}a + x^{2^t}\beta a + x(a^{2^{2t}} + \beta a^{2^t}) + F(a) \\ &= L_a(x) + F(a). \end{aligned}$$

Applying Lemma 2 we see that the kernel of L_a has dimension at most 2 implying that F is differentially 4-uniform, since it was proved in [1, Theorem 6]) that any function $x \mapsto xL(x)$, where L is any linear function, cannot be APN.

There is a unique a such that $a^{2^{2t}} + \beta a^{2^t} = 0$, since $2^{2t} - 2^t$ and $2^n - 1$ are coprime. For this a

$$D_aF(x)+F(a)=ax^{2^t}(x^{2^{2t}-2^t}+\beta).$$

Thus, in this case D_aF is 2-to-1 implying that F is not two-valued. Then the proof is completed by applying Theorem 1. $\diamond$

We now present other results that we obtain by applying Lemma 1. These relate in particular with the power functions and the differentially two-valued functions.

Let $F(x) = x^d$ be a power function over $\mathbb{F}_{2^n}$. When F is a permutation all its components f_λ have the same Walsh spectrum; moreover all $\nu(f_\lambda)$ are equal. It is well known that if F is APN, then $\gcd(d, 2^n - 1) = 1$ for odd n and $\gcd(d, 2^n - 1) = 3$ for even n. Consequently, F APN and n odd imply that $\nu(f_\lambda) = 2^{2n+1}$, $\lambda \in \mathbb{F}_{2^n}^*$ [1, Proposition 5]. Then one can deduce an upper bound for power APN functions as $NL(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$, though it gives not any new information. While for even n, the situation is more complicated, the last result is due to Canteaut and is listed below. Note that some congruences allow to study the nonlinearity of Boolean functions [24] which are components of a power function.

Theorem 2 *[15, Theorem 8.14] Let $n = 2m$ and let the power function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $F(x) = x^d$. Assume that $\gcd(d, 2^n - 1) > 1$. Then $NL(F) \leq 2^{n-1} - 2^m$. If $NL(F) = 2^{n-1} - 2^m$ then $\gcd(d, 2^n - 1) = 3$ and $W_F(\lambda, 0)$ equals*

$$\begin{cases} (-1)^{m+1}2^{m+1}, & \text{if } \lambda \in \{x^3,\ x \in \mathbb{F}_{2^n}^*\}, \\ (-1)^m 2^m, & \text{if } \lambda \notin \{x^3,\ x \in \mathbb{F}_{2^n}^*\}. \end{cases}$$

Applying Lemma 1 to power permutations, we obtain a precise result. Since all $\nu(f_\lambda)$ are equal, we get (with notation of Lemma 1)

$$(2^n-1)\nu(f_\lambda) \leq (2^n-1)2^{2n}\delta, \text{ for any } \lambda \in \mathbb{F}_{2^n}^*.$$

If F is differentially two-valued $\{0, 2^s\}$ then

$$\nu(f_\lambda) = 2^{2n+s} \leq 2^n L^2(f_\lambda), \text{ for any } \lambda \in \mathbb{F}_{2^n}^*.$$

Further $L(f_\lambda) \geq 2^{(n+s)/2}$ with equality if and only if f_λ is plateaued and this property holds for F. Note the similarity of the next proposition and of Proposition 1.

Proposition 2 *Let $F(x) = x^d$ with $\gcd(d, 2^n - 1) = 1$. Assume that F is differentially δ-uniform.*

Then, for any λ, $\nu(f_\lambda) \leq 2^{2n}\delta$ with equality if and only if F is differentially two-valued $\{0, 2^s\}$. In this case, $\mathcal{L}(F) \geq 2^{(n+s)/2}$ with equality if and only if F is a vectorial plateaued function.

Little is known on the lower bound of the nonlinearity of any differentially δ-uniform function, δ being fixed. It seems that the nonlinearity of all known APN functions is rather good. It would be of interest and importance to find the reason. Recently, Carlet proposed a nonzero lower bound for the nonlinearity of APN power functions F in [17, Theorem V.6], where he used the fourth moment of the Walsh transform to show that $NL(F) \geq 2^{n-1} - 2^{\frac{3n-3}{4}}$ for n odd and $NL(F) \geq 2^{n-1} - 2^{\frac{3n-2}{4}}$ for n even.

Like the APN functions, the nonlinearity of most known differentially 4-uniform permutations on $\mathbb{F}_{2^n}$ for even n also seems to be not low (see Table 1, [30, 31] and references therein). By the next theorem, we propose a lower bound which increases with differential uniformity for the nonlinearity of bijective power functions.

Theorem 3 *Let F be a power permutation over $\mathbb{F}_{2^n}$ with differential uniformity δ. Then we have*

$$NL(F) \geq 2^{n-1} - 2^{\frac{3n-4}{4}} \sqrt[4]{\delta}.$$

Proof. By Lemma 1, according to Proposition 2 it holds for any λ:

$$L^4(f_\lambda) \leq \sum_{c \in \mathbb{F}_{2^n}} W_F^4(\lambda, c) = 2^n \nu(f_\lambda) \leq 2^{3n}\delta.$$

Consequently,

$$NL(F) \geq 2^{n-1} - 2^{\frac{3n-4}{4}} \sqrt[4]{\delta}.$$

This completes the proof. ◇

Example 1 *For $\delta = 2$ we get $L(f_\lambda) \leq 2^{(3n+1)/4}$ for any λ; thus, we obtain the lower bound given in [17], i.e., $NL(F) \geq 2^{n-1} - 2^{(3n-3)/4}$. Note that in this case n is odd because an APN power function cannot be bijective for n even.. When $\delta = 4$ we get $L(f_\lambda) \leq 2^{(3n+2)/4}$ and then $NL(F) \geq 2^{n-1} - 2^{(3n-2)/4}$.*

