ON PLANAR FUNCTIONS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

FUAD HAMIDLI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

SEPTEMBER 2011

Approval of the thesis:

ON PLANAR FUNCTIONS

submitted by **FUAD HAMIDLI** in partial fulfillment of the requirements for the degree of **Master of Science in Department of Cryptography, Middle East Technical University** by,

Ersan Akyıldız _____
Director, Graduate School of **Applied Mathematics**

Ferruh Özbudak _____
Head of Department, **Cryptography**

Ferruh Özbudak _____
Supervisor, **Department of Mathematics**

Examining Committee Members:

Prof.Dr. Ersan Akyıldız _____
Institute of Applied Mathematics,METU

Prof.Dr. Ferruh Özbudak _____
Department of Mathematics, METU

Asst.Prof.Dr Ömer Küçüksakallı _____
Department of Mathematics, METU

Dr. Muhiddin Uğuz _____
Department of Mathematics, METU

Dr. H.Murat Yıldırım _____
Computer Technology and Information Systems, Bilkent University

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: FUAD HAMIDLI

Signature :

ABSTRACT

ON PLANAR FUNCTIONS

Hamidli, Fuad
M.S., Department of Cryptography
Supervisor : Ferruh Özbudak

September 2011, 35 pages

The notion of ”Planar functions” goes back to Dembowski and Ostrom, who introduced it in 1968 first time to describe projective planes with special properties in finite geometry. Recently, they attracted an interest from cryptography because of having an optimal resistance to differential cryptanalysis.This thesis is based on the paper ”New semifields, PN and APN functions” by Jürgen Bierbrauer. The whole purpose of this thesis is to understand and present a detailed description of the results of the paper of Bierbrauer about planar functions. Here and throughout this thesis ”new” means ”new” in the paper of Bierbrauer. In particular we have no new constructions here and we only explain the results of Bierbrauer.

Keywords: Planar function, semifield, APN function

ÖZ

DÜZLEMSEL FONKSİYONLAR ÜZERİNE

Hamidli, Fuad
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Ferruh Özbudak

Eylül 2011, 35 sayfa

Düzlemsel fonksiyonlar Dembowski ve Ostrom tarafından 1968'de sonlu geometride projektif düzlemleri belirli özellikleri ile tanımlamak için tanıtıldı. Son zamanlarda, diferensiyel kriptanalize karşı optimal direnci olduğu için kriptografide ilgi gördü. Bu tez Jürgen Bierbrauer'in "New semifields, PN and APN functions" isimli makalesine dayanmaktadır. Bu tezin bütün amacı makaleyi anlamak ve Bierbrauer'in düzlemsel fonksiyonlar hakkında olan sonuçlarının detaylı tanımını vermektir. Burada ve bu tez boyunca "yeni" Bierbrauer'in makalesindeki "yeni"yi ifade eder. Özellikle biz bu tezde yeni yapılar kurgulamayıp sadece Bierbrauer'in sonuçlarını açıklıyoruz.

Anahtar Kelimeler: "düzlemsel"(planar) fonksiyon, yarı cisimler (semifields), APN-fonksiyon

To my family and friends

ACKNOWLEDGMENTS

I humbly acknowledge all the help and support extended to me by my advisor Prof.Dr. Ferruh Özbudak. Completion of this thesis would have been impossible without his able guidance and advice. His continued encouragement and direction helped me through difficult times during this thesis and enabled me to fulfill the aimed requirements.

I would also like to show my gratitude to my colleagues Mr Mansoor, Murat and Halil, who were always there to assist me whenever I needed help.

Finally, I would like to mention the support extended by my long-time friend Mr Ruslan Hummatov for his motivational role which also helped me achieve my goal.

TABLE OF CONTENTS

CHAPTER 1

Introduction

The notion of "Planar functions" goes back to Dembowski and Ostrom, who introduced it in 1968 first time to describe projective planes with special properties in finite geometry. Recently, they attracted an interest from cryptography because of having an optimal resistance to differential cryptanalysis. In cryptography, planar functions were first considered in the work of Nyberg and renamed as "perfect nonlinear" (PN).This name describes roughly the importance of planar functions in cryptography as being far from linearity. In addition, the notion "almost perfectly nonlinear" (APN) arose in the theory of S-boxes in characteristic 2 in order to prevent linear attacks. This thesis is a survey on new results of the paper of Bierbrauer about new family of functions that are PN and APN and corresponding new semifields. This part consists of basic definitions and theorems that will be used in next chapters.

