New links between nonlinearity and differential uniformity

Pascale Charpin, Jie Peng

New links between nonlinearity and differential uniformity

Pascale Charpin* Jie Peng†

July 12, 2018

Abstract

This paper establishes some new links between the nonlinearity and differential uniformity of some large classes of functions, such as power functions, differentially two-valued functions and quadratic functions. We obtain a lower bound for the nonlinearity of general differential uniform power permutations, an upper bound for general differentially two-valued functions, together with some important results for quadratic functions. In particular, we show that the quadratic differentially 4-uniform permutations should be two-valued and possess the best known nonlinearity.

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, 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* [10]. This criteria is called the *nonlinearity*. In this context, the knowledge of nonlinearity and differential uniformity of

*INRIA Paris, 2 rue Simone Iff, 75012, FRANCE

†Mathematics and Science College of Shanghai Normal University, Shanghai, CHINA

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. We mainly focus on power functions, differentially two-valued functions and quadratic functions, which were widely studied but are not yet classified. Many problems on these functions remain open.

For any APN function, a lower bound for the sum of all the sum-of-square indicators of its components has been obtained, and the number of its bent components has been characterized in [1]. Besides, a lower bound for the nonlinearity of APN power functions has been derived in [7]. In this paper, we derive similar results for such functions with general differential uniformity. For any function we obtain an upper bound for the sum of all the sum-of-square indicators of its components, which are achieved by differentially two-valued ones. Based on that, we show that any differentially 4-uniform plateaued function must have bent components, unless it is differentially two-valued. Moreover, we derive a lower bound for the nonlinearity of power permutations, and an upper bound for the nonlinearity of general differentially two-valued functions. We later focus on 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. Some important results are then deduced. In particular, we show that the quadratic differentially 4-uniform permutations should be differentially two-valued and possess the best known nonlinearity.

The rest of the paper is organized as follows. The next section gives some necessary definitions on the cryptographic properties of functions over $\mathbb{F}_{2^n}$ and their components. 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. Finally an interesting application of the results for quadratic functions is given in Section 5. This paper is an extended abstract and some proofs are omitted.

2 Preliminaries

A mapping $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m}$ is usually called an (n, m)-function or a *vectorial Boolean function*. When $m = 1$, we say that F is an n-variable Boolean function and usually use small letter f instead; we denote by B_n the set of all n-variable Boolean functions. When $m = n$, 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 its *components functions*.

For any function F over $\mathbb{F}_{2^n}$, the components of F are those n-variable Boolean functions represented as

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

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

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

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 $(D_a F)^{-1}(b)$: set

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

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). The function F 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 can be found in [3]. 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 $\{0, \pm 2^{s/2}\}$ for some even integer s. The value $2^{s/2}$ is 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 components have the same amplitude.

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

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

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

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

$$W_F(\lambda, a) = W_{f_\lambda}(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda F(x) + ax)}, \ (\lambda, a) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}. \tag{4}$$

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 $NL(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$ [8], where the upper bound is achieved by the AB functions. But for even n, the known maximum nonlinearity is $2^{n-1} - 2^{\frac{n}{2}}$, which is conjectured to be an upper bound [9].

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 $f_\lambda, \lambda \in \mathbb{F}_{2^n}^*$. 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 result on the lower bound is obtained by [1, Corollary 1]. For the upper bound, one has

$$\begin{aligned}
\sum_{\mu\in\mathbb{F}_{2^n}^*}\nu(f_\mu) &= \sum_{\mu\in\mathbb{F}_{2^n}^*}\sum_{a\in\mathbb{F}_{2^n}} W_{D_af_\mu}^2(0)\\
&= \sum_{a\in\mathbb{F}_{2^n}^*}\sum_{\mu\in\mathbb{F}_{2^n}} W_{D_af_\mu}^2(0)\\
&= (2^n-1)2^{2n+1}+2^n\sum_{a\in\mathbb{F}_{2^n}^*}\sum_{b\in\mathbb{F}_{2^n}}\delta(a,b)(\delta(a,b)-2)\\
&\le (2^n-1)2^{2n+1}+(\delta-2)(2^n-1)2^{2n}\\
&= (2^n-1)2^{2n}\delta,
\end{aligned}$$

with equality if and only if F is differentially two-valued. ◇

Thus we have, since δ is even,

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

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

In this paper we are interested by this problem: the number of bent components of vectorial functions over $\mathbb{F}_{2^n}$, n even. A general approach is proposed by [11, Theorem 3]. For APN functions, this number has been characterized for plateaued such functions [1, Corollary 3]. For differentially 4-uniform functions, we give part of the answer in the following result.

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 (the one in (5)) $1<\gamma\le 2$ depending on F, such that*

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

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 differentially two-valued.