Remark 2 *Note that many power functions wih a low differential uniformity are in fact permutations. Let $F(x) = x^d$. For instance, it has been proved in [3] that*

(i) *If n or $n/2$ is odd and F is differentially 4-uniform then F is a permutation;*

(ii) *If n or $n/2$ is odd, with $\gcd(3,n)=1$, and F is differentially 6-uniform then F is a permutation;*

(iii) *If n or $n/2$ is odd, $\gcd(3,n)=3$ and $\gcd(7,n)=1$, and F is differentially 6-uniform then F is a permutation.*

When n is even and $n/2$ odd, Theorem 1 implies that if F is plateaued and differentially 4-uniform then it is two-valued. For instance, it is the case for Kasami functions $F(x)=x^{2^{2t}-2^t+1}$ with $\gcd(n,t)=2$, whose Walsh spectrum takes values $\{0,\pm 2^{(n+2)/2}\}$ (see [3, Theorem 2]).

Thanks to Lemma 1, we can also derive an upper bound for the nonlinearity of any differentially two-valued function.

Theorem 4 *Let F be a differentially two-valued $\{0,2^s\}$ function over $\mathbb{F}_{2^n}$. Then it holds*

$$NL(F)\leq 2^{n-1}-2^{\frac{n+s}{2}-1}.$$

where s should be odd when n is odd.

Proof. Recall that $\mathcal{L}^2(F)=\max_{\substack{\lambda\in\mathbb{F}_{2^n}^*,\\ b\in\mathbb{F}_{2^n}}} W_F^2(\lambda,b)$. First it is clear that

$$\mathcal{L}^2(F)\sum_{\substack{\lambda\in\mathbb{F}_{2^n}^*,\\ b\in\mathbb{F}_{2^n}}} W_F^2(\lambda,b)\geq \sum_{\substack{\lambda\in\mathbb{F}_{2^n}^*,\\ b\in\mathbb{F}_{2^n}}} W_F^4(\lambda,b)$$

By Parseval's relation one has

$$\sum_{\substack{\lambda\in\mathbb{F}_{2^n}^*,\\ b\in\mathbb{F}_{2^n}}} W_F^2(\lambda,b)=(2^n-1)2^{2n}.$$

Moreover, by Lemma 1 and (3), it holds

$$\sum_{\substack{\lambda\in\mathbb{F}_{2^n}^*,\\ b\in\mathbb{F}_{2^n}}} W_F^4(\lambda,b)=2^n\sum_{\lambda\in\mathbb{F}_{2^n}^*}\nu(f_\lambda)=(2^n-1)2^{3n+s},$$

since F is differentially two-valued $\{0,2^s\}$. Consequently, we arrive at

$$\mathcal{L}^2(F)\geq\frac{(2^n-1)2^{3n+s}}{(2^n-1)2^{2n}}=2^{n+s},$$

and hence

$$NL(F)\leq 2^{n-1}-2^{\frac{n+s}{2}-1}.$$

According to Corollary 1, if n is odd then s is odd too. ◇

4 Quadratic functions

We will now deal with quadratic functions and we begin by fixing notation and definitions. We assume that F over $\mathbb{F}_{2^n}$ is of the form

$$F(x)=\sum_{i,j} a_{i,j}x^{2^i+2^j},\ 0\leq i<j\leq n-1, \tag{7}$$

so that $F(0) = 0$. Then $f_\lambda(x) = Tr(\lambda F(x))$ is a quadratic form for any $\lambda \in \mathbb{F}_{2^n}$, and the function

$$(x,a)\mapsto Tr(\lambda Q(x,a)),\ \text{where } Q(x,a)=F(x+a)+F(x)+F(a). \tag{8}$$

is an alternative bilinear form.The corresponding radical of this quadratic form is

$$rad_\lambda(F) := \{a \in \mathbb{F}_{2^n} \mid Tr(\lambda Q(x,a)) = 0,\ \forall\ x \in \mathbb{F}_{2^n}\}. \tag{9}$$

Note that $rad_\lambda(F)$ is actually the *linear space* of f_λ, *i.e.,* the set of a such that the derivative of f_λ in point a is constant. Such a is called a *linear structure* of f_λ. We will denote by $\ell(\lambda)$ the dimension of $rad_\lambda(F)$. It is well known and easily checked that for any $\lambda \in \mathbb{F}_{2^n}^*$ and for any $b \in \mathbb{F}_{2^n}$

$$W_F^2(\lambda,b)=\sum_{a\in\mathbb{F}_{2^n}}(-1)^{Tr(ba+\lambda F(a))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr(\lambda Q(x,a))}, \tag{10}$$

while it holds

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr(\lambda Q(x,a))}=\begin{cases}2^n, & \text{if } a\in rad_\lambda(F),\\ 0, & \text{otherwise}\end{cases}$$

