On the (non-)existence of APN (n, n)-functions of algebraic degree n

Lilya Budaghyan, Claude Carlet, Tor Helleseth, Nian Li

***Abstract*—In this paper, we study the problem of existence of almost perfect nonlinear (APN) functions of algebraic degree n over $\mathbb{F}_{2^n}$. We characterize such functions by means of derivatives and power moments of the Walsh transform. We deduce some non-existence results which imply, in particular, that for most of the known APN functions F over $\mathbb{F}_{2^n}$ the function $x^{2^n-1}+F(x)$ is not APN.**

***Index Terms*—almost perfect nonlinear, almost bent, Boolean function, differential uniformity, nonlinearity**

I. Introduction

A substitution box (S-box) in a block cipher is a mapping that takes n binary inputs and whose image is a binary m-tuple, for some positive integers n and m. The security of most modern block ciphers importantly relies on cryptographic properties of their S-boxes, since these are the only nonlinear elements of these cryptosystems. It is therefore significant to employ S-boxes with good cryptographic properties such as high nonlinearity, low differential uniformity and high algebraic degree, in order to resist linear, differential and higher order differential attacks.

Differential attacks introduced by Biham and Shamir in [1] are one of the most efficient cryptanalyst tools for block ciphers. The differential attack is based on the study of how differences in an input can affect the resulting difference at the output. Thus, in order to resist differential attacks, for each S-box in the cipher, the difference between two outputs corresponding to inputs whose nonzero difference is arbitrarily fixed should be as uniformly distributed as possible. Among S-boxes almost perfect nonlinear (APN) functions have the best resistance to differential attacks [25]. Due to this reason, much work has been dedicated to the notion of APN functions. Constructing APN functions is a difficult problem. Up to now, there are, up to CCZ-equivalence, only six known infinite classes of APN monomials and a few known infinite classes of quadratic APN multinomials (see [10]).

Another powerful attack on block ciphers is linear cryptanalysis by Matsui [23] which is based on finding affine approximations to the action of a cipher. Almost bent (AB) functions are S-boxes providing optimal resistance to this attack [13]. Moreover every AB function is APN and therefore is optimal against differential attacks as well. However, AB functions exist only over binary fields of odd dimensions while APN functions exist for even dimensions too.

When choosing S-boxes, functions with high algebraic degrees are preferable in order to resist higher order differential cryptanalysis [21]. In this sense finding upper bounds for algebraic degrees of APN and AB functions and constructing such functions reaching these upper bounds are of particular interest. On the other hand, finding restrictions on algebraic degrees naturally reduces the set of functions when searching for new APN or AB functions, and, therefore, facilitates the problem of constructing these functions. The problem of an upper bound for algebraic degree is completely settled for AB functions and wide open for APN functions. Algebraic degree of any AB function over the finite field of dimension n is upper bounded by $(n+1)/2$ and the inverses of Gold power AB functions have this algebraic degree [12], [25]. There is no known upper bounds for algebraic degrees of APN functions. For n odd, the known APN function over the finite field $\mathbb{F}_{2^n}$ with the highest algebraic degree is the inverse APN function [25] which has algebraic degree $n-1$. For n even the known APN functions with high algebraic degrees are Dobbertin function [16] with algebraic degree $n/5+3$ (n must be divisible by 5 then) and Kasami functions [20] with algebraic degree $i+1$ for $i \leq (n-1)/2$, $\gcd(n,i)=1$.

This paper is dedicated to the problem of existence of APN functions over $\mathbb{F}_{2^n}$ with maximal algebraic degree n. Solving this problem would provide complete answer to the upper bound problem for n odd case. Besides, this would indicate whether it is possible to preserve APN property by changing one point in a given APN function. This natural question has not been addressed in publications, even if it has been present in the minds of many researchers on APN functions. For this goal, throughout this paper, let F be any function from $\mathbb{F}_{2^n}$ to itself of algebraic degree strictly less than n, and define a function G over $\mathbb{F}_{2^n}$ as follows:

$$G(x) = x^{2^n-1} + F(x). \tag{1}$$

Then, the objective of this paper is to characterize the APNness of the function G in order to find new APN functions with the maximal degree or to prove the non-existence of such functions. We provide such characterizations using derivatives and Walsh transform values of the function F. As a consequence, non-existence results for APN functions with maximal degree are obtained for some special cases of F which include all power functions, almost bent functions, quadratic functions and plateaued functions in general. This covers almost all

L. Budaghyan, T. Helleseth and N. Li are with the Department of Informatics, University of Bergen, PB 7803, 5020 Bergen, NORWAY; e-mail: {Lilya.Budaghyan, Tor.Helleseth, Nian.Li}@uib.no

C. Carlet is with LAGA, Department of Mathematics, University of Paris 8 (and Paris 13 and CNRS), Saint–Denis cedex 02, France; e-mail: claude.carlet@univ-paris8.fr

This research was co-funded by the Norwegian Research Council, the EEA Grant SK06-IV-01-001, and the state budget of the Slovak Republic from the EEA Scholarship Programme Slovakia.

known cases of APN functions F and supports the following conjectures.

Conjecture 1. There exists no APN function over $\mathbb{F}_{2^n}$ of algebraic degree n for $n \geq 3$.

This conjecture is true for $n \in \{3, 4, 5\}$ (see [4]). If Conjecture 1 is proven to be true then the following conjecture would be true too.

Conjecture 2. Let F be an APN function over $\mathbb{F}_{2^n}$ with $n \geq 3$ and F' a function obtained from F by changing the values of F in one point. Then F' is not APN.

Note that, similar to Conjecture 1, Conjecture 2 is obvious when reformulated for AB functions. That is, if F is AB and F' is obtained from F by changing a single point then F' is not AB.

The remainder of this paper is organized as follows. Section II introduces the preliminaries. Section III characterizes the APN functions of the form (1) by means of the derivatives and of the power moments of the Walsh transform, and then some non-existence results on APN functions of the form (1) are obtained in Section IV. In Section V we study equivalence classes of maximum degree functions. Section VI concludes the paper.

II. Preliminaries

For positive integers n and m, an S-box is a vectorial function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$, also called an (n, m)-function. When $n = m$ it has a unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$ of the form

$$F(x) \quad = \quad \sum_{i=0}^{2^n-1} a_i x^i, a_i \in \mathbb{F}_{2^n}.$$

Let $w_2(i) = \sum_{s=0}^{n-1} i_s$ denote the 2-weight of i, where $0 \leq i \leq 2^n - 1$ has binary expansion $i = \sum_{s=0}^{n-1} 2^s i_s$. Then, the *algebraic degree* of F is equal to

$$\deg(F) \quad = \quad \max\{w_2(i) : a_i \neq 0, 0 \leq i \leq 2^n - 1\}.$$

Clearly $\deg(F) \leq n$.

For an (n, n)-function F and any $a, b \in \mathbb{F}_{2^n}$, define $\Delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} : F(x + a) + F(x) = b\}|$. Then, the differential uniformity of F is defined as

$$\Delta_F \quad = \quad \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}.$$

F is called *differentially δ-uniform* if $\Delta_F = \delta$. If $\delta = 2$, then F is called *almost perfect nonlinear* (APN).

APN functions over $\mathbb{F}_{2^n}$ can be characterized in several different ways. In this paper, we focus, in particular, on the characterization by means of power moments of the Walsh transform. For a Boolean function f in n variables (that is, an $(n, 1)$-function) the Walsh transform is defined by

$$W_f(a) \quad = \quad \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ax)}, \qquad a \in \mathbb{F}_{2^n},$$

where $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the absolute trace function of $\mathbb{F}_{2^n}$. For an (n, m)-function F its Walsh transform $W_F(a, b)$ at the point $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}^*$ is the Walsh transform of its *component function* $\mathrm{Tr}_1^m(bF(x))$ at the point a. That is,

$$W_F(a, b) \quad = \quad \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^m(bF(x))+\mathrm{Tr}_1^n(ax)}.$$

Lemma 1 (see e.g. [10])**.** Let F be an (n, n)-function. Then F is APN if and only if

$$\sum_{a \in \mathbb{F}_{2^n}} \sum_{b \in \mathbb{F}_{2^n}^*} W_F^4(a, b) = 2^{3n+1}(2^n - 1).$$

APN functions have also a natural characterization by means of its derivatives. The *derivatives* of a given (n, n)-function F are functions

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

A Boolean function f in n variables is called *bent* if $W_f(a) \in \{\pm 2^{n/2}\}$ for all $a \in \mathbb{F}_{2^n}$. An (n, m)-function F is called bent if all its component functions are bent, that is, $W_F(a, b) \in \{\pm 2^{n/2}\}$ for all $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}^*$. Bent functions have optimum resistance against linear attacks because their *nonlinearity* has optimal value $2^{n-1} - 2^{n/2-1}$. The nonlinearity N_F of an (n, n)-function F is the minimum Hamming distance between its component functions and affine functions. It equals $N_F = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*} |W_F(a, b)|$. Nyberg in [24] proved that (n, m)-bent functions exist if and only if n is even and $m \leq n/2$. When n is odd, there exists no (n, m)-bent function. When n is odd and $n = m$, the optimal functions from the viewpoint of nonlinearity are almost bent functions. An (n, n)-function F is called *almost bent* (AB) if $W_F(a, b) \in \{0, \pm 2^{(n+1)/2}\}$ for all $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}^*$. Any AB function is APN, but not vice versa. However, for n odd, every quadratic APN function is also AB, and, more generally, every plateaued APN function is also AB.