In the following, we present some results which are derived from Lemma 1, concerning respectively the power functions and the two-valued functions.

First 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.

Theorem 2 *[6, Theorem 8.14] Let $n = 2m$ and let the power function $F(x) = x^d$ over $\mathbb{F}_{2^n}$. Assume that $\gcd(d, 2^n-1) > 1$. Then $NL(F) \leq 2^{n-1} - 2^{m+1}$. If $NL(F) = 2^{n-1} - 2^{m+1}$ then $\gcd(d, 2^n-1) = 3$ and*

$$W_F(\lambda, 0) = \begin{cases} (-1)^{m+1} 2^{m+1}, & \text{if } \lambda \in \{x^3,\ x \in \mathbb{F}_{2^n}^*\} \\ (-1)^m 2^m, & \text{if } \lambda \notin \{x^3,\ x \in \mathbb{F}_{2^n}^*\}\ , \end{cases}$$

Applying Lemma 1 to power permutations, we obtain a precise result.

Proposition 1 *Let $F(x) = x^d$ be differentially δ-uniform with $\gcd(d, 2^n - 1) = 1$. Then $\nu(f_\lambda) \leq 2^{2n}\delta$ for any $\lambda \in \mathbb{F}_{2^n}^*$, 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 plateaued.*

Little is known on the lower bound of the nonlinearity of differential uniform functions, even for APN functions. It seems that the nonlinearity of all known APN functions is rather good. It is of interest and importance to find the reason. Recently, Carlet proposed a nonzero lower bound for the nonlinearity of APN power functions F in [7, Theorem 5.6], 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. Using Lemma 1, we are able to generalize this result for bijective power functions of any differential uniformity with a simple proof.

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 1 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,

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

◇

Moreover, by applying Lemma 1 to differentially two-valued functions, we can obtain an upper bound for their nonlinearity.

Theorem 4 *Let F be differentially two-valued $\{0, 2^s\}$. Then it holds*

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

where s should be odd when n is odd.

4 Quadratic functions

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

$$F(x) = \sum_{i,j} a_{i,j} x^{2^i + 2^j}, \ 0 \leq i < j \leq n-1, \tag{6}$$

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

$$(x, a) \mapsto Tr(\lambda Q(x, a)), \text{ where } Q(x, a) = F(x+a) + F(x) + F(a). \tag{7}$$

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

$$rad_\lambda(F) := \{a \in \mathbb{F}_{2^n} \mid Tr(\lambda Q(x, a)) = 0, \ \forall \ x \in \mathbb{F}_{2^n}\}. \tag{8}$$

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 direction a is constant. Such a point 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 $b \in \mathbb{F}_{2^n}$

$$W_F^2(\lambda, b) = \sum_{a \in \mathbb{F}_{2^n}} (-1)^{Tr(ba+\lambda F(a))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda Q(x,a))}, \tag{9}$$

which leads easily to

$$\begin{aligned} W_F^2(\lambda, b) &= 2^n \sum_{a \in rad_\lambda(F)} (-1)^{Tr(ba+\lambda F(a))} \\ &= \begin{cases} 2^{n+\ell(\lambda)}, & \text{if } Tr(ba+\lambda F(a)) \text{ vanishes on } rad_\lambda(F) \\ 0, & \text{otherwise,} \end{cases} \end{aligned} \tag{10}$$

since by definition $a \mapsto Tr(ba + \lambda F(a))$ 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 (10) that

$$n \equiv \ell(\lambda) \pmod 2. \tag{11}$$

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

$$ker_a(F) := \{\lambda \in \mathbb{F}_{2^n} \mid Tr(\lambda Q(x, a)) = 0, \ \forall\ x \in \mathbb{F}_{2^n}\}. \tag{12}$$

and denote by $d(a)$ the dimension of the vector space $ker_a(F)$ for convenience. Our main results are based on the following observation.

Lemma 2 *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 (12). Hence $\delta = \max_{a \in \mathbb{F}_{2^n}^*} 2^{d(a)}$.*

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 also applies to quadratic functions with higher 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 [4]. 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 [12].

Example 1 *Let $n = 6$ and let α be a primitive element of $\mathbb{F}_6$. The function*

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

is APN with a five-valued Walsh spectrum. By 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, $NL(F) = 2^{n-1} - 2^{\frac{n+4}{2}-1} = 16$. Note that the number of bent components is greater than the lower bound which is 42 as we recall later in Remark 1.