Therefore, we arrive at

$$\begin{aligned} W_F^2(\lambda,b) &= 2^n\sum_{a\in rad_\lambda(F)}(-1)^{Tr(ba+\lambda F(a))}\\ &= \begin{cases}2^{n+\ell(\lambda)}, & \text{if } Tr(ba+\lambda F(a)) \text{ vanishes on } rad_\lambda(F),\\ 0, & \text{otherwise,}\end{cases}\end{aligned} \tag{11}$$

since by definition the function $a \mapsto Tr(ba + \lambda F(a))$ is linear on $rad_\lambda(F)$. Therefore, all quadratic functions are plateaued and their derivatives are

either balanced or constant. Moreover, as $W_F(\lambda, b)$ is an integer, it follows from (11) that

$$n \equiv \ell(\lambda) \pmod 2, \text{ for any } \lambda \in \mathbb{F}_{2^n}^*. \tag{12}$$

Note also that for any $\lambda \in \mathbb{F}_{2^n}^*$ the Walsh transform $b \mapsto W_F(\lambda, b)$ of f_λ takes the values $\{0, \pm 2^{(n+\ell(\lambda))/2}\}$ if f_λ is non-bent and the values $\{\pm 2^{n/2}\}$ if f_λ is bent. Therefore, the best nonlinearity of quadratic functions over $\mathbb{F}_{2^n}$ is $2^{n-1} - 2^{\frac{n-1}{2}}$ for odd n and $2^{n-1} - 2^{\frac{n}{2}}$ for even n, which is also called the *quadratic bound*. Now we define

$$ker_a(F) := \{\lambda \in \mathbb{F}_{2^n} \mid Tr(\lambda Q(x, a)) = 0, \ \forall \ x \in \mathbb{F}_{2^n}\} \tag{13}$$

and denote by $d(a)$ the dimension of the vector space $ker_a(F)$ for convenience. The subspace $ker_a(F)$ is related with the image set of D_aF, which is an affine subspace since D_aF is an affine function. Further, the image set of $x \mapsto Q(x, a)$ is a subspace, since $Q(0, a) = 0$. Our main results are based on the following observation.

Lemma 3 *Let F be quadratic and differentially δ-uniform. For any $a \in \mathbb{F}_{2^n}^*$, the function D_aF is $2^{d(a)}$-to-1, where $d(a)$ is the dimension of the vector space $ker_a(F)$ defined by (13). Hence $\delta = \max_{a \in \mathbb{F}_{2^n}^*} 2^{d(a)}$.*

Proof. The hyperplanes in $\mathbb{F}_{2^n}$ can, as usual, be defined as follows:

$$H_\lambda = \{y \in \mathbb{F}_{2^n} \mid Tr(\lambda y) = 0\}, \ \lambda \in \mathbb{F}_{2^n}^*. \tag{14}$$

Thus, $ker_a(F)$ is the set of those λ such that H_λ contains the image set of $x \mapsto Q(x, a)$. This implies that this image set is a subspace of dimension $n - d(a)$ so that D_aF is $2^{d(a)}$-to-1. Therefore $\delta(a, b) \in \{0, 2^{d(a)}\}$ for any b, completing the proof. ◇

In this paper we put forward a different approach for the study of those $\ell(\lambda)$ by studying some relations between the subspaces related to the function F. Our method applies to quadratic functions with any differential uniformity.

4.1 A relation between nonlinearity and differential uniformity

It appears that the quadratic functions can be classified by their differential uniformity as well as by their nonlinearity. The link between these two

concepts is really not clear, as proves the next example due to Dillon and indicated in [7]. It is an example of APN quadratic function whose nonlinearity is not the quadratic bound for $n = 6$. More such examples for $n = 8$ can be found in the list of [34].

Example 2 *Let $n = 6$ and let α be a primitive element of $\mathbb{F}_6$. The following function is APN and its Walsh spectrum has five values:*

$$F(x)=x^3+\alpha^{11}x^5+\alpha^{13}x^9+x^{17}+\alpha^{11}x^{33}+x^{48}.$$

By using the MAGMA package, we obtain that F has 46 bent components ($\ell(\lambda) = 0$), 16 components such that $\ell(\lambda) = 2$ and one $\lambda \in \mathbb{F}_{2^n}^*$ such that $\ell(\lambda) = 4$. Therefore, $NL(F) = 2^{n-1} - 2^{\frac{n+2}{2}} = 16$. Note that the number of bent components is greater than the lower bound which is 42 as we recall later in Remark 3.

Theorem 5 *Let F be a quadratic function over $\mathbb{F}_{2^n}$. Notation is as above, defined by (9) to (13). Then we have*

$$\sum_{\lambda\in\mathbb{F}_{2^n}^*} 2^{\ell(\lambda)}=\sum_{a\in\mathbb{F}_{2^n}^*} 2^{d(a)}. \tag{15}$$

Proof. It is simpy obtained by computing:

$$\begin{aligned}
\sum_{\lambda\in\mathbb{F}_{2^n}^*} 2^{\ell(\lambda)} &= \sum_{\lambda\in\mathbb{F}_{2^n}^*} |\{a \in \mathbb{F}_{2^n} \mid Tr(\lambda Q(x,a))=0,\ \forall\ x \in \mathbb{F}_{2^n}\}| \\
&= 2^n-1+\sum_{a\in\mathbb{F}_{2^n}^*} |\{\lambda \in \mathbb{F}_{2^n}^* \mid Tr(\lambda Q(x,a))=0,\ \forall\ x \in \mathbb{F}_{2^n}\}| \\
&= \sum_{a\in\mathbb{F}_{2^n}^*} |\{\lambda \in \mathbb{F}_{2^n} \mid Tr(\lambda Q(x,a))=0,\ \forall\ x \in \mathbb{F}_{2^n}\}| \\
&= \sum_{a\in\mathbb{F}_{2^n}^*} 2^{d(a)}.
\end{aligned}$$

This completes the proof. ◇

Theorem 5 establishes a link between the values $\ell(\lambda)$ and the values $d(a)$, where the former ones are related to the nonlinearity of F and the latter ones are related to the differential uniformity of F.