A *plateaued* Boolean function is a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ whose Walsh transform takes values from $\{0, \pm\mu\}$ for some positive integer μ (μ is called the *amplitude* of the plateaued Boolean function). Plateaued Boolean functions were introduced by Zheng and Zhang and were shown to possess various desirable cryptographic characteristics [26]. More generally, for an (n, m)-function, Carlet introduced the following two notions in [10], [11].

Definition 1. An (n, m)-function F is called *plateaued* if all its component functions $\mathrm{Tr}_1^m(uF(x))$, $u \neq 0$, are plateaued, with possibly different amplitudes.

Definition 2. An (n, m)-function F is called *plateaued with single amplitude* if all its component functions are plateaued with the same amplitude.

Notice that the amplitude for a plateaued Boolean function f should be a power of two whose exponent is at least $\frac{n}{2}$, due to the well-known *Parseval's identity* $\sum_{a \in \mathbb{F}_{2^n}} W_f^2(a) = 2^{2n}$. Moreover, the distribution of its Walsh transform can be determined as follows.

Lemma 2. Let f be a plateaued Boolean function over $\mathbb{F}_{2^n}$ with amplitude 2^λ. Then the distribution of its Walsh transform

values is given by

Walsh Transform Value	Frequency
0	$2^n - 2^{2n-2\lambda}$
2^λ	$2^{2n-2\lambda-1} + (-1)^{f(0)}\, 2^{n-\lambda-1}$
-2^λ	$2^{2n-2\lambda-1} - (-1)^{f(0)}\, 2^{n-\lambda-1}$

and we have $\sum_{a\in\mathbb{F}_{2^n}} W_f^3(a) = (-1)^{f(0)}\, 2^{n+2\lambda}$ and $\sum_{a\in\mathbb{F}_{2^n}} W_f^4(a) = 2^{2n+2\lambda}$.

Proof. Let us denote by N_+ (resp. N_-) the number of occurences of 2^λ (resp. -2^λ), we have according to the Parseval identity that $2^{2\lambda}(N_+ + N_-) = 2^{2n}$, and according to the inverse Walsh transform formula $\sum_{a\in\mathbb{F}_{2^n}} W_f(a) = 2^n(-1)^{f(0)}$, that $2^\lambda(N_+ - N_-) = 2^n(-1)^{f(0)}$. This directly gives the table above. The two other relations can be deduced either from this table, or from (again) the inverse Walsh transform formula and the Parseval identity, since we have $\sum_{a\in\mathbb{F}_{2^n}} W_f^3(a) = 2^{2\lambda}\sum_{a\in\mathbb{F}_{2^n}} W_f(a)$ and $\sum_{a\in\mathbb{F}_{2^n}} W_f^4(a) = 2^{2\lambda}\sum_{a\in\mathbb{F}_{2^n}} W_f^2(a)$. □

Since the algebraic degree of a Boolean plateaued function in n variables with amplitude 2^λ is upper bounded by $n-\lambda+1$ [22] then algebraic degree of a plateaued (n,n)-function F is upper bounded by $\max_{b\in\mathbb{F}_{2^n}^*}(n-\lambda_b+1)$ where 2^{λ_b} is the amplitude of $\mathrm{Tr}_1^n(bF(x))$, $b\neq 0$. Since the minimum value for the amplitude of a plateaued function is $2^{n/2}$ there exists no bent (n,n)-function then this maximum is less or equal to $n-n/2+1 = n/2+1$. Hence a plateaued function can have algebraic degree n only if $n\leq 2$.

Proposition 1. Let F be an (n,n)-function satisfying $\deg(F)\neq n$ and G be defined by (1). Then G is not plateaued for $n\geq 3$. In particular, if F is AB or, more generally, plateaued, then G is not AB.

A. Equivalence Relations of Functions

There are several equivalence relations of functions for which differential uniformity and nonlinearity are invariant. Due to these equivalence relations, having only one APN (respectively, AB) function, one can generate a huge class of APN (respectively, AB) functions.

Two functions F and F' from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ are called

- *affine equivalent* (or *linear equivalent*) if $F' = A_1\circ F\circ A_2$, where the mappings A_1 and A_2 are affine (resp. linear) permutations of $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}$, respectively;
- *extended affine equivalent* (EA-equivalent) if $F' = A_1\circ F\circ A_2 + A$, where the mappings $A:\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}$, $A_1:\mathbb{F}_{2^m}\to\mathbb{F}_{2^m}$, $A_2:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ are affine, and where A_1, A_2 are permutations;
- *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}\times\mathbb{F}_{2^m}$ the image of the graph of F is the graph of F', that is, $\mathcal{L}(G_F) = G_{F'}$ where $G_F = \{(x,F(x)) \mid x\in\mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x,F'(x)) \mid x\in\mathbb{F}_{2^n}\}$.

Although different, these equivalence relations are connected to each other. It is obvious that linear equivalence is a particular case of affine equivalence, and that affine equivalence is a particular case of EA-equivalence. As shown in [12], EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalent to its inverse. The algebraic degree of a function (if it is not affine) is invariant under EA-equivalence but, in general, it is not preserved by CCZ-equivalence. Let us recall why the structure of CCZ-equivalence implies this: for a function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ and an affine permutation $\mathcal{L}(x,y) = \big(L_1(x,y), L_2(x,y)\big)$ of $\mathbb{F}_{2^n}\times\mathbb{F}_{2^m}$, where $L_1:\mathbb{F}_{2^n}\times\mathbb{F}_{2^m}\to\mathbb{F}_{2^n}$ and $L_2:\mathbb{F}_{2^n}\times\mathbb{F}_{2^m}\to\mathbb{F}_{2^m}$, we have $\mathcal{L}(G_F) = \{\big(F_1(x),F_2(x)\big) : x\in\mathbb{F}_{2^n}\}$ where $F_1(x) = L_1(x,F(x))$, $F_2(x) = L_2(x,F(x))$. Hence, $\mathcal{L}(G_F)$ is the graph of a function if and only if the function F_1 is a permutation. The function CCZ-equivalent to F whose graph equals $\mathcal{L}(G_F)$ is then $F' = F_2\circ F_1^{-1}$. The composition by the inverse of F_1 modifies in general the algebraic degree, except, for instance, when $L_1(x,y)$ depends only on x, which corresponds to EA-equivalence of F and F' [9].

Proposition 2. [9] Let F and F' be functions from $\mathbb{F}_2^n$ to itself. The function F' is EA-equivalent to the function F or to the inverse of F (if it exists) if and only if there exists an affine permutation $\mathcal{L} = (L_1, L_2)$ on $\mathbb{F}_2^{2n}$ such that $\mathcal{L}(G_F) = G_{F'}$ and the function L_1 depends only on one variable, i.e. $L_1(x,y) = L(x)$ or $L_1(x,y) = L(y)$.

Let functions F and F' be CCZ-equivalent. Then

- $\{\Delta_F(a,b) : a,b\in\mathbb{F}_{2^n}, a\neq 0\} = \{\Delta_{F'}(a,b) : a,b\in\mathbb{F}_{2^n}, a\neq 0\}$;
- if F is APN then F' is APN too;
- if F is AB then F' is AB too;
- if F is plateaued with single amplitude λ then F' is plateaued with the same single amplitude λ;
- if F is plateaued with different amplitudes then F' is not necessarily plateaued, it can happen that F' has no plateaued components at all. However if F and F' are EA-equivalent then F' is plateaued with the same set of amplitudes.

III. Characterizations of the APNness of Maximum Degree Function G

Let n be a positive integer and G be a function over $\mathbb{F}_{2^n}$ of algebraic degree n. Then $G(x) = ux^{2^n-1} + F(x)$ for some $u\in\mathbb{F}_{2^n}^*$ and some function F of algebraic degree strictly less than n. Obviously, G is APN if and only if the function $G'(x) = x^{2^n-1} + u^{-1}F(x) = x^{2^n-1} + F'(x)$ is APN since G and G' are EA-equivalent. Hence, when studying the problem of existence of APN functions of maximum degree it is sufficient to consider functions G of the form (1) where F is any (n,n)-function of algebraic degree strictly less than n.

