ON THE WALSH SPECTRUM OF ALMOST PERFECT NONLINEAR FUNCTIONS

by
YAĞMUR SAK

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of Master of Science

Sabancı University
July 2023

ABSTRACT

ON THE WALSH SPECTRUM OF ALMOST PERFECT NONLINEAR FUNCTIONS

YAĞMUR SAK

MATHEMATICS M.A. THESIS JULY 2023

Thesis Supervisor: Asst. Prof. NURDAGÜL ANBAR MEIDL

APN functions, Walsh spectrum, Biprojective polynomials, Nonlinearity, Finite fields

In this thesis, we study the Walsh spectrum of "Almost Perfect Nonlinear" (APN) functions over finite fields of characteristic 2. We first give a characterization of APN functions in terms of the Walsh spectrum. We also gather recent characterization results of APN functions. Then, we give upper bounds for the Walsh spectrum of two families of biprojective APN functions, which have been recently introduced by Göloğlu. As a result, we obtain lower bounds for the nonlinearity of those APN functions. Our method is based on Bezout's theorem, i.e., the intersection theory of two projective plane curves.

ÖZET

NEREDEYSE MÜKEMMEL LİNEER OLMAYAN FONKSİYONLARIN WALSH SPEKTRUMU ÜZERİNE

YAĞMUR SAK

MATEMATİK YÜKSEK LİSANS TEZİ, TEMMUZ 2023

Tez Danışmanı: Asst. Prof. NURDAGÜL ANBAR MEIDL

Anahtar Kelimeler: APN fonksiyoları, Walsh spektrum, Biprojektif polinomlar, Doğrusal olmama, Sonlu cisimler

Bu tezde, karakteristiği 2 olan sonlu cisimler üzerinde tanımlanan "Neredeyse Mükemmel Lineer Olmayan" (APN) fonksiyonların Walsh spektrumlarını inceledik. İlk önce APN fonksiyonlarının Walsh spektrumu açısından bir karakterizasyonunu verdik. Ayrıca, yakın zamanda verilen APN fonksiyonlarının karakterizasyonlarını toparladık. Daha sonra, yakın zamanda Göloğlu tarafından verilen iki biprojektif APN fonksiyon sınıfının Walsh spektrumları için üst sınırlar verdik. Sonuç olarak, verilen bu APN fonksiyonlarının non-lineerliği için alt sınırlar elde ettik. Metodumuz Bezout teoremine, yani iki tasarımsal düzlem eğrisinin kesişim teorisine, dayanmaktadır.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Asst. Prof. Dr. Nurdagül Anbar Meidl who guided and supported me throughout the whole process, and patiently dealt with me. I have been very lucky to have such a gentle advisor.

I would like to thank my family, especially my father, who supported me throughout my education life. Their support and belief in me have always motivated me.

Finally, I would like to thank all my friends who were with me in my graduate education, especially Gülsemin Çonoğlu, Elshani Kamberi, Antigona Pajaziti, and Melih Mert Oskay.

To my father, İsmet

TABLE OF CONTENTS

1. Introduction

Vectorial Boolean functions have a wide range of uses in cryptography and coding theory. The nonlinearity of the function measures the resistance to linear attacks, see Matsui (1993). The higher the nonlinearity of a vectorial Boolean function, the better its resistance to linear attacks. Almost perfect nonlinear(APN) functions are of critical importance in symmetric cryptography since they ensure optimal resistance to differential attacks, see Biham & Shamir (1991).

Let n and m be two positive integers, p prime, and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a function. For any $a \in \mathbb{F}_{p^n}^* (\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \backslash \{0\})$, the derivative $D_aF : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ of F with respect to a is defined by

$$D_aF(x) = F(x+a) - F(x).$$

In the case $m = n$, if for any $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, the equation $D_aF(x) = b$ has 0 or 2 solutions, then F is called APN function. This thesis contains the characterization of APN functions. One of the important characterizations for APN-ness is given by Janwa-Wilson-Rodier in Janwa & Wilson (1993). A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if and only if the following holds:

$$F(x) + F(y) + F(z) + F(x+y+z) = 0 \text{ if and only if } x = y \text{ or } x = z \text{ or } y = z.$$

Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a function. For $\lambda \in \mathbb{F}_{p^m}$, a function $f_\lambda : \mathbb{F}_{p^n} \to \mathbb{F}_p$ defined by $f_\lambda(x) = Tr_n(\lambda F(x))$ is the component of F corresponding to λ. For a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, Walsh (Fourier) transform is defined by

$$W_f(a) = \sum_{x \in \mathbb{F}_{p^n}} \varepsilon_p^{f(x) - Tr_n(ax)}$$

where ε_p be a primitive p-th root of unity in $\mathbb{C}$. The Walsh spectrum of f is the multiset defined by

$$\{|W_f(a)| : a \in \mathbb{F}_{p^n}\}.$$

The Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called bent if $|W_{f_\lambda}(a)| = 2^{n/2}$. Moreover, f is called semibent if $|W_f(a)| \in \{0, 2^{\frac{n+1}{2}}\}$ (respectively $|W_f(a)| \in \{0, 2^{\frac{n+2}{2}}\}$) when n

is odd (respectively n is even) for all $a \in \mathbb{F}_{p^n}$. If a vectorial Boolean function has only bent and semibent components, then we say that the function has the classical spectrum, see Pott (2016) for more details.

The nonlinearity of $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by

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

The nonlinearity of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is defined by

$$\mathcal{N}(F) = 2^{n-1} - \frac{1}{2}\mathcal{L}(F), \text{ where } \mathcal{L}(F) = \max_{\substack{\lambda \in \mathbb{F}_{2^m}^* \\ a \in \mathbb{F}_{2^n}}} |W_{f_\lambda}(a)|$$

where f_λ is the component of F corresponding to λ.

If $\mathcal{N}(F) = 2^{\frac{n+1}{2}}$, then F is said to be almost bent(AB). Suppose that n is odd. Every AB function on $\mathbb{F}_{2^n}$ is APN, see Chabaud & Vaudenay (1994). Moreover, if F is quadratic and APN, then F is AB, see Carlet, Charpin & Zinoviev (1998). Suppose that n is even. If F has no bent component, then F is not APN. Moreover, if F is APN, then the number of bent components is $2(2^n - 1)/3$ if and only if $\mathcal{L}(F) = 2^{(n+2)/2}$, see Berger, Canteaut, Charpin & Laigle-Chapuy (2005).

Most known quadratic APN functions have the classical spectrum. It is known that there exists an APN function that has no classical spectrum, see Dillon (2006). However, there is no infinite family known to have a non-classical spectrum.

In this thesis, gold and inverse functions are given as an example of APN functions. For more infinite families of quadratic APN polynomials, see Budaghyan, Helleseth & Kaleyski (2020).

In 2022, two infinite families of biprojective polynomial pairs are constructed in Göloğlu (2022). We used the method introduced in Anbar, Kalaycı & Meidl (2019) to estimate the nonlinearity of those APN functions.

The thesis is organized as follows. In Chapter 2, we introduce basic concepts and facts related to finite fields, trace functions, and permutation polynomials. In Chapter 3, we introduce APN function and the Walsh spectrum of the Boolean function. We give the characterization of the APN function in terms of the Walsh spectrum. We give examples of APN monomials, such as cube, gold, and inverse functions. Then we compute the Walsh spectrum of the cube function by using the definition of the Walsh spectrum and using the dimension of its linear space. Chapter 3 contains also the further characterization of APN functions stated in Berger et al. (2005). In Chapter 4, we give the essential definitions and theorems to state Bezout's Theorem for projective curves. In Chapter 5, we state the biprojective APN functions and determine the lower bound for the nonlinearity of two infinite families of biprojective polynomial pairs presented in Göloğlu (2022).

2. Preliminaries

2.1 Finite Fields

This chapter gives the main definitions and theorems which are used in the following chapters. In this section, we will first give the definition and basic properties of finite fields; we will then define trace and balanced functions and their related theorems.

Definition 2.1. A field is a set $\mathbb{F}$, together with two binary operations of $\mathbb{F}$, addition and multiplication, denoted by "$+$" and "$.$" which satisfies the following properties:

(i) $\mathbb{F}$ is an abelian group under "$+$" with identity element $0_{\mathbb{F}}$;

(ii) $\mathbb{F}\backslash\{0\}$ is an abelian group under "$.$" with identity element $1_{\mathbb{F}}$;

(iii) Multiplication distributes over addition, i.e., $x.(y+z)=x.y+x.z$ for $x,y,z\in\mathbb{F}$.

Definition 2.2. The characteristic of a field $\mathbb{F}$ is the smallest positive integer n such that $n.1_{\mathbb{F}}=0$ if n exists. Then $\mathbb{F}$ is said to have characteristic n and is denoted by $char(\mathbb{F})$. If no such positive integer n exists, $\mathbb{F}$ is said to have characteristic 0.

Theorem 2.1. *A finite field $\mathbb{F}$ has a prime characteristic.*

Theorem 2.2 (Lidl & Niederreiter (1994), Chapter 2, Theorem 2.2)**.** *Let $\mathbb{F}$ be a finite field. Then the cardinality $|\mathbb{F}|$ is p^n where p is the characteristic of $\mathbb{F}$ with $n\in\mathbb{Z}^+$.*

Theorem 2.3 (Lidl & Niederreiter (1994), Chapter 2, Theorem 2.8)**.** *For every finite field $\mathbb{F}$, the multiplicative group $\mathbb{F}^*$ of nonzero elements of $\mathbb{F}$ is cyclic.*

Definition 2.3. The field $\overline{\mathbb{F}}$ is called an algebraic closure of $\mathbb{F}$ if $\overline{\mathbb{F}}$ is algebraic over $\mathbb{F}$ and if every polynomial $f(x)\in\mathbb{F}[x]$ factors completely into linear factors in $\overline{\mathbb{F}}[x]$.

Now, we will give some theorems about finite fields which are necessary in the following chapters.

Lemma 2.1. If $\mathbb{F}_q$ is finite with q elements and $\alpha \in \mathbb{F}_q$ with $\alpha \neq 0$, then $\alpha^{q-1} = 1$. Thus, $\alpha^q = \alpha$ for all $\alpha \in \mathbb{F}_q$.

Proof. Let $\alpha \in \mathbb{F}_q$ be a nonzero element, then α is a unit in $\mathbb{F}_q$. There are $q-1$ units in $\mathbb{F}_q$ and the set of units in $\mathbb{F}_q$, say $\mathbb{F}_q^*$, is a multiplicative group of order $q-1$. $\mathbb{F}_q^*$ is a cyclic group of order $q-1$ since any finite multiplicative subgroup of a field is cyclic. Then, the multiplicative order of α divides $q-1$ by using Lagrange's theorem. Thus, we have $\alpha^{q-1} = 1$ and, by multiplying both sides with α, we obtain $\alpha^q = \alpha$. □

Theorem 2.4. *Let $\mathbb{F}_{p^n}$ be the finite field of order p^n. For any divisor s of $p^n - 1$, there exists $y \in \mathbb{F}_{p^n}$ such that $ord(y) = s$.*

Proof. Note that $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \backslash \{0\}$ is a multiplicative group of order $p^n - 1$. Since the cardinality of $\mathbb{F}_{p^n}^*$ is finite, $\mathbb{F}_{p^n}^*$ is cyclic. Then there exists $\zeta \in \mathbb{F}_{p^n}^*$ such that $\mathbb{F}_{p^n}^* =< \zeta >$. In particular, $ord(\zeta) = p^n - 1$. Let s be a divisor of $p^n - 1$. Consider $y = \zeta^{\frac{p^n-1}{s}} \in \mathbb{F}_{p^n}^*$. Then, we obtain the following equations:

$$ord(y) = \frac{ord(\zeta)}{\gcd(\frac{p^n-1}{s}, p^n - 1)} = \frac{p^n - 1}{\frac{p^n-1}{s}} = s.$$

□

Now, we will give a useful lemma for a finite field with characteristic p.

Lemma 2.2. Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a function defined by

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

Then $F(x)^{p^n} = F(x^{p^n})$.

Proof. Note that $a_i^{p^n} = a_i$ since $a_i \in \mathbb{F}_{p^n}$. Then we have the following equalities:

$$F(x)^{p^n} = \left(\sum_{i=1}^{n} a_i x^i \right)^{p^n} = \sum_{i=1}^{n} a_i^{p^n} (x^i)^{p^n} = \sum_{i=1}^{n} a_i (x^{p^n})^i = F(x^{p^n}).$$

□

Now, we will give the definition and basic properties of the trace function which is required to define the Walsh spectrum of the APN function.

Definition 2.4. Let $\alpha \in \mathbb{F}_{q^n}$ where q is a prime power and n is positive integer. The trace function $Tr_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is defined by

$$Tr_n(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}} \text{ for } \alpha \in \mathbb{F}_{q^n}.$$

Theorem 2.5. *The trace function, $Tr_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$ satisfies the following properties:*

(i) $Tr_n(\alpha+\beta) = Tr_n(\alpha) + Tr_n(\beta)$ *where* $\alpha, \beta \in \mathbb{F}_{q^n}$ *;*

(ii) $Tr_n(c\alpha) = c\,Tr_n(\alpha)$ *where* $\alpha \in \mathbb{F}_{q^n}$ *and* $c \in \mathbb{F}_q$ *;*

(iii) $Tr_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$ *is a linear function and it is onto ;*

(iv) $Tr_n(\alpha) = n\alpha$ *for* $\alpha \in \mathbb{F}_q$ *and* n *is a non-negative integer ; and*

(v) $Tr_n(\alpha^q) = Tr_n(\alpha)$ *for any* $\alpha \in \mathbb{F}_{q^n}$*.*

Proof. (i) For any $\alpha, \beta \in \mathbb{F}_q$, we have the following equalities:

$$\begin{aligned} Tr_n(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^q + (\alpha+\beta)^{q^2} + \cdots + (\alpha+\beta)^{q^{n-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \alpha^{q^2} + \beta^{q^2} + \cdots + \alpha^{q^{n-1}} + \beta^{q^{n-1}} \\ &= (\alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}) + (\beta + \beta^q + \cdots + \beta^{q^{n-1}}) \\ &= Tr_n(\alpha) + Tr_n(\beta). \end{aligned}$$

(ii) Note that $c^q = c$ for any $c \in \mathbb{F}_q$ by Lemma 2.1. For any $\alpha \in \mathbb{F}_{q^n}$ and $c \in \mathbb{F}_q$, we have the following equalities:

$$\begin{aligned} Tr_n(c\alpha) &= c\alpha + (c\alpha)^q + (c\alpha)^{q^2} + \cdots + (c\alpha)^{q^{n-1}} \\ &= c\alpha + c^q\alpha^q + c^{q^2}\alpha^{q^2} + \cdots + c^{q^{n-1}}\alpha^{q^{n-1}} \\ &= c(\alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}) = c\,Tr_n(\alpha). \end{aligned}$$

(iii) From the properties (i) and (ii), $Tr_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is a linear function. To prove that $Tr_n(x)$ is onto, we first show the existence of an $\alpha \in \mathbb{F}_{q^n}$ with $Tr_n(\alpha) \neq 0$. Note that $Tr_n(\alpha) = 0$ if and only if α is a root of the polynomial $Tr_n(x) = x + x^q + \cdots + x^{q^{n-1}} \in \mathbb{F}_q[x]$ in $\mathbb{F}_{q^n}$. Since the degree of $Tr_n(x)$ is q^{n-1}, the polynomial can have at most q^{n-1} roots in $\mathbb{F}_{q^n}$. So, there must be at least one $\alpha \in \mathbb{F}_{q^n}$ such that $Tr_n(\alpha) \neq 0$.

Now, we will show that Tr_n is onto. Set $Tr_n(\alpha) = b \in \mathbb{F}_q$ and let $c \in \mathbb{F}_q$. We will show that there exists $\beta \in \mathbb{F}_{q^n}$ such that $Tr_n(\beta) = c$. As $\frac{c}{b} \in \mathbb{F}_q$, we have

$$Tr_n\left(\frac{c}{b}\,\alpha\right) = \frac{c}{b}\,Tr_n(\alpha) = \frac{c}{b}\,b = c.$$

(iv) By Lemma 2.1, if $\alpha \in \mathbb{F}_q$, then $\alpha^{q^i} = \alpha$ for any positive integer i. Then we have the following equalities:

$$\begin{aligned} Tr_n(\alpha) &= \alpha + \alpha^q + \alpha^{q^2} + \alpha^{q^3} + \cdots + \alpha^{q^{n-1}} \\ &= \alpha + \alpha + \cdots + \alpha = n\alpha. \end{aligned}$$

(v) For $\alpha \in \mathbb{F}_{2^n}$, we have the following equalities:

$$\begin{aligned} Tr_n(\alpha^q) &= \beta + \beta^q + \beta^{q^2} + \cdots + \beta^{q^{n-1}} \\ &= \alpha^q + (\alpha^q)^q + (\alpha^q)^{q^2} + \cdots + (\alpha^q)^{q^{n-1}} \\ &= \alpha^q + \alpha^{q^2} + \alpha^{q^3} + \cdots + \alpha^{q^{n-1}} + \alpha^{q^n} \\ &= \alpha^q + \alpha^{q^2} + \alpha^{q^3} + \cdots + \alpha^{q^{n-1}} + \alpha = Tr_n(\alpha). \end{aligned}$$

□

Theorem 2.6. *Let $Tr_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$ be a trace function. Set $\mathcal{Z} = \{\alpha \in \mathbb{F}_{q^n} : Tr_n(\alpha) = 0\}$ and, $\mathcal{S} = \{\beta^q - \beta : \beta \in \mathbb{F}_{q^n}\}$. Then $\mathcal{Z} = \mathcal{S}$.*

Proof. By Theorem 2.5, we observed that $Tr_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is an $\mathbb{F}_q$-linear map. Note that $\mathcal{Z}$ is equal to kernel $Ker(Tr_n(x))$ of the Tr_n map. By the dimension theorem,

$$dim_{\mathbb{F}_q}(\mathbb{F}_{q^n}) = dim_{\mathbb{F}_q}(Im(Tr_n(x))) + dim_{\mathbb{F}_q}(Ker(Tr_n(x)))$$

where $Im(Tr_n(x))$ denotes the image of $Tr_n(x)$. Since Tr_n is an onto map, we have

$$n = 1 + dim_{\mathbb{F}_q}(Ker(Tr_n(x))).$$

That is, $dim_{\mathbb{F}_q}(Ker(Tr_n(x))) = n - 1$. This implies that the cardinality of $Ker(Tr_n(x))$ is q^{n-1}, i.e., $|\mathcal{Z}| = q^{n-1}$.

Set $\mathcal{S} = \{\beta^q - \beta : \beta \in \mathbb{F}_{q^n}\}$. Let $\varphi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be a $\mathbb{F}_q$-linear map given by $\varphi(\beta) = \beta^q - \beta$. Then $\mathcal{S} = Im(\varphi)$. We now determine the kernel $Ker(\varphi)$ of φ. An element $\beta \in \mathbb{F}_{q^n}$ is in $Ker(\varphi)$ if and only if $\varphi(\beta) = \beta^q - \beta = 0$. This holds if and only if

$\beta^q = \beta$, i.e., $\beta \in \mathbb{F}_q$. Hence, we observed that $Ker(\varphi) = \mathbb{F}_q$. By dimension theorem,

$$\begin{aligned} n = dim_{\mathbb{F}_q}(\mathbb{F}_{q^n}) &= dim_{\mathbb{F}_q}(Im(\varphi)) + dim_{\mathbb{F}_q}(Ker(\varphi)) \\ n &= dim_{\mathbb{F}_q}(Im(\varphi)) + 1. \end{aligned}$$

That is, $dim_{\mathbb{F}_q}(Im(\varphi)) = n-1$, i.e., $|Im(\varphi)| = |\mathcal{S}| = q^{n-1}$. Hence, $|\mathcal{S}| = |\mathcal{Z}|$. Therefore, to show $\mathcal{S} = \mathcal{Z}$, it is enough to observe that

$$\mathcal{S} = Im(\varphi) \subseteq \mathcal{Z} = Ker(Tr_n(x)).$$

By Theorem 2.5, we know that $Tr_n(\beta) = Tr_n(\beta^q)$. Then we have the following:

$$Tr_n(\beta^q) - Tr_n(\beta) = Tr_n(\beta^q - \beta) = 0.$$

This implies that $\beta^q - \beta \in \mathcal{Z}$, i.e., $\mathcal{S} \subseteq \mathcal{Z}$. □

Definition 2.5. Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a function. F is called balanced if for all $b \in \mathbb{F}_{p^m}$, it has the same number inverse image. That is, $|F^{-1}(b)| = \frac{p^n}{p^m} = p^{n-m}$ for any $b \in \mathbb{F}_{p^m}$.

Remark 2.1. Note that $Tr_n : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is an onto $\mathbb{F}_q$-linear map, the inverse image of any element has the same cardinality, namely $|Ker(Tr_n)| = q^{n-1}$. Then Tr_n is a balanced function.

Lemma 2.3. The equation $z^2 + az + b = 0$ has a solution in $\mathbb{F}_{2^n}$, $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, if and only if $Tr_n(\frac{b}{a^2}) = 0$ where $Tr_n : \mathbb{F}_{2^n} \to \mathbb{F}_2$.