1.0.1 Basic definitions, PN and APN functions

Definition 1.0.1 *Let f be a function from $\boldsymbol{F}$ to $\boldsymbol{F}$. Directional derivative of a function f is defined as $f(x+a)-f(x)$ for every $a \in \boldsymbol{F}$ and $a \neq 0$.*

Definition 1.0.2 *Let p be an odd prime and $\boldsymbol{F} = \mathbb{F}_{p^n}$. A function $f : \boldsymbol{F} \to \boldsymbol{F}$ is called a planar function or perfectly nonlinear (PN) if for each $a \neq 0$ and $a \in \boldsymbol{F}$ the directional derivative defined as above is bijective.*

Or, equivalently we can say that f is planar over finite field $\mathbb{F}_q$ if and only if
$\triangle_a(x) = f(x+a) - f(x) - f(a)$ is one to one for any $0 \neq a \in \mathbb{F}_q$. Here we may think of f as a polynomial with coefficients in $\mathbf{F}$. In this thesis, in order to prove planarity of a given function

we will use this equivalent definition. When characteristic is an odd number then there are close connections to finite geometries and algebra.

Example 1.0.3 *Let $\mathbb{F}_{q^n}$ be finite field. Then $f(x) = x^2$ is a planar function over $\mathbb{F}_{q^n}$ (folklore). This is obvious, since $\triangle_a(x) = f(x+a) - f(x) - f(a) = 2ax$ which is one to one function.*

Definition 1.0.4 *Let $p = 2$ and $\boldsymbol{F} = \mathbb{F}_{2^n}$. A function $f : \boldsymbol{F} \to \boldsymbol{F}$ is called an almost perfectly nonlinear (APN) if for each $a \neq 0$ and $a \in \boldsymbol{F}$ the directional derivative defined as above is two-to-one.*
Equivalently, f is an APN if and only if kernel of $\triangle_a(x)$ has the dimension 1 over finite field $\boldsymbol{F}$.

Definition 1.0.5 *Let $\boldsymbol{F} = \mathbb{F}_{p^n}$ be a finite field with p an odd prime. A polynomial $L : \boldsymbol{F} \to \boldsymbol{F}$ is called a* linearized polynomial *(or additive polynomial or p-polynomial) if L is of the shape*

$$L(x) = \sum_{i}^{n-1} a_i x^{p^i}$$

Observe that, any linearized polynomial satisfies $L(x) + L(y) = L(x+y)$ and $L(\alpha x) = \alpha L(x)$ where $x, y \in \mathbb{F}_q$ and $\alpha \in \mathbb{F}_p$. Conversely, any polynomial satisfying this conditions has to be a linearized polynomial.

Definition 1.0.6 *Let $\boldsymbol{F} = \mathbb{F}_{p^n}$ and p be an odd prime number. A function $f : \boldsymbol{F} \to \boldsymbol{F}$ is called Dembowski-Ostrom (DO) polynomial if all the exponents are sums of two powers of p or f is the form*

$$f(x) = \sum_{i,j=0}^{k} a_{ij} x^{p^i + p^j}$$

1.0.2 Semifields and Presemifields

Let f be a planar function so that $f(0) = 0$. Interpret $f(x+a) - f(x) - f(a) = a * x$. Then observe the followings:
1) $a * x = f(x+a) - f(x) - f(a) = x * a$
2) $a * x = 0$ holds if and only if either $x = 0$ or $a = 0$.
In addition, if we let f to be a Dembowski-Ostrom polynomial then we get an extra property in odd characteristic:

3) $a * (x + y) = a * x + a * y$ and $(a + x) * y = a * y + x * y$ (to prove use the shape of $f(x) = \sum_{i,j=0}^{k} a_{ij} x^{p^i + p^j}$ and put instead)
This properties leads to the notion of semifields and presemifields.

Definition 1.0.7 *An algebra* $\boldsymbol{F}$ *with at least two elements and binary operations + (addition) and* $*$ *is called a finite* ***semifield*** *if it satisfies the followings:*
1) $(\boldsymbol{F}, +)$ *is a group with identity element 0.*
2) $a * (b + c) = a * b + a * c$ *and* $(a + b) * c = a * c + b * c$ *for all a,b,c* $\in \boldsymbol{F}$.
3) $a * b = 0$ *implies* $a = 0$ *or* $b = 0$.
4) There exists $1 \in \boldsymbol{F}$ *such that* $1 * a = a * 1 = a$ *for all* $a \in \boldsymbol{F}$.
If all the conditions above are satisfied except 4) then $\boldsymbol{F}$ *is called a* ***presemifield****. Note that a semifield (presemifield)* $\boldsymbol{F}$ *is commutative if* $*$ *is commutative.(See [3] for details)*

Example 1.0.8 *(1) A finite field is a trivial example of a semifield.*
(2) $(\mathbb{F}_{q^k}^2, +, *)$ *is a nontrivial semifield of order* q^{2k} *with addition and multiplication defined as follows:*
$(a, b) + (c, d) = (a + c, b + d)$
$(a, b) * (c, d) = (ac + \alpha b^q d^q, ad + bc)$
where q is an odd prime power and α *is a non-square in* $\mathbb{F}_{q^k}$. *(Dickson [4]).*

The relationship between presemifields and D.O polynomials is stated in the following theorem discovered recently by Coulter-Henderson [2]:

Theorem 1.0.9 *The following notions are equivalent:*
i) Commutative presemifields in odd characteristic.
ii) Dembowski-Ostrom polynomials that are planar functions.