Considering the problem of preserving APN property when changing a single point in an APN function also leads to functions of the form (1). Indeed, if an (n,n)-function G is obtained from a function F by changing its value at a point $v\in\mathbb{F}_{2^n}$ to $u\in\mathbb{F}_{2^n}\setminus\{F(v)\}$, then

$$G(x) = \begin{cases} F(x) & \text{if } x\in\mathbb{F}_{2^n}\setminus\{v\} \\ u & \text{if } x = v \end{cases} = F'(x) + u'(x+v)^{2^n-1},$$

where $F'(x) = F(x) + u + F(v)$ and $u' = u + F(v)\neq 0$. Clearly, G is EA-equivalent to $G'(x) = F''(x) + x^{2^n-1} = 1/u'F'(x+v) + x^{2^n-1}$ which has the form (1).

Below we present necessary and sufficient conditions on derivatives and Walsh coefficients of an (n,n)-function F so that the function G defined by (1) is APN.

A. Characterization by means of derivatives

For any $a \in \mathbb{F}_{2^n}^*$

$$D_aG(x) = G(x+a) + G(x) = D_aF(x) + 1_{\{0,a\}}(x),$$

where $1_{\{0,a\}}(x)$ denotes the indicator of the pair $\{0,a\}$ (that is, $1_{\{0,a\}}(x) = 1$ if $x \in \{0,a\}$ and $1_{\{0,a\}}(x) = 0$ otherwise). Hence, $\Delta_G \leq \Delta_F + 2$, and, in particular, $\Delta_G \leq 4$ when F is APN.

Obviously, G is APN if and only if, for every $a \in \mathbb{F}_{2^n}^*$ and every $b \in \mathbb{F}_{2^n}$, the equation $D_aF(x) + 1_{\{0,a\}}(x) = b$ has 0 or 2 solutions. This implies that G can be APN only if F is either APN or differentially 4-uniform. Another necessary condition is that $D_aF(x) + D_aF(0)$ never takes value 1 (since otherwise, the equation $D_aF(x) + 1_{\{0,a\}}(x) = D_aF(0) + 1$ would have 4 solutions). When F is APN, this condition is also sufficient for G to be APN.

Proposition 3. Let F be a function over $\mathbb{F}_{2^n}$ and G be defined by (1). Then G is APN if and only if the following three conditions are satisfied:

1) for any nonzero $a \in \mathbb{F}_{2^n}$, the function $D_aF(x)$ is 2-to-1 on $\mathbb{F}_{2^n} \setminus \{0,a\}$,
2) for any nonzero $a \in \mathbb{F}_{2^n}$, the equation $D_aF(x) = D_aF(0) + 1$ has no solutions.

Corollary 1. Let F be an APN function over $\mathbb{F}_{2^n}$ and G be defined by (1). Then G is APN if and only if $D_aF(x) = D_aF(0) + 1$ has no solutions for any nonzero $a \in \mathbb{F}_{2^n}$.

B. Characterization by means of the Walsh transform

For any $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}^*$ we calculate the values of the Walsh transform of G

$$\begin{aligned} W_G(a,b) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bx^{2^n-1} + bF(x) + ax)} \qquad (2) \\ &= 1 - (-1)^{\mathrm{Tr}_1^n(b)} + (-1)^{\mathrm{Tr}_1^n(b)} W_F(a,b). \end{aligned}$$

Hence, $W_G(a,b) \in \{ W_F(a,b), 2 - W_F(a,b) \}$ and $N_F - 1 \leq N_G \leq N_F + 1$. Since AB functions have highest possible nonlinearity and since there exists no AB functions of algebraic degree n then for an AB function F the function G is not AB and $N_G = 2^{n-1} - 2^{\frac{n-1}{2}} - 1$. This fact together with other straightforward observations are summarized in the proposition below. The last claim there follows from restriction on algebraic degree of plateaued functions.

Proposition 4. Let F be a function over $\mathbb{F}_{2^n}$ and G be defined by (1). Then

1) G is not a permutation when $\deg(F) \neq n$;
2) $\Delta_G \leq \Delta_F + 2$, in particular, $\Delta_G \leq 4$ when F is APN;
3) $W_G(a,b) \in \{ W_F(a,b), 2 - W_F(a,b) \}$ for any $a, b \in \mathbb{F}_{2^n}$, $b \neq 0$, and then $N_F - 1 \leq N_G \leq N_F + 1$;
4) for $n \geq 3$ if F is plateaued or $\deg(F) \neq n$ then G is not plateaued, in particular, if F is AB then G is not AB and $N_G = 2^{n-1} - 2^{\frac{n-1}{2}} - 1$.

For characterization of G by means of the Walsh transform we shall use Lemma 1. For this reason first we calculate the fourth power of $W_G(a,b)$. Observe that $(-1)^{\mathrm{Tr}_1^n(b)} W_F(a,b) = W_{F+1}(a,b)$. Then, by (2) one obtains that

$$\begin{aligned} \sum_{\substack{a \in \mathbb{F}_{2^n} \\ b \in \mathbb{F}_{2^n}^*}} W_G^4(a,b) &= \sum_{\substack{a \in \mathbb{F}_{2^n} \\ bu \in \mathbb{F}_{2^n}^*}} \left(1 - (-1)^{\mathrm{Tr}_1^n(b)} + W_{F+1}(a,b)\right)^4 \\ &= \sum_{\substack{a \in \mathbb{F}_{2^n} \\ b \in \mathbb{F}_{2^n}^*}} \Big(\epsilon_b^4 + 4\epsilon_b^3 W_{F+1}(a,b) \\ &\quad + 6\epsilon_b^2 W_{F+1}^2(a,b) + 4\epsilon_b W_{F+1}^3(a,b) + W_{F+1}^4(a,b) \Big), \end{aligned}$$

where $\epsilon_b = 1 - (-1)^{\mathrm{Tr}_1^n(b)}$ equals 0 if $\mathrm{Tr}_1^n(b) = 0$, and 2 otherwise. This leads to

$$\sum_{\substack{a \in \mathbb{F}_{2^n} \\ b \in \mathbb{F}_{2^n}^*}} \epsilon_b^4 = \sum_{\substack{a,b \in \mathbb{F}_{2^n} \\ \mathrm{Tr}_1^n(b) = 1}} 2^4 = 2^{2n+3}$$

since the trace function is balanced and

$$|b \in \mathbb{F}_{2^n}^* : \mathrm{Tr}_1^n(b) = 1| = 2^{n-1}.$$

Similarly, for any function f over $\mathbb{F}_{2^n}$, by the inverse Walsh transform formula and Parseval's identity, both recalled above, and using that $\epsilon_b^3 = 4\epsilon_b$, one has:

$$\begin{aligned} &\sum_{\substack{a \in \mathbb{F}_{2^n} \\ b \in \mathbb{F}_{2^n}^*}} 4\epsilon_b^3 W_{F+1}(a,b) \\ &= \sum_{\substack{a \in \mathbb{F}_{2^n} \\ b \in \mathbb{F}_{2^n}^*}} 2^4 (1 - (-1)^{\mathrm{Tr}_1^n(b)}) W_{F+1}(a,b) \\ &= \sum_{b \in \mathbb{F}_{2^n}^*} 2^{n+4} ((-1)^{\mathrm{Tr}_1^n(b)} - 1) = -2^{2n+4}, \end{aligned}$$

since

$$\begin{aligned} \sum_{a \in \mathbb{F}_{2^n}} W_{F+1}(a,b) &= 2^n (-1)^{\mathrm{Tr}_1^n(b)}, \\ \sum_{b \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b)} &= 0, \\ \sum_{\substack{a \in \mathbb{F}_{2^n} \\ b \in \mathbb{F}_{2^n}^*}} 6\epsilon_b^2 W_{F+1}^2(a,b) &= 3 \cdot 2^{3n+2}. \end{aligned}$$

Then, by a simple calculation, we arrive at

$$\begin{aligned} \sum_{\substack{a \in \mathbb{F}_{2^n} \\ b \in \mathbb{F}_{2^n}^*}} W_G^4(a,b) &= \sum_{\substack{a \in \mathbb{F}_{2^n} \\ b \in \mathbb{F}_{2^n}^*}} (W_{F+1}^4(a,b) + 4\epsilon_b W_{F+1}^3(a,b)) \\ &\quad + 2^{2n+3}(3 \cdot 2^{n-1} - 1). \end{aligned}$$

Again by the fact that $W_{F+1}(a,b) = (-1)^{\mathrm{Tr}_1^n(b)} W_F(a,b)$, we have $W_{F+1}^4(a,b) = W_F^4(a,b)$ and

$$4\epsilon_b W_{F+1}^3(a,b) = \begin{cases} 0 & \text{if} \quad \mathrm{Tr}_1^n(b) = 0 \\ -8W_F(a,b)^3 & \text{if} \quad \mathrm{Tr}_1^n(b) = 1 \end{cases}.$$

Thus, the above equality can be written as

$$\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} W_G^4(a,bu) = \sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} W_F^4(a,b) - 8\sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{Tr}_1^n(b)=1}} W_F^3(a,b) + 2^{2n+3}(3\cdot 2^{n-1}-1).$$

Therefore, we can obtain the following result about the APNness of G according to Lemma 1.