Proof. Set $z = ay$. Then we have $z^2 + az + b = a^2y^2 + a^2y + b$. This implies that $z^2 + az + b = 0$ for some $z \in \mathbb{F}_{2^n}$ if and only if $y^2 + y + \frac{b}{a^2} = 0$. Hence, we need to show that $y^2 + y + \frac{b}{a^2} = 0$ if and only if $Tr_n(\frac{b}{a^2}) = 0$. Suppose that there exists y such that $y^2 + y + \frac{b}{a^2} = 0$, i.e., $y^2 + y = \frac{b}{a^2}$. Then we have the following.

$$Tr_n\left(\frac{b}{a^2}\right) = Tr_n(y^2 + y) = Tr_n(y^2) + Tr_n(y) = 0,$$

since $Tr_n(y^2) = Tr_n(y)$.
Conversely, suppose that $Tr\left(\frac{b}{a^2}\right) = 0$. By Theorem 2.6, $Tr_n\left(\frac{b}{a^2}\right) = 0$ if and only if $\frac{b}{a^2} = y^2 + y$ for some $y \in \mathbb{F}_{2^n}$, i.e., $y^2 + y + \frac{b}{a^2} = 0$ has a solution in $\mathbb{F}_{2^n}$. □

Theorem 2.7. *Let $c \in \mathbb{F}_{p^n}$ and ε_p be a primitive p-th root of unity. Let $Tr_n : \mathbb{F}_{p^n} \to$*

$\mathbb{F}_p$ *defined by* $Tr_n(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}}$. *Then we have the following.*

$$\sum_{u \in \mathbb{F}_{p^n}} \varepsilon_p^{Tr_n(cu)} = \begin{cases} p^n, & \text{if } c = 0; \\ 0, & \text{if } c \neq 0. \end{cases}$$

Proof. If $c = 0$, then $Tr_n(cu) = 0$ for all $u \in \mathbb{F}_{q^n}$. Therefore, we have

$$\sum_{u \in \mathbb{F}_{p^n}} \varepsilon_p^0 = \sum_{u \in \mathbb{F}_{p^n}} 1 = p^n.$$

If $c \neq 0$, consider the function $\psi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that $\psi(u) = cu$ with $c \in \mathbb{F}_{p^n}^*$. Note that

$$Ker(\psi) = \{u \in \mathbb{F}_{p^n} : \psi(u) = 0\} = \{0\}.$$

Then ψ is one-to-one and hence ψ is onto. Therefore, ψ is a permutation function. Since ψ is a permutation and $Tr_n(u)$ is a balanced function, $Tr_n(cu)$ is a balanced function. Then the inverse image of $Tr_n(cu)$ has cardinality p^{n-1} for every $u \in \mathbb{F}_p$. Then we have

$$\sum_{u \in \mathbb{F}_{p^n}} \varepsilon_p^{Tr_n(cu)} = p^{n-1}\varepsilon^0 + p^{n-1}\varepsilon^1 + p^{n-1}\varepsilon^2 + \cdots + p^{n-1}\varepsilon^{p-1} = p^{n-1}(1 + \varepsilon^1 + \varepsilon^2 + \cdots + \varepsilon^{p-1}).$$

Since ε_p be a primitive p-th root of unity, the minimal polynomial of ε_p is $1 + x + \cdots + x^{p-1}$, i.e., $1 + \varepsilon^1 + \varepsilon^2 + \cdots + \varepsilon^{p-1} = 0$. Therefore,

$$\sum_{u \in \mathbb{F}_{p^n}} \varepsilon_p^{Tr_n(cu)} = p^{n-1}0 = 0.$$

□

Lemma 2.4. Let $\mathbb{F}_{p^n}$ be a finite field and $\xi \in \mathbb{F}_{p^n}$ be a primitive element of $\mathbb{F}_{p^n}$. Suppose that $\beta \in \mathbb{F}_{p^n}^*$ with $ord(\beta) = s$. If $\xi^{k_1}\langle\beta\rangle = \xi^{k_2}\langle\beta\rangle$ for some $k_1, k_2 \in 1, \ldots, \frac{p^n-1}{s}$, then $k_1 = k_2$.

Proof. Suppose that $ord(\beta) = s$, then β can be written as $\beta = \xi^{\frac{p^n-1}{s}j}$ for some positive integer j with $\gcd(p^n - 1, j) = 1$. Suppose that $\xi^{k_1}\langle\beta\rangle = \xi^{k_2}\langle\beta\rangle$, and let $k_1 \geq k_2$ without loss of generality. Then we have the following implication.

$$\begin{aligned} \xi^{k_1-k_2}\langle\beta\rangle = \langle\beta\rangle \Longleftrightarrow \xi^{k_1-k_2} \in \langle\beta\rangle \Longleftrightarrow \xi^{k_1-k_2} = (\xi^{\frac{p^n-1}{s}j})^l, \text{ for some } l \text{ such that } 1 \geq l \geq s \\ \Longleftrightarrow \xi^{\frac{p^n-1}{s}jl-(k_1-k_2)} = 1 \end{aligned}$$

Since $ord(\xi) = p^n - 1$,

$$p^n - 1 \mid \frac{p^n-1}{s} jl - (k_1 - k_2).$$

Then

$$\frac{p^n-1}{s} \mid \frac{p^n-1}{s} jl - (k_1 - k_2).$$

That is,

$$\frac{p^n-1}{s} \mid k_1 - k_2 \text{ where } k_1, k_2 \in \{1, \ldots, \frac{p^n-1}{s}\}.$$

This holds if and only if $k_1 - k_2 = 0$, i.e., $k_1 = k_2$.

□

Remark 2.2. Any function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ can be given as a polynomial $P_F(x) \in \mathbb{F}_{p^n}[x]$. Moreover, $P_F(x)$ is unique modulo $x^{p^n} - x$, i.e., any function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ can be uniquely represented as a polynomial of degree less than p^n.

Proof. By Lagrange Interpolation, any function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ can be represented as a polynomial $P_F(x) \in \mathbb{F}_{p^n}[x]$ of degree less than or equal to $p^n - 1$ as follows:

$$P_F(x) = \sum_{a \in \mathbb{F}_{p^n}} f(a)(1 - (x-a)^{p^n - 1}).$$

Note that for $b \neq a$, we have $(b-a)^{p^n-1} = 1$, i.e.,

$$f(a)(1 - (b-a)^{p^n-1}) = f(a)(1-1) = 0.$$

For $b = a$, we have

$$f(b)(1 - (b-b)^{p^n-1}) = f(b).$$

That is, $P_F(x) = f(b)$. Let $P(x)$ and $Q(x)$ be two representations of $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ less than degree p^n. Then we obtain that $P(\alpha) = Q(\alpha) = F(\alpha)$ for all $\alpha \in \mathbb{F}_{p^n}$. That is, $P(\alpha) - Q(\alpha) = (P-Q)(\alpha) = 0$ for all $\alpha \in \mathbb{F}_{p^n}$. Therefore, the polynomial $P(x) - Q(x)$ has p^n roots. Moreover, $deg(P(x) - Q(x)) \leq p^n - 1$ by our assumption. This is possible if and only if $P(x) - Q(x) = 0$, i.e., $P(x) = Q(x)$. □

2.2 Permutation Polynomials

In this section, we will give the definition and characterization of permutation polynomials.

Definition 2.6. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation if its associated map $\alpha \to f(\alpha)$ is a permutation of $\mathbb{F}_q$.

The following lemma characterizes a polynomial $f(x) \in \mathbb{F}_{p^n}[x]$ being a permutation. We will not give proof of this lemma since the proof is straightforward by definition.

Lemma 2.5. The polynomial $f \in \mathbb{F}_{p^n}[x]$ is a permutation polynomial of $\mathbb{F}_{p^n}$ if and only if one of the following conditions holds:

(i) f is one-to-one ;

(ii) f is onto ;

(iii) $f(x) = a$ has a unique solution in $\mathbb{F}_{p^n}$ for each $a \in \mathbb{F}_{p^n}$.

Now, we will give Hermite's Criteria for permutation polynomials which is used in the following chapters. The following lemma is needed to prove Hermite's Criteria. Before the lemma, we must first recall the formula for the sum of the first n terms of a geometric series. Let $\mathbb{F}$ be a field and let $a \in \mathbb{F}, a \neq 1$. Then the following identity holds:

$$\sum_{i=0}^{n-1} a^i = \frac{1-a^n}{1-a}.$$

Lemma 2.6 (Shallue (2012), Chapter 1, Lemma 1.4)*.* Let $a_0, a_1, \ldots, a_{q-1}$ be elements of $\mathbb{F}_q$. Then the following two conditions are equivalent:

(i) $a_0, a_1, \ldots, a_{q-1}$ are distinct;

(ii) $\sum\limits_{i=0}^{q-1} a_i^t = \begin{cases} 0, & \text{for } t = 0, 1, \ldots, q-2; \\ -1, & \text{for } t = q-1. \end{cases}$

Proof. For fixed i with $0 \leq i \leq q-1$, consider the polynomial

$$g_i(x) = 1 - \sum_{t=0}^{q-1} a_i^t x^{q-1-t}.$$

Then we have the following.

$$g_i(a_i) = 1 - \sum_{t=0}^{q-1} a_i^t a_i^{q-1-t} = 1 - \sum_{t=0}^{q-1} a_i^{q-1} = 1 \text{ for all } 0 \leq i \leq q-1$$

And for all $b \in \mathbb{F}_q$ such that $b \neq a_i$, we have the following equalities.

$$g_i(b) = 1 - \sum_{t=0}^{q-1} a_i^t b^{q-1-t} = 1 - \sum_{t=0}^{q-1} (a_i b^{-1})^t = 1 - \frac{1-(a_i b^{-1})^q}{1-(a_i b^{-1})} = 1 - 1 = 0$$

Note that we have used the fact that $a_i b^{-1} \neq 1$ since $a_i \neq b$. Hence, the polynomial $g(x)$ satisfies the following equalities.

$$\begin{aligned} g(x) = \sum_{i=0}^{q-1} g_i(x) &= \sum_{i=0}^{q-1} 1 - \sum_{i=0}^{q-1} \left(\sum_{t=0}^{q-1} a_i^t x^{q-1-t} \right) \\ &= q.1 - \sum_{t=0}^{q-1} \left(\sum_{i=0}^{q-1} a_i^t \right) x^{q-1-t} \\ &= \begin{cases} 1 & \text{if } x \in \{a_0, \ldots, a_{q-1}\}; \\ 0 & \text{if } x \in \mathbb{F}_q \backslash \{a_0, \ldots, a_{q-1}\} \end{cases} \end{aligned}$$

Therefore, $g(x)$ maps any element of $\mathbb{F}_q$ to 1 if and only if $\{a_0, \ldots, a_{q-1}\} = \mathbb{F}_q$. Since $deg(g) \leq q-1$, the function g maps every element to 1, this holds if and only if $g(x) = 1$. That is,

$$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0, & \text{for } t = 0, \ldots, q-2; \\ 1, & \text{for } t = q-1. \end{cases}$$

□

Theorem 2.8 (Hermite's Criterion)**.** *[Lidl & Niederreiter (1997), Chapter 7, Theorem 7.4] Let $\mathbb{F}_q$ be of characteristic p. Then $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions hold:*

(i) f has exactly one root in $\mathbb{F}_q$;

(ii) for each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \mod p$, the degree of $f(x)^t \mod x^q - x$ is less than or equal to $q-2$.

Proof. Let f be a permutation polynomial of $\mathbb{F}_q$. Since $f(x) = a$ has exactly one solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$ by the definition, part (i) holds. The reduction of

$f(x)^t \mod x^q - x$ is some polynomial

$$\sum_{i=0}^{q-1} b_i^{(t)} x^i.$$

Note that by Remark 2.2, $b_{q-1}^{(t)} = -\sum_{c \in \mathbb{F}_q} f(c)^t$.

Since $\{f(c) : c \in \mathbb{F}_q\} = \mathbb{F}_q$, we observe the following by Lemma 2.6.

$$b_{q-1}^{(t)} = -\sum_{c \in \mathbb{F}_q} f(c)^{q-1} = 0 \text{ for all } 1 \le t \le q-2$$

This means that the degree of $\sum_{i=0}^{q-1} b_i^{(t)} x^i$ is less than or equal to $q-2$.
Now, suppose that (i) and (ii) are satisfied. Then (i) implies that

$$\sum_{c \in \mathbb{F}_q} f(c)^{q-1} = q-1 = -1.$$

And (ii) implies that

$$-b_{q-1}^{(t)} = \sum_{c \in \mathbb{F}_q} f(c)^{q-1} = 0 \text{ for all } 1 \le t \le q-2,\ t \not\equiv 0 \mod p.$$

If $t \equiv 0 \mod p$, then we can write $t = t'p^j$ where $1 \le t' \le q-2$ and $t' \not\equiv 0 \mod p$. Therefore, we obtain the following equalities.

$$\sum_{c \in \mathbb{F}_q} f(c)^t = \sum_{c \in \mathbb{F}_q} f(c)^{t'p^j} = \left(\sum_{c \in \mathbb{F}_q} f(c)^{t'} \right)^{p^j} = 0$$

Since $\sum_{c \in \mathbb{F}_q} f(c)^t = 0$ for $t = 0, \ldots, q-2$ and $f(c)^{q-1} = -1$, we conclude that $f(x)$ is a permutation polynomial of $\mathbb{F}_q$ by Lemma 2.6. □

Lemma 2.7. The monomial x^n is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$.

Proof. x^n is a permutation polynomial of $\mathbb{F}_q$ if and only if the function $f(x) = x^n$ is onto $\mathbb{F}_q^*$. Recall that $\mathbb{F}_q^*$ is a cyclic group of order $q-1$. Let $\mathbb{F}_q^* =< a >$ for some $a \in \mathbb{F}_q^*$. Then f is a onto if and only if $< a^n >= \mathbb{F}_q^*$. This holds if and only if $\gcd(n, q-1) = 1$. □

Lemma 2.8. Let n and k be positive integers. Then

$$\gcd(2^n - 1, 2^k - 1) = 2^{\gcd(k,n)} - 1.$$

Proof. Assume that $d = \gcd(2^n - 1, 2^k - 1)$. Then $2^n \equiv 1 \mod d$ and $2^k \equiv 1 \mod d$. Let $s = \gcd(k,n)$, which means that $nt + kr = s$ for some integers t and r. Then $2^s = 2^{nt+kr}$. Therefore, we have

$$2^s = 2^{nt+kr} = (2^n)^t (2^k)^r \equiv 1 \mod d.$$

That is, d divides $2^s - 1$ where $2^s - 1 = 2^{\gcd(k,n)} - 1$.
Conversely, $s \mid n$ and $s \mid k$ since $s = \gcd(k,n)$. That is, there exists some integers l and l' such that $sl = n$ and $sl' = k$. Then we have $2^{sl} - 1 = 2^n - 1$ and $2^{sl'} - 1 = 2^k - 1$. Hence, we have the following equalities.

$$2^n - 1 = (2^{sl} - 1) = (2^s - 1)(2^{s(l-1)} + \cdots + 1)$$

$$2^k - 1 = (2^{sl'} - 1) = (2^s - 1)(2^{s(l'-1)} + \cdots + 1)$$

That is, $2^s - 1$ divides $\gcd(2^n - 1, 2^s - 1)$ where $\gcd(2^n - 1, 2^s - 1) = d$. Hence, $\gcd(2^n - 1, 2^k - 1) = 2^{\gcd(k,n)-1}$. □

Theorem 2.9. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a function defined by $F(x) = x^t$. If $\gcd(t, p^n - 1) = s$, then $F(x) = c$ has no solution or exactly s solutions for any non-zero c.*

Proof. Note that if $s = 1$, then we are done by Lemma 2.7. Suppose that $s > 1$. Then consider the map $\varphi : \mathbb{F}_{p^n}^* \to \mathbb{F}_{p^n}^*$ defined by $\varphi(x) = x^t$. Note that φ is a group homomorphism. An element $\alpha \in Ker(\varphi)$ if and only if $\alpha^t = 1$. Since $\gcd(t, p^n - 1) = s$, there exist s many elements, i.e., $|Ker(\varphi)| = s$. Hence, any non-zero element $c \in Im(\varphi)$, we have $\varphi^{-1}(c) = |\{x \in \mathbb{F}_{p^n} : \varphi(x) = c\}| = s$, which gives the required conclusion.

□

3. Almost Perfect Nonlinear Functions and the Walsh Spectrum

3.1 APN Functions

In this section, we first give the definition of the directional derivative which is needed to define the APN function and linear space of the function.

Definition 3.1. Let n and m be two positive integers and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a function. For any $a \in \mathbb{F}_{p^n}$, the (directional) derivative $D_aF : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ of F with respect to a is defined by

$$D_aF(x) = F(x+a) - F(x).$$

Theorem 3.1. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a function defined by*

$$F(x) = \sum_{0 \le i,j \le n} c_{ij} x^{p^i + p^j}, \quad c_{ij} \in \mathbb{F}_{p^n}.$$

Then we have the following.

$$D_aF(x) - F(a) = \sum_{i=1}^{n-1} c_{ij}(x^{p^i} a^{p^j} + a^{p^i} x^{p^j}) \quad \textit{for any } a \in \mathbb{F}^*_{p^n}$$

Proof. For any $a \in \mathbb{F}^*_{p^n}$, we obtain the following equalities.

$$\begin{aligned} D_aF(x) = F(x+a) - F(x) &= \sum_{0 \le i,j \le n} c_{ij}(x+a)^{p^i + p^j} - \sum_{0 \le i,j \le n} c_{ij} x^{p^i + p^j} \\ &= \sum_{0 \le i,j \le n} c_i (x+a)^{p^i} (x+a)^{p^j} - \sum_{0 \le i,j \le n} c_i x^{p^i + p^j} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{0\leq i,j\leq n} c_i(x^{p^i}+a^{p^i})(x^{p^j}+a^{p^j}) - \sum_{i=1}^{n-1} c_i x^{p^i+p^j} \\
&= \sum_{0\leq i,j\leq n} c_i(x^{p^i+p^j}+x^{p^i}a^{p^j}+a^{p^i}x^{p^j}+a^{p^i+p^j}) - \sum_{0\leq i,j\leq n} c_i x^{p^i+p^j} \\
&= \sum_{0\leq i,j\leq n} c_i(x^{p^i+p^j}+x^{p^i}a^{p^j}+a^{p^i}x^{p^j}+a^{p^i+p^j}-x^{p^i+p^j}) \\
&= \sum_{0\leq i,j\leq n} c_i(x^{p^i}a^{p^j}+a^{p^i}x^{p^j}+a^{p^i+p^j}) \\
&= \sum_{0\leq i,j\leq n} c_i(x^{p^i}a^{p^j}+a^{p^i}x^{p^j}) + \sum_{0\leq i,j\leq n} c_i a^{p^i+p^j} \\
&= \sum_{0\leq i,j\leq n} c_i(x^{p^i}a^{p^j}+a^{p^i}x^{p^j}) + F(a).
\end{aligned}
$$

Therefore, we conclude the following.

$$D_aF(x) - F(a) = \sum_{i=1}^{n-1} c_i(x^{p^i}a + a^{p^i}x).$$

□

Remark 3.1. By Theorem 3.1, we observe that if $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is a quadratic function, $D_aF(x) - F(a)$ is a linear function, see Definition 3.12.

Theorem 3.2. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. We define*

$$\wedge(f) := \{a \in \mathbb{F}_{p^n} : D_af(x) = f(x+a) - f(x) = c, \textit{ for some fixed } c \in \mathbb{F}_p\}.$$

That is, $\wedge(f)$ is a set consisting of $a \in \mathbb{F}_{p^n}$ for which $D_af(x)$ is a constant function. Then $\wedge(f)$ is a linear space.

Proof. Firstly, for $a = 0$, we have $D_af(x) = f(x) - f(x) = 0$. Then $0 \in \wedge(f)$.
Now, we will show that, if $a, b \in \wedge(f)$, then $a + \lambda b$ is also in $\wedge(f)$ for any $\lambda \in \mathbb{F}_p$. We have $a + \lambda b \in \wedge(f)$ if and only if $f(x + a + \lambda b) - f(x) = c$ for some $c \in \mathbb{F}_p$.
Firstly, we have the following equalities.

$$f(x+a+\lambda b) - f(x) = f(x+a+\lambda b) - f(x+\lambda b) + f(x+\lambda b) - f(x)$$

Set $y = x + \lambda b$, then we have

$$f(x+a+\lambda b) - f(x+\lambda b) + f(x+\lambda b) - f(x) = f(y+a) - f(y) + f(x+\lambda b) - f(x).$$

Since $a \in \wedge(f)$, we have $f(y+a) - f(y)$ is constant for all $y \in \mathbb{F}_{p^n}$. Say $f(y+a) -$

$f(y) = c$ for some $c \in \mathbb{F}_p$. Moreover, we have the following equalities.

$$\begin{aligned} f(x+\lambda b) - f(x) &= f(x+\lambda b) - \sum_{i=1}^{\lambda-1} f(x+(\lambda-i)b) + \sum_{i=1}^{\lambda-1} f(x+(\lambda-i)b) - f(x) \\ &= \sum_{i=1}^{\lambda} f(x+(\lambda-i)b+b) - \sum_{i=1}^{\lambda} f(x+(\lambda-i)b) \end{aligned}$$

Set $x_i = x+(\lambda-i)b$ for $i = 1,\dots,\lambda$. Then we have

$$f(x+\lambda b) - f(x) = \sum_{i=1}^{\lambda} f(x_i+b) - \sum_{i=1}^{\lambda} f(x_i) = \sum_{i=1}^{\lambda} f(x_i+b) - f(x_i).$$

Since $b \in \wedge(f)$, we have $f(x_i+b) - f(x_i)$ is constant for all $i = 1,\dots,\lambda$, say $f(x_i+b) - f(x_i) = c_i$. This means that $f(x+\lambda b) - f(x)$ is constant, namely $f(x+\lambda b) - f(x) = \sum\limits_{i=1}^{\lambda} c_i$. Then we have the following.

$$f(x+a+\lambda b) - f(x) = f(y+a) - f(y) + f(x+\lambda b) - f(x) = c + \sum_{i=1}^{\lambda} c_i$$

This means that $f(x+a+\lambda b) - f(x)$ is constant. Therefore, $a+\lambda b$ is in $\wedge(f)$. Hence, $\wedge(f)$ is a linear space. □

Now, we will make some observations on the derivative function and then give the definition of the almost perfect nonlinear function.

Remark 3.2. Consider the derivative $D_aF : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ of F with respect to $a \in \mathbb{F}_{2^n}$. Let x_0 be a solution of $D_aF(x) = b$ where $b \in \mathbb{F}_{2^n}$. Set $y_0 = x_0 + a$. Then we have the following equalities.

$$\begin{aligned} D_aF(y_0) = D_aF(x_0+a) &= F(x_0+a+a) + F(x_0+a) \\ &= F(x_0) + F(x_0+a) = D_aF(x_0) = b \end{aligned}$$

Hence, we obtain that $y_0 = x_0 + a$ is also a solution of $D_aF(x) = b$.

Remark 3.3. Let $\{x_0, x_1, x_2\}$ be the set of solutions of $D_aF(x) = b$ for $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. Assume that x_0, x_1, x_2 are distinct. Since x_0 is a solution of $D_aF(x) = b$, then $x_0 + a$ is also a solution by Remark 3.2, i.e., $x_0 + a \in \{x_0, x_1, x_2\}$. Without loss of generality, say $x_1 = x_0 + a$. Moreover, since x_2 is a solution of $D_aF(x) = b$, the element $x_2 + a$ is also a solution. Then either $x_2 + a = x_0$ or $x_2 + a = x_1$. If $x_2 + a = x_0$, then $x_2 = x_0 + a = x_1$, which is impossible since x_1 and x_2 are distinct. Hence, $x_2 + a = x_1$. However, this implies that $x_2 = x_1 + a = x_0 + a + a = x_0$, which is also a contradiction. Hence, the inverse image of b under $D_aF(x)$ is disjoint union of sets $\{x, x+a\}$ for $x \in \mathbb{F}_{2^n}$.

Definition 3.2. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function. If for any $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$,

$$D_a F(x) = F(x+a) + F(x) = b$$

has 0 or 2 solutions, then F is APN.