Corollary 3 *Let F be a quadratic function over $\mathbb{F}_{2^n}$, such that $\delta = 2^s$ and $\mathcal{L}(F) = 2^{(n+t)/2}$. For any integers i and j such that $1 \leq i \leq s$ and $j \in J$ where $J = \{j \mid 0 \leq j \leq t,\ n+j \text{ even}\}$, we set*

$$N_i = \#\{a \in \mathbb{F}_{2^n}^* \mid D_aF \text{ is } 2^i\text{-to-1}\} \text{ and } n_j = \#\{\lambda \in \mathbb{F}_{2^n}^* \mid \ell(\lambda) = j\}$$

Then it holds

$$\sum_{j \in J} 2^j n_j = \sum_{i=1}^{s} 2^i N_i, \tag{16}$$

where $\sum_i N_i = \sum_j n_j = 2^n - 1$. In particular, if F is differentially two-valued $\{0, 2^s\}$, then we have

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} 2^{\ell(\lambda)} = 2^s(2^n - 1) \quad \text{where } t \geq s,\ t = \max_{\lambda}\{\ell(\lambda)\}. \tag{17}$$

If F has single amplitude $2^{(n+t)/2}$ then

$$\sum_{a \in \mathbb{F}_{2^n}^*} 2^{d(a)} = 2^t(2^n - 1) \quad \text{where } 1 \leq d(a),\ s \geq t,\ s = \max_{a}\{d(a)\}. \tag{18}$$

Proof. By Lemma 3, any function D_aF is 2^i-to-1 if and only if $d(a) = i$. Further, (16) follows from Theorem 5.

Now assume that F is two-valued $\{0, 2^s\}$. We get directly (17) because in this case $N_1 = \cdots = N_{s-1} = 0$ so that $N_s = 2^n - 1$. In this case, $t \geq s$ since it is impossible to have $\ell(\lambda) < s$ for all λ.

Similarly, we prove (18) by noticing that $d(a)$ cannot be zero. Indeed, any function $x \mapsto D_aF(x) + F(a)$ is linear and its image set is contained in at least one affine space of codimension 1, *i.e.,* there is at least one λ such that $Tr(\lambda Q(x, a)) = 0$ for all x. ◇

Remark 3 *Well-known properties of any APN quadratic function F are directly derived from the previous results:*
– If n is odd, then $2(n_1 + 2^2A) = 2(2^n - 1)$ from (17). But we must have $n_1 + 2^2A = (2^n - 1)$ which forces $A = 0$ and $n_1 = 2^n - 1$, since $\sum_i n_i = (2^n - 1)$. Then $\mathcal{L}(F) = 2^{(n+1)/2}$, i.e., F is an AB function.
– Assume that n is even. Then $n_0 + 2^2A = 2(2^n - 1)$. Thus $n_0 > 0$ and F

has an even number of bent components. Now, since $(2^n-1)-\sum_{i\neq 0} n_i = n_0$ *we get*

$$3\sum_{i=2}^{t} n_i \leq \sum_{i=2}^{t}(2^i-1)n_i = (2^n-1), \text{ where } i \text{ is even.}$$

Hence the number of non bent components is less than or equal to $(2^n-1)/3$. *The number of bent components equals* $2(2^n-1)/3$ *if and only if* $\mathcal{L}(F) = 2^{(n+2)/2}$ *(*$t=2$*).*

4.2 Differentially two-valued quadratic functions

In this section we explore in some details the link between the nonlinearity and the two-valued property. We later focus on quadratic functions with low differential uniformity, that is $\delta \in \{2,4,8\}$. First, we can be more precise, regarding Theorem 4.

Theorem 6 *Let* F *be quadratic differentially two-valued* $\{0, 2^s\}$ *over* $\mathbb{F}_{2^n}$. *Then, for even* n

$$NL(F) \leq \begin{cases} 2^{n-1}-2^{(n+s-1)/2}, & \text{if } s \text{ is odd,} \\ 2^{n-1}-2^{(n+s-2)/2}, & \text{if } s \text{ is even.} \end{cases}$$

Moreover, for any n, *with* $n+s$ *even,* $NL(F) = 2^{n-1}-2^{(n+s-2)/2}$ *if and only if* $\ell(\lambda)$ *is constant for all* $\lambda \in \mathbb{F}_{2^n}^*$, *i.e.* F *is plateaued with single amplitude.*

For n *even and* s *odd, equality cannot occur when* F *is plateaued with single amplitude.*

Proof. First, assume that n is even. Thus $\ell(\lambda)$ should be even for any λ. According to (17) we deduce that

$$\max_{\lambda\in\mathbb{F}_{2^n}^*} \ell(\lambda) \geq \begin{cases} s+1, & \text{if } s \text{ is odd,} \\ s, & \text{if } s \text{ is even.} \end{cases}$$

Combining with (11) we get

$$\mathcal{L}(F) = \max_{\lambda\in\mathbb{F}_{2^n}^*} 2^{(n+\ell(\lambda))/2} \geq \begin{cases} 2^{(n+s+1)/2}, & \text{if } s \text{ is odd,} \\ 2^{(n+s)/2}, & \text{if } s \text{ is even,} \end{cases} \tag{19}$$

which gives the required upper bound for the nonlinearity.