Theorem 1. Let F be any function over $\mathbb{F}_{2^n}$ with $F(0)=0$, and G be defined by (1). Then G is APN if and only if

$$\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} W_F^4(a,b) - 8\sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{Tr}_1^n(b)=1}} W_F^3(a,b) = \big(2^{3n+1} - 2^{2n+3}\big)(2^n-1) - 2^{3n+2}. \quad (3)$$

Theorem 1 characterizes the APNness of the function G defined by (1) in terms of the power sums of the Walsh transform values of F. Sometimes it is more convenient to express the power sums of Walsh transform values by the numbers of solutions to certain equations over finite fields.

According to the definition, one can obtain that

$$\begin{aligned}
&\sum_{a,b\in\mathbb{F}_{2^n}} W_F^4(a,b)\\
=\ &\sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ x,y\in\mathbb{F}_{2^n}\\ z,w\in\mathbb{F}_{2^n}}} (-1)^{\mathrm{Tr}_1^n(b(F(x)+F(y)+F(z)+F(w))+a(x+y+z+w))}\\
=\ &2^n\sum_{b,x,y,z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(x)+F(y)+F(z)+F(x+y+z)))}\\
=\ &2^{2n}M_0,
\end{aligned}$$

where

$$M_0 = |\{(x,y,z)\in\mathbb{F}_{2^n}^3 : F(x)+F(y)+F(z)+F(x+y+z)=0\}|. \quad (4)$$

Similarly to above, one also has:

$$\begin{aligned}
&\sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{Tr}_1^n(b)=1}} W_F^3(a,b)\\
&= \sum_{\substack{a,b,x,y,z\in\mathbb{F}_{2^n}\\ \mathrm{Tr}_1^n(b)=1}} (-1)^{\mathrm{Tr}_1^n(b(F(x)+F(y)+F(z))+a(x+y+z))}\\
&= 2^n\sum_{\substack{b,x,y\in\mathbb{F}_{2^n}\\ \mathrm{Tr}_1^n(b)=1}} (-1)^{\mathrm{Tr}_1^n(b(F(x)+F(y)+F(x+y)))}\\
&= 2^{2n-1}(N_0-N_1),
\end{aligned}$$

where

$$N_i = |\{(x,y)\in\mathbb{F}_{2^n}^2 : F(x)+F(y)+F(x+y)=i\}|. \quad (5)$$

Indeed, for any fixed $(x,y)\in\mathbb{F}_{2^n}^2$ we have $\sum_{\mathrm{Tr}_1^n(b)=1}(-1)^{\mathrm{Tr}_1^n(b(F(x)+F(y)+F(x+y)))} = 0$ if $F(x)+F(y)+F(x+y)\notin\{0,1\}$ due to the two-tuple-balance property of the trace function (i.e., $(\mathrm{Tr}_1^n(x),\mathrm{Tr}_1^n(\delta x))$ for $\delta\neq 0,1$ takes each pair $(0,0),(0,1),(1,0),(1,1)$ exactly 2^{n-2} times when x runs through $\mathbb{F}_{2^n}$).

Then, the APNness of the function G defined by (1) can be characterized in terms of the values of M_0, N_0, N_1 defined by (4) and (5) as follows.

Theorem 2. Let F be any function over $\mathbb{F}_{2^n}$ with $F(0)=0$, and G be defined by (1). Then G is APN if and only if

$$M_0 - 4(N_0-N_1) = (3\cdot 2^n-2)(2^n-4),$$

where M_0, N_0, N_1 are defined by (4) and (5) respectively.

Proof. This result follows from the above discussion, Theorem 1 and the fact $\sum_{a\in\mathbb{F}_{2^n}}\sum_{b\in\mathbb{F}_{2^n}^*} W_F^4(a,b) = 2^{2n}M_0 - 2^{4n}$ is based on a simple computation. □

When F is APN, the characterizations of APN functions G defined by (1) can be further simplified, and some non-existence results about APN functions with maximal algebraic degree are obtained. Indeed, if F is APN, then by Theorem 1 and Lemma 1 we have:

Corollary 2. Let F be APN with $F(0)=0$ and G be defined by (1). Then G is APN if and only if

$$\sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{Tr}_1^n(b)=1}} W_F^3(a,b) = 2^{2n}(3\cdot 2^{n-1}-1).$$

On the other hand, for an APN function F, the values of M_0 and N_0 defined by (4) and (5) respectively are well-known (see [11] for example):

$$M_0 = 2^n(3\cdot 2^n-2), N_0 = 3\cdot 2^n - 2.$$

Then, by Theorem 2, we have:

Corollary 3. Let F be APN with $F(0)=0$ and G be defined by (1). Then G is APN if and only if $N_1=0$, i.e.,

$$|\{(x,y)\in\mathbb{F}_{2^n}^2 : F(x)+F(y)+F(x+y)=1\}| = 0.$$

IV. Some Non-existence Results

A. When F is a Power Function

Let $F(x)=x^d$. According to Proposition 3, if G is APN, then the equation $D_aF(x)+D_aF(0)=1$, that is, $x^d+(x+a)^d+a^d=1$ has no solution for any nonzero $a\in\mathbb{F}_{2^n}$. In particular, taking $a=1$ we get that the equation $(1/x+1)^d=1$ (with $x\neq 0$) has no solution. Hence $\gcd(d,2^n-1)=1$ and F must be a permutation. Denoting $y=x/a$, we rewrite the equation above as

$$y^d+(y+1)^d = 1/a^d+1.$$

Note now that the right side of this equation ranges over $\mathbb{F}_{2^n}\setminus\{1\}$ when a ranges over $\mathbb{F}_{2^n}^*$. Hence, a necessary condition for G being APN is that $y^d+(y+1)^d$ equals the constant function 1 and $x^d+(x+a)^d$ equals the constant function a^d, which contradicts G being APN when $n\geq 3$.

We deduce:

Proposition 5. Let $n\geq 3$, $1\leq d\leq 2^n-2$, and $F(x)=x^d$ be a power function over $\mathbb{F}_{2^n}$. Then the function $G(x)=F(x)+x^{2^n-1}$ over $\mathbb{F}_{2^n}$ is not APN.

Remark 1. (1) Let $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$. If $v \neq 0$ then there exists some $w \in \mathbb{F}_{2^n}^*$ such that $u(x+v)^{2^n-1} + x^d$ is EA-equivalent to $w(x+1)^{2^n-1} + x^d$. Indeed, $u(x+v)^{2^n-1} + x^d = u(x/v+1)^{2^n-1} + v^d(x/v)^d$ and replacing $y = x/v$ we get $w(y+1)^{2^n-1} + y^d$ where $w = u/v^d$. Hence when considering a function $u(x+v)^{2^n-1} + x^d$ we can restrict the study to the cases $v \in \mathbb{F}_2$.
(2) In general, for a function $G(x) = u(x+1)^{2^n-1} + x^d$ with $u \in \mathbb{F}_{2^n}^*$ there does not necessarily exist $u' \in \mathbb{F}_{2^n}^*$ such that G is CCZ-equivalen to $G'(x) = u'x^{2^n-1} + x^d$. For example, if $n \in \{5, 6\}$ and d is the inverse exponent then for any $u, u' \in \mathbb{F}_{2^n}^*$ functions G and G' are CCZ-inequivalent. □

Consider the general case when $F(x) = u(x+v)^d$ for some $1 \leq d \leq 2^n - 2$ and $u \in \mathbb{F}_{2^n}^*$, $v \in \mathbb{F}_2$, and $G(x) = F(x) + x^{2^n-1}$. According to the second condition in Proposition 3, if G is APN, then the equation $D_aF(x) + D_aF(0) = 1$, that is, $u(x+v)^d + u(x+v+a)^d = uv^d + u(v+a)^d + 1$ has no solution for any nonzero $a \in \mathbb{F}_{2^n}$. Denoting $y = (x+v)/a$ we can rewrite the latter equation

$$y^d + (y+1)^d = \left(\frac{v}{a}\right)^d + \left(\frac{v}{a} + 1\right)^d + \frac{1}{ua^d}.$$

In the particular case of $\gcd(d, 2^n - 1) = 1$ and $v = 0$ the right hand side of this equation ranges over $\mathbb{F}_{2^n} \setminus \{1\}$ when a ranges over $\mathbb{F}_{2^n}^*$, and, if it has no solutions for all $a \neq 0$ then $ux^d + u(x+1)^d$ cannot be 2-to-1 on $\mathbb{F}_{2^n} \setminus \{0, 1\}$. Hence G cannot be APN according to the first condition of Proposition 3.