Corollary 3.1. Let F be any function on $\mathbb{F}_{2^n}$. Then F is APN if and only if for any nonzero $a \in \mathbb{F}_{2^n}$, the set $\{D_a F(x) : x \in \mathbb{F}_{2^n}\}$ has cardinality 2^{n-1}.

Proof. By Remark 3.3, the cardinality of the preimage of $D_a F(x)$ is the distinct union of the sets with two elements. We know that F is APN if and only if $D_a F(x) = b$ has 0 or 2 solutions for all $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. Then for every $b \in \mathbb{F}_{2^n}$, there are at most two solutions x_b, $x_b + a$ of $D_a F(x) = b$. That is, for every element of the image $Im(D_a F(x))$ of $D_a F(x)$, there are exactly two elements x_b, $x_b + a$ such that $D_a F(x_b) + D_a F(x_b + a) = b$. Hence, F is APN if and only if $|\{D_a F(x), x \in \mathbb{F}_{2^n}\}| = 2^{n-1}$. □

Now, we will give the characterization of APN functions stated in Janwa & Wilson (1993).

Theorem 3.3 (Janwa-Wilson-Rodier Theorem). *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function. F is APN if and only if the following holds:*

$$F(x) + F(y) + F(z) + F(x+y+z) = 0 \textit{ if and only if } x = y \textit{ or } x = z \textit{ or } y = z.$$

Proof. Note that if $x = y$, we have

$$F(x) + F(y) + F(z) + F(x+y+z) = F(x) + F(x) + F(z) + F(z) = 0$$

since characteristic is 2. Similarly, if $x = z$ or $y = z$, we have

$$F(x) + F(y) + F(z) + F(x+y+z) = 0.$$

Suppose that there exist pairwise distinct $x, y, z \in \mathbb{F}_{2^n}$ satisfying

$$F(x) + F(y) + F(z) + F(x+y+z) = 0. \tag{3.1}$$

Now, we will show that F is not APN. As $x \neq y$, we have $y = x + a$ for some $a \in \mathbb{F}_{2^n}^*$.

Then Equation 3.1 implies that $F(x)+F(x+a)+F(z)+F(z+a)=0$. That is,

$$D_aF(x) = D_aF(z) = b \text{ for some } b \in \mathbb{F}_{2^n}.$$

Then the elements x, $x+a$, z, $z+a$ lie in the inverse image of b under D_aF. By our assumption, we have $x \neq x+a = y$ and $x \neq z$, i.e., the inverse image of $b \in \mathbb{F}_{2^n}$ contains at least 3 distinct elements of $\mathbb{F}_{2^n}$. Hence, we have a contradiction by the definition of APN.

□

3.2 Walsh Spectrum and Nonlinearity

In this section, we will give the Walsh spectrum and the nonlinearity of the function. We need the definition of the components of the vectorial function to define the Walsh spectrum of the function.

Definition 3.3. Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a function. For $\lambda \in \mathbb{F}_{p^m}^*$, a function $f_\lambda : \mathbb{F}_{p^n} \to \mathbb{F}_p$ defined by

$$f_\lambda(x) = Tr_n(\lambda F(x))$$

is called the components of F corresponding to λ.

Definition 3.4. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a function and ε_p be a primitive p-th root of unity in $\mathbb{C}$. For any $a \in \mathbb{F}_{p^n}$, we define $W_f : \mathbb{F}_{p^n} \to \mathbb{C}$ by

$$W_f(a) = \sum_{x \in \mathbb{F}_{p^n}} \varepsilon_p^{f(x)-Tr_n(ax)}.$$

W_f is called the Walsh (Fourier) transform of f, and $W_f(a)$ is called the Walsh coefficient of f at a. The Walsh spectrum of f is the multiset defined by

$$\{|W_f(a)| : a \in \mathbb{F}_{p^n}\}.$$

Remark 3.4. If $p = 2$, then $\varepsilon_p = -1$. Hence, $W_f(a)$ is an integer for all $a \in \mathbb{F}_{2^n}$.

Lemma 3.1. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a function. The function f is balanced if and only if $W_f(0) = 0$.

Proof. By definition of W_f, we have

$$W_f(0) = \sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)+Tr_n(0)} = \sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)}.$$

For $\beta \in \mathbb{F}_p$, set $c_\beta = |\{x \in \mathbb{F}_{p^n} : f(x) = \beta\}|$. Then we can write the following:

$$W_f(0) = \sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)} = \sum_{\beta\in\mathbb{F}_{p^n}} c_\beta\, \varepsilon_p^{\beta}.$$

Suppose that f is a balanced function. By definition of balancedness, each $\beta \in \mathbb{F}_p$ has the same number inverse image, i.e., $c_\beta = p^{n-1}$. Then we have the following equalities.

$$\begin{aligned} W_f(0) = \sum_{\beta\in\mathbb{F}_p} p^{n-1}\varepsilon_p^{\beta} &= p^{n-1}\varepsilon_p^0 + p^{n-1}\varepsilon_p^1 + \cdots + p^{n-1}\varepsilon_p^{p-1} \\ &= p^{n-1}(\varepsilon_p^0 + \varepsilon_p^1 + \cdots + \varepsilon_p^{p-1}) \end{aligned}$$

Since ε_p be a primitive p-th root of unity, the minimal polynomial of ε_p is $\varphi(x) = 1 + x + \cdots + x^{p-1}$, i.e., $1 + \varepsilon_p^1 + \varepsilon_p^2 + \cdots + \varepsilon_p^{p-1} = 0$. Therefore,

$$W_f(0) = \sum_{\beta\in\mathbb{F}_p} p^{n-1}\varepsilon_p^{\beta} = 0.$$

Conversely, suppose that $W_f(0) = 0$. Then ε_p is a root of the polynomial $g(x) = c_0 + c_1x + \cdots + c_{p-1}x^{p-1} \in \mathbb{Z}[x]$. Therefore, $g(\varepsilon_p) = 0$ if and only if $\varphi(x)$ divides $g(x)$. Then $g(x) = f(x)\varphi(x)$ for $f(x) \in \mathbb{Z}[x]$. Since $g(x)$ and $\varphi(x)$ have the same degree, $f(x)$ is constant. This means that $g(x) = \alpha\varphi(x)$ for some $\alpha \in \mathbb{Z}$, i.e., $c_0 = c_1 = \cdots = c_{p-1}$. Hence, f is balanced. □

Definition 3.5. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a function. The nonlinearity $\mathcal{N}(f)$ of f is defined by

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

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function and let $f_\lambda : \mathbb{F}_{2^n} \to \mathbb{F}_2$, $\lambda \in \mathbb{F}_{2^n}^*$, denote its components such that $f_\lambda(x) = Tr_n(\lambda F(x))$. The nonlinearity of F is defined by

$$\mathcal{N}(F) = 2^{n-1} - \frac{1}{2}\mathcal{L}(F) \text{ where } \mathcal{L}(F) = \max_{\lambda\in\mathbb{F}_{2^n}^*} \mathcal{L}(f_\lambda) = \max_{\substack{\lambda\in\mathbb{F}_{2^n}^* \\ a\in\mathbb{F}_{2^n}}} |W_{f_\lambda}(a)|.$$

Definition 3.6. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function. If $\mathcal{L}(F) = 2^{\frac{n+1}{2}}$, then F is said to be almost bent (AB). That is, F is AB if and only if $|W_{f_\lambda}(a)| \in \{0, 2^{\frac{n+1}{2}}\}$ for any $a \in \mathbb{F}_{2^n}$ and $\lambda \in \mathbb{F}_{2^n}^*$.

Note that AB functions exist when n is odd only.

Definition 3.7. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a function.

(i) If $|W_f(a)| = p^{n/2}$ for all $a \in \mathbb{F}_{p^n}$, then f is called bent.

(ii) If $|W_f(a)| \in \{0, p^{\frac{n+k}{2}}\}$ for all $a \in \mathbb{F}_{p^n}$ and some non-negative integer k with $0 \leq k \leq n$, then f is called plateaued (k-plateaued).

(iii) For $p > 2$, the function f is called semibent if $k = 1$.

(iv) For $p = 2$, we observed in Remark 3.4 that Walsh coefficients should be integers. Hence for $p = 2$, the function is called semibent if $k = 1$ in the case that n is odd, and $k = 2$ in the case that n is even.

Definition 3.8. If a vectorial Boolean function has only bent and semibent components, then we say that the function has the classical spectrum.

Note that bent functions achieve the upper bound on nonlinearity. Now, we give a characterization of bent functions in terms of the directional derivative of the function. For this, we continue with the definition of the Hadamard matrix and useful lemma.

Definition 3.9. Let $H = (h_{ij})_{1 \leq i,j \leq k}$ where $h_{ij} \in \mathbb{C}$. Then $H^* = (\overline{h_{ji}})_{1 \leq i,j \leq k}$ is called an Hermitian transpose of H where $\overline{h_{ij}}$ is the complex conjugate of h_{ij}.

Definition 3.10. Let H be the matrix of size $k \times k$. H is called a complex Hadamard matrix if $HH^* = kI_k$.

Remark: If H is a Hadamard matrix, then H is invertible.

Consider $H = (h_{u,z})_{u,z \in \mathbb{F}_{2^n}}$ such that $h_{u,z} = \varepsilon_p^{Tr_n(uz)}$.
Claim: H is a complex Hadamard matrix.

Proof. Let Ru_1 and Ru_2 be the rows of H corresponding to $u_1, u_2 \in \mathbb{F}_{p^n}$, respectively. Then u_1, u_2 entry of HH^* is given by

$$Ru_1.Ru_2 = \sum_{z \in \mathbb{F}_{p^n}} \varepsilon_p^{Tr_n(u_1 z)} \varepsilon_p^{-Tr_n(u_2 z)} = \sum_{z \in \mathbb{F}_{p^n}} \varepsilon^{Tr_n((u_1 - u_2)z)}$$
$$= \begin{cases} p^n, & \text{if } u_1 = u_2; \\ 0, & \text{otherwise} \end{cases}$$

by Theorem 2.7. That is, $HH^* = p^n I$. Hence, H is a complex Hadamard matrix. □

Lemma 3.2. Let $h : \mathbb{F}_{p^n} \to \mathbb{R}$ be a function. Then

$$\psi(u) = \sum_{z\in\mathbb{F}_{p^n}} h(z)\varepsilon_p^{Tr_n(uz)} = h(0) \text{ for all } u \in \mathbb{F}_{p^n}$$

if and only if $h(z) = 0$ for all $z \in \mathbb{F}_{p^n} \setminus \{0\}$.

Proof. Suppose that

$$\psi(u) = \sum_{z\in\mathbb{F}_{p^n}} h(z)\varepsilon_p^{Tr_n(uz)} = h(0)$$

for all $u \in \mathbb{F}_{p^n}$. This implies that

$$\sum_{\substack{z\in\mathbb{F}_{p^n}\\ z\neq 0}} h(z)\varepsilon_p^{Tr_n(uz)} = 0 \tag{3.2}$$

for all $u \in \mathbb{F}_{p^n}$. Note that Equation 3.2 gives a linear combination of the columns of H, and this contradicts the invertibility of H. Hence $h(z) = 0$ for all $z \in \mathbb{F}_{p^n}\backslash\{0\}$. The converse of the statement is straightforward. □

Theorem 3.4. *A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is bent if and only if $D_a f(x) = f(x+a) - f(x)$ is balanced for all $a \in \mathbb{F}_{p^n}^*$.*

Proof. By definition, $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is bent if and only if $|W_f(u)| = p^{n/2}$. Note that

$$|W_f(u)|^2 = (\sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)-Tr_n(ux)})(\sum_{y\in\mathbb{F}_{2^n}} \varepsilon_p^{-f(y)+Tr_n(uy)}) = \sum_{x,y\in\mathbb{F}_{2^n}} \varepsilon_p^{f(x)-f(y)+Tr_n(u(y-x))}.$$

Set $y = x+a$, i.e., $a = y-x$. Then we have the following equalities.

$$|W_f(u)|^2 = \sum_{x,a\in\mathbb{F}_{2^n}} \varepsilon_p^{f(x)-f(x+a)+Tr_n(ua)} = \sum_{a\in\mathbb{F}_{2^n}} \varepsilon_p^{Tr_n(ua)} \sum_{x\in\mathbb{F}_{2^n}} \varepsilon_p^{f(x)-f(x+a)} \tag{3.3}$$

Suppose that $D_a f = f(x+a) - f(x)$ is balanced for all $a \in \mathbb{F}_{p^n}^*$, then

$$W_{D_a f}(0) = \sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)-f(x+a)} = 0$$

by Lemma 3.1. If $a = 0$, we have

$$\sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)-f(x)} = \sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^0 = \sum_{x\in\mathbb{F}_{p^n}} 1 = p^n.$$

Then we have

$$|W_f(u)|^2 = p^n + \sum_{a\in\mathbb{F}_{p^n}^*} \varepsilon_p^{Tr_n(ua)} \sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)-f(x+a)} = p^n.$$

Therefore, f is bent by definition. Conversely, suppose that f is bent, i.e., $|W_f(u)|^2 = p^n$. Set

$$h(a) = \sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)-f(x+a)}.$$

Note that

$$h(0) = \sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^0 = p^n.$$

Then by the Equation 3.3, we have the following.

$$|W_f(u)|^2 = \sum_{a\in\mathbb{F}_{p^n}} h(a)\varepsilon_p^{Tr_n(ua)} = p^n = h(0)$$

Then by Lemma 3.2, we have $h(a) = 0$ for all $a \in \mathbb{F}_{p^n} \setminus \{0\}$. That is,

$$\sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)-f(x+a)} = 0.$$

This holds if and only if $f(x) - f(x+a)$ is balanced. □

Theorem 3.5 (Perseval's Identity). *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a function. Then*

$$\sum_{u\in\mathbb{F}_{p^n}} |W_f(u)|^2 = p^{2n}$$

Proof. Let ε_p be primitive p-th root of unity. Note that the following equalities for $|W_f(u)|^2$ hold.

$$\begin{aligned}\sum_{u\in\mathbb{F}_{p^n}} |W_f(u)|^2 &= \sum_{u\in\mathbb{F}_{p^n}} \left(\sum_{x\in\mathbb{F}_{p^n}} {\varepsilon_p}^{f(x)-Tr_n(ux)}\right)\left(\sum_{y\in\mathbb{F}_{p^n}} {\varepsilon_p}^{-f(y)+Tr_n(uy)}\right) \\ &= \sum_{x,y\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)-f(y)} \sum_{u\in\mathbb{F}_{p^n}} {\varepsilon_p}^{Tr_n(u(y-x))}.\end{aligned}$$

Set $z = y - x$, i.e., $y = x + z$. Then we have

$$\sum_{u\in\mathbb{F}_{p^n}} |W_f(u)|^2 = \sum_{x,z\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)-f(x+z)} \sum_{u\in\mathbb{F}_{p^n}} {\varepsilon_p}^{Tr_n(uz)}$$

$$
\begin{aligned}
&= \sum_{\substack{x,z\in\mathbb{F}_{p^n}\\ z\neq 0}} \varepsilon_p^{f(x)-f(x+z)} \sum_{u\in\mathbb{F}_{p^n}} \varepsilon_p{}^{Tr_n(uz)} + \sum_{x\in\mathbb{F}_{p^n}} \varepsilon_p^{f(x)-f(x)} \sum_{u\in\mathbb{F}_{p^n}} \varepsilon_p{}^{0}\\
&= 0 + p^n p^n = p^{2n}
\end{aligned}
$$

by Theorem 2.7. □

Lemma 3.3. Let $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ is a k-plateaued function. Then the number of $a\in\mathbb{F}_{p^n}$ satisfying $|W_f(a)| = p^{\frac{n+k}{2}}$ is equal to p^{n-k}.

Proof. Set $S=\{a\in\mathbb{F}_{p^n} : |W_f(a)| = p^{\frac{n+k}{2}}\}$. By Parseval's identity, we have the following equations.

$$p^{2n} = \sum_{a\in\mathbb{F}_{p^n}} |W_f(a)|^2 = \sum_{a\in S} (p^{\frac{n+k}{2}})^2 = |S|.p^{n+k}$$

That is, $|S| = \frac{p^{2n}}{p^{n+k}} = p^{n-k}$. □

3.3 Characterization of APN Functions over Odd Dimensional Spaces

We give the characterization of APN functions in the case n odd by using the Sidelnikov-Chabaud-Vaudenay bound, see Sidelnikov (1971) and Chabaud & Vaudenay (1994).

Theorem 3.6 (The Sidelnikov-Chabaud-Vaudenay bound)**.** *Let F be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ with $m\geq n-1$, then*

$$\mathcal{N}(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{3.2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}.$$

Proof. Let $f_\lambda:\mathbb{F}_{2^n}\to\mathbb{F}_2$ be the component of F such that $f_\lambda(x) = Tr_n(\lambda F(x))$ for nonzero $\lambda\in\mathbb{F}_{2^m}$. By Perseval's identity,

$$\sum_{b\in\mathbb{F}_{2^n}} W_{f_\lambda}{}^2(b)| = 2^{2n}.$$

By Definition 2.1.5, we have $\mathcal{N}(F) = 2^{n-1} - \frac{1}{2}\mathcal{L}(F)$ where $\mathcal{L}(F) = \max\limits_{\lambda\in\mathbb{F}^*_{2^m}} \mathcal{L}(f_\lambda)$ and

$\mathcal{L}(f_\lambda) = \max\limits_{b \in \mathbb{F}_{2^n}} |W_{f_\lambda}(b)|$. Therefore, our target is to estimate:

$$\max_{\substack{\lambda \in \mathbb{F}_{2^m}^* \\ b \in \mathbb{F}_{2^n}}} |W_{f_\lambda}(b)| = \max_{\substack{\lambda \in \mathbb{F}_{2^m}^* \\ b \in \mathbb{F}_{2^n}}} |\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(x) + Tr_n(bx)}|.$$

Set

$$A = \max_{\substack{\lambda \in \mathbb{F}_{2^m}^* \\ b \in \mathbb{F}_{2^n}}} \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(x) + Tr_n(bx)} \right)^2,$$

$$C = \sum_{\substack{\lambda \in \mathbb{F}_{2^m}^* \\ b \in \mathbb{F}_{2^n}}} \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(x) + Tr_n(bx)} \right)^2, and$$

$$B = \sum_{\substack{\lambda \in \mathbb{F}_{2^m}^* \\ b \in \mathbb{F}_{2^n}}} \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(x) + Tr_n(bx)} \right)^4.$$

Then we have $AC \geq B$. That is, $A \geq \frac{B}{C}$. In other words,

$$\max_{\substack{\lambda \in \mathbb{F}_{2^m}^* \\ b \in \mathbb{F}_{2^n}}} W_{f_a}(b)^2 \geq \frac{\sum\limits_{\substack{\lambda \in \mathbb{F}_{2^m}^* \\ b \in \mathbb{F}_{2^n}}} W_{f_a}(b)^4}{\sum\limits_{\substack{\lambda \in \mathbb{F}_{2^m}^* \\ b \in \mathbb{F}_{2^n}}} W_{f_a}(b)^2}$$

Set $B' = \sum\limits_{\substack{\lambda \in \mathbb{F}_{2^m} \\ b \in \mathbb{F}_{2^n}}} \left(\sum\limits_{x \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(x) + Tr_n(bx)} \right)^4$. Note that $B = B' - 2^{4n}$. Now, we estimate B'.

$$\begin{aligned} B' &= \sum_{\substack{\lambda \in \mathbb{F}_{2^m} \\ b \in \mathbb{F}_{2^n}}} \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(x) + Tr_n(bx)} \right)^4 \\ &= \sum_{\substack{\lambda \in \mathbb{F}_{2^m} \\ b \in \mathbb{F}_{2^n}}} \sum_{x,y,z,t \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(x) + f_\lambda(y) + f_\lambda(z) + f_\lambda(t) + Tr_n(b(x+y+z+t))} \\ &= \sum_{x,y,z,t \in \mathbb{F}_{2^n}} \sum_{\lambda \in \mathbb{F}_{2^m}} (-1)^{Tr_m(\lambda(F(x)+F(y)+F(z)+F(t))} \sum_{b \in \mathbb{F}_{2^n}} (-1)^{Tr_n(b(x+y+z+t)))} \end{aligned}$$

By Theorem 2.7, we have the following equalities.

$$\sum_{\lambda\in\mathbb{F}_{2^m}}(-1)^{Tr_m(\lambda(F(x)+F(y)+F(z)+F(t))}=\begin{cases} 2^m, & \text{if } F(x)+F(y)+F(z)+F(t)=0;\\ 0, & \text{otherwise.}\end{cases}$$

$$\sum_{b\in\mathbb{F}_{2^n}}(-1)^{Tr_n(b(x+y+z+t))}=\begin{cases} 2^n, & \text{if } x+y+z+t=0;\\ 0, & \text{otherwise.}\end{cases}$$

Then we conclude the following.

$$B'=2^{n+m}|\{(x,y,z,t)\in(\mathbb{F}_{2^n})^4 : x+y+z+t=0 \text{ and } F(x)+F(y)+F(z)+F(t)=0\}|$$

Set $t=x+y+z$. Then we have the following.

$$\begin{aligned}B'&=2^{n+m}|\{(x,y,z)\in(\mathbb{F}_{2^n})^3 : F(x)+F(y)+F(z)+F(x+y+z)=0\}|\\ &\geq 2^{n+m}|\{(x,y,z)\in(\mathbb{F}_{2^n})^3 : x=y \text{ or } x=z \text{ or } y=z\}| \qquad (3.4)\\ &=2^{n+m}\left(3|\{(x,x,y) : x,y\in\mathbb{F}_{2^n}\}|-2|\{(x,x,x)\} : x\in\mathbb{F}_{2^n}\}|\right)\\ &=2^{n+m}(3.2^{2n}-2.2^n)\end{aligned}$$

Hence, we obtain $B=B'-2^{4n}\geq 2^{n+m}(3.2^{2n}-2.2^n)-2^{4n}$. Then we can write the following inequality.

$$A=\max_{\substack{\lambda\in\mathbb{F}^*_{2^m}\\ b\in\mathbb{F}_{2^n}}}W_{f_\lambda}(b)^2\geq\frac{2^{n+m}(3.2^{2n}-2.2^n)-2^{4n}}{\sum\limits_{\substack{\lambda\in\mathbb{F}^*_{2^m}\\ b\in\mathbb{F}_{2^n}}}W_{f_\lambda}(b)^2}$$

But by Parseval's identity, for $\lambda\in\mathbb{F}^*_{2^m}$, we have

$$\sum_{b\in\mathbb{F}_{2^n}}W_{f_\lambda}(b)^2=2^{2n}.$$

Hence, we obtain

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

Hence

$$\begin{aligned}A&\geq\frac{2^{n+m}(3.2^{2n}-2.2^n)-2^{4n}}{(2^m-1)2^{2n}}=\frac{2^m(2^n3-2)-2^{2n}}{2^m-1} \qquad (3.5)\\ &=\frac{3.2^n.2^m-2^{m+1}-2^{2n}}{2^m-1}=3.2^n-2-2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1},\end{aligned}$$

which gives the desired inequality. □

Corollary 3.2. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function. Then

$$\max_{\substack{\lambda \in \mathbb{F}_{2^m}^* \\ b \in \mathbb{F}_{2^n}}} |W_{f_\lambda}(b)| \geq 2^{\frac{n+1}{2}}.$$

Proof. By Equation (3.5), we have

$$A \geq 3.2^n - 2 - 2(2^{n-1} - 1) = 3.2^n - 2 - 2^n + 2 = 2^{n+1}.$$

That is, $\max\limits_{\substack{\lambda \in \mathbb{F}_{2^n}^* \\ b \in \mathbb{F}_{2^n}}} |W_{f_a}(b)| \geq 2^{\frac{n+1}{2}}$. □

Corollary 3.3. Let n be an odd integer. Then f_λ is semibent for all nonzero $\lambda \in \mathbb{F}_{2^n}$ if and only if $\max\limits_{\substack{\lambda \in \mathbb{F}_{2^n}^* \\ b \in \mathbb{F}_{2^n}}} |W_{f_a}(b)| = 2^{\frac{n+1}{2}}$. That means equality holds in Equation 3.4, i.e., F is APN. Hence, for n odd, F is AB if and only if F is APN.