Theorem 5 *Let F be a quadratic function over $\mathbb{F}_{2^n}$. Notation is as above, defined by (8) to (12). Then we have*

$$\sum_{\lambda\in\mathbb{F}_{2^n}^*} 2^{\ell(\lambda)}=\sum_{a\in\mathbb{F}_{2^n}^*} 2^{d(a)}. \tag{13}$$

Proof. It is simply obtained by computing:

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

◇

Corollary 1 *Let F be quadratic 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 $1 \le i \le s$ and $j \in J := \{\ j \mid 0 \le j \le t,\ n+j \text{ even}\ \}$, 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

$$\sum_{j \in J} 2^j n_j = \sum_{i=1}^{s} 2^i N_i, \tag{14}$$

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

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} 2^{\ell(\lambda)} = 2^s(2^n - 1) \quad \text{where } t \ge s,\ t = \max_{\lambda}\{\ell(\lambda)\}. \tag{15}$$

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

$$\sum_{a \in \mathbb{F}_{2^n}^*} 2^{d(a)} = 2^t(2^n - 1) \quad \text{where } 1 \le d(a),\ s \ge t,\ s = \max_{a}\{d(a)\}. \tag{16}$$

Remark 1 *Well-known properties of any APN quadratic function F are directly derived from the previous results:*
– If n is odd, then $2(n_1 + 2^2 A) = 2(2^n - 1)$ from (15), where $A = n_3 + 2^3 n_5 + \cdots$ and $n_i = 0$ for i even. But we must have $n_1 + 2^2 A = (2^n - 1)$ 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 $n_0 + 2^2 A = 2(2^n - 1)$, where $A = n_2 + 2^2 n_4 + \cdots$ and $n_i = 0$ for i odd. Thus $n_0 > 0$, which means that F has an even number of bent components. Now, since $(2^n - 1) - \sum_{i \ne 0} n_i = n_0$ we get

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

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 Quadratic differentially two-valued functions

In this section we explore in some detail the link between the nonlinearity and the two-valued property. We will also focus on quadratic differentially 4-uniform functions. First, we give a useful result for differentially two-valued functions.

Lemma 3 *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.*

Then 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.

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, then n must be even by Lemma 3. 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 1, 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. $\diamond$

Assume that F is a quadratic permutation over $\mathbb{F}_{2^n}$ with $\delta = 4$, where n is even. We know from Theorem 1 that F is two-valued. 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., $NL(F) = 2^{n-1} - 2^{n/2}$.*

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

Corollary 2 *Let F be quadratic over $\mathbb{F}_{2^n}$ such that $\delta = 4$, which is not two-valued. With notations as in Corollary 1. 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 particular, N_2 is divisible by 3.*

5 An application

In this section we want to give an interesting application of our results. Notation is fixed in all this section. Throughout this section the quadratic function F is as follows defined.

$$F(x) = \sum_{r\in Q} \nu_r x^r, \text{ where } Q = \{2^i + 2^j \mid 0 \leq i < j \leq n-1\}. \tag{17}$$

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

Theorem 8 *Let F, given by (17), be any quadratic function over $\mathbb{F}_{2^n}$ which 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 $r \in Q$, $r = 2^i + 2^j$, such that $\nu_r \neq 0$.*

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 $\pm 2^{(n+t)/2}$ with $n+t$ even. The Walsh spectrum of F has values $\{0, \pm 2^{(n+t)/2}\}$.

The following theorem is actually [5, Theorem 1.2] that we are able to complete. The properties (i) and (ii) are proved in [5]. The authors later proved that $NL(F) = 2^{n-1} - 2^{(n+2)/2-1}$, for $t = 2$ and n even, and that $NL(F) \geq 2^{n-1} - 2^{(n+t-e)/2-1}$, $e \equiv n + t \pmod 2$. The proof is specific and technical. In fact, we can directly prove (iii) by applying Theorem 8.

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 over $\mathbb{F}_{2^n}$*

$$F(x) = \alpha x^{2^s+1} + \alpha^{2^k} x^{2^{n-k}+2^{k+s}},$$

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

(i) *F is a permutation;*

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

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

Proof. We are going to prove (iii) by using our previous results. First, if $t = 2$ we apply Theorem 7. More generally, we can apply Theorem 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. ◇

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, 2006.

[2] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems, *J. Cryptol.*, 4(1):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 10:2478–2482, Austin, USA, June 2010.

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

[5] 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.

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

[7] C. Carlet. Characterizations of the differential uniformity of vectorial functions by the walsh transform, to appear.

[8] 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.

[9] 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.

[10] M. Matsui. Linear cryptanalysis method for DES cipher, In *Advances in Cryptology–EUROCRYPT'93*, LNCS, 765:386-397, Springer-Verlag, 1993.

[11] A. Pott, E. Pasalic, A. Muratović-Ribić and S. Bajrić. On the maximum number of bent component of vectorial functions, *IEEE Transactions on Information Theory*, 64(1):403-411, 2018.

[12] Y. Yu, M. Wang and Y. Li. A Matrix Approach for Constructing Quadratic APN Functions. *Cryptology ePrint Archive. Report* (2013/2007).