Corollary 4. Let $n \geq 3$ and $F(x) = ux^d$ be a function over $\mathbb{F}_{2^n}$ with $u \in \mathbb{F}_{2^n}^*$, $1 \leq d \leq 2^n - 2$ and $\gcd(d, 2^n - 1) = 1$. Then the function $G(x) = F(x) + x^{2^n-1}$ over $\mathbb{F}_{2^n}$ is not APN.

For particular case of the inverse function we get the following proposition.

Proposition 6. Let $n \geq 3$ and $F(x) = u(x+v)^{2^n-2}$ be a function over $\mathbb{F}_{2^n}$ with $u \in \mathbb{F}_{2^n}^*$, $v \in \mathbb{F}_{2^n}$. Then the function G defined by (1) is not APN.

Proof. The equation $D_aF(x) = D_aF(0) + 1$, $a \in \mathbb{F}_{2^n}^*$, can be written as

$$u(x+v)^d + u(x+a+v)^d = uv^d + u(a+v)^d + 1.$$

for $d = 2^n - 2$. If we find a solution for $D_aF(x) = D_aF(0) + 1$ for some $a \in \mathbb{F}_{2^n}^*$ then the function G is not APN by Proposition 2. According to Remark 1 (1) we can restrict to the cases $v \in \mathbb{F}_2$. Besides, we can consider only $n \geq 4$ since $n = 3$ is easy to check with a computer.

(1): $v = 0$.

In this case, $D_aF(x) = D_aF(0) + 1$ is reduced to $x^d + (x+a)^d = a^d + u^d$. Multiplying both sides by $x(x+a)$, it gives

$$x^2 + ax + \frac{a^2u}{a+u} = 0. \tag{6}$$

Notice that (6) has solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(\frac{u}{a+u}) = 0$. Clearly, there exists some $a \in \mathbb{F}_{2^n}$ such that $\mathrm{Tr}_1^n(\frac{u}{a+u}) = 0$ when a runs through the nonzero elements in $\mathbb{F}_{2^n}$. This means that $D_aF(x) = D_aF(0) + 1$ has solutions in $\mathbb{F}_{2^n}$ for some nonzero $a \in \mathbb{F}_{2^n}$.

(2): $v = 1$.

By a simple calculation, for this case from $D_aF(x) = D_aF(0) + 1$ we can obtain that

$$x^2 + ax + a + 1 + \frac{a}{1 + (a+1)^d + u^d} = 0. \tag{7}$$

Then, (7) has solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(\frac{a+1}{a^2} + \frac{1}{a(1+(a+1)^d+u^d)}) = 0$, i.e.,

$$\mathrm{Tr}_1^n\left(\frac{1}{a(1 + (a+1)^d + u^d)}\right) = 0, \tag{8}$$

where $a \neq 0, 1, (u+1)^d$. For simplicity, define

$$\phi(a) = \frac{1}{a(1 + (a+1)^d + u^d)} = \frac{ua + u}{(u+1)a^2 + a}.$$

In what follows, we prove that there exists at least one nonzero $a \in \mathbb{F}_{2^n}$ with $a \neq 0, 1, (u+1)^d$ such that $\mathrm{Tr}_1^n(\phi(a)) = 0$. First, we show that $\phi(a) \neq h(a)^2 + h(a)$ for any rational function $h(a) \in \overline{\mathbb{F}}_{2^n}[a]$, where $\overline{\mathbb{F}}_{2^n}$ denotes the algebraic closure of $\mathbb{F}_{2^n}$. Assume that $\phi(a) = \frac{\nu(a)^2}{\mu(a)^2} + \frac{\nu(a)}{\mu(a)}$ for some $\mu(a), \nu(a) \in \overline{\mathbb{F}}_{2^n}[a]$ with $\gcd(\mu(a), \nu(a)) = 1$, then one gets

$$u(a+1)\mu(a)^2 = ((u+1)a^2 + a)(\nu(a)^2 + \mu(a)\nu(a))$$

which implies that $a|\mu(a)$ and then $a^2|\mu(a)^2$. However, $a^2 \nmid ((u+1)a^2 + a)(\nu(a)^2 + \mu(a)\nu(a))$ since $\gcd(\mu(a), \nu(a)) = 1$ and $a|\mu(a)$. This leads to a contradiction. Therefore, $\phi(a) \neq h(a)^2 + h(a)$ for any rational function $h(a) \in \overline{\mathbb{F}}_{2^n}[a]$. By Lemma 3 presented below, we have

$$\Big|\sum_{a \in \mathbb{F}_{2^n}, a \neq 0, (u+1)^{-1}} (-1)^{\mathrm{Tr}_1^n(\phi(a))}\Big| \leq (2 + 2 - 2)\sqrt{2^n} + 1.$$

Thus, if $\mathrm{Tr}_1^n(\phi(a)) = 1$ for any $a \in \mathbb{F}_{2^n}$ with $a \neq 0, 1, (u+1)^d$, then we have $2^n - 3 \leq (2+2-2)\sqrt{2^n} + 1$, i.e., $2^n \leq (1+\sqrt{5})^2 < 16$. This shows that there exists at least one nonzero $a \in \mathbb{F}_{2^n}$ with $a \neq 0, 1, (u+1)^d$ such that $\mathrm{Tr}_1^n(\phi(a)) = 0$ if $n \geq 4$. □

Lemma 3. ([19, Lemma 2]) Let $\overline{\mathbb{F}}_{2^n}$ denote the algebraic closure of $\mathbb{F}_{2^n}$. Let $f(z), g(z) \in \mathbb{F}_{2^n}[z]$, where $\deg f < r = \deg g$ and $g(z)$ is a polynomial with t distinct zeros in $\overline{\mathbb{F}}_{2^n}$. If $\frac{f(z)}{g(z)} \neq h(z)^2 + h(z)$ for any rational function $h(z) \in \overline{\mathbb{F}}_{2^n}[z]$, then

$$\Big|\sum_{a \in L} (-1)^{\mathrm{Tr}_1^n(\frac{f(z)}{g(z)})}\Big| \leq (t + r - 2)\sqrt{2^n} + 1,$$

where L consists of all elements of $\mathbb{F}_{2^n}$ except the zeros of $g(z)$.

We checked with a computer that for $3 \leq n \leq 13$ there are no APN functions of the form $x^{2^n-1} + u(x+v)^d$ where $1 \leq d \leq 2^n - 2$, $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$.

B. When F is a Plateaued Function

Majority of the known APN functions are plateaued. We prove nonexistence of APN functions of the form (1) for plateaued F by applying Theorem 1.

Theorem 3. Let F be a plateaued function over $\mathbb{F}_{2^n}$ with $n \geq 3$ and G be defined by (1). Then G is not APN.

Proof. Let n be odd. Let 2^{λ_b} be the amplitude of the component function $\mathrm{Tr}_1^n(bF(x))$ for $b \in \mathbb{F}_{2^n}^*$. We have $\lambda_b \geq \frac{n+1}{2}$. According to Lemma 2, we have $\sum_{a\in\mathbb{F}_{2^n}} W_F^3(a,b) = (-1)^{\mathrm{Tr}_1^n(bF(0))} 2^{n+2\lambda_b}$ and $\sum_{a\in\mathbb{F}_{2^n}} W_F^4(a,b) = 2^{2n+2\lambda_b}$. Hence, $\sum_{a\in\mathbb{F}_{2^n}} W_F^3(a,b)$ is divisible by 2^{2n+1} and $\sum_{a\in\mathbb{F}_{2^n}} W_F^4(a,b)$ is divisible by 2^{3n+1}, and therefore by 2^{2n+4} since $n \geq 3$. Then Relation (3) cannot be satisfied since the term on the left hand side is divisible by 2^{2n+4} and the term on the right hand side is not.