By Corollary 3.3, we know that in the case n odd, a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if and only if F is almost bent. From now on, we consider the case n even while working on APN functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

3.4 Sum-of-square Indicator

The sum-of-square indicator that is related to the Walsh spectrum is introduced in Zhang & Zheng (1996). In this section, we will give the definition and some related theorems of sum-of-square indicator which are needed to characterize APN functions in the following sections.

Definition 3.11. Let f be a Boolean function on $\mathbb{F}_{2^n}$. Then the sum-of-square indicator is defined by

$$v(f) = \sum_{a \in \mathbb{F}_{2^n}} {W_{D_a f}}^2(0).$$

Theorem 3.7. *Let f be a Boolean function on $\mathbb{F}_{2^n}$. Then*

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

Proof. We have the following equations.

$$\sum_{a\in\mathbb{F}_{2^n}} {W_f}^4(a) = \sum_{a\in\mathbb{F}_{2^n}} \left(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+Tr_n(ax)}\right) \times \left(\sum_{y\in\mathbb{F}_{2^n}} (-1)^{f(y)+Tr_n(ay)}\right)$$

$$\times \left(\sum_{z\in\mathbb{F}_{2^n}} (-1)^{f(z)+Tr_n(az)}\right) \times \left(\sum_{t\in\mathbb{F}_{2^n}} (-1)^{f(t)+Tr_n(at)}\right)$$

$$= \sum_{a\in\mathbb{F}_{2^n}} \left(\sum_{x,y,z,t\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(y)+f(z)+f(t)+Tr_n(a(x+y+z+t))}\right)$$

$$= \sum_{x,y,z,t\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(y)+f(z)+f(t)} \sum_{a\in\mathbb{F}_{2^n}} (-1)^{Tr_n(a(x+y+z+t))}.$$

Set $c = x+y+z+t$. If $c \neq 0$, then

$$\sum_{a\in\mathbb{F}_{2^n}} (-1)^{Tr_n(a(x+y+z+t))} = \sum_{a\in\mathbb{F}_{2^n}} (-1)^{Tr_n(ac)} = 0$$

by Theorem 2.7. If $c = x+y+z+t = 0$, then set $t = x+y+z$. Then we have

$$\sum_{a\in\mathbb{F}_{2^n}} {W_f}^4(a) = 2^n \sum_{x,y,z\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(y)+f(z)+f(x+y+z)} \text{ , by Theorem 2.7 .}$$

Set $y = x+b$, then we have the following equalities.

$$\sum_{a\in\mathbb{F}_{2^n}} {W_f}^4(a) = 2^n \sum_{x,z,b\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(x+b)+f(z)+f(z+b)}$$

$$= 2^n \sum_{b\in F_{2^n}} \left(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(x+b)}\right)\left(\sum_{z\in\mathbb{F}_{2^n}} (-1)^{f(z)+f(z+b)}\right)$$

$$= 2^n \sum_{b\in\mathbb{F}_{2^n}} {W_{D_bf}}^2(0) = 2^n \sum_{a\in\mathbb{F}_{2^n}} {W_{D_af}}^2(0)$$

□

The following lemma states the relation between the plateaued level and the sum-of-square indicator of the Boolean function.

Lemma 3.4. If $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is k-plateaued, then $v(f) = 2^{2n+k}$.

Proof. Since f is k-plateaued, $|W_f(a)| \in \{0, 2^{\frac{n+k}{2}}\}$. Then we have the following equalities by Theorem 3.7 and Lemma 3.3.

$$v(f) = 2^{-n} \sum_{a \in \mathbb{F}_{2^n}} {W_f}^4(a) = 2^{-n}.2^{n-k}.(2^{\frac{n+k}{2}})^4$$
$$= 2^{-n}.2^{n-k}.2^{2n+2k} = 2^{2n+k}$$

□

3.5 Quadratic Functions

In this section, we will give the definition of quadratic functions and the Walsh spectrum in terms of the dimension of its linear space.

Definition 3.12. Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a function defined by $F(x) = x^d$ for an integer d with $0 \leq d \leq p^n - 1$. We can write d in a unique way such that $d = d_0 + d_1 p + \cdots + d_{n-1} p^{n-1}$ where $0 \leq d_i \leq p-1$ for all $i = 1, \ldots, n$. Then the algebraic degree of F, which we call simply the degree of F, is defined by $deg(F) = \sum_{i=0}^{n-1} d_i$.

Let $F(x) = \sum_{t=0}^{n} c_t x^t$. Then $deg(F(x)) = max\{deg(x^t) : c_t \neq 0\}$.
Note that linear and affine functions are degree 1, and functions of (algebraic) degree 2 are called quadratic.

Recall 3.1. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Recall that by Theorem 3.2,

$$\wedge(f) = \{a \in \mathbb{F}_{p^n} : D_a f(x) = f(x+a) - f(x) = c, \text{ for some fixed } c \in \mathbb{F}_p\}.$$

Note that $f(x+a) - f(x)$ is a constant function if and only if $f(x+a) - f(x) - f(a)$ is a constant function. Then we can write

$$\wedge(f) = \{a \in \mathbb{F}_{p^n} : f(x+a) - f(x) - f(a) \text{ is a constant function}\}.$$

In the case $f(0) = 0$, we observe that if $x = 0$ or $a \in \wedge(f)$, then

$$f(x+a) - f(x) - f(a) = 0.$$

Hence,

$$\wedge(f) = \{a \in \mathbb{F}_{p^n} : f(x+a) - f(x) - f(a) = 0\}.$$

Lemma 3.5. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a function such that $f(0) = 0$. Then $g(z) = f(z) - Tr_n(\beta z)$ is a linear function on $\wedge(f)$ for any $\beta \in \mathbb{F}_{p^n}$.

Proof. We need to show that $g(z_1 + z_2) = g(z_1) + g(z_2)$ for any $z_1, z_2 \in \wedge(f)$. Note that $f(z_1+z_2) - f(z_1) - f(z_2) = 0$ since $z_2 \in \wedge(f)$. That is, $f(z_1+z_2) = f(z_1)+f(z_2)$. Then we have the following equalities.

$$\begin{aligned} g(z_1+z_2) &= f(z_1+z_2) - Tr_n(\beta(z_1+z_2)) \\ &= f(z_1) + f(z_2) - Tr_n(\beta z_1) - Tr_n(\beta z_2) \\ &= f(z_1) - Tr_n(\beta z_1) + f(z_2) - Tr_n(\beta z_2) \\ &= g(z_1) + g(z_2) \end{aligned}$$

Hence, $g(z)$ is a linear function on $\wedge(f)$. □

Now, we will give an important theorem that gives the Walsh spectrum of the function in terms of the dimension of its linear space. We will use this theorem to calculate the Walsh spectrum of the APN functions in the following sections.

Theorem 3.8. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a quadratic function with $f(0) = 0$. Then $|W_f(\beta)| \in \{0, p^{\frac{n+s}{2}}\}$ where s is a dimension of $\wedge(f)$.*

Proof. Note that

$$|W_f(\beta)|^2 = (\sum_{x \in \mathbb{F}_{p^n}} \varepsilon_p^{f(x) - Tr_n(\beta x)})(\sum_{y \in \mathbb{F}_{p^n}} \varepsilon_p^{-f(y) + Tr_n(\beta y)}) = \sum_{x,y \in \mathbb{F}_{p^n}} \varepsilon_p^{f(x) - f(y) - Tr_n(\beta(x-y))}.$$

Set $z = x - y$, i.e., $x = y + z$. Then we have the following equalities.

$$\begin{aligned} |W_f(\beta)|^2 &= \sum_{z,y \in \mathbb{F}_{p^n}} \varepsilon_p^{f(y+z) - f(y) - Tr_n(\beta z)} \\ &= \sum_{z \in \mathbb{F}_{p^n}} \varepsilon_p^{-Tr_n(\beta z)} \sum_{y \in \mathbb{F}_{p^n}} \varepsilon_p^{f(y+z) - f(y)} \\ &= \sum_{z \in \mathbb{F}_{p^n}} \varepsilon_p^{f(z) - Tr_n(\beta z)} \sum_{y \in \mathbb{F}_{p^n}} \varepsilon_p^{f(y+z) - f(y) - f(z)} \end{aligned}$$

Note that since f is a quadratic function, $f(y+z) - f(y) - f(z)$ is a linear function on $\mathbb{F}_{p^n}$, see Remark 3.1. We have the following by Theorem 2.7.

$$\sum_{y \in \mathbb{F}_{p^n}} \varepsilon_p^{f(y+z) - f(y) - f(z)} = \begin{cases} p^n, & \text{if } f(y+z) - f(y) - f(z) = 0; \\ 0, & \text{otherwise.} \end{cases}$$

This means that

$$\sum_{y\in\mathbb{F}_{p^n}} \varepsilon_p^{f(y+z)-f(y)-f(z)} = \begin{cases} p^n, & \text{if } z\in\wedge(f);\\ 0, & \text{otherwise.}\end{cases}$$

Therefore, we have

$$|W_f(\beta)|^2 = p^n \sum_{z\in\wedge(f)} \varepsilon_p^{f(z)-Tr_n(\beta z)}.$$

Since $f(z)-Tr_n(\beta z)$ is a linear function on $\wedge(f)$ and $|\wedge(f)| = p^s$ by Theorem 2.7:

$$\sum_{z\in\wedge(f)} \varepsilon_p^{f(z)-Tr_n(\beta z)} = \begin{cases} p^s, & \text{if } f(z)-Tr_n(\beta z)=0;\\ 0, & \text{otherwise.}\end{cases}$$

Hence,

$$|W_f(\beta)|^2 = \begin{cases} p^{n+s}, & \text{if } f(z)-Tr_n(\beta z)=0;\\ 0, & \text{otherwise.}\end{cases}.$$

Therefore, we have $|W_f(\beta)| \in \{0, p^{\frac{n+s}{2}}\}$. □

Now, we will give some theorems related to APN-ness in terms of the Walsh spectrum and the sum-of-square indicator.

Theorem 3.9. *Let $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be a quadratic function, and let $f_\lambda:\mathbb{F}_{2^n}\to\mathbb{F}_2, \lambda\in\mathbb{F}_{2^n}^*$, denote its component function such that $f_\lambda = Tr_n(\lambda F(x))$. Then for any $a\in\mathbb{F}_{2^n}^*$,*

$$\sum_{\lambda\in\mathbb{F}_{2^n}} W^2_{D_af_\lambda}(0) \geq 2^{2n+1}.$$

Moreover, F is APN if and only if for all nonzero $a\in\mathbb{F}_{2^n}$

$$\sum_{\lambda\in\mathbb{F}_{2^n}} W^2_{D_af_\lambda}(0) = 2^{2n+1}.$$

Proof. Note that $D_af_\lambda(x) = f_\lambda(x)+f_\lambda(x+a)$, then we have the following equalities.

$$\sum_{\lambda\in\mathbb{F}_{2^n}} W^2_{D_af_\lambda}(0) = \sum_{\lambda\in\mathbb{F}_{2^n}} \left(\sum_{x\in\mathbb{F}_{2^n}} (-1)^{f_\lambda(x)+f_\lambda(x+a)}\right)\left(\sum_{y\in\mathbb{F}_{2^n}} (-1)^{f_\lambda(y)+f_\lambda(y+a)}\right)$$

$$= \sum_{\lambda\in\mathbb{F}_{2^n}} \left(\sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{f_\lambda(x)+f_\lambda(x+a)+f_\lambda(y)+f_\lambda(y+a)}\right)$$

$$= \sum_{\lambda,x,y\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda(F(x)+F(x+a)+F(y)+F(y+a))}$$

$$= \sum_{x,y\in\mathbb{F}_{2^n}} \sum_{\lambda\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda(D_aF(x)+D_aF(y)))}$$

Note that, by Theorem 2.7,

$$\sum_{\lambda\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda(D_aF(x)+D_aF(y)))} = \begin{cases} 2^n, & \text{if } D_aF(x) = D_aF(y); \\ 0, & \text{if } D_aF(x) \neq D_aF(y). \end{cases}$$

Therefore,

$$\sum_{\lambda\in\mathbb{F}_{2^n}} W^2_{D_af_\lambda}(0) = 2^n \mid \{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} : D_aF(x) = D_aF(y)\} \mid .$$

For a given x, there exist 2 pairs (x,y) of the form $(x,x),(x,x+a)$ such that $D_aF(x) = D_aF(y)$. Then

$$(3.6) \quad \sum_{\lambda\in\mathbb{F}_{2^n}} W^2_{D_af_\lambda}(0) = 2^n2^n2 + 2^n\#\{(x,y) : D_aF(x) = D_aF(y), x \neq y, x \neq y+a\},$$

which means that

$$\sum_{\lambda\in\mathbb{F}_{2^n}} W^2_{D_af_\lambda}(0) \geq 2^{2n+1}.$$

Note that by Equation 3.6, $\sum_{\lambda\in\mathbb{F}_{2^n}} W^2_{D_af_\lambda}(0) = 2^{2n+1}$ if and only if the following holds:

$$D_aF(x) = D_aF(y) \text{ if and only if } x = y \text{ or } x = y+a.$$

In other words, $\sum_{\lambda\in\mathbb{F}_{2^n}} W^2_{D_af_\lambda}(0) = 2^{2n+1}$ if and only if F is APN by definition.

□

Before the following corollary, recall that for a Boolean function f on $\mathbb{F}_{2^n}$,

$$v(f) = \sum_{a\in\mathbb{F}_{2^n}} {W_{D_af}}^2(0).$$

Corollary 3.4. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function and let $f_\lambda : \mathbb{F}_{2^n} \to \mathbb{F}_2, \lambda \in \mathbb{F}_{2^n}$, denote its component function such that $f_\lambda = Tr_n(\lambda F(x))$. Then

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} v(f_\lambda) \geq (2^n - 1)2^{2n+1}.$$

Moreover, F is APN if and only if

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} v(f_\lambda) = (2^n - 1)2^{2n+1}. \tag{3.7}$$

Consequently, if $v(f_\lambda) = 2^{2n+1}$ for all nonzero λ, then F is APN.

Proof. Set

$$A = \sum_{a \in \mathbb{F}_{2^n}^*} \sum_{\lambda \in \mathbb{F}_{2^n}} W_{D_a f_\lambda}^2(0).$$

By Theorem 3.9, we have

$$\sum_{\lambda \in \mathbb{F}_{2^n}} W_{D_a f_\lambda}^2(0) \geq 2^{2n+1}.$$

Then $A \geq 2^{2n+1}(2^n - 1)$. Since $W_{D_0 f_\lambda}^2(0) = W_{D_a f_0}^2(0) = 2^n$ for any a and λ, we can write

$$A = \sum_{a \in \mathbb{F}_{2^n}^*} \sum_{\lambda \in \mathbb{F}_{2^n}} W_{D_a f_\lambda}^2(0) = \sum_{\lambda \in \mathbb{F}_{2^n}^*} \sum_{a \in \mathbb{F}_{2^n}} W_{D_a f_\lambda}^2(0) = \sum_{\lambda \in \mathbb{F}_{2^n}^*} v(f_\lambda). \tag{3.8}$$

Then we have

$$A = \sum_{\lambda \in \mathbb{F}_{2^n}^*} v(f_\lambda) \geq (2^n - 1)2^{2n+1},$$

which gives the first claim of the theorem. For the second part, by Theorem 3.9, F is APN if and only if for a nonzero $a \in \mathbb{F}_{2^n}$

$$\sum_{\lambda \in \mathbb{F}_{2^n}} W_{D_a f_\lambda}^2(0) = 2^{2n+1}.$$

Therefore, by Equation 3.8,

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

□

Corollary 3.5. Berger et al. (2005) Let n be even and let $f_\lambda : \mathbb{F}_{2^n} \to \mathbb{F}_2$, $\lambda \in \mathbb{F}_{2^n}^*$, be the component functions defined by $f_\lambda = Tr_n(\lambda F(x))$. Suppose that f_λ is plateaued for all $\lambda \in \mathbb{F}_{2^n}^*$. Let B be the number of f_λ, which are bent. Then we have the following.

(i) If $B = 0$, then F is not APN.

(ii) If F is APN, then $B \geq 2(2^n - 1)/3$ with equality if and only if $\mathcal{L}(F) = 2^{(n+2)/2}$. Conversely, if $B = 2(2^n - 1)/3$ and $\mathcal{L}(F) = 2^{(n+2)/2}$ then F is APN.

Proof. (i) Assume that there is no $\lambda \neq 0$ such that f_λ bent, i.e., $B = 0$. We know that $|W_{f_\lambda}(a)| = \{0, 2^{\frac{n+k}{2}}\}$ since f_λ is plateaued. Since f_λ is not bent for nonzero λ and n is even, $k \geq 2$. Let S be a number of a such that $|W_{f_\lambda}(a)| = 2^{\frac{n+k}{2}}$. Then by Lemma 3.3, $S = 2^{n-k}$. Moreover, $v(f_\lambda) = 2^{2n+k}$ by Lemma 3.4. Then $v(f_\lambda) = 2^{2n+k} \geq 2^{2n+2}$ since $k \geq 2$. This shows that

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} v(f_\lambda) \geq (2^n - 1)2^{2n+2}.$$

Therefore, F is not APN by Corollary 3.4.

(ii) Suppose that F is APN. Then there exists $\lambda \in \mathbb{F}_{2^n}^*$ such that f_λ is bent by (i), i.e., $|W_{f_\lambda}(a)| = 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_{2^n}$. Therefore, we have

$$v(f_\lambda) = 2^{-n} \sum_{a \in \mathbb{F}_{2^n}} {W_{f_\lambda}}^4(a) = 2^{-n} \sum_{a \in \mathbb{F}_{2^n}} 2^{2n} = 2^{-n}2^n2^{2n} = 2^{2n}$$

by Theorem 3.7. Now, suppose that there exists $\lambda \in \mathbb{F}_{2^n}^*$ such that f_λ is not bent. Then $|W_{f_\lambda}(a)| \in \{0, 2^{\frac{n+k}{2}}\}$ for some $k \geq 2$ since n is an even integer, i.e., $2^{\frac{n+2}{2}}$ divides $|W_{f_\lambda}(a)|$ for all $a \in \mathbb{F}_{2^n}$.

If f_λ is k_λ-plateaued for $k_\lambda \geq 2$, we have $v(f_\lambda) = 2^{2n+k_\lambda}$ by Lemma 3.4. Suppose that B is the number of bent components and A is the number of non-bent components. Then $A + B = 2^n - 1$. Since F is APN, by Corollary 3.4, we obtain the following equalities.

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} v(f_\lambda) = (2^n - 1)2^{2n+1} = B2^{2n} + \sum_{\lambda \in \mathbb{F}_{2^n}^*} 2^{2n+k_\lambda} = B2^{2n} + N2^{2n+2} \tag{3.9}$$

for some integer $N \geq A$. Then we have

$$\begin{aligned}\sum_{\lambda \in \mathbb{F}_{2^n}^*} v(f_\lambda) = (2^n - 1)2^{2n+1} &= B2^{2n} + N2^{2n+2} \\ &= B2^{2n} + 4N2^{2n} \\ &= 2^{2n}(B + 4N).\end{aligned}$$

This implies that

$$B+4N=\frac{(2^n-1)2^{2n+1}}{2^{2n}}=2(2^n-1).$$

Since $A+B=2^n-1$ and $N\geq A$, we have $N+B\geq 2^n-1$, i.e., $N\geq(2^n-1)-B$. By using this fact, we can write the following implications.

$$\begin{aligned}
&2(2^n-1)=B+4N\geq B+4[(2^n-1)-B]\\
&\Rightarrow 2(2^n-1)\geq B+4(2^n-1)-4B\\
&\Rightarrow 2(2^n-1)\geq 4(2^n-1)-3B\\
&\Rightarrow 3B\geq 2(2^n-1)\\
&\Rightarrow B\geq \frac{2}{3}(2^n-1)
\end{aligned}$$

Now, suppose that F is APN, and $B=\frac{2}{3}(2^n-1)$, i.e., $A=\frac{1}{3}(2^n-1)$. If we write B in Equation 3.9, we obtain the following equations.

$$\begin{aligned}
(2^n-1)2^{2n+1}&=\frac{2}{3}(2^n-1)2^{2n}+N2^{2n+2}\\
N2^{2n+2}&=(2^n-1)2^{2n+1}-\frac{1}{3}(2^n-1)2^{2n+1}\\
&=(2^n-1)2^{2n+1}\left(1-\frac{1}{3}\right)\\
&=(2^n-1)2^{2n+1}\frac{2}{3}
\end{aligned}$$

Therefore, $N=\frac{1}{3}(2^n-1)$, i.e., $N\geq A$. That is, any non-bent component is 2-plateaued. This holds if and only if $\mathcal{L}(F)=2^{\frac{n+2}{2}}$. For the last part of the corollary, assume that $B=2(2^n-1)/3$ and $\mathcal{L}(F)=2^{(n+2)/2}$. That is, any non-bent component is 2-plateaued. Then $v(f_\lambda)=2^{2n+2}$ for any non-bent component f_λ, by Lemma 3.4. Therefore, we have the following equations by Equation 3.9.

$$\begin{aligned}
\sum_{\lambda\in\mathbb{F}_{2n}^*}v(f_\lambda)=B2^{2n}+A2^{2n+2}&=\frac{2}{3}(2^n-1)2^{2n}+\frac{2^n-1}{3}2^{2n+2}\\
&=\frac{2^n-1}{3}(2^{2n+1}+2^{2n+2})=\frac{2^n-1}{3}(2^{2n+1}+2.2^{2n+1})\\
&=\frac{2^n-1}{3}2^{2n+1}3=(2^n-1)2^{2n+1}
\end{aligned}$$

This means that F is APN by Corollary 3.4.