Now we assume that $n+s$ is even for any n. From (19) and Theorem 4, we have $\mathcal{L}(F) \geq 2^{(n+s)/2}$ where equality holds if and only if $\ell(\lambda)$ takes the same value for all $\lambda \in \mathbb{F}_{2^n}^*$. It is because if $\max_{\lambda \in \mathbb{F}_{2^n}^*} 2^{\ell(\lambda)} = 2^s$ then

$$2^s(2^n-1) = \sum_{i \leq s} n_i 2^i \quad \Rightarrow \quad n_s = 2^n - 1,\ n_1 = \ldots = n_{s-1} = 0.$$

We know that for n odd and s even then F cannot be two-valued $\{0, 2^s\}$. Let n be even, s be odd and $\max_{\lambda \in \mathbb{F}_{2^n}^*} 2^{\ell(\lambda)} = 2^{s+1}$. Clearly, it is impossible to have $2^{\ell(\lambda)} = 2^{s+1}$ for all λ. $\diamond$

An application of Theorem 6 is given by Theorem 8 in Section 5. Now we treat differentially two-valued $\{0, 4\}$ functions.

Lemma 4 *Let F be a quadratic function over $\mathbb{F}_{2^n}$ which is differentially two-valued $\{0, 4\}$. Then n is even and $NL(F) = 2^{n-1} - 2^{n/2}$ if and only if F does not have bent components. Moreover, in this case $\ell(\lambda) = 2$ for any $\lambda \in \mathbb{F}_{2^n}^*$.*

Proof. For $\delta = 2^s$ with s even, we know that n must be even (see Corollary 1). If F does not have any bent components, say there is not any $\lambda \in \mathbb{F}_{2^n}^*$ such that $\ell(\lambda) = 0$, then $\ell(\lambda) \geq 2$ for all $\lambda \in \mathbb{F}_{2^n}^*$. But from Corollary 3, we have

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} 2^{\ell(\lambda)} = 2^2(2^n - 1).$$

which is possible if and only if $\ell(\lambda) = 2$ for all λ.

Now suppose that F has the best nonlinearity. Then F is plateaued with single amplitude, from Theorem 6. This amplitude is $2^{(n+2)/2}$ providing that F has no bent component[1]. $\diamond$

Assume that F is a quadratic permutation over $\mathbb{F}_{2^n}$, where n is even, such that $\delta = 4$. We know from Theorem 1 that F is two-valued $\{0, 4\}$. Moreover $\mathcal{L}(F) = 2^{(n+2)/2}$, from Lemma 4.

Theorem 7 *Let n be even. Then any quadratic differentially 4-uniform permutation is two-valued $\{0, 4\}$ and has the best nonlinearity, i.e., $NL(F) = 2^{n-1} - 2^{n/2}$, and such a function is with single amplitude.*

[1]The set of bent components cannot contain a subspace of dimension k such that $k > n/2$ [26].

When F is differentially 4-uniform, but not two-valued, there are surely a number of different Walsh spectrum. However specific properties appear.

Corollary 4 *Let F be quadratic over $\mathbb{F}_{2^n}$ such that $\delta = 4$, which is not two-valued. With notations as in Corollary 3. We have*

$$\sum_{j\in J} 2^j n_j = \sum_{\lambda\in\mathbb{F}_{2^n}^*} 2^{\ell(\lambda)} = 2N_1 + 4N_2.$$

In particular,

- *If n is odd and $\mathcal{L}(F) = 2^{(n+3)/2}$ then $n_1 \neq 0$. Moreover $N_2 = 3n_3$.*
- *If n is even and $\mathcal{L}(F) = 2^{(n+2)/2}$ then $n_0 \neq 0$. Moreover, the number n_0 of bent components satisfies $n_0 = 2(2^n - 1 - N_2)/3$.*

In both cases, N_2 is divisible by 3.

Proof. The first formula is derived from Corollary 3. Note that $N_1 \neq 0$ since F is not two-valued. We assume that F satisfies $\mathcal{L}(F) = 2^{(n+s)/2}$ with $s = 3$ for n odd and $s = 2$ for n even.

When n is odd, we get $2N_1 + 4N_2 = 2n_1 + 8n_3$. Note that

$$N_1 = 2^n - 1 - N_2 \text{ and } n_1 = 2^n - 1 - n_3,$$

so that $(2^n - 1) + N_2 = (2^n - 1) + 3n_3$ providing $N_2 = 3n_3$. It is impossible to have $n_1 = 0$, which would imply

$$8(2^n - 1) = 2(2^n - 1) + 2N_2 \text{ with } N_2 < (2^n - 1).$$

When n is even, we get $2N_1 + 4N_2 = n_0 + 4n_2$ where $n_0 \neq 0$ from Theorem 1. Since $n_2 = 2^n - 1 - n_0$, we obtain $3n_0 = 2(2^n - 1 - N_2)$. Note that this indicates that $2^n - 1 - N_2$ is not zero and is divisible by 3. ◇

When n is even F can be two-valued $\{0, 4\}$ with bent components (see Problem 5.1, Section 5). When n is odd there are permutations which are differentially 4-uniform but are not two-valued, as we show by the next example.