Let now n be even. This case is more technical. Without loss of generality we can assume that $F(0) = 0$. Suppose that G is APN. Then, by Proposition 3, we get for any $a \neq 0$:

$$\sum_{b\in\mathbb{F}_{2^n}} \Delta_F(a,b)^2 = (2^{n-1}-2)\cdot 2^2 + 4^2$$

if $D_aF(x) = D_aF(0)$ has 4 solutions and

$$\sum_{b\in\mathbb{F}_{2^n}} \Delta_F(a,b)^2 = (2^{n-1}-2)\cdot 2^2 + 2\cdot 2^2$$

otherwise. That is,

$$\sum_{b\in\mathbb{F}_{2^n}} \Delta_F(a,b)^2 = 2^{n+1} + 8t_a,$$

where $t_a = 1$ if $D_aF(x) = D_aF(0)$ has 4 solutions and $t_a = 0$ otherwise. Indeed, we know that D_aF is 2-to-1 on $\mathbb{F}_{2^n}\backslash\{0,a\}$; we deduce that $D_aF(\mathbb{F}_{2^n}\backslash\{0,a\})$ has size $2^{n-1}-1$ and includes the element $D_aF(0)$ in the first case and does not include it in the second case.

Because $\Delta_F(0,b) = 0$ for any $b \neq 0$ then

$$\begin{aligned}\sum_{(a,b)\neq(0,0)} \Delta_F(a,b)^2 &= (2^n-1)2^{n+1} + 8\sum_{a\in\mathbb{F}_{2^n}^*} t_a \\ &= (2^n-1)2^{n+1} + 8T, \end{aligned} \tag{9}$$

where $0 \leq T \leq 2^n - 1$.

Since $\Delta_F(0,0) = 2^n$, $W_F(0,0) = 2^n$ and $W_F(a,0) = 0$ for $a \neq 0$ then the equality from [13]

$$\sum_{a,b\in\mathbb{F}_{2^n}} \Delta_F(a,b)^2 = \frac{1}{2^{2n}} \sum_{a,b\in\mathbb{F}_{2^n}} W_F(a,b)^4$$

leads to

$$\sum_{(a,b)\neq(0,0)} \Delta_F(a,b)^2 = \frac{1}{2^{2n}} \sum_{(a,b)\neq(0,0)} W_F(a,b)^4. \tag{10}$$

Let 2^{λ_b} be again the amplitude of $\mathrm{Tr}_1^n(bF(x))$ for $b \in \mathbb{F}_{2^n}^*$. Then $\lambda_b = \frac{n+s_b}{2}$ for $0 \leq s_b \leq n$ and by Lemma 2

$$\frac{1}{2^{2n}} \sum_{(a,b)\neq(0,0)} W_F(a,b)^4 = 2^n \sum_{b\in\mathbb{F}_{2^n}^*} 2^{s_b}. \tag{11}$$

The values s_b are even for all $b \neq 0$, and $2^{s_b}-1$ and 2^n-1 are divisible by 3. Hence using (9)-(11) we get

$$\sum_{b\in\mathbb{F}_{2^n}^*} 2^{s_b} = 2(2^n-1) + T' \tag{12}$$

where $T' = T/2^{n-3}$, $0 \leq T' \leq 7$. Then

$$\sum_{b\in\mathbb{F}_{2^n}^*} (2^{s_b}-1) = 2^n - 1 + T'$$

and T' is divisible by 3. Hence $T' \in \{0,3,6\}$.

Using (11) and (12) we get

$$\begin{aligned}\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} W_F(a,b)^4 &= 2^{3n}\sum_{b\in\mathbb{F}_{2^n}^*} 2^{s_b} = 2^{3n}\big(2^{n+1}+v\big) \\ &= 2^{4n+1} + 2^{3n}v, \end{aligned} \tag{13}$$

where $v = -2$ if $T' = 0$ and $v = 1$ if $T' = 3$ and $v = 4$ if $T' = 6$.

Since G is APN then (3) holds by Theorem 1 and using (13):

$$\begin{aligned}\sum_{\substack{a,b\in\mathbb{F}_{2^n}\\ \mathrm{Tr}_1^n(b)=1}} W_F^3(a,b) &= \frac{1}{8}\sum_{a\in\mathbb{F}_{2^n}}\sum_{b\in\mathbb{F}_{2^n}^*} W_F^4(a,b) \\ &\quad -(2^{3n-2}-2^{2n})(2^n-1) + 2^{3n-1} \\ &= 2^{2n}(7\cdot 2^{n-2} + 2^{n-3}v - 1) \\ &= \begin{cases} 2^{2n}(3\cdot 2^{n-1}-1) & \text{if } v=-2 \\ 2^{2n}(15\cdot 2^{n-3}-1) & \text{if } v=1 \\ 2^{2n}(9\cdot 2^{n-2}-1) & \text{if } v=4. \end{cases} \end{aligned} \tag{14}$$

By Lemma 2 and using (13), we get:

$$\sum_{\substack{a\in\mathbb{F}_{2^n}\\ b\in\mathbb{F}_{2^n}^*}} W_F^3(a,b) = 2^{2n}\sum_{b\in\mathbb{F}_{2^n}^*} 2^{s_b} = 2^{2n}(2^{n+1}+v). \tag{15}$$

Besides,

$$\begin{aligned}\sum_{\substack{a\in\mathbb{F}_{2^n},b\in\mathbb{F}_{2^n}^*\\ \mathrm{Tr}_1^n(b)=0}} W_F^3(a,b) &= 2^{2n}\sum_{\substack{b\in\mathbb{F}_{2^n}^*\\ \mathrm{Tr}_1^n(b)=0}} 2^{s_b} \\ &\geq 2^{2n}(2^{n-1}-1). \end{aligned} \tag{16}$$

Hence by (14)-(16):

$$\begin{aligned}2^{2n}(2^{n+1}+v) = \sum_{a\in\mathbb{F}_{2^n}}\sum_{b\in\mathbb{F}_{2^n}^*} W_F^3(a,b) &\geq 2^{2n}(2^{n-1}-1) \\ &+ \begin{cases} 2^{2n}(3\cdot 2^{n-1}-1) & \text{if } v=-2 \\ 2^{2n}(15\cdot 2^{n-3}-1) & \text{if } v=1 \\ 2^{2n}(9\cdot 2^{n-2}-1) & \text{if } v=4 \end{cases}. \end{aligned}$$

Clearly, this inequality does not hold when $n \geq 4$ and $v \in \{1,4\}$. When $v = -2$ this corresponds to the case of F an APN function and the last inequality becomes an equality. That is, we get that $\mathrm{Tr}_1^n(bF(x))$ is bent for all $b \in \mathbb{F}_{2^n}^*$ satisfying $\mathrm{Tr}_1^n(b) = 0$. However, this is impossible if $n > 2$, since otherwise we would have an $(n, n-1)$-vectorial bent function. Indeed, take a basis $(b_1,..,b_{n-1})$ of the hyperplane of equation $\mathrm{Tr}_1^n(b) = 0$ and define the vectorial $(n,n-1)$-function whose coordinates are $f_i(x) = \mathrm{Tr}_1^n(b_iF(x))$ for $i = 1,..,n-1$. Then all its component functions are bent

and, by definition, the function is then bent. This contradicts the fact recalled above that (n, m)-vectorial bent functions exist only for $2m \leq n$ [24]. □

Note that Theorem 3 does not hold when $n \leq 2$. For example, x^3 is a plateaued APN function over $\mathbb{F}_{2^2}$ of algebraic degree 2.

Theorem 3 leads to a nonexistence result for APN functions G with F quadratic or AB.

Corollary 5. Let F be a quadratic function and G be defined by (1). Then G is not APN.

Corollary 6. Let F be an AB function and G be defined by (1). Then G is not APN.

V. Characterizations of Equivalence Classes of Maximum Degree Functions

In this section we study the connection between EA- and CCZ-equivalence classes of a function F over $\mathbb{F}_{2^n}$ and the respective classes of the function G given by (1). We also deduce some non-existence results for functions of the form (1) where F is CCZ-equivalent to known APN functions.

Next proposition describes EA-equivalence classes of G via EA-equivalence classes of F.

Proposition 7. Let F be a function over $\mathbb{F}_{2^n}$ and $G(x) = x^{2^n-1} + F(x)$. If a function G' is EA-equivalent to G then there exist some $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$, and a function F' EA-equivalent to F such that $G'(x) = u(x + v)^{2^n-1} + F'(x)$.

Proof. For EA-equivalent functions G and G' there exist affine permutations A_1, A_2 and affine A such that $G'(x) = A_1 \circ G \circ A_2(x) + A(x)$. Note that

$$A_1 \circ G \circ A_2(x) + A(x) = A_1 \circ F \circ A_2(x) + A(x) + A_1((A_2(x))^{2^n-1})$$

and denoting $F'(x) = A_1 \circ F \circ A_2(x) + A(x) + A_1(0)$ and $A'_1(x) = A_1(x) + A_1(0)$ we get

$$G'(x) = F'(x) + A'_1(1)(x + A_2^{-1}(0))^{2^n-1}$$

since $A'_1((A_2(x))^{2^n-1})$ takes value $A'_1(1)$ if $x \neq A_2^{-1}(0)$ (that is, $A_2(x) \neq 0$) and 0 otherwise, and we can rewrite it as $A'_1(1)(x + A_2^{-1}(0))^{2^n-1})$ (which takes the same values). Hence $G'(x) = F'(x) + u(x + v)^{2^n-1}$ for $u = A'_1(1) \neq 0$ and $v = A_2^{-1}(0)$ and the function F' is EA-equivalent to F. □

Note that if F and F' are EA-equivalent then it does not necessarily mean that functions $G(x) = x^{2^n-1} + F(x)$ and $G'(x) = u(x + v)^{2^n-1} + F'(x)$ are EA-equivalent for any $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$. However, there exist some $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$ (in some cases these elements are unique) giving EA-equivalent functions G and G' according to the following proposition.