□

3.6 Further Characterization of APN Functions

In this section, we will give a further characterization of APN functions in terms of the sum of square indicator and permutation polynomials.

Theorem 3.10. *Let r be a divisor of n. Let $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be any function. Assume that $F\in\mathbb{F}_{2^r}[x]$. If for some $a\in\mathbb{F}_{2^r}$, there exists $y\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^r}$ such that $y^{2^r}+y+a\neq 0$, and*

$$F(y)+F(y+a)=\beta \text{ for some } \beta\in\mathbb{F}_{2^r},$$

then F is not APN.
Consequently, if F is APN with $F(x)=x^d$, then $\gcd(d,2^n-1)=1$ for odd n and $\gcd(d,2^n-1)=3$ for even n.

Proof. Let $G(x)=F(x)+F(x+a)$. Since $F(x)$ lies in $\mathbb{F}_{2^r}[x]$ and $a\in\mathbb{F}_{2^r}$, the polynomial $G(x)$ is also lies in $\mathbb{F}_{2^r}[x]$. Suppose that there exists $y\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^r}$ such that $y^{2^r}+y+a\neq 0$, and y satisfies $G(y)=\beta$ for some $\beta\in\mathbb{F}_{2^r}$. That is,

$$G(y)=F(y)+F(y+a)=\beta \text{ for some } \beta\in\mathbb{F}_{2^r}.$$

If we take the 2^r-th power of both sides, we have

$$G(y)^{2^r}=(F(y)+F(y+a))^{2^r}=F(y)^{2^r}+F(y+a)^{2^r}=\beta^{2^r}.$$

Since $F\in\mathbb{F}_{2^r}$, by Lemma 2.1 and 2.2, we can write

$$F(y)^{2^r}+F(y+a)^{2^r}=F(y^{2^r})+F(y^{2^r}+a^{2^r})=F(y^{2^r})+F(y^{2^r}+a)=\beta.$$

We have $y^{2^r}\neq y$ since $y\notin\mathbb{F}_{2^r}$, and we have $y^{2^r}\neq y+a$ since $y^{2^r}+y+a\neq 0$. Hence, $y^{2^r}\notin\{y,y+a\}$. Then y^{2^r} is another solution of $G(y)=\beta$. This implies that $y,y+a,y^{2^r},y^{2^r}+a$ are pairwise distinct solutions of $G(y)=\beta$. Therefore, F is not APN by definition.
For the last part of the theorem, suppose that F is an APN function defined by $F(x)=x^d$. Set $s=\gcd(d,2^n-1)$. Note that F is in $F_2[x]$. Assume that $s>1$. By Theorem 2.4, there exists $y\in\mathbb{F}_{2^n}^*$ such that $ord(y)=s$. Note that since $s>1$, we have $y\notin\mathbb{F}_2$.

Consider the function $G:\mathbb{F}_{2^n}\backslash\{0,1\}\to\mathbb{F}_{2^n}\backslash\{0,1\}$ defined by $G(x)=\frac{x+1}{x}$. If $G(x)=G(y)$, i.e., $\frac{x+1}{x}=\frac{y+1}{y}$, then $xy+y=xy+x$. Therefore, $x=y$, i.e., G is one-to-one

on $\mathbb{F}_{2^n}\backslash\{0,1\}$. Hence, G is a bijection on $\mathbb{F}_{2^n}\backslash\{0,1\}$.
Set $y = \frac{z+1}{z}$ as $y \in \mathbb{F}_{2^n}\backslash\{0,1\}$. Note that $y^d = 1$ since $ord(y) = s = \gcd(d, 2^n-1)$. Then we obtain the following implications.

$$F(y) = y^d = \frac{(z+1)^d}{z^d} = 1 \Longleftrightarrow (z+1)^d = z^d \Longleftrightarrow (z+1)^d + z^d = 0$$

Therefore, we have $z \in \mathbb{F}_{2^n}\backslash\mathbb{F}_2$ such that $F(z+1)+F(z) = 0$.
Assume that n is odd. Set $r = 1$ and $a = 1$. Then for $\beta = 0$, we have $F(z+1)+F(z) = 0$. Moreover, by Lemma 2.3, $z^2+z+1 \neq 0$ since $Tr_n(1) = 1$. Then by the first part of the theorem, F is not APN. This contradicts the assumption. Hence, s must be 1 for odd n.
Assume now that n is even. If F is APN, by the first part of the theorem $z^2+z+1 = 0$. Since T^2+T+1 is irreducible over $\mathbb{F}_2$, the root z of T^2+T+1 is in $\mathbb{F}_2(z) = \mathbb{F}_4$. Then $\frac{z+1}{z} = y \in \mathbb{F}_{2^2}\backslash\mathbb{F}_2$, which means that $ord(y) = 3$. Hence, s must be 3 for even n.

□

Theorem 3.11. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be any function such that $F(x) = x^d$. Let $f_\lambda : \mathbb{F}_{2^n} \to \mathbb{F}_2$, $\lambda \in \mathbb{F}_{2^n}$, denote its component $f_\lambda = Tr_n(\lambda F(x))$. Set $s = \gcd(d, 2^n-1)$ and $2^n - 1 = us$. Let ξ be a primitive element of $\mathbb{F}_{2^n}$. Then*

$$W_{D_a f_\lambda}(0) = W_{D_1 f_{\lambda a^d}}(0) \tag{3.10}$$

for all $a, \lambda \in \mathbb{F}_{2^n}^*$. Moreover,

$$v(f_\lambda) = 2^{2n} + s\sum_{k=1}^{u} W^2_{D_1 f_{\lambda\xi^{kd}}}(0).$$

Proof. For any nonzero $a \in \mathbb{F}_{2^n}^*$, we have the following equalities.

$$\begin{aligned}
W_{D_a f_\lambda}(0) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f_\lambda(x+a)+f_\lambda(x)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda(F(x+a)+F(x))} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda((x+a)^d+x^d))} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda a^d(\frac{(x+a)^d}{a^d}+\frac{x^d}{a^d}))} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda a^d((\frac{x}{a}+1)^d+(\frac{x}{a})^d))}
\end{aligned}$$

Set $y=\frac{x}{a}$. Then we have

$$\begin{aligned}W_{D_af_\lambda}(0)&=\sum_{y\in\mathbb{F}_{2^n}}(-1)^{Tr_n(\lambda a^d((y+1)^d+y^d))}=\sum_{y\in\mathbb{F}_{2^n}}(-1)^{Tr_n(\lambda a^d(F(y+1)+F(y))}\\&=\sum_{y\in\mathbb{F}_{2^n}}(-1)^{f_{\lambda a^d}(y+1)+f_{\lambda a^d}(y)}=W_{D_1f_{\lambda a^d}}(0),\end{aligned}$$

which gives the first claim of the theorem.

Let ξ be a primitive element of $\mathbb{F}_{2^n}$. By definition of $v(f_\lambda)$,

$$v(f_\lambda)=\sum_{a\in\mathbb{F}_{2^n}}W^2_{D_af_\lambda}(0)=W^2_{D_0f_\lambda}(0)+\sum_{a\in\mathbb{F}^*_{2^n}}W^2_{D_af_\lambda}(0)=2^{2n}+\sum_{a\in\mathbb{F}^*_{2^n}}W^2_{D_af_\lambda}(0).$$

Let H be the subgroup of $\mathbb{F}^*_{2^n}$ generated by $\beta\in\mathbb{F}^*_{2^n}$ with order s. Then β is of the form $\beta=\xi^{\frac{2^n-1}{s}l}$ where $\gcd(l,2^n-1)=1$ and $H=\langle\beta\rangle$. Then

$$\mathbb{F}^*_{2^n}=\bigsqcup_{k=1}^{\frac{2^n-1}{s}}\xi^kH.$$

For any $\alpha,\gamma\in\xi^kH$, $k=1,\ldots,\frac{2^n-1}{s}$, we have the following:

$$\alpha=\xi^k\beta^i=\xi^k\xi^{\frac{2^n-1}{s}li},$$

$$\gamma=\xi^k\beta^j=\xi^k\xi^{\frac{2^n-1}{s}lj}.$$

Then

$$\alpha^d=(\xi^k\xi^{\frac{2^n-1}{s}li})^d=\xi^{kd}\xi^{\frac{2^n-1}{s}lid}=\xi^{kd},$$
$$\gamma^d=(\xi^k\xi^{\frac{2^n-1}{s}lj})^d=\xi^{kd}\xi^{\frac{2^n-1}{s}ljd}=\xi^{kd},\text{ since } s \text{ divides } d.$$

That is, $\alpha^d=\gamma^d$. Then

$$W_{D_1f_{\lambda\alpha^d}}(0)=W_{D_1f_{\lambda\gamma^d}}(0).$$

By Equation 3.10,

$$W_{D_\alpha f_\lambda}(0)=W_{D_\gamma f_\lambda}(0).$$

Since $\mathbb{F}^*_{2^n}$ is disjoint union of H, any $a\in\mathbb{F}_{2^n}$ can be uniquely written as $a=\xi^k\beta^j$ for some $k\in\{1,\ldots\frac{2^n-1}{s}\}$ and $j\in\{1,\ldots s\}$. Then we have the following equalities.

$$\begin{aligned}
v(f_\lambda) &= 2^{2n} + \sum_{a\in\mathbb{F}_{2^n}^*} W^2_{D_a f_\lambda}(0)\\
&= 2^{2n} + \sum_{k=1}^{\frac{2^n-1}{s}} \sum_{j=1}^{s} W^2_{D_{\xi^k\beta^j} f_\lambda}(0)\\
&= 2^{2n} + \sum_{k=1}^{\frac{2^n-1}{s}} \sum_{j=1}^{s} W^2_{D_1 f_{\lambda\left(\xi^k\beta^j\right)^d}}(0) \text{ by the fist part of the theorem}\\
&= 2^{2n} + \sum_{k=1}^{\frac{2^n-1}{s}} \sum_{j=1}^{s} W^2_{D_1 f_{\lambda\xi^{kd}}}(0) \text{ since } s|d \text{ and } ord(\beta)=s\\
&= 2^{2n} + s\sum_{k=1}^{\frac{2^n-1}{s}} W^2_{D_1 f_{\lambda\xi^{kd}}}(0)\\
&= 2^{2n} + s\sum_{k=1}^{u} W^2_{D_1 f_{\lambda\xi^{kd}}}(0)
\end{aligned}$$

□

Theorem 3.12. *Let H be a polynomial on $\mathbb{F}_{2^n}$ such that H is one-to-one from $\mathbb{F}_{2^n}\backslash\{0\}$ to $\mathbb{F}_{2^n}$. Suppose that $H(e)=0$ for a unique $e\neq 0$. Then the degree of H is exactly 2^n-1.*

Proof. Let $H(x)$ be the polynomial on $\mathbb{F}_{2^n}$ such that H is one-to-one from $\mathbb{F}_{2^n}\backslash\{0\}$ to $\mathbb{F}_{2^n}$, and $H(0)=\alpha$ for some $\alpha\in\mathbb{F}_{2^n}^*$. Consider the polynomial $\widetilde{H}(x)=H(x)+\alpha$. Note that $\widetilde{H}(0)=\alpha+\alpha=0$. Since H is one-to-one on $\mathbb{F}_{2^n}\backslash\{0\}$, there exists unique $\widetilde{e}$ such that $H(\widetilde{e})=\alpha$. Then $\widetilde{H}(\widetilde{e})=H(\widetilde{e})+\alpha=\alpha+\alpha=0$. Hence, without loss of generality, we assume that $H(0)=0$. Since $H(0)=H(e)=0$, the image of H, i.e., the set $\{H(x):x\in\mathbb{F}_{2^n}\}$, contains 2^n-1 elements. Therefore, there is only one nonzero element that is not in the image of H, say $\beta\in\mathbb{F}_{2^n}$. Let $P:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be the polynomial defined by

$$P(x)=\begin{cases} H(x), & \text{for } x\neq e;\\ \beta, & \text{for } x=e.\end{cases}$$

Since the image of P has cardinality 2^n, the polynomial $P(x)$ is a permutation. Let $W(x):\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be the polynomial such that $W(x)=H(x)+P(x)$. We have the following conclusion.

If $x\neq e$, then $P(x)=H(x)$. Therefore, $W(x)=H(x)+H(x)=0$. If $x=e$, then $P(e)=\beta$ and $H(e)=0$. Therefore $W(e)=H(e)+P(e)=\beta$.

We claim that the unique representation of W modulo $x^{2^n}+x$ is

$$W(x)=\beta((x+e)^{2^n-1}+1).$$

Note that the degree is 2^n-1. Moreover, for $x=e$, we have $W(e)=\beta((e+e)^{2^n-1}+1)=\beta$ since $e+e=0$. For $x\neq e$, we have $W(e)=\beta((x+e)^{2^n-1}+1)=\beta(1+1)=0$ because $(x+e)^{2^n-1}=1$ for $(x+e)\in\mathbb{F}_{2^n}$. Hence, we proved that

$$P(x)=H(x)+W(x)=H(x)+\beta((x+e)^{2^n-1}+1).$$

Since P is a permutation, its degree is less than 2^n-1 by Hermite's criterion, see Theorem 2.8. Then H must have the term βx^{2^n-1} to simplify the term of degree 2^n-1 in $W(x)$. □

Theorem 3.13. *Let $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be a function defined by*

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

Then F is APN if and only if the polynomial $Q(x)=\frac{F(x)}{x^2}$, i.e., $Q(x)=\sum\limits_{i=1}^{n-1}c_i x^{2^i-1}$, is a permutation polynomial on $\mathbb{F}_{2^n}$.

Proof. By Theorem 3.1, we have the following equation.

$$D_aF(x)+F(a)=\sum_{i=1}^{n-1}c_i(x^{2^i}a+a^{2^i}x)\text{ for any }a\in\mathbb{F}_{2^n}^*.$$

Note that $x=0$ and $x=a$ are zeros of $D_aF(x)+F(a)$. Suppose that $|Ker(D_aF(x)+F(a))|=2^s$, then we have the following:

$$|\{D_aF(x)+F(a):x\in\mathbb{F}_{2^n}\}|=\frac{|\mathbb{F}_{2^n}|}{|Ker(D_aF(x)+F(a))|}=\frac{2^n}{2^s}=2^{n-s}.$$

Therefore, we can conclude that $\{D_aF(x):x\in\mathbb{F}_{2^n}\}$ has cardinality 2^{n-1} if and only if $|Ker(D_aF(x)+F(a))|=2$, i.e., $Ker(D_aF(x)+F(a))=\{0,a\}$. Consider the polynomial $Q(x)=\sum\limits_{i=1}^{n-1}c_i x^{2^i-1}$, we can write the following equations.

$$\frac{D_aF(x)+F(a)}{xa}=\sum_{i=1}^{n-1}c_i(x^{2^i-1}+a^{2^i-1})=\sum_{i=1}^{n-1}c_i x^{2^i-1}+\sum_{i=1}^{n-1}c_i a^{2^i-1}=Q(x)+Q(a)$$

Therefore, we can write the following implications.

$$\begin{aligned} F \text{ is APN} &\iff D_aF(x)+F(a) \text{ has only two solutions, namely } 0,a \\ &\iff \frac{D_aF(x)+F(a)}{xa} \neq 0 \text{ for all } x \in \mathbb{F}_{2^n}\backslash\{0,a\} \\ &\iff Q(x) \neq Q(a) \text{ for all } x \in \mathbb{F}_{2^n}\backslash\{0,a\} \\ &\Longleftarrow Q \text{ is one-to-one on } \mathbb{F}_{2^n}\backslash\{0\} \end{aligned}$$

Suppose that Q is not permutation and F is APN. That is, there exists unique $e \in \mathbb{F}_{2^n}^*$ such that $Q(e) = Q(0)$. Then by Theorem 3.12, $deg(Q(x)) = 2^n - 1$, a contradiction since $deg(Q(x)) = deg\left(\sum\limits_{i=1}^{n-1} c_i x^{2^i-1}\right) \leq 2^{n-1} - 1$. Hence, Q is permutation if and only if F is APN. □

3.7 Examples of APN Functions and Their Walsh Spectrum

In this section, we will give some examples of APN functions which are the polynomial x^3(cube function), gold, and inverse functions. Then we will compute the Walsh spectrum of the polynomial x^3.

Example 3.1. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function defined by $F(x) = x^3$. For any $a \in \mathbb{F}_{2^n}^*$, we have

$$\begin{aligned} D_aF(x) = F(x+a)+F(x) &= (x+a)^3 + x^3 \\ &= x^3 + ax^2 + a^2x + a^3 + x^3 \\ &= ax^2 + a^2x + a^3 = b. \end{aligned}$$

Note that the equation $D_aF(x) = b$ has at most 2 solutions since $deg(D_aF(x)) = 2$. Hence, $F(x) = x^3$ is APN over $\mathbb{F}_{2^n}$ for any integer $n \geq 1$ by definition.

Example 3.2. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function defined by $F(x) = x^{2^k+1}$. The polynomial $G(x) = F(x+a)+F(x)+F(a)$ is a linear function by Remark 3.1. Then F is APN if and only of $|Ker(G(x))| = 2$. By Theorem 3.1, we have the following.

$$G(x) = F(x+a)+F(x)+F(a) = (x+a)^{2^k+1} + x^{2^k+1} + a^{2^k+1} = ax^{2^k} + a^{2^k}x$$

Note that 0 and a are zeros of $G(x)$. Then $\{0,a\} \subseteq Ker(G(x))$.
Suppose that $\gcd(k,n) = 1$, i.e., $\gcd(2^k - 1, 2^n - 1) = 1$ by Lemma 2.8. For $x \neq 0$ and $a \neq 0$, the following holds.

$$\begin{aligned}
& ax^{2^k} + a^{2^k}x = 0 \\
\Leftrightarrow\ & \frac{ax^{2^k} + a^{2^k}x}{ax} = 0 \\
\Leftrightarrow\ & x^{2^k-1} + a^{2^k-1} = 0 \\
\Leftrightarrow\ & x^{2^k-1} = a^{2^k-1} \\
\Leftrightarrow\ & \frac{x^{2^k-1}}{a^{2^k-1}} = \left(\frac{x}{a}\right)^{2^k-1} = 1 \\
\Leftrightarrow\ & \frac{x}{a} = 1 \quad \text{since } \gcd(2^k - 1, 2^n - 1) = 1
\end{aligned}$$

Then $x = a$. Hence, $Ker(G(x)) = \{0,a\}$, which means that F is APN.
Now, suppose that $\gcd(k,n) = s > 1$, i.e., $\gcd(2^k - 1, 2^n - 1) = 2^s - 1$. For $x \neq 0$ and $a \neq 0$,

$$ax^{2^k} + a^{2^k}x = 0 \Leftrightarrow \left(\frac{x}{a}\right)^{2^k-1} = 1.$$

Set $y = \frac{x}{a}$. Then $y^{2^k-1} = 1$. Therefore, there exists $2^s - 1$ elements that satisfy the equation $y^{2^k-1} = 1$. There exists $\xi \in \mathbb{F}_{2^n} \backslash \{0,1\}$ such that $\xi^{2^s-1} = 1$. Then $y = \frac{x}{a} = \xi$ is a solution. That is, $x = \xi a$ is a solution of $ax^{2^k} + a^{2^k}x = 0$. Note that $x = \xi a \notin \{0,a\}$, which means that $|Ker(G(x))| > 2$. Therefore, F is not APN.

Corollary 3.6. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function defined by $F(x) = x^{2^k+1}$ where k is a positive integer. Then F is APN if and only if $\gcd(k,n) = 1$.

Definition 3.13. The function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $F(x) = x^{2^k+1}$ is called Gold function.

Example 3.3. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function defined by $F(x) = x^{2^n-2}$. We will show that $D_aF(x) = b$ has at most two solutions for $a, b \in \mathbb{F}_{2^n}$ and $a \neq 0$ if and only if n is odd. The equation $D_aF(x) = b$ has at most two solutions if and only if $D_aF(x) + F(a) = b$ has at most two solutions.

$$D_aF(x) + F(a) = F(x+a) + F(x) + F(a) = (x+a)^{2^n-2} + x^{2^n-2} + a^{2^n-2} = b$$

Case 1: Set $b = 0$. Then $x = a$ and $x = 0$ are solutions of $D_aF(x) + F(a) = 0$.

Suppose that $x \neq a$ and $x \neq 0$. Then the following equalities hold.

$$\begin{aligned} F(x+a)+F(x)+F(a) &= (x+a)^{2^n-2}+x^{2^n-2}+a^{2^n-2} \\ &= \frac{(x+a)^{2^n-1}}{x+a}+\frac{x^{2^n-1}}{x}+\frac{a^{2^n-1}}{a} \\ &= \frac{1}{x+a}+\frac{1}{x}+\frac{1}{a}=0 \end{aligned}$$

This holds if and only if $a(x+a)+x(x+a)+ax=0$. That is, $x^2+ax+a^2=0$. By Lemma 2.3, we have the following results.

- If n is even, $x^2+ax+a^2=0$ has solution since $Tr_n(\frac{a^2}{a^2})=Tr_n(1)=n.1=0$. Note that the solution is different from a and 0. Then F is not APN.
- If n is odd, then $x^2+ax+a^2=0$ has no solution in $\mathbb{F}_{2^n}$ since $Tr_n(\frac{a^2}{a^2})=Tr_n(1)=1$. Hence, a and 0 are only solutions, and hence $D_aF(x)+F(a)=0$ has exactly two solutions.

Case 2: Set $b \neq 0$. Then 0 and a are not solutions of $D_aF(x)+F(a)=b$. Hence for $x \neq a$ and $x \neq 0$, we have the following conclusion.

$$\begin{aligned} & F(x+a)+F(x)+F(a)=\frac{1}{x+a}+\frac{1}{x}+\frac{1}{a}=b \\ & \Longleftrightarrow ax+a(x+a)+x(x+a)=bax(x+a) \\ & \Longleftrightarrow a^2+x^2+ax+bax^2+ba^2x=0 \\ & \Longleftrightarrow (1+ba)x^2+(a+ba^2)x+a^2=0. \end{aligned}$$

Since the degree is at most 2, there exists at most 2 solutions. Hence, we observe that $D_aF(x)+F(x)=b$ has at most 2 solutions for all b when n is odd. That is, F is APN for odd n.

Corollary 3.7. Let $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be a function defined by $F(x)=x^{2^n-2}$, which is called the inverse function. Then F is APN if and only if n is odd.