It is already explained in introductory part of semifields that if we choose f as a planar D.O polynomial in odd characteristic q and define our multiplication $*$ as $a * x = f(a + x) - f(x) - f(a)$ then $\mathbf{F} = (\mathbb{F}_q, +, *)$ is a commutative presemifield.
Conversely, if $\mathbf{F} = (\mathbb{F}_q, +, *)$ is a commutative presemifield of odd characteristic, then the polynomial given by $f(x) = \frac{1}{2}(x * x)$ is a planar D.O polynomial.
There is also a way to turn presemifield into a semifield. For this we choose our favourite

element, say $e \in \mathbf{F}$ and define new multiplication $\star$ as:

$$(x * e) \star (y * e) = x * y$$

Now with respect to this new multiplication we still have presemifield with an identity element $e * e$.

On the other hand, only a small number of commutative semifields of odd order has been found. Some classes are the followings:

1)The Dickson semifelds, [4]

2) The commutative twisted fields of Albert, [5]

3)The Cohen-Ganley semifields, [6]

4)The Ganley semifields, [7]

5)The Penttila-Williams semifield of order 3^{10}. [8]

Definition 1.0.10 *Let $\boldsymbol{F}_1 = (\mathbb{F}_q, +, *)$ and $\boldsymbol{F}_2 = (\mathbb{F}_q, +, \star)$ be two presemifields. We say that $\boldsymbol{F}_1$ and $\boldsymbol{F}_2$ are isotopic if and only if there exists three invertible polynomials $\boldsymbol{L}_1$, $\boldsymbol{L}_2$ and $\boldsymbol{L}_3 \in \mathbb{F}_q[x]$ such that $\boldsymbol{L}_1(x \star y) = \boldsymbol{L}_2(x) * \boldsymbol{L}_3(y)$ for all $x, y \in \mathbb{F}_q$. In other words, $(\boldsymbol{L}_2, \boldsymbol{L}_3, \boldsymbol{L}_1)$ is an isotopism between $\boldsymbol{F}_1$ and $\boldsymbol{F}_2$.*

1.0.3 Nucleus of a semifield

Definition 1.0.11 *The left nucleus $N_l(\boldsymbol{F})$, the middle nucleus $N_m(\boldsymbol{F})$ and the right nucleus $N_r(\boldsymbol{F})$ of a semifield $\boldsymbol{F}$ are defined as follows:*

$$N_l(\boldsymbol{F}) = \{a \in \boldsymbol{F} \mid a * (b * c) = (a * b) * c \ for\ all\ b, c \in \boldsymbol{F}\}$$

$$N_m(\boldsymbol{F}) = \{b \in \boldsymbol{F} \mid a * (b * c) = (a * b) * c \ for\ all\ a, c \in \boldsymbol{F}\}$$

$$N_r(\boldsymbol{F}) = \{c \in \boldsymbol{F} \mid a * (b * c) = (a * b) * c \ for\ all\ a, b \in \boldsymbol{F}\}$$

*Left nucleus is also called as **kernel**. In addition, $N(\boldsymbol{F})$ is called a nucleus of $\boldsymbol{F}$ if*

$$N(\boldsymbol{F}) = N_l(\boldsymbol{F}) \cap N_m(\boldsymbol{F}) \cap N_r(\boldsymbol{F})$$

Observe that, $N_l(\mathbf{F}) = N_r(\mathbf{F})$ when the semifield $\mathbf{F}$ is commutative.

Claim 1.0.12 *Kernel of a commutative semifield is contained in middle nucleus.*

Proof. We have to prove that $N_l(\mathbf{F}) \subset N_m(\mathbf{F})$. Choose an element $a \in N_l(\mathbf{F})$ and show that $a \in N_m(\mathbf{F})$, that is prove that a satisfies: $(b * a) * c = b * (a * c)$

$$
\begin{aligned}
(b * a) * c &= (a * b) * c && (\textit{commutativity}) \\
&= a * (b * c) && (a \in N_l(\mathbf{F})) \\
&= a * (c * b) && (\textit{commutativity}) \\
&= (a * c) * b && (a \in N_l(\mathbf{F})) \\
&= b * (a * c) && (\textit{commutativity})
\end{aligned}
$$

Hence $a \in N_m(\mathbf{F})$.