Proposition 8. If F and F' are EA-equivalent functions over $\mathbb{F}_{2^n}$ then the function $G'(x) = x^{2^n-1} + F'(x)$ is EA-equivalent to $u(x + v)^{2^n-1} + F(x)$ for some $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$.

Proof. For EA-equivalent functions F and F' there exist affine permutations A_1, A_2 and affine A such that $F'(x) = A_1 \circ F \circ A_2(x) + A(x)$. Without loss of generality we can assume $A_1(0) = 0$. Then $G'(x) = x^{2^n-1} + A_1 \circ F \circ A_2(x) + A(x)$ and it is EA-equivalent to $A_1^{-1}((A_2^{-1}(x))^{2^n-1}) + F(x) = A_1^{-1}(1)(x + A_2(0))^{2^n-1} + F(x) = u(x + v)^{2^n-1} + F(x)$ with $u = A_1^{-1}(1) \neq 0$ and $v = A_2(0)$. □

Using Proposition 8 we can deduce an important non-existence result on APN functions of the form (1).

Corollary 7. Let F and F' be EA-equivalent functions over $\mathbb{F}_{2^n}$. If for any $v \in \mathbb{F}_{2^n}$ and any nonzero $u \in \mathbb{F}_{2^n}$ the function $x^{2^n-1} + uF(x + v)$ is not APN then for any $v' \in \mathbb{F}_{2^n}$ and any nonzero $u' \in \mathbb{F}_{2^n}$ the function $x^{2^n-1} + u'F'(x + v')$ is not APN either.

Further we describe CCZ-equivalence classes of G via CCZ-equivalence classes of F.

Proposition 9. Let F be a function over $\mathbb{F}_{2^n}$ and G be defined by (1). If a function G' is CCZ-equivalent to G then there exist some $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$, and a function F' CCZ-equivalent to F such that $G'(x) = u(x + v)^{2^n-1} + F'(x)$.

Proof. Since G and G' are CCZ-equivalent then for some affine permutation

$$\begin{aligned} \mathcal{L}(x, y) &= \big(L_1(x, y), L_2(x, y)\big) \\ &= \big(A_1(x) + A_2(y), A_3(x) + A_4(y)\big), \end{aligned}$$

where A_1, A_2, A_3, A_4 are affine, we have $G'(x) = G_2 \circ G_1^{-1}(x)$ with

$$G_1(x) = L_1(x, G(x)) = A_1(x) + A_2 \circ G(x)$$

a permutation and

$$G_2(x) = L_2(x, G(x)) = A_3(x) + A_4 \circ G(x).$$

Note that $G_1(x) = A_1(x) + A_2 \circ F(x) + A_2(x^{2^n-1})$ and since it is a permutation then $A_2(0) = A_2(1)$ and $G_1(x) = A_1(x) + A_2 \circ F(x) + A_2(0)$. Take $F_1(x) = G_1(x)$ and $F_2(x) = A_3(x) + A_4 \circ F(x)$. Then, obviously, $F'(x) = F_2 \circ F_1^{-1}(x)$ is CCZ-equivalent to F and

$$\begin{aligned} G'(x) &= F'(x) + A_2((F_1(x))^{2^n-1}) \\ &= F'(x) + A_2(1)(x + F_1^{-1}(0)) \\ &= F'(x) + u(x + v)^{2^n-1} \end{aligned}$$

with $u = A_2(1)$ and $v = F_1^{-1}(0)$. Note that $u \neq 0$ since otherwise the system

$$\begin{aligned} A_1(x) + A_2(y) &= A_1(0) + A_2(0) \\ A_3(x) + A_4(y) &= A_3(0) + A_4(0) \end{aligned}$$

would have two solutions $(0, 0)$ and $(0, 1)$ and $\mathcal{L}$ would not be a permutation. □

Proposition 10. Let F and F' be CCZ-equivalent functions over $\mathbb{F}_{2^n}$, that is, $\mathcal{L}(G_F) = G_{F'}$ for some affine permutation $\mathcal{L}(x, y) = (L_1(x, y), L_2(x, y))$ of $\mathbb{F}_{2^n}^2$. If $L_1(0, y)$ is not a permutation of $\mathbb{F}_{2^n}$ then there exist some $u, v, w \in \mathbb{F}_{2^n}$, $u, w \neq 0$, such that functions $wx^{2^n-1} + F(x)$ and $u(x+v)^{2^n-1} + F'(x)$ are CCZ-equivalent.

Proof. When the affine function $L_1(0,y)$ is not a permutation of $\mathbb{F}_{2^n}$ there exists $w \in \mathbb{F}_{2^n}^*$ such that $L_1(0,0) = L_1(0,w)$. Clearly a linear function $\mathcal{L}^\circ(x,y) = (x, wy))$ is a permutation of $\mathbb{F}_{2^n}^2$ and

$$\mathcal{L} \circ \mathcal{L}^\circ(x,y) = (L_1(x,wy), L_2(x,wy))$$

maps the graph of the function $w^{-1}F(x)$ to the graph of the function $F'(x)$. Moreover, $\mathcal{L} \circ \mathcal{L}^\circ$ maps the graph of $G(x) = x^{2^n-1} + w^{-1}F(x)$ to the graph of $G'(x) = u(x+v)^{2^n-1} + F'(x)$ for $u = L_2(0,w) + L_2(0,0)$ and $v = L_1(0,F(0))$. Indeed, note that $u \neq 0$ since otherwise $\mathcal{L}$ would not be a permutation and we have

$$\begin{aligned}
G_1(x) &= L_1(x, wG(x)) = L_1\big(x, F(x) + wx^{2^n-1}\big) \\
&= L_1(x,F(x)) + \big(L_1(0,w) + L_1(0,0)\big)x^{2^n-1} \\
&= F_1(x), \\
G_2(x) &= L_2(x, wG(x)) = L_2\big(x, F(x) + wx^{2^n-1}\big) \\
&= L_2(x,F(x)) + ux^{2^n-1} = F_2(x) + ux^{2^n-1}, \\
G'(x) &= G_2 \circ G_1^{-1}(x) = F_2 \circ F_1^{-1}(x) + c\big(F_1^{-1}(x)\big)^{2^n-1} \\
&= F'(x) + u(x+v)^{2^n-1}.
\end{aligned}$$

Hence, G and G' are CCZ-equivalent, and, therefore, $wx^{2^n-1} + F(x)$ and G' are CCZ-equivalent. □

In Proposition 10 the condition on $L_1(0,y)$ being a permutation is essential. Indeed, take $F(x) = x^3$ and $F'(x) = F^{-1}(x) = x^{21}$ and $n = 5$, then F and F' are CCZ-equivalent with $\mathcal{L}(x,y) = (L_1(x,y), L_2(x,y)) = (y,x)$ where $L_1(0,y) = y$ is a permutation. It can be easily checked with a computer that for all $u, u' \in \mathbb{F}_{2^5}^*$, $v, v' \in \mathbb{F}_{2^5}$, the functions $G(x) = u(x+v)^{2^n-1} + F(x)$ and $G'(x) = u'(x+v')^{2^n-1} + F'(x)$ are CCZ-inequivalent.

For n odd all known APN functions except inverse and Dobbertin functions are AB. Hence, by Corollary 6 a function $u(x+v)^{2^n-1} + F(x)$, $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$, is not APN for any of these functions F and any F CCZ-equivalent to them (since CCZ-equivalence preserves AB property). For n even all known APN functions except Dobbertin functions and functions constructed in [8], [9] (and a sporadic example with $n = 6$ [17]) are plateaued and plateauedness is preserved by EA-equivalence. Therefore, $u(x+v)^{2^n-1} + F(x)$, $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$, is not APN for any of these functions F and any F EA-equivalent to them. When n is even and F is plateaued the following corollary of Proposition 10 is useful for CCZ-equivalence.