Now, we investigate the Walsh spectrum of the polynomial x^3.

Example 3.4. Let $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ be a function defined by $F(x)=x^3$. Then $f_\lambda:\mathbb{F}_{2^n}\to\mathbb{F}_2$, $\lambda\in\mathbb{F}_{2^n}^*$ denote its component $f_\lambda=Tr_n(\lambda F(x))$. Since $F(x)$ is a quadratic function, $f_\lambda(x)$ is also quadratic. Consider

$$\wedge(f_\lambda)=\{a\in\mathbb{F}_{2^n}: f_\lambda(x+a)+f_\lambda(x)+f_\lambda(a)=0 \text{ for all } x\in\mathbb{F}_{2^n}\}.$$

Recall that $\wedge(f_\lambda)$ is a linear subspace of $\mathbb{F}_{2^n}$, see Theorem 3.2. If $dim(\wedge(f_\lambda))=s$, then $|W_{f_\lambda}(a)| \in \{0, 2^{\frac{n+s}{2}}\}$ by Theorem 3.8. Now, we have the following equalities.

$$\begin{aligned}\wedge(f_\lambda) &= \{a \in \mathbb{F}_{2^n} : f_\lambda(x+a) + f_\lambda(x) + f_\lambda(a) = 0 \text{ for all } x \in \mathbb{F}_{2^n}\}\\ &= \{a \in \mathbb{F}_{2^n} : Tr_n(\lambda(x+a)^3) + Tr_n(\lambda x^3) + Tr_n(\lambda a^3) = 0 \text{ for all } x \in \mathbb{F}_{2^n}\}\\ &= \{a \in \mathbb{F}_{2^n} : Tr_n(\lambda(x^3 + x^2a + a^2x + a^3 + x^3 + a^3)) = 0 \text{ for all } x \in \mathbb{F}_{2^n}\}\\ &= \{a \in \mathbb{F}_{2^n} : Tr_n(\lambda(ax^2 + xa^2)) = 0 \text{ for all } x \in \mathbb{F}_{2^n}\}\end{aligned}$$

Then we can write the following equalities by Theorem 2.5.

$$\begin{aligned}Tr_n(\lambda(ax^2 + xa^2)) &= Tr_n(\lambda ax^2 + \lambda xa^2)\\ &= Tr_n(\lambda ax^2) + Tr_n(\lambda xa^2)\\ &= Tr_n(\lambda ax^2) + Tr_n(\lambda^2 x^2 a^4)\\ &= Tr_n(\lambda ax^2 + \lambda^2 x^2 a^4)\\ &= Tr_n((\lambda a + \lambda^2 a^4)x^2) = 0 \text{ for all } x \in \mathbb{F}_{2^n}.\end{aligned}$$

Since trace is a balanced function, $Tr_n((\lambda a + \lambda^2 a^4)x^2) = 0$ for all $x \in \mathbb{F}_{2^n}$ if and only if $\lambda a + \lambda^2 a^4 = 0$, i.e., $\lambda a = \lambda^2 a^4$. This holds if and only if $a^3 = \lambda^{-1}$ for $a \neq 0$.

- **Case 1:** If n is odd, $\gcd(2^n - 1, 3) = \gcd(2^n - 1, 2^2 - 1) = 2^{\gcd(n,2)} - 1 = 1$ by Lemma 2.8. Hence, for any $\lambda \in \mathbb{F}_{2^n}^*$, there exists a unique $a \in \mathbb{F}_{2^n}^*$ satisfying $a^3 = \lambda^{-1}$. Hence, $\wedge(f_\lambda) = \{0, a\}$, i.e., $s = 1$. We conclude that $|W_{f_{\lambda(a)}}| \in \{0, 2^{\frac{n+1}{2}}\}$ by Theorem 3.8.
- **Case 2:** If n is even, $\gcd(2^n - 1, 3) = \gcd(2^n - 1, 2^2 - 1) = 2^{\gcd(n,2)} - 1 = 3$ by Lemma 2.8. This means that $a^3 = \lambda^{-1}$ has either no solution or has exactly 3 solutions by Theorem 2.9. That is, either $|\wedge(f_\lambda)| = 1$, i.e., $s = 0$, or $|\wedge(f_\lambda)| = 4$, i.e., $s = 2$. Hence, $|W_{f_\lambda}(a)| \in \{0, 2^{\frac{n}{2}}, 2^{\frac{n+2}{2}}\}$ by Theorem 3.8.

Remark 3.5. By Corollary 3.5, there exist exactly $2(2^n - 1)/3$ elements $\lambda \in \mathbb{F}_{2^n}^*$ such that f_λ is bent.

Example 3.5. Now, we will find the Walsh spectrum of x^3 by using the definition of the Walsh coefficient.

$$\begin{aligned}W_{f_\lambda}^2(a) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(x) + Tr_n(ax)} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{f_\lambda(y) + Tr_n(ay)}\\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda x^3) + Tr_n(ax)} \sum_{y \in \mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda y^3) + Tr_n(ay)}\\ &= \sum_{x,y \in \mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda(x^3 + y^3)) + Tr_n(a(x+y))}\end{aligned}$$

Set $x+y=z$, i.e., $y=x+z$. Then we have

$$\begin{aligned}
W_{f_\lambda}^2(a) &= \sum_{x,z\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda(x^3+(x+z)^3))+Tr_n(az)} \\
&= \sum_{x,z\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda(x^3+x^3+zx^2+xz^2+z^3)+az)} \\
&= \sum_{x,z\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda zx^2+\lambda xz^2+\lambda z^3+az)} \\
&= \sum_{z\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda z^3+az)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda(zx^2+xz^2))}.
\end{aligned}$$

Note that $Tr(\lambda(zx^2+xz^2)) = Tr(\lambda zx^2+\lambda xz^2) = Tr_n(\lambda zx^2+\lambda^2x^2z^4)$ due to the fact that $Tr_n((\lambda xz^2)^2) = Tr_n(\lambda xz^2)$. Then we have

$$\begin{aligned}
W_{f_\lambda}^2(a) &= \sum_{z\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda z^3+az)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda zx^2+\lambda^2x^2z^4))} \\
&= \sum_{z\in\mathbb{F}_{2^n}} (-1)^{Tr_n(\lambda z^3+az)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_n(x^2(\lambda z+\lambda^2z^4))}.
\end{aligned}$$

Note that by Theorem 2.7, we have the following.

$$\sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_n(x^2(\lambda z+\lambda^2z^4))} = 0 \iff \lambda z+\lambda^2z^4 \neq 0$$

Moreover, we have the following implications by Theorem 2.7.

$$\begin{aligned}
\sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_n(x^2(\lambda z+\lambda^2z^4))} = 2^n &\iff \lambda z+\lambda^2z^4 = 0 \\
&\iff \lambda z = \lambda^2z^4 \\
&\iff \lambda^{-1} = z^3 \text{ or } z=0
\end{aligned}$$

Then we have the following equality.

$$W_{f_\lambda}^2(a) = 2^n \sum_{\substack{z\in\mathbb{F}_{2^n}\\ \lambda^{-1}=z^3\\ z=0}} (-1)^{Tr_n(\lambda z^3+az)} \tag{3.11}$$

Case 1: Suppose that n is odd. Note that $\lambda z^3+az=0$ for $z=0$. Moreover, $\gcd(2^n-1,3) = \gcd(2^n-1,2^2-1) = 2^{\gcd(n,2)}-1 = 1$ by Lemma 2.8. Therefore, for any $\lambda\in\mathbb{F}_{2^n}^*$, there exists unique $z\in\mathbb{F}_{2^n}$ satisfying $z^3=\lambda^{-1}$. Hence, by Equation

3.11, we have the following.

$$\begin{aligned} W_{f_\lambda}^2(a) &= 2^n \sum_{\substack{z\in\mathbb{F}_{2^n} \\ \lambda^{-1}=z^3 \\ z=0}} (-1)^{Tr_n(\lambda z^3+az)} \\ &= 2^n \left((-1)^{Tr_n(0)} + (-1)^{Tr_n(1+az)}\right) \end{aligned}$$

Since $Tr_n(az) = 1$ or $Tr_n(az) = -1$, we have the following conclusion.

$$W_{f_\lambda}^2(a) = 2^n(1 \pm 1) = 2^{n+1} \text{ or } 0$$

That is, $|W_{f_\lambda}| \in \{0, 2^{\frac{n+1}{2}}\}$, i.e., for all $\lambda \in \mathbb{F}_{2^n}^*$, the component function f_λ is semibent.
Case 2: Suppose that n is even. We have $\gcd(2^n-1,3) = \gcd(2^n-1,2^2-1) = 2^{\gcd(n,2)}-1 = 3$ by Lemma 2.8. Therefore, for any $\lambda \in \mathbb{F}_{2^n}^*$, the equation $\lambda^{-1} = z^3$ has either no solution or exactly 3 solutions by Theorem 3.12.
Firstly, assume that $\lambda^{-1} = z^3$ has no solution in $\mathbb{F}_{2^n}$ for a nonzero λ. Then $\lambda z^3 + az = 0$ if and only if $z = 0$. By Equation 3.11, this implies that

$$W_{f_\lambda}^2(a) = 2^n.1 = 2^n,$$

i.e., $|W_{f_\lambda}| = 2^{n/2}$. This implies that f_λ is bent. Now, assume that for any $\lambda \in \mathbb{F}_{2^n}^*$, the equation $\lambda^{-1} = z^3$ has exactly 3 solutions. Note that $\wedge(f_\lambda) = \{a \in \mathbb{F}_{2^n} : f_\lambda(x+a) + f_\lambda(x) + f_\lambda(a) = 0\}$ is a subspace of F_{2^n} and f_λ is linear on $\wedge(f_\lambda)$. Consider the function $\varphi(z) : \wedge(f_\lambda) \to \mathbb{F}_2$ defined by $\varphi(z) = Tr_n(f_\lambda(z) + az)$. If $\varphi(z) = 0$, then by Equation 3.11, we have

$$W_{f_\lambda}^2(a) = 2^n \sum_{\substack{z\in\mathbb{F}_{2^n} \\ z\in\wedge(f_\lambda)}} (-1)^{Tr_n(\lambda z^3+az)} = 2^n.4 = 2^{n+2},$$

i.e., f_λ is semibent. If $\varphi(z) \neq 0$, then $\varphi(z)$ is balanced function. Then $W_{f_\lambda}^2(a) = 0$. Hence, $|W_{f_\lambda}(a)| \in \{0, 2^{\frac{n}{2}}, 2^{\frac{n+2}{2}}\}$.

Remark 3.6. Let A be the number of f_λ components of F such that f_λ is bent. Then there exist $(2^n-1)-A$ non-bent components such that $W_{f_\lambda} = 2^{\frac{n+2}{2}}$, i.e., f_λ's are 2-plateaued. By Theorem 3.4, we have $v(f_\lambda) = 2^{2n}$ for bent components, and $v(f_\lambda) = 2^{2n+2}$ for 2-plateaued components. By Corollary 3.4, we know that

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

since F is APN. Then we can write the following equalities.

$$
\begin{aligned}
(2^n-1)2^{2n+1} = \sum_{\lambda\in\mathbb{F}_{2^n}^*} v(f_\lambda) &= 2^{2n}A + (2^n-1-A)2^{2n+2} \\
&= 2^{2n}(A + 2^2 2^n - 2^2 - 2^2 A).
\end{aligned}
$$

Therefore, we can conclude that $A = \frac{2}{3}(2^n-1)$. Hence, $\frac{2}{3}(2^n-1)$ components are bent and $\frac{2^n-1}{3}$ components are semibent, which confirms Corollary 3.5.

4. Bezout's Theorem and The Nonlinearity of Quadratic Functions

4.1 Bezout's Theorem and Common Zero Sets

In this chapter, we will give the definition of affine and projective curves. Then we will give related theorems which are necessary for the computation of the Walsh spectrum of biprojective functions.
We recall that $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$.

Definition 4.1. An affine curve $\mathcal{X}$ is the zero set of a polynomial $f(x,y) \in \overline{\mathbb{F}}[x,y]$. That is,

$$\mathcal{X} = \{(x,y) \in \overline{\mathbb{F}} \times \overline{\mathbb{F}} : f(x,y) = 0\}.$$

The polynomial $f(x,y)$ is called a defining polynomial of $\mathcal{X}$ and the degree of $\mathcal{X}$ is the degree of $f(x,y)$. If $f(x,y) \in \mathbb{F}_{2^m}[x,y]$, then we say $\mathcal{X}$ is a curve defined over $\mathbb{F}_{2^m}$.

Definition 4.2. A component of $\mathcal{X}$ is a curve $\mathcal{Y}$ such that the defining polynomial $g(x,y)$ of $\mathcal{Y}$ divides $f(x,y)$.

Remark 4.1. Let $\mathcal{X}$ be a curve with the defining equation $f(x,y)$ and ℓ be a line given by $bx - ay + c$, which is not a component of $\mathcal{X}$. Suppose that $P = (x_0, y_0)$ is an intersection point of $\mathcal{X}$ and ℓ. We can parametrize ℓ as follows:

$$x = x_0 + at \quad \text{and} \quad y = y_0 + bt \text{ for } t \in \overline{\mathbb{F}}.$$

As ℓ is not a factor of $f(x,y)$, we have

$$f(x,y) = f(x_0 + at, y_0 + bt) = h_m t^m + \cdots + h_d t^d \in \overline{\mathbb{F}}[t] \quad \text{with } h_m \neq 0.$$

Then $m := m(P, \mathcal{X} \cap \ell)$ is called the intersection multiplicity of $\mathcal{X}$ and ℓ at P.

Definition 4.3. For $P \in \mathcal{X}$,

$$m_P(\mathcal{X}) := \min_{\ell}\{m(P, \mathcal{X} \cap \ell)\}$$

is called the multiplicity of $\mathcal{X}$ at P where the multiplicity is determined over all lines ℓ through P such that they are not a factor of $f(x,y)$.

Lemma 4.1. Hirschfeld, Korchmáros, Torres & Orihuela (2008) Let $\mathcal{X}$ and $\mathcal{Y}$ be two plane curves such that $P \in \mathcal{X} \cap \mathcal{Y}$. Then $\mathcal{X}$ and $\mathcal{Y}$ intersect at P with multiplicity

$$m(P, \mathcal{X} \cap \mathcal{Y}) \geq m_P(\mathcal{X}) m_P(\mathcal{Y}),$$

and equality holds if and only if they do not have a common tangent line at P.

We can state Bezout's Theorem for plane curves as follows.

Theorem 4.1 (Bezout's Theorem). *Let $\mathcal{X}$ and $\mathcal{Y}$ be two plane curves of degree d_1 and d_2, respectively. If $\mathcal{X}$ and $\mathcal{Y}$ do not have a common component, then*

$$\sum_{P \in \mathcal{X} \cap \mathcal{Y}} m(P, \mathcal{X} \cap \mathcal{Y}) \leq d_1 d_2.$$

By Bezout's theorem we conclude that $\mathcal{X}$ and $\mathcal{Y}$ intersect at most $d_1 d_2$ distinct points.

Let F be a field and E_1 and E_2 be two extensions of F. Recall that E_1 and E_2 are called linearly disjoint extensions of F if $E_1 \cap E_2 = F$.

Lemma 4.2. Bracken, Byrne, Markin & McGuire (2009) Let E_1, E_2 be two linearly disjoint finite field extensions of F. Then any F-linearly independent subset $\{u_1, ..., u_k\}$ of E_1 is also linearly independent over E_2.

Proof. Suppose that E_1 and E_2 be finite field extensions of F of degree n and s, respectively. Let $E = E_1 E_2$ be the compositum of E_1 and E_2. Since E_1 and E_2 are linearly disjoint extensions, we have

$$[E : E_2] = [E_1 : F] = n.$$

Let $\{u_1, \ldots u_n\}$ be an F-basis of E_1 as a vector space over F and $\{v_1, \ldots, v_s\}$ an F-basis of E_2 as a vector space over F. Then the set $\{u_i v_j : 1 \leq i \leq n, 1 \leq j \leq s\}$ generates E as a vector space over F. Moreover, $\{u_1, u_2, \ldots, u_n\}$ generates E as a vector space over E_2. Since $[E : E_2] = n$, the set $\{v_1, \ldots v_n\}$ is a basis of E over E_2. Let $\{u_1, \ldots, u_k\}$ be a set of F-linearly independent elements of E_1. We can extend this set to a basis $\{u_1, \ldots, u_k, \ldots, u_n\}$. Since this set forms an E_2-basis of E, its subset $\{u_1, \ldots, u_k\}$ is linearly independent over E_2. □

Lemma 4.3 (Trachtenberg (1970)). Let k be an integer with $\gcd(k,m) = 1$, and let f be the polynomial of the form

$$f(x) = C_0 x + C_1 x^{2^k} + C_2 x^{2^{2k}} + \cdots + C_d x^{2^{dk}} \in \mathbb{F}_{2^m}[x] \tag{4.1}$$

of degree 2^{dk}. Then $f(x)$ has at most 2^d zeros in $\mathbb{F}_{2^m}$.

Proof. Firstly, we will show that the set of zeros $\mathbf{S}$ of $f(x)$ in $\mathbb{F}_{2^{mk}}$ forms a vector space over $\mathbb{F}_{2^k}$. Let $x, y \in \mathbf{S}$, i.e., $f(x) = f(y) = 0$. Then we can write the following equalities.

$$\begin{aligned} f(x+y) &= C_0(x+y) + C_1(x+y)^{2^k} + C_2(x+y)^{2^{2k}} + \cdots + C_d(x+y)^{2^{dk}} \\ &= C_0 x + C_1 x^{2^k} + C_2 x^{2^{2k}} + \cdots + C_d x^{2^{dk}} + C_0 y + C_1 y^{2^k} + C_2 y^{2^{2k}} + \cdots + C_d y^{2^{dk}} \\ &= f(x) + f(y) = 0 \end{aligned}$$

Then $x + y \in \mathbf{S}$. Let $\alpha \in \mathbb{F}_{2^k}$ and $x \in \mathbf{S}$. Note that $\alpha^{2^k} = \alpha$ by Theorem 2.5. Then we have the following.

$$\begin{aligned} f(\alpha x) &= C_0(\alpha x) + C_1(\alpha x)^{2^k} + C_2(\alpha x)^{2^{2k}} + \cdots + C_d(\alpha x)^{2^{dk}} \\ &= \alpha C_0 x + \alpha^{2^k} C_1 x^{2^k} + \alpha^{2^{2k}} C_2 x^{2^{2k}} + \cdots + \alpha^{2^{dk}} C_d x^{2^{dk}} \\ &= \alpha C_0 x + \alpha C_1 x^{2^k} + \alpha C_2 x^{2^{2k}} + \cdots + \alpha C_d x^{2^{dk}} \\ &= \alpha(C_0 x + C_1 x^{2^k} + C_2 x^{2^{2k}} + \cdots + C_d x^{2^{dk}}) = \alpha f(x) = 0 \end{aligned}$$

Then $\alpha x \in \mathbf{S}$. Hence, $\mathbf{S}$ is a vector space over $\mathbb{F}_{2^k}$. Moreover, $\mathbf{S}$ is a finite-dimensional vector space since f can have only finitely many zeros. In fact, $|\mathbf{S}| \leq 2^{dk}$. Let $u_1, u_2, \ldots u_s$ be a basis for $\mathbf{S}$ over $\mathbb{F}_{2^k}$. Since $|\mathbf{S}| \leq 2^{dk}$, we have $s \leq d$. Since $\gcd(k,m) = 1$, extensions $\mathbb{F}_{2^k}$ and $\mathbb{F}_{2^m}$ are linearly disjoint over $\mathbb{F}_2$. Then any linearly independent subset of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ stays linearly independent of $\mathbb{F}_{2^k}$. Hence, the zero set $\mathbf{Z}$ of $f(x)$ in $\mathbb{F}_{2^m}$, which is linearly independent over $\mathbb{F}_2$, stays linearly independent over $\mathbb{F}_{2^k}$. Hence, $|\mathbf{Z}| = 2^s \leq 2^d$. □

Remark 4.2. Let $f_1(x,y), f_2(x,y) \in \mathbb{F}_{2^m}[x,y]$ be polynomials of the form (4.1) in two variables. Then the common zero set $\mathcal{Z}_{\mathbb{F}_{2^m}}(f_1, f_2)$ of f_1 and f_2 in $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ is defined by

$$\mathcal{Z}_{\mathbb{F}_{2^m}}(f_1, f_2) = \{(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} : f_1(x,y) = f_2(x,y) = 0\}.$$

In a similar way, we can observe that $\mathcal{Z}_{\mathbb{F}_{2^m}}(f_1, f_2)$ forms a vector space over $\mathbb{F}_2$.

Theorem 4.2. *Let k be an integer with $\gcd(k,m) = 1$, and let $f_1(x,y), f_2(x,y)$ be polynomials of the form (4.1) of degree $2^{d_1 k}$ and $2^{d_2 k}$, respectively. If f_1 and f_2 do not have any common factor, then*

$$|\mathcal{Z}_{\mathbb{F}_{2^m}}(f_1, f_2)| \leq 2^{d_1+d_2}. \tag{4.2}$$

Proof. Note that $|\mathcal{Z}_{\mathbb{F}_{2^m}}(f_1, f_2)|$ is finite dimensional vector space by Bezout's theorem since f_1 and f_2 do not have a common factor. Also, the assumption $\gcd(k,m) = 1$ implies that $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^k}$ are linearly disjoint over $\mathbb{F}_2$. Let $S = \{v_1, \dots v_s\}$ be a basis for $V_1 = \mathcal{Z}_{\mathbb{F}_{2^m}}(f_1, f_2)$ over $\mathbb{F}_2$. Consider the $\mathbb{F}_{2^k}$-vector space V_2 generated by S. Note that for any $c \in \mathbb{F}_{2^k}$, we have

$$f_1(cx, cy) = cf_1(x,y) \text{ and } f_2(cx, cy) = cf_2(x,y)$$

as f_1 and f_2 are of the form (4.1). Hence, any element of V_2 is a common zero of f_1 and f_2 in $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. This means $V_2 = \mathcal{Z}_{\mathbb{F}_{2^{km}}}(f_1, f_2)$. Since $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^k}$ are also linearly disjoint over $\mathbb{F}_2$, the set S is linearly independent over $\mathbb{F}_{2^k}$ by Lemma 4.2. Therefore,

$$dim_{\mathbb{F}_{2^k}}(V_2) = dim_{\mathbb{F}_2}(V_1).$$

Note that V_2 is a subset of $\mathbb{F}_{2^{km}}$. As f_1, f_2 do not have any common factor, by Bezout's theorem, we have

$$|V_2| \leq deg(f_1)deg(f_2) = 2^{d_1 k} 2^{d_2 k} = 2^{(d_1+d_2)k}.$$

This means that $dim_{\mathbb{F}_{2^k}} V_2 \leq d_1 + d_2$. Hence,

$$dim_{\mathbb{F}_2}(V_1) = dim_{\mathbb{F}_{2^k}}(V_2) \leq d_1 + d_2,$$

which means

$$|\mathcal{Z}_{\mathbb{F}_{2^m}}(f_1, f_2)| \leq 2^{d_1+d_2}.$$

□

Corollary 4.1. Let k be an integer with $\gcd(k,m) = 1$, and let $f_1(x,y), f_2(x,y)$ be polynomials of the form (4.1), which do not have a common factor. If $|\mathcal{Z}_{\mathbb{F}_{2^{km}}}(f_1, f_2)| \leq 2^{kd}$, then $\mathcal{Z}_{\mathbb{F}_{2^m}}(f_1, f_2) \leq 2^d$.