Example 3 *It was proved in [5] that the APN quadratic function* $G(x) = x^3 + Tr(x^9)$*, introduced in [13], has the best nonlinearity. Further, it was proved by [19, Proposition 8] that the function*

$$F(x)=x^3+Tr(x^9+x^3) \quad \textit{over } \mathbb{F}_{2^n}\textit{, where } n \textit{ is odd,}$$

is a permutation such that $\delta(F) = 4$*. Moreover* D_aF *is* 2*-to-*1 *if and only if* $Tr(a^{-3}) = 1$*, implying* $N_2 = 2^{n-1} - 1$*. We are going to prove that* F *has the best possible nonlinearity amongst quadratic differentially* 4*-uniform functions (for odd* n*), say* $\mathcal{L}(F) = 2^{(n+3)/2}$*. We have for any* λ *such that* $Tr(\lambda) = 1$*:*

$$\begin{aligned} Tr\left(\lambda(D_aF(x)+F(a))\right) &= Tr(\lambda(x^2a+a^2x)+(x^2a+a^2x+x^8a+a^8x)Tr(\lambda)) \\ &= Tr(\mu(x^2a+a^2x)+x^8a+a^8x),\ \mu=\lambda+1 \\ &= Tr\left(x^8(a+a^{2^6}+(\mu a)^{2^2}+\mu^{2^3}a^{2^4})\right) \\ &= Tr(x^8L(a)). \end{aligned}$$

The linear function L *is of the form* $L(x) = e_0x + e_1x^{2^2} + e_2x^{2^4} + e_3x^{2^6}$ *where* $\gcd(2, n) = 1$*. Then the kernel of* L *has dimension at most three, by applying Lemma 2. Clearly, if* $Tr(\lambda) = 0$ *then* $\ell(\lambda) = 1$*. Hence* $\ell(\lambda) \leq 3$ *for any* λ *and we conclude that* $\mathcal{L}(F) = 2^{(n+3)/2}$ *and, using Corollary 4,*

$$n_3=\frac{2^{n-1}-1}{3},\ n_1=\frac{5\times 2^{n-1}-2}{3} \quad \textit{and } N_1=2^{n-1}.$$

5 On some special quadratic functions

In this section we want to show that our results lead to interesting tools to study quadratic functions. Notation is fixed in all this section. Throughout this section any quadratic function F over $\mathbb{F}_{2^n}$ is defined as follows

$$F(x)=\sum_{r\in R}\nu_r x^r,\ \text{where}\ \ R\subseteq Q=\{2^i+2^j \mid 0\leq i<j\leq n-1\}, \tag{20}$$

where the ν_r are nonzero elements of $\mathbb{F}_{2^n}$. Hence, for any $a \in \mathbb{F}_{2^n}^*$, the derivative in point a is expressed as follows:

$$D_aF(x)=\sum_{r\in R, r=2^i+2^j}\nu_r(a^{2^i}x^{2^j}+a^{2^j}x^{2^i})+F(a). \tag{21}$$

By using Theorem 6, we can prove the following property.

Theorem 8 *Let F be any function given by (20). Assume that F has no bent component (when n is even). Let t be a nonzero integer which divides n and the nonzeros i and j, for all $r \in R$, $r = 2^i + 2^j$.*

Then F is differentially two-valued $\{0, 2^t\}$ if and only if the component functions of F have all the same amplitude which is $2^{(n+t)/2}$ with $n+t$ even, i.e., the set of Walsh coefficients of F is $\{0, \pm 2^{(n+t)/2}\}$.

Proof. We have to be more precise about the case where $t = 1$. When n is odd, we know that F is APN, and then AB, if and only if $\ell(\lambda) = 1$ for all λ. Moreover n cannot be even when $t = 1$, since in this case F has bent components.

Now, we assume that $t \geq 2$. We compute the linear space of any component function f_λ, $\lambda \in \mathbb{F}_{2^n}^*$:

$$\begin{aligned} D_a f_\lambda(x) &= Tr\left(\lambda D_a F(x)\right) \\ &= Tr\left(\lambda\left(\sum_{r\in R, r=2^i+2^j} \nu_r(a^{2^i}x^{2^j} + a^{2^j}x^{2^i}) + F(a)\right)\right) \\ &= Tr\left(x\left(\sum_{r=2^i+2^j} (a^{2^{n-j+i}}(\nu_r\lambda)^{2^{n-j}} + a^{2^{n-i+j}}(\nu_r\lambda)^{2^{n-i}})\right) + \lambda F(a)\right) \\ &= Tr\left(xL(a) + \lambda F(a)\right). \end{aligned}$$

Since F has no bent component, the kernel of the linear application L has dimension at last 2 for even n and at least 1 for odd n.

First, we fix λ. If $L(a) = 0$ then $L(\xi a) = 0$ too, for all $\xi \in \mathbb{F}_{2^t}$. Indeed, for any $r \in R$, $r = 2^i + 2^j$, t divides n and the nonzeros i and j so that $(\xi a)^{2^{n-j+i}} = \xi a^{2^{n-j+i}}$, for instance. Therefore, $\ell(\lambda) \geq t$. Assuming that F is two-valued $\{0, 2^t\}$, we apply Corollary 3:

$$\sum_{\lambda\in\mathbb{F}_{2^n}^*} 2^{\ell(\lambda)} = 2^t(2^n - 1), \quad \text{where } \max_\lambda \ell(\lambda) \geq t,$$

implying that $\ell(\lambda) = t$ for all λ, which is possible for even $n + t$ only. Conversely, if the Walsh spectrum of F is $\{0, \pm 2^{(n+t)/2}\}$, we have

$$\sum_{a\in\mathbb{F}_{2^n}^*} 2^{d(a)} = 2^t(2^n - 1), \quad \text{where } \max_a d(a) \geq t.$$

Fixing a in the expression of $D_a f_\lambda(x)$ above, we see that if there is λ such that $D_a f_\lambda(x)$ is constant, it holds also for $\xi\lambda$ with $\xi \in \mathbb{F}_{2^t}$. $\diamond$

The following theorem is actually [9, Theorem 1.2] that we are able to complete, as we explain in the proof below.