■

CHAPTER 2

New family of functions

In this chapter, a large class of new functions are defined and the method to prove whether such kind of functions are PN or APN in different characteristic [1].

Definition 2.0.13 *Let $q=p^s$, $q'=p^t$, for some positive integers s and t, $\boldsymbol{K}=\mathbb{F}_q \subset \mathbb{F}_{q^k} = \boldsymbol{F}$ and $\boldsymbol{T}: \boldsymbol{F} \to \boldsymbol{K}$ be the trace.*
Let $P(X_0, X_1, \ldots, X_{k-1}, Y_0, Y_1, \ldots, Y_{k-1})=P(X, Y)$ be a homogeneous quadratic polynomial with coefficients in $\boldsymbol{F}$. We can write P as:

$$P(X,Y) = \sum_{o\le i\le j\le k-1} a_{ij}X_iX_j + \sum_{o\le i\le j\le k-1} b_{ij}Y_iY_j + \sum_{o\le i\le j\le k-1} c_{ij}X_iY_j$$

Our new family of function $f: \boldsymbol{F} \to \boldsymbol{F}$ is defined as

$$f(x) = P(x, x^q, \ldots, x^{q^{k-1}}, x^{q'q}, \ldots, x^{q'q^{k-1}}) \tag{2.1}$$

Large class of these functions are PN and APN for different values of k, in odd and in characteristic 2 respectively.

2.1 Method to prove

To prove whether above functions are PN or APN in the cases $k = 3$ and $k = 4$ we will proceed the method described in [1]. We assume $k \le 4$. If $p > 2$ and $\triangle_a(ax)$ is invertible (or has kernel of dimension 0) for all $a \neq 0$ then f is PN or planar. If $p = 2$ and $\triangle_a(ax)$ has a kernel of dimension 1 for all $a \neq 0$ then f is APN.The method is described as follows:

1. Separation: Consider the equation $\mathbf{T}(c\triangle_a(ax)) = 0$ for suitable $c \in \mathbb{F}_{q^k}$. Collect the terms with q' in the exponent to the right side and use elementary properties of trace function to get the equation:

$$T(c_1 x) = T(c_2 x^{q'})$$

where c_1 and c_2 are in $\mathbb{F}_{q^k}$ (depend on c).

2. $\mathbb{F}_q$-linear equation: Find values of c so that either $c_1 = 0$ and $c_2 \neq 0$ or $c_1 \neq 0$ and $c_2 = 0$. Obtain :

$$T(c_2 x^{q'}) = 0$$

$$T(c_1^{q'} x^{q'}) = 0$$

in the first case and in the second case respectively.

3. Non-degeneracy: Show that these two $\mathbb{F}_q$-linear equations for the unknown $x^{q'}$ are linearly independent.

4. Reduction: Show that $x \in \mathbb{F}_q$ satisfies both equations in case $k = 3$. Show that $x \in \mathbb{F}_{q^2}$ satisfies both equations in case $k = 4$.

5. Final: Show that for arbitrary $a \neq 0$ and $x \in \mathbb{F}_q$ (when $k = 3$) respectively $x \in \mathbb{F}_{q^2}$ (for $k = 4$) the kernel of the linear mapping $\triangle_a(ax)$ has the dimension 0 in odd characteristic (for planar case), and dimension 1 in characteristic 2.

Before passing to the chapter 3, we need to prove some basic things related to elementary algebra.

Lemma 2.1.1 *For any integers $p \geq 2$, $k \geq 1$ and $m \geq 1$ we have*

$$gcd(p^k - 1, p^m - 1) = p^{gcd(k,m)} - 1$$

Proof. Let $b = gcd(k, m)$. Then it is obvious that, $p^b - 1$ divides $p^k - 1$ and $p^m - 1$ and hence $c = gcd(p^k - 1, p^m - 1)$. If we show that c divides $p^b - 1$ then proof will be done.

Obviously, $c \mid (p^k - 1)$ and $c \mid (p^m - 1)$. Now write $k = md_1 + e_1$ for some integers with $d \geq 0$ and $m > e \geq 0$.

Write $p^k - 1 = (p^{dm} - 1)p^e + (p^e - 1)$. Since $c \mid (p^m - 1)$ and $(p^m - 1) \mid (p^{dm} - 1)$, $c \mid (p^{dm} - 1)$. And since $c \mid p^k - 1 \Rightarrow c \mid p^e - 1$. We continue this process in analogue with the Euclidean algorithm for k and m. (i.e, in second step we get $m = e_1 f_1 + e_2$ and find that $c \mid p^{e_2} - 1$)

When we reach to the last step we get $c \mid p^{gcd(k,m)} - 1 = p^b - 1$. Hence $c = p^{gcd(k,m)} - 1$.