Now, we will give some definitions and theorems related to projective plane curves which will be needed for the following chapter.

Definition 4.4. Let $\mathbb{F}$ be any field. A projective plane over $\mathbb{F}$ is defined by the set of all 1-dimensional linear subspaces of $\mathbb{F}^3$. It is denoted by $\mathbb{P}^2(\mathbb{F})$.

We say that $x = (x_0, x_1, x_2)$ and $y = (y_0, y_1, y_2)$ are related by " $\sim$ " if $x = \lambda y$, i.e., $(x_0, x_1, x_2) = (\lambda y_0, \lambda y_1, \lambda y_2)$. Note that the relation " $\sim$ " is an equivalence relation.

Definition 4.5. The equivalence class of (x_0, x_1, x_2) is denoted by $P = (x_0 : x_1 : x_2) \in \mathbb{P}^2$. The coordinates x_0, x_1, and x_2 are called homogeneous coordinates of the point P.

Definition 4.6. Menon (2011) Any polynomial $f \in \mathbb{F}[x_0, x_1]$ of degree d can be written as $f = f_0 + f_1 + \cdots + f_d$ where each f_i is a homogeneous polynomial of degree i for $i = 0, \ldots, d$. Then we set

$$f^*(x_0, x_1, x_2) = x_2^d f_0 + x_2^{d-1} f_1 + \ldots x_2 f_{d-1} + f_d = \sum_{i=0}^{d} x_2^{d-i} f_i.$$

This process is called the homogenization of f.

Definition 4.7. A projective curve is the set of points $(x : y : z) \in \mathbb{P}^2$ such that $f(x, y, z) = 0$ where f is a homogeneous polynomial. A point $P = (x : y : z)$ is called a point at infinity if $z = 0$.

Theorem 4.3 (Bezout's Theorem). *Fulton (2008) Let $\mathcal{X}$ and $\mathcal{Y}$ be two projective plane curves of degree d_1 and d_2, respectively. If $\mathcal{X}$ and $\mathcal{Y}$ do not have a common component, then*

$$\sum_{P \in \mathcal{X} \cap \mathcal{Y}} m(P, \mathcal{X} \cap \mathcal{Y}) = d_1 d_2.$$

Lemma 4.4. Let $\mathcal{X}_1$ and $\mathcal{X}_2$ be two plane curves. If they do not have an intersection point at infinity, then they have no common components.

Proof. Let $\mathcal{X}_1$ and $\mathcal{X}_2$ be curves defined by $f_1(x, y)$ and $f_2(x, y)$, respectively. Suppose that $\mathcal{X}_1$ and $\mathcal{X}_2$ have a common component. Then there exists $g(x, y)$ such that $g(x, y)$ divides $f_1(x, y)$ and $f_2(x, y)$. That is, the curve $\mathcal{G}$ defined by $g(x, y)$ is a component of $\mathcal{X}_1$ and $\mathcal{X}_2$. Consider the projective line ℓ defined at $z = 0$, i.e., the line at infinity. By Bezout's Theorem, there exists a point $P \in \mathcal{G} \cap \ell$. This means that P is a point at infinity lying on $\mathcal{X}_1$ and $\mathcal{X}_2$. Hence, we can conclude that if $\mathcal{X}_1$ and $\mathcal{X}_2$ do not have an intersection point at infinity, then they have no common components. □

4.2 Determining the Nonlinearity of a Class of Quadratic Functions

In this section, we will give the definition of directional derivative for the bivariate form.

Definition 4.8. Let $F \in \mathbb{F}_{2^m}[x,y]$ be a polynomial of algebraic degree 2, i.e., quadratic. Let f be the quadratic Boolean function given in bivariate trace representation as $f(x,y) = Tr_m(F(x,y))$. Then the directional derivative of f in the direction of $(u,v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ is given by

$$D_{u,v}f(x,y) = Tr_m(F(x+u,y+v)+F(x,y)).$$

Remark 4.3. Since F is quadratic, $D_{u,v}f(x,y)$ is affine. Consider the linear part $\widetilde{D}_{u,v}f(x,y) = D_{u,v}f(x,y)+f(u,v)$. Note that $\widetilde{D}_{u,v}f(x,y)$ can be written in the form $Tr_m(L_1(x))+Tr_m(L_2(y))$ for some polynomials of the form (4.1):

$$L_1(x) = \sum_{i=0}^{\delta_1} a_i x^{2^i} \text{ and } L_2(x) = \sum_{i=0}^{\delta_2} b_i y^{2^i}$$

where the coefficients depend on u and v. Note that $Tr_m(a^{2^j}) = Tr_m(a)$ for any $j \geq 1$ by Theorem 2.5. Then we can write the following.

$$Tr_m(a_i x^{2^i}) = Tr_m((a_i x^{2^i})^{2^j}) = Tr_m(a_i^{2^j} x^{2^{i+j}}) \text{ for any } j \geq 0$$

By using this fact, we obtain the following equalities.

$$\begin{aligned}
\widetilde{D}_{u,v}f(x,y) &= Tr_m\left(\sum_{i=0}^{\delta_1} a_i x^{2^i}\right) + Tr_m\left(\sum_{i=0}^{\delta_2} b_i y^{2^i}\right) \\
&= \sum_{i=0}^{\delta_1} Tr_m(a_i x^{2^i}) + \sum_{i=0}^{\delta_2} Tr_m(b_i y^{2^i}) \\
&= \sum_{i=0}^{\delta_1} Tr_m((a_i x^{2^i})^{2^{\delta_1-i}}) + \sum_{i=0}^{\delta_2} Tr_m((b_i y^{2^i})^{2^{\delta_2-i}}) \\
&= \sum_{i=0}^{\delta_1} Tr_m(a_i^{2^{\delta_1-i}} x^{2^{\delta_1}}) + \sum_{i=0}^{\delta_2} Tr_m(b_i^{2^{\delta_2-i}} y^{2^{\delta_2}}) \\
&= Tr_m\left((\sum_{i=0}^{\delta_1} a_i^{2^{\delta_1-i}}) x^{2^{\delta_1}}\right) + Tr_m\left((\sum_{i=0}^{\delta_2} b_i^{2^{\delta_2-i}}) y^{2^{\delta_2}}\right)
\end{aligned}$$

Let $A(u,v) = \sum\limits_{i=0}^{\delta_1} a_i^{2^{\delta_1-i}}$ and $B(u,v) = \sum\limits_{i=0}^{\delta_2} b_i^{2^{\delta_2-i}}$. Then we get

$$\widetilde{D}_{u,v}f(x,y) = Tr_m(A(u,v)x^{2^{\delta_1}} + B(u,v)y^{2^{\delta_2}}). \tag{4.3}$$

Note that $A, B \in \mathbb{F}_{2^m}[u,v]$. Clearly, $\widetilde{D}_{u,v}f(x,y)$ is zero if and only if $A(u,v) = B(u,v) = 0$, i.e., $\wedge_f$ is the common zero set $\mathscr{Z}_{\mathbb{F}_{2^m}}(A,B)$ of A and B.

Corollary 4.2. Let $f(x,y) = Tr_m(F(x,y))$ be a quadratic function from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_2$. Suppose that the corresponding polynomials $A(u,v)$ and $B(u,v)$ in (4.3) are of the form (4.1) of degrees kd_1 and kd_2 for some integer k with $\gcd(k,m) = 1$. If A and B do not have a common factor, then f is s-plateaued with $s \leq d_1 + d_2$.

5. Biprojective APN Functions

In this chapter, we first give the definition of biprojective polynomial. Then we investigate the Walsh spectrum of two infinite families of (q,r)-biprojective APN polynomial pairs that have been presented in Göloğlu (2022).

Definition 5.1. Let $F(x,y) = [f(x,y), g(x,y)] \in \mathbb{F}_{2^m}[x,y] \times \mathbb{F}_{2^m}[x,y]$, with $q = 2^i, r = 2^j$, $i,j \geq 0$ where

$$\begin{aligned} f(x,y) &= a_0 x^{q+1} + b_0 x^q y + c_0 x y^q + d_0 y^{q+1}, \\ g(x,y) &= a_1 x^{r+1} + b_1 x^r y + c_1 x y^r + d_0 y^{r+1}. \end{aligned}$$

Then $f(x,y)$ (respectively $g(x,y)$) is said to be a q-biprojective (respectively r-biprojective) polynomial. In this case, $F(x,y)$ is a (q,r)-biprojective polynomial. We denote $f(x,y)$ and $g(x,y)$ by $(a_0,b_0,c_0,d_0)_q$ and $(a_1,b_1,c_1,d_1)_r$, respectively. Moreover, we denote $F(x,y)$ by $[(a_0,b_0,c_0,d_0)_q, (a_1,b_1,c_1,d_1)_r]$.

Theorem 5.1. *Göloğlu (2022) The following (q,r)-biprojective polynomial pairs $F(x,y) = [f(x,y), g(x,y)]$ are APN on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.*

($\mathcal{F}_1$) If $\gcd(3i,m) = 1$, then $F_1 = [(1,0,1,1)_{2^i}, (1,1,0,1)_{2^{2i}}]$ is APN.

($\mathcal{F}_2$) If $\gcd(3i,m) = 1$, and m is odd, then $F_2 = [(1,0,1,1)_{2^i}, (0,1,1,0)_{2^{3i}}]$ is APN.

5.1 Family $\mathcal{F}_1$

Firstly, we start with investigating the Walsh spectrum of $\mathcal{F}_1$. Let

$$F(x,y) = F_1(x,y) = [f(x,y), g(x,y)] = (x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{2i}+1} + x^{2^{2i}}y + y^{2^{2i}+1})$$

where $\gcd(3i,m)=1$. Then the components of $F(x,y)$ corresponding to $(\lambda,\mu)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}\backslash\{(0,0)\}$ are given by:

$$F_{\lambda,\mu}=Tr_m(\lambda f(x,y)+\mu g(x,y)).$$

Recall $\wedge(F_{\lambda,\mu})=\{(u,v)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}:F_{\lambda,\mu}(x+u,y+v)+F_{\lambda,\mu}(x,y)+F_{\lambda,\mu}(u,v)=0\}$. We know that $\wedge(F_{\lambda,\mu})$ is a vector space over $\mathbb{F}_2$, see Theorem 3.2 and $|W_{F_{\lambda,\mu}}|\in\{0,p^{\frac{n+s}{2}}\}$ where s is a dimension of $\wedge(F_{\lambda,\mu})$. Hence, we first compute $F_{\lambda,\mu}(x+u,y+v)+F_{\lambda,\mu}(x,y)+F_{\lambda,\mu}(u,v)$. We have the following equations.

(5.1)

$$\begin{aligned}&F_{\lambda,\mu}(x+u,y+v)+F_{\lambda,\mu}(x,y)+F_{\lambda,\mu}(u,v)\\&=Tr_m[\lambda f(x+u,y+v)+\mu g(x+u,y+v)+\lambda f(x,y)+\mu g(x,y)+\lambda f(u,v)+\mu g(u,v)]\\&=Tr_m[\lambda(f(x+u,y+v)+f(x,y)+f(u,v))+\mu(g(x+u,y+v)+g(x,y)+g(u,v))]\end{aligned}$$

Then we obtain the following equalities.

(5.2)

$$\begin{aligned}&f(x+u,y+v)+f(x,y)+f(u,v)\\&=(x+u)^{2^i+1}+(x+u)(y+v)^{2^i}+(y+v)^{2^i+1}+x^{2^i+1}+xy^{2^i}+y^{2^i+1}+u^{2^i+1}+uv^{2^i}+v^{2^i+1}\\&=x^{2^i+1}+x^{2^i}u+xu^{2^i}+u^{2^i+1}+xy^{2^i}+xv^{2^i}+uy^{2^i}+uv^{2^i}+y^{2^i+1}+yv^{2^i}+y^{2^i}v+v^{2^i+1}\\&\qquad+x^{2^i+1}+xy^{2^i}+y^{2^i+1}+u^{2^i+1}+uv^{2^i}+v^{2^i+1}\\&=x^{2^i}u+xu^{2^i}+xv^{2^i}+uy^{2^i}+yv^{2^i}+y^{2^i}v\end{aligned}$$

$$\begin{aligned}&g(x+u,y+v)+g(x,y)+g(u,v)\\&=(x+u)^{2^{2i}+1}+(x+u)^{2^{2i}}(y+v)+(y+v)^{2^{2i}+1}+x^{2^{2i}+1}+x^{2^{2i}}y+y^{2^{2i}+1}+u^{2^{2i}+1}+u^{2^{2i}}v+v^{2^{2i}+1}\\&=x^{2^{2i}+1}+x^{2^{2i}}u+xu^{2^{2i}}+u^{2^{2i}+1}+x^{2^{2i}}y+x^{2^{2i}}v+u^{2^{2i}}y+u^{2^{2i}}v+y^{2^{2i}+1}+y^{2^{2i}}v+yv^{2^{2i}}+v^{2^{2i}+1}\\&\qquad+x^{2^{2i}+1}+x^{2^{2i}}y+y^{2^{2i}+1}+u^{2^{2i}+1}+u^{2^{2i}}v+v^{2^{2i}+1}\\&=x^{2^{2i}}u+xu^{2^{2i}}+x^{2^{2i}}v+u^{2^{2i}}y+y^{2^{2i}}v+yv^{2^{2i}}\end{aligned}$$

Then we can write the following equations.

$$\begin{aligned}
&F_{\lambda,\mu}(x+u,y+v)+F_{\lambda,\mu}(x,y)+F_{\lambda,\mu}(u,v)\\
&=Tr_m[\lambda(x^{2^i}u+xu^{2^i}+xv^{2^i}+uy^{2^i}+yv^{2^i}+y^{2^i}v)\\
&\quad+\mu(x^{2^{2i}}u+xu^{2^{2i}}+x^{2^{2i}}v+u^{2^{2i}}y+y^{2^{2i}}v+yv^{2^{2i}})]\\
&=Tr_m[x(\lambda u^{2^i}+\lambda v^{2^i}+\mu u^{2^{2i}})+x^{2^i}\lambda u+x^{2^{2i}}(\mu u+\mu v)\\
&\quad+y(\lambda v^{2^i}+\mu u^{2^{2i}}+\mu v^{2^{2i}})+y^{2^i}(\lambda u+\lambda v)+y^{2^{2i}}\mu v]
\end{aligned}$$

We set

$$\begin{aligned}
&A_1=\lambda u^{2^i}+\lambda v^{2^i}+\mu u^{2^{2i}} \quad , \quad A_2=\lambda u \quad , \quad A_3=\mu u+\mu v, \text{ and}\\
&B_1=\lambda v^{2^i}+\mu u^{2^{2i}}+\mu v^{2^{2i}} \quad , \quad B_2=\lambda u+\lambda v \quad , \quad B_3=\mu v.
\end{aligned}$$

Then we can represent $F_{\lambda,\mu}(x+u,y+v)+F_{\lambda,\mu}(x,y)+F_{\lambda,\mu}(u,v)$ as follows.

$$\begin{aligned}
&F_{\lambda,\mu}(x+u,y+v)+F_{\lambda,\mu}(x,y)+F_{\lambda,\mu}(u,v)\\
&=Tr_m[xA_1+x^{2^i}A_2+x^{2^{2i}}A_3+yB_1+y^{2^i}B_2+y^{2^{2i}}B_3]\\
&=Tr_m(xA_1)+Tr_m(x^{2^i}A_2)+Tr_m(x^{2^{2i}}A_3)+Tr_m(yB_1)+Tr_m(y^{2^i}B_2)+Tr_m(y^{2^{2i}}B_3)\\
&=Tr_m(x^{2^{2i}}A_1^{2^{2i}})+Tr_m(x^{2^{2i}}A_2^{2^i})+Tr_m(x^{2^{2i}}A_3)+Tr_m(y^{2^{2i}}B_1^{2^{2i}})+Tr_m(y^{2^{2i}}B_2^{2^i})+Tr_m(y^{2^{2i}}B_3)\\
&=Tr_m(x^{2^{2i}}(A_1^{2^{2i}}+A_2^{2^i}+A_3))+Tr_m(y^{2^{2i}}(B_1^{2^{2i}}+B_2^{2^i}+B_3))
\end{aligned}$$

Note that A_i's and B_i's depend on u and v for $i,j=1,2,3$. So, we set

$$\begin{aligned}
A(u,v)&=A_1^{2^{2i}}+A_2^{2^i}+A_3 \text{ and}\\
B(u,v)&=B_1^{2^{2i}}+B_2^{2^i}+B_3.
\end{aligned}$$

Then we can compute $A(u,v)$ and $B(u,v)$ as follows.

$$\begin{aligned}
A(u,v)&=(\lambda u^{2^i}+\lambda v^{2^i}+\mu u^{2^{2i}})^{2^{2i}}+(\lambda u)^{2^i}+(\mu u+\mu v)\\
&=\lambda^{2^{2i}}u^{2^{3i}}+\lambda^{2^{2i}}v^{2^{3i}}+\mu^{2^{2i}}u^{2^{4i}}+\lambda^{2^i}u^{2^i}+\mu u+\mu v\\
&=\mu^{2^{2i}}u^{2^{4i}}+\lambda^{2^{2i}}(u^{2^{3i}}+v^{2^{3i}})+\lambda^{2^i}u^{2^i}+\mu(u+v)
\end{aligned}$$

$$\begin{aligned}
B(u,v)&=(\lambda v^{2^i}+\mu u^{2^{2i}}+\mu v^{2^{2i}})^{2^{2i}}+(\lambda u+\lambda v)^{2^i}+\mu v\\
&=\lambda^{2^{2i}}v^{2^{3i}}+\mu^{2^{2i}}u^{2^{4i}}+\mu^{2^{2i}}v^{2^{4i}}+\lambda^{2^i}u^{2^i}+\lambda^{2^i}v^{2^i}+\mu v\\
&=\mu^{2^{2i}}(u^{2^{4i}}+v^{2^{4i}})+\lambda^{2^{2i}}v^{2^{3i}}+\lambda^{2^i}(u^{2^i}+v^{2^i})+\mu v
\end{aligned}$$

We investigate the zeros of the polynomials $A(u,v)$ and $B(u,v)$ case by case depending on λ and μ.

Case 1: Let $\lambda=0$, and hence $\mu\neq 0$. Then

$$A(u,v)=\mu^{2^{2i}}u^{2^{4i}}+\mu(u+v), \text{ and } B(u,v)=\mu^{2^{2i}}(u^{2^{4i}}+v^{2^{4i}})+\mu v.$$

By Theorem 2.5, $Tr_m(x^{2^{2i}}A(u,v))+Tr_m(y^{2^{2i}}B(u,v))=0$ for all $x,y\in\mathbb{F}_{2^m}$ if and only if $A(u,v)=B(u,v)=0$. Now, assume that $\mathcal{X}_1$ be the curve defined by $A(u,v)$ and $\mathcal{X}_2$ be the curve defined by $B(u,v)$. Then $(u,v)\in\wedge(F_{0,\mu})$ if and only if $(u,v)\in\mathcal{X}_1\cap\mathcal{X}_2$. Note that the point $(u:v:z)$ at infinity lies on $\mathcal{X}_1$ if and only if $u=0$. That is, $(0:1:0)$ is the only point of $\mathcal{X}_1$ at infinity. And the point $(u:v:z)$ at infinity lies on $\mathcal{X}_2$ if and only if $u=v$. That is, $(1:1:0)$ is the only point of $\mathcal{X}_2$ at infinity. Hence, $\mathcal{X}_1$ and $\mathcal{X}_2$ have no intersection point at infinity, which means that they have no common components by Lemma 4.4. Therefore, we can apply Theorem 4.2.

$$|\mathcal{Z}_{\mathbb{F}_{2^m}}(A,B)|\leq 2^{2^{4i}}2^{2^{4i}}=2^{8i}$$

Hence, we have the following cases by Theorem 4.2.

- If m is odd, then $\gcd(4i,m)=1$. Hence, $k=4i$, which means $d_1=d_2=1$. Therefore, we have $s=dim_{\mathbb{F}_2}\wedge_{0,\mu}\leq 2$. That is $s=0$ or $s=2$. Hence, $F_{0,\mu}$ is either bent or semibent, respectively.
- If m is even, we know that $\gcd(i,m)=1$ since $\gcd(3i,m)=1$. Hence, $k=i$, which means $d_1=d_2=4$. Therefore, we have $s=dim_{\mathbb{F}_2}\wedge_{0,\mu}\leq 8$.

Case 2: Let $\mu=0$, and hence $\lambda\neq 0$. Then

$$\begin{aligned}A(u,v)&=\lambda^{2^{2i}}(u^{2^{3i}}+v^{2^{3i}})+\lambda^{2^i}u^{2^i}=(\lambda^{2^i}(u^{2^{2i}}+v^{2^{2i}})+\lambda u)^{2^i},\\ B(u,v)&=\lambda^{2^{2i}}v^{2^{3i}}+\lambda^{2^i}(u^{2^i}+v^{2^i})=(\lambda^{2^i}v^{2^{2i}}+\lambda(u+v))^{2^i}.\end{aligned}$$

Note that

$$A(u,v)=0 \qquad \text{if and only if} \qquad \widetilde{A}(u,v)=\lambda^{2^i}(u^{2^{2i}}+v^{2^{2i}})+\lambda u=0,$$

and

$$B(u,v)=0 \qquad \text{if and only if} \qquad \widetilde{B}(u,v)=\lambda^{2^i}v^{2^{2i}}+\lambda(u+v)=0.$$

Now, assume that $\mathcal{X}_1$ be the curve defined by $\widetilde{A}(u,v)$ and $\mathcal{X}_2$ be the curve defined by $\widetilde{B}(u,v)$. Then $(u,v)\in\wedge(F_{\lambda,0})$ if and only if $(u,v)\in\mathcal{X}_1\cap\mathcal{X}_2$. Similarly, the point of $\mathcal{X}_1$ at infinity is $(1:1:0)$ and the point of $\mathcal{X}_2$ at infinity is $(1:0:0)$. Hence, $\mathcal{X}_1$ and

$\mathcal{X}_2$ have no intersection point at infinity, which means that they have no common components by Theorem 4.4. Then we can apply Theorem 4.2.

$$|\mathcal{Z}_{\mathbb{F}_{2^m}}(A,B)| \leq 2^{2^{2i}} 2^{2^{2i}} = 2^{4i}$$

Hence, we have the following cases by Theorem 4.2.