Corollary 8. Let F and F' be CCZ-equivalent APN functions over $\mathbb{F}_{2^n}$ where F is plateaued and n is even. Then for an affine permutation $\mathcal{L}(x,y) = (L_1(x,y), L_2(x,y))$ of $\mathbb{F}_{2^n}^2$ satisfying $\mathcal{L}(G_F) = G_{F'}$ there exists $w \in \mathbb{F}_{2^n}^*$ such that $L_1(0,w) = L_1(0,0)$ and $u(x+v)^{2^n-1} + F'(x)$ is not APN for $u = L_2(0,w) + L_2(0,0)$ and $v = L_1(0,F(0))$.

Proof. If $L_1(0,w) \neq L_1(0,0)$ for any $w \in \mathbb{F}_{2^n}^*$ then $L_1(0,y)$ is a permutation of $\mathbb{F}_{2^n}$ and $F_1(x) = L_1(x,F(x))$ is a plateaued APN permutation which leads to a contradiction since all plateaued APN functions have bent components when n is even. Hence, there exists $w \in \mathbb{F}_{2^n}^*$ such that $L_1(0,w) = L_1(0,0)$. Since $w^{-1}F(x)$ is plateaued APN then $G(x) = wx^{2^n-1} + F(x)$ is not APN by Theorem 3. It follows from the proof of Corollary 10 that for $u = L_2(0,w) + L_2(0,0)$ and $v = L_1(0,F(0))$ the function $G'(x) = u(x+v)^{2^n-1} + F'(x)$ is CCZ-equivalent to G, and, therefore, it is not APN. □

All APN functions with n even constructed in [8] and [9] satisfy the conditions in Corollary 8 with $v = 0$ and $u = w$ satisfying

1) $\mathrm{Tr}_1^n(u) = 0$ for functions
$$x^{2^i+1} + (x^{2^i} + x + 1)\mathrm{Tr}_1^n(x^{2^i+1})$$
and
$$x^3 + \mathrm{Tr}_1^n(x^9) + (x^2 + x + 1)\mathrm{Tr}_1^n(x^3)$$
where $\gcd(n,i) = 1$;
2) $\mathrm{Tr}_3^n(u + u^2) = 0$ for functions
$$\Big(x + \mathrm{Tr}_3^n(x^{2(2^i+1)} + x^{4(2^i+1)}) + \mathrm{Tr}_1^n(x)\mathrm{Tr}_3^n(x^{2^i+1} + x^{2^{2i}(2^i+1)})\Big)^{2^i+1}$$
and
$$\Big(x + \mathrm{Tr}_3^n(x^6 + x^{12}) + \mathrm{Tr}_1^n(x)\mathrm{Tr}_3^n(x^3 + x^{12})\Big)^3 + \mathrm{Tr}_1^n\Big(\big(x + \mathrm{Tr}_3^n(x^6 + x^{12}) + \mathrm{Tr}_1^n(x)\mathrm{Tr}_3^n(x^3 + x^{12})\big)^9\Big)$$
where n divisible by 6 and $\gcd(n,i) = 1$.

Hence it is not possible to get APN function by adding ux^{2^n-1} to any of these functions. Besides, using Proposition 3, Corollary 7 and computer search we confirmed that for $n \leq 10$ there are no APN functions of the form (1) for any F EA-equivalent to the functions above.

When F is EA-equivalent to the inverse function then $u(x+v)^{2^n-1} + F(x)$, $u, v \in \mathbb{F}_{2^n}$, $v \neq 0$, is not APN by Proposition 6 and Corollary 7. For F a Dobbertin function, the function $ux^{2^n-1} + F(x)$, $u \in \mathbb{F}_{2^n}^*$, is not APN for n odd by Proposition 4, and for n even $x^{2^n-1} + F(x)$ is not APN by Proposition 5. However, these results do not give complete information about $u(x+v)^{2^n-1} + F(x)$, $u, v \in \mathbb{F}_{2^n}$, $u \neq 0$, when F is EA-equivalent to Dobbertin functions. Using Proposition 3, Corollary 7 and computer search we confirmed that for $n \leq 15$ there are no APN functions of the form (1) for any F EA-equivalent to Dobbertin functions. Regarding to CCZ-equivalence, it is not known whether for inverse and Dobbertin functions it coincides with EA-equivalence (in case of Dobbertin functions together with EA-equivalence of their inverses when they exist).

VI. Conclusion

The major objective of this paper was to characterize APN functions over the finite field $\mathbb{F}_{2^n}$ having algebraic degree n, or equivalently, of the form $G(x) = x^{2^n-1} + F(x)$, where F is any function from $\mathbb{F}_{2^n}$ to itself having algebraic degree less than n, in order to find new APN functions with maximal algebraic degree or to prove the non-existence of such APN functions. We obtained some characterizations of those APN functions by means of the derivatives and of the

power moments of their Walsh transform, and then some non-existence results on APN functions with maximal algebraic degree were proved. This includes all power functions and all plateaued functions and covers most of the known cases of APN functions F. These results also imply that for most of the known APN functions changing their value in a single point results in non-APN functions.

REFERENCES

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", J. Cryptol., vol. 4, no. 1, pp. 3-72, 1991.

[2] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials", Finite Fields Appl., vol. 14, no. 3, pp. 703-714, 2008.

[3] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "A few more quadratic APN functions", Cryptogr. Commun., vol. 3, no. 1, pp. 43-53, 2011.

[4] M. Brinkmann, G. Leander, "On the classification of APN functions up to dimension five", Des. Codes Cryptography, vol. 49(1-3), pp. 273-288, 2008.

[5] L. Budaghyan and C. Carlet, "Classes of quadratic APN trinomials and hexanomials and related structures", IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2354-2357, May 2008.

[6] L. Budaghyan, C. Carlet, G. Leander, "On a construction of quadratic APN functions", Proceedings of IEEE Information Theory Workshop, ITW'09, pp. 374-378, 2009.

[7] L. Budaghyan, C. Carlet, G. Leander, "Two classes of quadratic APN binomials inequivalent to power functions", IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4218-4229, 2008.

[8] L. Budaghyan, C. Carlet, G. Leander, "Constructing new APN functions from known ones", Finite Fields Appl., vol. 15, no. 2, pp. 150-159, 2009.

[9] L. Budaghyan, C. Carlet, A. Pott, "New classes of almost bent and almost perfect nonlinear functions", IEEE Trans. Inf. Theory, vol. 52, no. 3, pp. 1141-1152, 2006.

[10] C. Carlet, "Vectorial Boolean Functions for Cryptography", Chapter of the monography Boolean Methods and Models, Cambridge University Press, pp. 398-472, 2010.

[11] C. Carlet, "Boolean and vectorial plateaued functions, and APN functions", IEEE Trans. Inf. Theory, vol. 61, no. 11, pp. 6272-6289, 2015.

[12] C. Carlet, P. Charpin and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems", Des. Codes Cryptography, vol. 15(2), pp. 125-156, 1998.

[13] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis", Advances in Cryptology–EUROCRYPT'94, Lecture Notes in Computer Science, vol. 950, pp. 356-365, 1995.

[14] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case", IEEE Trans. Inf. Theory, vol. 45, no. 4, pp.1271-1275, 1999.

[15] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: The Niho case", Inf. Comput., vol. 151, pp. 57-72, 1999.

[16] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5", Proceedings of the conference on Finite Fields and Applications 1999, pp. 113-121, 2001.

[17] Y. Edel and A. Pott, "A new almost perfect nonlinear function which is not quadratic", Adv. in Math. of Comm., vol. 3, no. 1, pp. 59-81, 2009.

[18] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions", IEEE Trans. Inf. Theory, vol. 14, no. 1, pp. 154-156, Jan. 1968.

[19] T. Helleseth, T. Kløve, V. Levenshtein. "Hypercubic 4 and 5-designs from double-error-correcting BCH codes", Des. Codes Cryptography, vol. 28(3), pp. 265-282, 2003.

[20] T. Kasami, "The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes", Inf. Control, vol. 18, pp. 369-394, 1971.

[21] X. Lai, "Higher order derivatives and differential cryptanalysis", Communications and Cryptography, vol. 276, pp. 227-233, 1994.

[22] P. Langevin, "Covering radius of $RM(1,9)$ in $RM(3,9)$", Eurocode'90, Lecture Notes in Computer Science, vol. 514, pp. 51-59, 1991.

[23] M. Matsui, "Linear cryptanalysis method for DES cipher", Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, pp. 386-397, 1994.

[24] K. Nyberg, "Perfect non-linear S-boxes", Proceedings of EUROCRYPT'91, Lecture Notes in Computer Science, vol. 547, pp. 378-386, 1992.

[25] K. Nyberg, "Differentially uniform mappings for cryptography", Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, pp. 55-64, 1994.

[26] Y. Zheng and X. Zhang, "Plateaued functions", Proceedings of ICICS'99, Lecture Notes in Computer Science vol. 1726, pp. 284-300, 1999.