■

In the following claim we collect the main facts that are used in the proofs in the next chapter.

Claim 2.1.2 *Let p be a prime*

i) Let $1 \leq l \leq p^n - 1$ *and a be a nonzero element o* $\mathbb{F}_{p^n}$*. Then* $x^l = a$ *has a solution in* $\mathbb{F}_{p^n}$ *if and only if a is an l-th power in* $\mathbb{F}_{p^n}$*.*

ii) Let u be a primitive element of $\mathbb{F}_{p^n}$ *and* $1 \leq l \leq p^n - 1$ *be a divisor of* $p^n - 1$*. Then a nonzero element a of* $\mathbb{F}_{p^n}$ *is an l-th power in* $\mathbb{F}_{p^n}$ *if and only if* $a = u^r$ *where* $l \mid r$*.*

iii) Let p be odd and $1 \leq s \leq n$*. Then the equation* $x^{p^s-1} = -1$ *has a solution in* $\mathbb{F}_{p^n}$ *if and only if* $\frac{n}{gcd(n,s)}$ *is an even number.*

Proof. i) This part is trivial, since first assume $x^l = a$ has a solution in $\mathbb{F}_{p^n}$ say, w. Then, $a = w^l$, ie, a is an l-th power in $\mathbb{F}_{p^n}$. For the second part, obviously if a is an l-th power then it satisfies the equation $x^l = a$ in $\mathbb{F}_{p^n}$.

ii) a is an l-th power if and only if $a = w^l$ for some $w \in \mathbb{F}_{p^n}$. And since u is a primitive element, $w = u^k$ for some k. Then we get $a = u^{lk} = u^r$.

iii) Let $t = gcd(n, s)$. Then $gcd(p^s - 1, p^n - 1) = p^t - 1$ (see previous lemma)

Since u is a primitive element then it satisfies,

$$(-1) = u^{(p^n-1)/2}$$

Then the equation $x^{p^s-1} = (-1)$ has a solution if and only if

$$p^s - 1 \mid (p^n - 1)/2$$

(from i) and ii)). And since $p^t - 1 \mid p^s - 1$,

$$p^t - 1 \mid (p^n - 1)/2$$

We can assume that $n = tv$ for some integer v (because $t = gcd(n, s)$). Then observe that,

$$p^n - 1 = p^{tv} - 1 = (p^t - 1)(p^{t(v-1)} + p^{t(v-2)} + ... + p + 1)$$

So $p^t - 1 \mid (p^n - 1)/2$ if and only if $(p^{t(v-1)} + p^{t(v-2)} + ... + p + 1)$ is even. Equivalently, it has an even number of summands, i.e $v = \frac{n}{gcd(n,s)}$ is even.

■

CHAPTER 3

Planar functions

Definition 3.0.3 *Let p be an odd prime, $q=p^s$, $q'=p^t$, for some positive integers s and t, $\boldsymbol{K}=\mathbb{F}_q \subset \mathbb{F}_{q^k} = \boldsymbol{F}$ and $\boldsymbol{T}: \boldsymbol{F} \to \boldsymbol{K}$ be the trace.*
Let $P(X_0, X_1, \ldots, X_{k-1}, Y_0, Y_1, \ldots, Y_{k-1})=X_0Y_0 - vX_{k-1}Y_1$ where $v \in (\boldsymbol{F}^*)^{q-1}$ and P(X,Y) is the homogeneous quadratic polynomial with coefficients in $\boldsymbol{F}$.
Our new family of function $f: \boldsymbol{F} \to \boldsymbol{F}$ is defined as

$$f(x) = P(x, x^q, \ldots, x^{q^{k-1}}, x^{q'q}, \ldots, x^{q'q^{k-1}}) \tag{3.1}$$

By simple substitutions we can easily see that:

$$f(x) = x^{q'+1} - vx^{q^{k-1}+q'q} \tag{3.2}$$

Note that, f(x) is constructed in the way that described in Definition 2.0.6. In this chapter, we will try to understand and explain the reason why f(x) is PN when k=3 and k=4 following the method described in Chapter 2 for planar case. Note also that the result is new for the case k=4.[1]

Lemma 3.0.4 *Under the assumptions of definition 3.0.3 and definitions in introduction part we have:*

$$\frac{\triangle_a(ax)}{a^{1+q'}} = (x + x^{q'}) - u(x^{q^{k-1}} + x^{q'q})$$

where, $u = va^m = w^{q-1} \in (\boldsymbol{F}^*)^{q-1}$ and $m = q^{k-1} + qq' - q' - 1$