- If m is odd, then $\gcd(2i,m) = 1$. Hence, $k = 2i$, which means $d_1 = d_2 = 1$. Therefore, we have $s = dim_{\mathbb{F}_2} \wedge_{\lambda,0} \leq 2$. That is $s = 0$ or $s = 2$. Hence, $F_{\lambda,0}$ is either bent or semibent, respectively.
- If m is even, then $\gcd(2i,m) = 2$. Hence, $k = i$, which means $d_1 = d_2 = 2$. Hence, we have $s = dim_{\mathbb{F}_2} \wedge_{\lambda,0} \leq 4$. That is, $s = 0$ or $s = 2$ or $s = 4$.

Case 3: Let $\lambda \neq 0$ and $\mu \neq 0$. Then

$$A(u,v) = \mu^{2^{2i}} u^{2^{4i}} + \lambda^{2^{2i}} (u^{2^{3i}} + v^{2^{3i}}) + \lambda^{2^i} u^{2^i} + \mu(u+v), \text{ and}$$
$$B(u,v) = \mu^{2^{2i}} (u^{2^{4i}} + v^{2^{4i}}) + \lambda^{2^{2i}} v^{2^{3i}} + \lambda^{2^i} (u^{2^i} + v^{2^i}) + \mu v.$$

Assume that $\mathcal{X}_1$ be the curve defined by $A(u,v)$ and $\mathcal{X}_2$ be the curve defined by $B(u,v)$. Then $(u,v) \in \wedge(F_{\lambda,\mu})$ if and only if $(u,v) \in \mathcal{X}_1 \cap \mathcal{X}_2$. Similarly, the point of $\mathcal{X}_1$ at infinity is $(0:1:0)$ and the point of $\mathcal{X}_2$ at infinity is $(1:1:0)$. Hence, $\mathcal{X}_1$ and $\mathcal{X}_2$ have no intersection point at infinity, which means that they have no common components by Theorem 4.4. Then we can apply Theorem 4.2.

$$|\mathcal{Z}_{\mathbb{F}_{2^m}}(A,B)| \leq 2^{2^{4i}} 2^{2^{4i}} = 2^{8i}$$

Note that $\gcd(i,m) = 1$ since $\gcd(3i,m) = 1$. Hence, $k = i$, which means $d_1 = d_2 = 4$. Therefore, we have $s = dim_{\mathbb{F}_2} \wedge_{\lambda,\mu} \leq 8$.

By the above calculations, we observe that for the component function corresponding to $(\lambda,\mu) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \backslash \{(0,0)\}$, we have $|W_{F_{\lambda,\mu}}| \leq 2^{m+4}$ for all $(u,v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ since $s = dim_{\mathbb{F}_2} \wedge_{\lambda,\mu} \leq 8$. Hence, we obtain the following theorem.

Theorem 5.2. *Let*

$$F(x,y) = (x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{2i}+1} + x^{2^{2i}} y + y^{2^{2i}+1})$$

be a function on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ *where* $\gcd(3i,m) = 1$. *Then* $|W_{F_{\lambda,\mu}}(u,v)| \leq 2^{m+4}$ *for all* $(u,v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

In particular, by Theorem 5.2, we have the following conclusion.

Corollary 5.1. The nonlinearity of F given in Theorem 5.2 is $\mathcal{N}(F) \geq 2^{2m-1} - 2^{m+3}$.

Proof. By Definition 3.5, for the components $F_{\lambda,\mu}$ of $F(x,y)$ corresponding to $(\lambda,\mu) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \backslash \{(0,0)\}$, we have

$$\mathcal{L}(F_{\lambda,\mu}) = \max_{(u,v)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}} |W_{F_{\lambda,\mu}}(u,v)| \leq 2^{m+4}$$

by Theorem 5.2. Then

$$\mathcal{L}(F) = \max_{(\lambda,\mu)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}\backslash\{(0,0)\}} \mathcal{L}(F_{\lambda,\mu}) \leq 2^{m+4}.$$

Therefore, the nonlinearity of F is

$$\mathcal{N}(F) = 2^{2m-1} - \frac{1}{2}\mathcal{L}(F) \geq 2^{2m-1} - \frac{1}{2}2^{m+4} = 2^{2m-1} - 2^{m+3}.$$

□

5.2 Family $\mathcal{F}_2$

In this section, we investigate the Walsh spectrum of $\mathcal{F}_2$. Let

$$F(x,y) = F_2(x,y) = (f(x,y), g(x,y)) = (x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{3i}}y + xy^{2^{3i}})$$

where $\gcd(3i,m) = 1$, and m is odd. Then the components $F_{\lambda,\mu}$ of $F(x,y)$ corresponding to $(\lambda,\mu) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \backslash \{(0,0)\}$ are given by:

$$F_{\lambda,\mu}(x,y) = Tr_m(\lambda f(x,y) + \mu g(x,y)).$$

Recall that

$$\wedge_{\lambda,\mu} = \{(u,v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} : F_{\lambda,\mu}(x+u, y+v) + F_{\lambda,\mu}(x,y) + F_{\lambda,\mu}(u,v) = 0\}.$$

By Equation (5.1), we have

$$\begin{aligned}&F_{\lambda,\mu}(x+u,y+v) + F_{\lambda,\mu}(x,y) + F_{\lambda,\mu}(u,v)\\ &= Tr_m[\lambda(f(x+u,y+v) + f(x,y) + f(u,v)) + \mu(g(x+u,y+v) + g(x,y) + g(u,v))].\end{aligned}$$

By Equation (5.2), we know that:

$$f(x+u,y+v)+f(x,y)+f(u,v) = x^{2^i}u+xu^{2^i}+xv^{2^i}+y^{2^i}u+y^{2^i}v+yv^{2^i}.$$

Also, we have the following equalities.

$$\begin{aligned}
&g(x+u,y+v)+g(x,y)+g(u,v)\\
&=(x+u)^{2^{3i}}(y+v)+(x+u)(y+v)^{2^{3i}}+x^{2^{3i}}y+xy^{2^{3i}}+u^{2^{3i}}v+uv^{2^{3i}}\\
&=(x^{2^{3i}}+u^{2^{3i}})(y+v)+(x+u)(y^{2^{3i}}+v^{2^{3i}})+x^{2^{3i}}y+xy^{2^{3i}}+u^{2^{3i}}v+uv^{2^{3i}}\\
&=x^{2^{3i}}y+x^{2^{3i}}v+yu^{2^{3i}}+u^{2^{3i}}v+xy^{2^{3i}}+xv^{2^{3i}}+y^{2^{3i}}u+uv^{2^{3i}}+x^{2^{3i}}y+xy^{2^{3i}}+u^{2^{3i}}v+uv^{2^{3i}}\\
&=x^{2^{3i}}v+yu^{2^{3i}}+xv^{2^{3i}}+y^{2^{3i}}u
\end{aligned}$$

Then we can write the following equations.

$$\begin{aligned}
&F_{\lambda,\mu}(x+u,y+v)+F_{\lambda,\mu}(x,y)+F_{\lambda,\mu}(u,v)\\
&=Tr_m[\lambda(x^{2^i}u+xu^{2^i}+xv^{2^i}+y^{2^i}u+y^{2^i}v+yv^{2^i})+\mu(x^{2^{3i}}v+yu^{2^{3i}}+xv^{2^{3i}}+y^{2^{3i}}u)]\\
&=Tr_m\Big[x(\lambda u^{2^i}+\lambda v^{2^i}+\mu v^{2^{3i}})+x^{2^i}\lambda u+x^{2^{3i}}\mu v)+y(\lambda v^{2^i}+\mu u^{2^{3i}})+y^{2^i}(\lambda u+\lambda v)+y^{2^{3i}}\mu u)\Big]\\
&=Tr_m\Big(x^{2^{3i}}((\lambda u^{2^i}+\lambda v^{2^i}+\mu v^{2^{3i}})^{2^{3i}}+(\lambda u)^{2^{2i}}+\mu v)+\\
&+y^{2^{3i}}((\lambda v^{2^i}+\mu u^{2^{3i}})^{2^{3i}}+(\lambda u+\lambda v)^{2^{2i}}+\mu u)\Big)
\end{aligned}$$

We set

$$\begin{aligned}
A(u,v)&=(\lambda u^{2^i}+\lambda v^{2^i}+\mu v^{2^{3i}})^{2^{3i}}+(\lambda u)^{2^{2i}}+\mu v\ \text{, and}\\
B(u,v)&=(\lambda v^{2^i}+\mu u^{2^{3i}})^{2^{3i}}+(\lambda u+\lambda v)^{2^{2i}}+\mu u.
\end{aligned}$$

Then we can obtain the following equalities.

$$\begin{aligned}
A(u,v)&=(\lambda u^{2^i}+\lambda v^{2^i}+\mu v^{2^{3i}})^{2^{3i}}+(\lambda u)^{2^{2i}}+\mu v\\
&=\lambda^{2^{3i}}u^{2^{4i}}+\lambda^{2^{3i}}v^{2^{4i}}+\mu^{2^{3i}}v^{2^{6i}}+\lambda^{2^{2i}}u^{2^{2i}}+\mu v\\
&=\mu^{2^{3i}}v^{2^{6i}}+\lambda^{2^{3i}}(u^{2^{4i}}+v^{2^{4i}})+\lambda^{2^{2i}}u^{2^{2i}}+\mu v
\end{aligned}$$

$$\begin{aligned}
B(u,v)&=(\lambda v^{2^i}+\mu u^{2^{3i}})^{2^{3i}}+(\lambda u+\lambda v)^{2^{2i}}+\mu u\\
&=\lambda^{2^{3i}}v^{2^{4i}}+\mu^{2^{3i}}u^{2^{6i}}+\lambda^{2^{2i}}u^{2^{2i}}+\lambda^{2^{2i}}v^{2^{2i}}+\mu u\\
&=\mu^{2^{3i}}u^{2^{6i}}+\lambda^{2^{3i}}v^{2^{4i}}+\lambda^{2^{2i}}(u^{2^{2i}}+v^{2^{2i}})+\mu u
\end{aligned}$$

We investigate the zeros of $A(u,v)$ and $B(u,v)$ case by case depending on $(\lambda,\mu) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \backslash \{(0,0)\}$.

Case 1: Let $\lambda = 0$, and hence $\mu \neq 0$. Then we set

$$\begin{aligned} A(u,v) &=: A(v) = \mu^{2^{3i}} v^{2^{6i}} + \mu v, \\ B(u,v) &=: B(u) = \mu^{2^{3i}} u^{2^{6i}} + \mu u. \end{aligned}$$

Note that $\gcd(2^{3i}-1, 2^m-1) = 1$ since $\gcd(3i,m) = 1$ by Lemma 2.8. Note that $v = 0$ is a trivial solution of $A(v) = 0$. Suppose that $v \in \mathbb{F}_{2^m}$ is a nonzero solution of $A(v) = 0$. Then we have the following implications.

$$\begin{aligned} A(v) = 0 &\Longleftrightarrow \mu^{2^{3i}} v^{2^{6i}} = \mu v \\ &\Longleftrightarrow \mu^{2^{3i}-1} v^{2^{6i}-1} = 1 \text{ since } v \neq 0 \\ &\Longleftrightarrow (\mu v^{2^{3i}+1})^{2^{3i}-1} = 1 \text{ since } \gcd(2^{3i}-1, 2^m-1) = 1 \\ &\Longleftrightarrow \mu v^{2^{3i}+1} = 1 \\ &\Longleftrightarrow v^{2^{3i}+1} = \mu^{-1} \end{aligned}$$

Note that in the 4-th implication, we used Lemma 2.1. We observed that $\gcd(6i,m) = 1$ since $\gcd(3i,m) = 1$ and m is odd. Hence, $\gcd(2^{6i}-1, 2^m-1)$ by Lemma 2.8. Then we obtain the following equalities.

$$\begin{aligned} 1 = \gcd(2^{6i}-1, 2^m-1) &= \gcd(2^{3i}-1, 2^m-1)\gcd(2^{3i}+1, 2^m-1) \\ &= \gcd(2^{3i}+1, 2^m-1) \end{aligned}$$

That is, $\gcd(2^{3i}+1, 2^m-1) = 1$. Then $v^{2^{3i}+1}$ is a permutation on $\mathbb{F}_{2^m}$ by Lemma 2.7. That is, $v^{2^{3i}+1} = \mu^{-1}$ has a unique solution for any $\mu \in \mathbb{F}_{2^m}^*$. Then the solution set of $A(v) = 0$ is $\{0, v_\mu\}$ where v_μ is the unique solution depending on $\mu \in \mathbb{F}_{2^m}^*$. Similarly, the solution set of $B(u)$ is $\{0, u_\mu\}$ where u_μ is the unique solution depending on $\mu \in \mathbb{F}_{2^m}^*$. Therefore, the solution set of $\wedge_{0,\mu}$ is $\{(0,0),(0,v_\mu),(u_\mu,0),(u_\mu,v_\mu)\}$. Hence, $s = dim_{\mathbb{F}_2} \wedge_{0\mu} = 2$, i.e., $F_{0,\mu}$ is semibent.

Case 2: Let $\mu = 0$, and hence $\lambda \neq 0$. Then

$$\begin{aligned} A(u,v) &= \lambda^{2^{3i}} u^{2^{4i}} + \lambda^{2^{3i}} v^{2^{4i}} + \lambda^{2^{2i}} u^{2^{2i}} = (\lambda^{2^i} u^{2^{2i}} + \lambda^{2^i} v^{2^{2i}} + \lambda u)^{2^{2i}} \\ B(u,v) &= \lambda^{2^{3i}} v^{2^{4i}} + \lambda^{2^{2i}} u^{2^{2i}} + \lambda^{2^{2i}} v^{2^{2i}} = (\lambda^{2^i} v^{2^{2i}} + \lambda u + \lambda v)^{2^{2i}} \end{aligned}$$

Note that

$$A(u,v) = 0 \qquad \text{if and only if} \qquad \widetilde{A}(u,v) = \lambda^{2^i} u^{2^{2i}} + \lambda^{2^i} v^{2^{2i}} + \lambda u = 0,$$

and

$$B(u,v)=0 \qquad \text{if and only if} \qquad \widetilde{B}(u,v)=\lambda^{2^i}v^{2^{2i}}+\lambda u+\lambda v=0.$$

Now, assume that $\mathcal{X}_1$ be the curve defined by $\widetilde{A}(u,v)$ and $\mathcal{X}_2$ be the curve defined by $\widetilde{B}(u,v)$. Then $(u,v)\in\wedge(F_{\lambda,0})$ if and only if $(u,v)\in\mathcal{X}_1\cap\mathcal{X}_2$. Similarly, the point of $\mathcal{X}_1$ at infinity is $(1:1:0)$ and the point of $\mathcal{X}_2$ at infinity is $(1:0:0)$. Hence, $\mathcal{X}_1$ and $\mathcal{X}_2$ have no intersection point at infinity, which means that they have no common components by Theorem 4.4. Then we can apply Bezout's Theorem.

$$|\mathcal{Z}_{\mathbb{F}_{2^m}}(A,B)|\leq 2^{2^{2i}}2^{2^{2i}}=2^{4i}$$

Since m is odd, then $\gcd(2i,m)=1$. Hence, $k=2i$, which means $d_1=d_2=1$. Therefore, we have $s=dim_{\mathbb{F}_2}\wedge_{\lambda,0}\leq 2$. That is, $s=0$ or $s=2$. Hence, $F_{\lambda,0}$ is either bent or semibent, respectively.

Case 3: Let $\lambda\neq 0$ and $\mu\neq 0$. Then

$$\begin{aligned}A(u,v)&=\mu^{2^{3i}}v^{2^{6i}}+\lambda^{2^{3i}}(u^{2^{4i}}+v^{2^{4i}})+\lambda^{2^{2i}}u^{2^{2i}}+\mu v\\ B(u,v)&=\mu^{2^{3i}}u^{2^{6i}}+\lambda^{2^{3i}}v^{2^{4i}}+\lambda^{2^{2i}}(u^{2^{2i}}+v^{2^{2i}})+\mu u\end{aligned}$$

Assume that $\mathcal{X}_1$ be the curve defined by $A(u,v)$ and $\mathcal{X}_2$ be the curve defined by $B(u,v)$. Then $(u,v)\in\wedge(F_{\lambda,\mu})$ if and only if $(u,v)\in\mathcal{X}_1\cap\mathcal{X}_2$. Similarly, the point of $\mathcal{X}_1$ at infinity is $(1:0:0)$ and the point of $\mathcal{X}_2$ at infinity is $(0:1:0)$. Hence, $\mathcal{X}_1$ and $\mathcal{X}_2$ have no intersection point at infinity, which means that they have no common components by Theorem 4.4. Then we can apply Bezout's Theorem.

$$|\mathcal{Z}_{\mathbb{F}_{2^m}}(A,B)|\leq 2^{2^{6i}}2^{2^{6i}}=2^{12i}$$

Since $\gcd(3i,m)=1$ and m is odd, $\gcd(2i,m)=1$. Hence, $k=2i$, which means $d_1=d_2=3$. Therefore, we have $s=dim_{\mathbb{F}_2}\wedge_{\lambda,\mu}\leq 6$.

By the above calculations, we observe that for the component function corresponding to $(\lambda,\mu)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}\backslash\{(0,0)\}$, we have $|W_{F_{\lambda,\mu}}(u,v)|\leq 2^{m+3}$ for all $(u,v)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ since $s=dim_{\mathbb{F}_2}\wedge_{\lambda,\mu}\leq 6$. Hence, we obtain the following theorem.

Theorem 5.3. *Let*

$$F(x,y)=(x^{2^i+1}+xy^{2^i}+y^{2^i+1},x^{2^{3i}}y+xy^{2^{3i}})$$

be a function on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ *where* $\gcd(3i,m)=1$, *and* m *is odd. Then* $|W_{F_{\lambda,\mu}}(u,v)|\leq 2^{m+3}$ *for all* $(u,v)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$.

In particular, by Theorem 5.3, we have the following conclusion.

Corollary 5.2. The nonlinearity of F given in Theorem 5.3 is $\mathcal{N}(F) \geq 2^{2m-1} - 2^m$.

Proof. By Definition 3.5, for the components $F_{\lambda,\mu}$ of $F(x,y)$ corresponding to $(\lambda,\mu) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \backslash \{(0,0)\}$, we have

$$\mathcal{L}(F_{\lambda,\mu}) = \max_{(u,v)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}} |W_{F_{\lambda,\mu}}(u,v)| \leq 2^{m+3}$$

by Theorem 5.2. Then

$$\mathcal{L}(F) = \max_{(\lambda,\mu)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}\backslash\{(0,0)\}} \mathcal{L}(F_{\lambda,\mu}) \leq 2^{m+3}.$$

Therefore, the nonlinearity of F is

$$\mathcal{N}(F) = 2^{2m-1} - \frac{1}{2}\mathcal{L}(F) \geq 2^{2m-1} - \frac{1}{2}2^{m+3} = 2^{2m-1} - 2^{m+2}.$$

□

BIBLIOGRAPHY

Anbar, N., Kalaycı, T., & Meidl, W. (2019). Determining the walsh spectra of taniguchi's and related apn-functions. *Finite Fields and Their Applications*, *60*, 101577.

Berger, T. P., Canteaut, A., Charpin, P., & Laigle-Chapuy, Y. (2005). *Almost perfect nonlinear functions*. PhD thesis, INRIA.

Biham, E. & Shamir, A. (1991). Differential cryptanalysis of des-like cryptosystems. *Journal of CRYPTOLOGY*, *4*, 3–72.

Bracken, C., Byrne, E., Markin, N., & McGuire, G. (2009). Fourier spectra of binomial apn functions. *SIAM Journal on Discrete Mathematics*, *23*(2), 596–608.

Budaghyan, L., Helleseth, T., & Kaleyski, N. (2020). A new family of apn quadrinomials. *IEEE Transactions on Information Theory*, *66*(11), 7081–7087.

Carlet, C., Charpin, P., & Zinoviev, V. (1998). Codes, bent functions, and permutations suitable for des-like cryptosystems. *Designs, Codes and Cryptography*, *15*, 125–156.

Chabaud, F. & Vaudenay, S. (1994). Links between differential and linear cryptanalysis. In *Workshop on the Theory and Application of of Cryptographic Techniques*, (pp. 356–365). Springer.

Dillon, J. (2006). slides from talk given at "polynomials over finite fields and applications", held at banff international research station.

Fulton, W. (2008). Algebraic curves. *An Introduction to Algebraic Geometri*, *54*.

Göloğlu, F. (2022). Biprojective almost perfect nonlinear functions. *IEEE Transactions on Information Theory*, *68*(7), 4750–4760.

Hirschfeld, J. W. P., Korchmáros, G., Torres, F., & Orihuela, F. E. T. (2008). *Algebraic curves over a finite field*, volume 20. Princeton University Press.

Janwa, H. & Wilson, R. M. (1993). Hyperplane sections of fermat varieties in p 3 in char. 2 and some applications to cyclic codes. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 10th International Symposium, AAECC-10 San Juan de Puerto Rico, Puerto Rico, May 10–14, 1993 Proceedings 10*, (pp. 180–194). Springer.

Lidl, R. & Niederreiter, H. (1994). *Introduction to finite fields and their applications*. Cambridge university press.

Lidl, R. & Niederreiter, H. (1997). *Finite fields*. Number 20. Cambridge university press.

Matsui, M. (1993). Linear cryptanalysis method for des cipher. In *Workshop on the Theory and Application of Cryptographic Techniques*, (pp. 386–397). Springer.

Menon, D. (2011). Bezout's theorem for curves. *Semantic Scholar, Corpus ID, 50023091*.

Pott, A. (2016). Almost perfect and planar functions. *Designs, Codes and Cryptography*, *78*, 141–195.

Shallue, C. J. (2012). Permutation polynomials of finite fields. *arXiv preprint arXiv:1211.6044*.

Sidelnikov, V. M. (1971). On mutual correlation of sequences. In *Sovi. Math. Dokl.*, volume 12, (pp. 197–201).

Trachtenberg, H. M. (1970). *On the cross-correlation function of maximal linear recurring sequences.* University of Southern California.

Zhang, X.-M. & Zheng, Y. (1996). Gac—the criterion for global avalanche characteristics of cryptographic functions. *J. UCS The Journal of Universal Computer Science: Annual Print and CD-ROM Archive Edition Volume 1 • 1995*, 320–337.