Theorem 9 *Let $n = 3k$ with $\gcd(3, k) = 1$. Let t be a divisor of k such that k/t is odd. Let s be an integer such that $\gcd(n, s) = t$ and 3 divides $k + s$. Define the function*

$$F:\ \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ F(x) = \alpha x^{2^s+1} + \alpha^{2^k} x^{2^{n-k}+2^{k+s}}.$$

where α is a primitive element of $\mathbb{F}_{2^n}$. Then

(i) *F is a permutation;*

(ii) *F is differentially two-valued with spectrum $\{0, 2^t\}$.*

(iii) *Moreover $NL(F) = 2^{n-1} - 2^{(n+t)/2-1}$ and all components of F have the same amplitude; the Walsh coefficients of F are $\{0, \pm 2^{(n+t)/2}\}$.*

Proof. The properties (i) and (ii) are proved in [9]. The authors later proved that $NL(F) = 2^{n-1} - 2^{n/2}$, for $t = 2$ and n even, and that $NL(F) \geq 2^{n-1} - 2^{(n+t-e)/2-1}$, for any $t > 1$ where t, e are such that $e \equiv n + t \pmod 2$. The proof is specific and technical.

We are able to prove (iii) by using directly our previous results. First, if $t = 2$ we apply Theorem 7. More generally, we can apply Proposition 8. Indeed, F is a permutation and then cannot have a bent component. Further, t divides n, s, k and then it divides $n - k$ and $k + s$ too. $\diamond$

The binomials which are treated in the previous theorem were obtained in [9], by changing certain conditions, from the APN binomials constructed in [14]. Looking at the list of known APN quadratic functions in [6], it appears that those F which depend on a positive integer s share same properties. The field $\mathbb{F}_{2^n}$ has always subfields in these examples and almost all such F may be modified to satisfy the hypothesis of Theorem 8. Another quadratic function is discussed in several papers, which could be studied by using our tools. The problem of determining its properties is as follows.

Problem 5.1 [9] Let $n = 3k$, s, k be positive integers with $k + s$ divisible by 3 and

$$\gcd(s,k)=t \text{ with } t>1,\ \ \gcd(s,3)=\gcd(3,k)=1,\ \ \frac{k}{t} \text{ is odd.}$$

Let α be a primitive element of $\mathbb{F}_{2^n}$ and $v, w \in \mathbb{F}_{2^k}$ with $vw \neq 1$. Define the function F on $\mathbb{F}_{2^{3k}}$ as

$$F(x)=\alpha x^{2^s+1}+\alpha^{2^k} x^{2^{2k}+2^{k+s}}+vx^{2^{2k}+1}+w\alpha^{2^k+1}x^{2^s+2^{k+s}}. \tag{22}$$

The authors propose to prove that F is bijective, two-valued $\{0, 2^t\}$ and highly nonlinear.

It was proved later in [33] that for $t = 2$, the function F is not always bijective and at the same time that $\delta = 4$. Moreover the authors suggest that the proofs given in [6, 11], for the APN case ($t = 1$), can be slightly modified to solve Problem 5.1. Reading in this proofs the expressions of the functions D_aF and D_af_λ, it appears that for $t > 1$:

- The derivatives D_aF are 2^i-to-1 with $i \geq t$ so that $d(a) \geq t$ for all $a \in \mathbb{F}_{2^n}^*$. From [33, Claim 2], we then deduce that for $t = 2$ the function F is two-valued $\{0, 4\}$ for any even k.

- Whenever the component f_λ is not bent, its linear space has dimension at last t so that $\ell(\lambda) \geq t$ for all such $\lambda \in \mathbb{F}_{2^n}^*$.

We now indicate our contribution to solve Problem 5.1:
– If F has no bent component then Theorem 8 applies. It is especially the case for odd n. In this case, one has to prove either that $\delta = 2^t$ or (equivalently) that $\mathcal{L}(F) = 2^{(n+t)/2}$.
– When n is even, we know that F is not always bijective and then can have some bent components. In this case, comparing to the the odd case, it is necessary to know the number of bent components and then disprove the bijectivity.

Problem 1 *Study the possible bent components of the function F, given by (22), i.e., does it exist such component and in this case what is the cardinality of the set of such bent functions?*

6 Conclusion

In this paper, our aim is to establish some relations beetween the differential uniformity and the nonlinearity of vectorial functions over $\mathbb{F}_{2^n}$. We propose a lower bound for the nonlinearity of monomial permutations depending on their differential uniformity. More generally, we show that the functions which are differentially two-valued are somehow optimal objects and then we pay a special attention to the quadratic case. Our relation (Theorem 5) fully applies to particular classes of functions, such as permutation whose differential uniformity is 4 when n is even. It reveals also the complexity of this corpus, in general.

Thus, we have adressed a number of problems which remain open although they are widely studied, especially for quadratic functions. We emphasize that the number of bent components is a key parameter to study these functions when n is even. We point out that almost all known quadratic APN functions have similar properties which allows to construct functions which are differentially two-valued $\{0, 2^s\}$, $s > 1$. These classes of functions correspond to specific polynomials and in this case $\mathbb{F}_{2^n}$ has special proper subfields.

References

[1] 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.

[2] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptol.*, vol. 4 number 1, pp. 3-72, 1991.