Proof. From definition of $\triangle$: $\triangle_a(x) = ax^{q'} + xa^{q'} - v(a^{q^{k-1}}x^{q'q} + a^{q'q}x^{q^{k-1}})$
Hence we have:

$\triangle_a(ax) = a^{q'+1}x^{q'} + a^{q'+1}x - v(a^{q^{k-1}+q'q}x^{q'q} + a^{q'q+q^{k-1}}x^{q^{k-1}})$

$\triangle_a(ax) = a^{q'+1}x^{q'} + a^{q'+1}x - a^{q^{k-1}+q'q}v(x^{q'q} + x^{q^{k-1}})$

$\triangle_a(ax) = a^{q'+1}[x^{q'} + x - a^{q^{k-1}+q'q-q'-1}v(x^{q'q} + x^{q^{k-1}})] \Rightarrow$ divide both side by $a^{1+q'}$ to get:

$$\frac{\triangle_a(ax)}{a^{1+q'}} = x^{q'} + x - a^{q^{k-1}+q'q-q'-1}v(x^{q'q} + x^{q^{k-1}})$$

Let $u = va^m = w \in (\mathbf{F}^*)^{q-1}$ where $m = q^{k-1} + qq' - q' - 1$ then we get

$$\frac{\triangle_a(ax)}{a^{1+q'}} = (x + x^{q'}) - u(x^{q^{k-1}} + x^{q'q})$$

that completes the proof. ■

Lemma 3.0.5 *Considering the same assumptions above,*

$$\triangle_a(ax) = 0$$

implies:

$$\boldsymbol{T}((\frac{1}{w^{q^{k-1}}} - \frac{1}{w^q})x^{q'}) = 0 \tag{3.3}$$

$$\boldsymbol{T}((w^{q'} - w^{q'q^2})x^{q'}) = 0 \tag{3.4}$$

where $\boldsymbol{T}$ *is the trace function.*

Proof. By previous lemma

$$\frac{\triangle_a(ax)}{a^{1+q'}} = (x + x^{q'}) - u(x^{q^{k-1}} + x^{q'q})$$

$\triangle_a(ax) = 0$ implies:

$$(x + x^{q'}) - ux^{q^{k-1}} - ux^{q'q} = 0$$

$$x - ux^{q^{k-1}} = ux^{q'q} - x^{q'}$$

then

$$cx - cux^{q^{k-1}} = cux^{q'q} - cx^{q'}$$

for any $c \in (\mathbf{F}^*)^{q-1}$. Hence by taking the trace of both side and using the linearity property of trace we get:

$$\mathbf{T}(cx) - \mathbf{T}(cux^{q^{k-1}}) = \mathbf{T}(cux^{q'q}) - \mathbf{T}(cx^{q'})$$

where $\mathbf{T}$ is the trace function. Now, we will use the fact that $\mathbf{T}(x) = \mathbf{T}(x^q)$ for any $x \in \mathbb{F}_{q^k}$. In this case, $\mathbf{T}(cux^{q^{k-1}}) = \mathbf{T}(c^q u^q x^{q^k}) = \mathbf{T}(c^q u^q x)$ and $\mathbf{T}(cux^{q'q}) = \mathbf{T}(c^{q^{k-1}} u^{q^{k-1}} x^{q'})$. Put everything in the equation above and use the linearity property of the trace function to get:

$$\mathbf{T}(cx - c^q u^q x) = \mathbf{T}(c^{q^{k-1}} u^{q^{k-1}} x^{q'} - cx^{q'})$$

$$\Rightarrow \mathbf{T}((c - c^q u^q)x) = \mathbf{T}((c^{q^{k-1}} u^{q^{k-1}} - c)x^{q'})$$

Now we want to find the value c such that left hand side to be vanished, i.e

$$c - c^q u^q = 0 \Rightarrow c^{1-q} = u^q \Rightarrow c = \frac{1}{w^q}$$

(Note that w and u are the same ones in previous lemma)
when $c = \frac{1}{w^q}$,

$$c^{q^{k-1}} u^{q^{k-1}} - c = \frac{1}{w^{q^{k-1}}} - \frac{1}{w^q}$$

Hence we get first result:

$$\mathbf{T}((\tfrac{1}{w^{q^{k-1}}} - \tfrac{1}{w^q})x^{q'}) = 0$$

Similarly we do same things for the right hand side,

$$c^{q^{k-1}} u^{q^{k-1}} - c = 0 \Rightarrow c^{1-q^{k-1}} = u^{q^{k-1}} \Rightarrow c = w \in \mathbb{F}_{q^k}$$

When $c = w$,

$$c - c^q u^q = w - w^{q^2}$$

We get our second result:

$$\mathbf{T}((w - w^{q^2})x) = 0 \Rightarrow \mathbf{T}((w^{q'} - w^{q'q^2})x^{q'}) = 0$$

■

Claim 3.0.6 *Two equations, (3.3) and (3.4) in Lemma 3.0.4 are satisfied for $x \in \boldsymbol{K} = \mathbb{F}_q$ when $k = 3$ and for $x \in \mathbb{F}_{q^2}$ when $k = 4$*

Proof.

i)Assume that $k = 3$.We will prove that $x \in \mathbb{F}_q$ satisfies both equation in case $k = 3$.

$$\mathbf{T}((\frac{1}{w^{q^{k-1}}} - \frac{1}{w^q})x^{q'}) =$$

$$= \mathbf{T}((\frac{1}{w^{q^2}} - \frac{1}{w^q})x^{q'}) =$$

$$= (\frac{1}{w^{q^2}} - \frac{1}{w^q})x^{q'} + (\frac{1}{w^{q^2}} - \frac{1}{w^q})^q x^{q'q} + (\frac{1}{w^{q^2}} - \frac{1}{w^q})^{q^2} x^{q'q^2} =$$

Use the facts $x \in \mathbb{F}_q \Rightarrow x^q = x$ and $w \in \mathbb{F}_{q^3} \Rightarrow w^{q^3} = w$ and $(a + b)^q = a^q + b^q$ in $\mathbb{F}_q$ with $q = p^s$:

$$= (\frac{1}{w^{q^2}} - \frac{1}{w^q})x^{q'} + (\frac{1}{w^{q^3}} - \frac{1}{w^{q^2}})x^{q'} + (\frac{1}{w^{q^4}} - \frac{1}{w^{q^3}})x^{q'} =$$

$$= (\frac{1}{w^{q^2}} - \frac{1}{w^q} + \frac{1}{w} - \frac{1}{w^{q^2}} + \frac{1}{w^q} - \frac{1}{w})x^{q'} = 0$$

Similarly, for the second equation:

$$\mathbf{T}((w^{q'} - w^{q'q^2})x^{q'}) = (w^{q'} - w^{q'q^2})x^{q'} + (w^{q'} - w^{q'q^2})^q x^{q'q} + (w^{q'} - w^{q'q^2})^{q^2} x^{q'q^2} =$$

$$= (w^{q'} - w^{q'q^2} + w^{q'q} - w^{q'} + w^{q'q^2} - w^{q'q})x^{q'} = 0$$

ii)Assume that $k = 4$ and $x \in \mathbb{F}_{q^2}$. Then $x^{q^2} = x$ and $w^{q^4} = w$. Similar calculations can be done to find:

$$\mathbf{T}((\frac{1}{w^{q^3}} - \frac{1}{w^q})x^{q'}) = (\frac{1}{w^{q^3}} - \frac{1}{w^q})x^{q'} + (\frac{1}{w^{q^3}} - \frac{1}{w^q})^q x^{q'q} + (\frac{1}{w^{q^3}} - \frac{1}{w^q})^{q^2} x^{q'q^2} + (\frac{1}{w^{q^3}} - \frac{1}{w^q})^{q^3} x^{q'q^3} =$$

$$= (\frac{1}{w^{q^3}} - \frac{1}{w^q} + \frac{1}{w^q} - \frac{1}{w^{q^3}})x^q + (\frac{1}{w} - \frac{1}{w^{q^2}} + \frac{1}{w^{q^2}} - \frac{1}{w})x^{q'q} = 0$$

and

$$\mathbf{T}((w^{q'} - w^{q'q^2})x^{q'}) = (w^{q'} - w^{q'q^2})x^{q'} + (w^{q'} - w^{q'q^2})^q x^{q'q} + (w^{q'} - w^{q'q^2})^{q^2} x^{q'q^2} + (w^{q'} - w^{q'q^2})^{q^3} x^{q'q^3} = 0$$

■

Lemma 3.0.7 *The two $\mathbb{F}_q$ - linear conditions on $x^{q'}$ are linearly dependent over $\mathbb{F}_q$ if and only if*

$$\frac{1}{u^{q+q'}} = (1 - u^{1+q^{k-1}})^{(q-1)(qq'-1)} \tag{3.5}$$

Proof. We will denote linear dependency by the sign ∼, i.e, if x and y are linearly dependent we will write $x \sim y$. We already know that $x \sim y$ over $F_q \Leftrightarrow \frac{x}{y} \in F_q \Leftrightarrow (\frac{x}{y})^{q-1} = 1 \Leftrightarrow x^{q-1} = y^{q-1}$.