[3] C. Blondeau, A. Canteaut and P. Charpin. Differential properties of power functions, In Proceedings of the *2010 IEEE International Symposium on Information Theory*, ISIT 10, PP. 2478–2482, Austin, USA, June 2010.

[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] C. Bracken, E. Byrne, N. Markin and G. Mcguire, On the Walsh spectrum of a new APN function, *Cryptography and Coding*, LNCS 4887, pp. 92-98, Springer-Verlag.

[6] C. Bracken, E. Byrne, N. Markin and G. Mcguire, A few more quadratic APN functions, *Cryptogr. Commun. (2011)* 3:43–53.

[7] C. Bracken, E. Byrne, N. Markin and G. Mcguire, Fourier spectra of binomial APN functions, *SIAM J. Discrete Math.*, 23(2), 596-608, 2009.

[8] C. Bracken and G. Leander, A highly nonlinearity differentially 4-uniform power mapping that permutes fields of even degree, *Finite Fields and Their Applications*, 16(4), 231-242, 2010.

[9] C. Bracken, C.H. Tan and Y. Tan, Binomial differentially 4-uniform permutations with high nonlinearity, *Finite Fields and Their Applications*, 18(3), 537-546, 2012.

[10] C. Bracken, C.H. Tan and Y. Tan, On a class of quadratic polynomials with no zeros and its application to APN functons, *Finite Fields and Their Applications*, 25 (2014) 26-36.

[11] C. Bracken and Z. Zha, On the fourier spectra of the infinite families of quadratic APN Functions, *Advances in Mathematics of Communications*, Vol. 3, No3, 2009,219–226.

[12] K. Browning, J. Dillon, M. Mcquistan and A. Wolfe, An APN permutation in dimension six, *Finite Fields: Theory and Applications-FQ9,* Ser. Contemporary Mathematics, 518, 33-42, 2010.

[13] L. Budaghyan, C. Carlet and G. Leander, Constructing new APN functions from known ones, *Finite Fields and Their Applications*, 15(2009) 150-159.

[14] L. Budaghyan, C. Carlet and G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, *IEEE Trans. on Information Theory*, 54 (9) 2008 4218–4229.

[15] A. Canteaut, Analyse et conception de chiffrements clef secrte. Habilitation diriger les recherches (HDR), Université Pierre et Marie Curie, Septembre 2006.

[16] C. Carlet, Boolean and vectorial plateaued function, and APN functions, *IEEE Transaction on Information Theory*, Vol. 61, N. 11, November 2015.

[17] C. Carlet, Characterizations of the differential uniformity of vectorial functions by the Walsh transform, *IEEE Transaction on Information Theory*, to appear.

[18] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, In: *Advances in Cryptology,* EUROCRYPT'94. LNCS, 950, 356-365. Springer-Verlag Berlin Heidelberg, 1995.

[19] P. Charpin, G. Kyureghyan and V. Suder, Sparse Permutations with Low Differential Uniformity, *Finite Fields and Their Applications*, Vol. 28 (214-243), July 2014.IACR Cryptology ePrint Archive, 2017:516, 2017.

[20] P. Charpin and J. Peng, Differential uniformity and the associated codes of cryptographic functions, In preparation.

[21] H. Dobbertin, One-to-one highly nonlinear power functions on $GF(2^n)$, *Applicable Algebra in Engineering, Communication and Computing*, 9(2), 139-152, 1998.

[22] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.), *IEEE Trans. on Information Theory*, 14(1), 154-156, 1968.

[23] T. Kasami, The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes, *Information and Control*, 18(4), 369-394, 1971.

[24] P. Langevin and P. Véron, On the non-linearity of power Functions, *Designs, Codes and Cryptography,* 37, 31-43, 2005.

[25] M. Matsui, Linear cryptanalysis method for DES cipher, In *Advances in Cryptology–EUROCRYPT'93*, LNCS 765, pp. 386-97, Springer-Verlag, 1993.

[26] K. Nyberg, Perfect nonlinear S-boxes, In *Advances in Cryptology–EUROCRYPT'91*, LNCS 547, pp. 378–385, Springer-Verlag, 1991.

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

[28] K. Nyberg. S-Boxes and Round Functions with Controllable Linearity and Differential Uniformity. *In Fast Software Encryption-FSE'94 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1008, 111-130, 1995.

[29] A. Pott, E. Pasalic, A. Muratovic-Ribic and S. Bajric, On the maximum number of bent component of vectorial functions, To appear in *IEEE Transactions on Information Theory*.

[30] J. Peng, C. Tan and Q. Wang, New secondary constructions of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$, *International Journal of Computer Mathematics*, 94, 1670-1693, 2017.

[31] L.J. Qu, Y. Tan, C.H. Tan and C. Li, Constructing differentially 4-uniform permutations over $F_{2^{2k}}$ via the switching method, *IEEE Trans. on Information Theory*, 59(7), 4675-4686, 2013.

[32] L. Qu, Y. Tan and C. Li, On the Walsh spectrum of a family of quadratic APN functions with five terms, *SCIENCE CHINA Information sciences*, 57, issue 2, pp. 1–7 , 2014.

[33] L. Qu, Y. Tan and C. Li, A negative answer to Bracken-Tan-Tan's problem on differentially 4-uniform permutations over $\mathbb{F}_{2^n}$, *Finite Fields and Their Applications*, 24(2013) 55-65.

[34] Y. Yu, M. Wang and Y. Li. A Matrix Approach for Constructing Quadratic APN Functions. *Cryptology ePrint Archive. Report* (2013/007).