Recall that, $u = w^{q-1}$, $w \in \mathbb{F}_{q^k}$. By doing simple operations we can get

$$\frac{1}{w^{q^{k-1}}} = \frac{u^{q^{k-1}}}{w}$$

and $uw = w^q$. We have to show that,

$$\frac{1}{w^{q^{k-1}}} - \frac{1}{w^q} \sim w^{q'} - w^{q'q^2} \Leftrightarrow \frac{1}{u^{q+q'}} = (1 - u^{1+q^{k-1}})^{(q-1)(qq'-1)}$$

Observe that,

$$\frac{1}{w^{q^{k-1}}} - \frac{1}{w^q} = \frac{u^{q^{k-1}}}{w} - \frac{1}{uw} = \frac{u^{q^{k-1}+1} - 1}{uw}$$

and

$$w^{q'} - w^{q'q^2} = (w - w^{q^2})^{q'} = w^{q'}(1 - w^{q^2-1})^{q'} = w^{q'}(1 - u^{q+1})^{q'}.$$

$$\frac{u^{q^{k-1}+1} - 1}{uw} \sim w^{q'}(1 - u^{q+1})^{q'} \Leftrightarrow (\frac{u^{q^{k-1}+1} - 1}{uw})^{q-1} = w^{q'(q-1)}(1 - u^{q+1})^{q'(q-1)}$$

Use the identity $w^{q-1} = u$ and simplify the equation to get:

$$\frac{1}{u^{q+q'}} = \frac{(1 - u^{q+1})^{q'(q-1)}}{(u^{q^{k-1}+1} - 1)^{q-1}}$$

Since $q - 1$ is even,

$$(u^{q^{k-1}+1} - 1)^{q-1} = (1 - u^{q^{k-1}+1})^{q-1}$$

If we show the following equality then proof will be completed:

$$\frac{(1 - u^{q+1})^{q'(q-1)}}{(1 - u^{1+q^{k-1}})^{q-1}} = (1 - u^{1+q^{k-1}})^{(q-1)(qq'-1)}$$

But this is obvious, since:

$$\begin{aligned}(1 - u^{1+q^{k-1}})^{q-1}(1 - u^{1+q^{k-1}})^{(q-1)(qq'-1)} &= (1 - u^{1+q^{k-1}})^{q(qq'-1)} \\ &= (1 - u^{q+q^k})^{q(qq'-1)} \\ &= (1 - u^{q+1})^{q'(q-1)}\end{aligned}$$

■

Lemma 3.0.8 *Let $d' = |(\boldsymbol{F}^*)^{q-1}/(\boldsymbol{F}^*)^m|$, (where $|F|$ denotes the order of given field F) then $d' = gcd(q^{k-1} + q^{k-2} + ... + 1, q^{k-1} - q')$. Furthermore, d' divides $p^{gcd(ks,(k-1)s-t)} - 1$.*

Proof. From elementary algebra we know that $|A/B| = |A|/|B|$ for any group A and B. Furthermore, $|A^n| = \frac{|A|}{gcd(|A|,n)}$. So, by using these identities we can obtain:

$$|(\mathbf{F}^*)^{q-1}| = \frac{|\mathbf{F}^*|}{gcd(|\mathbf{F}^*|, q-1)} = \frac{q^k - 1}{gcd(q^k - 1, q - 1)} = \frac{q^k - 1}{q - 1}$$

and

$$|(\mathbf{F}^*)^m| = \frac{|\mathbf{F}^*|}{gcd(|\mathbf{F}^*|, m)} = \frac{q^k - 1}{gcd(q^k - 1, m)}$$

Hence,

$$d' = |(\mathbf{F}^*)^{q-1}/(\mathbf{F}^*)^m| = \frac{gcd(q^k - 1, m)}{q - 1} = gcd(\frac{q^k - 1}{q - 1}, \frac{m}{q - 1})$$

We already know from Lemma 3.0.4 that

$m = q^{k-1} + qq' - q' - 1 = (q - 1)(q^{k-2} + q^{k-3} + ... + q + 1 + q')$

So,

$$d' = gcd(q^{k-1}+q^{k-2}+...+q+1, q^{k-2}+q^{k-3}+...+q+1+q') = gcd(q^{k-1}+q^{k-2}+...+q+1, q^{k-1}-q')$$

Now, we have to show the second part, ie, d' divides $p^{gcd(ks,(k-1)s-t)} - 1$.

Using that $q = p^s$ and $q' = p^t$ we obtain:

$$d' = gcd(p^{s(k-1)}+p^{s(k-2)}+...+1, p^{s(k-1)}-p^t) = gcd(p^{s(k-1)}+p^{s(k-2)}+...+1, p^t(p^{s(k-1)-t}-1)) =$$

$$= gcd(p^{s(k-1)} + p^{s(k-2)} + ... + 1, p^{s(k-1)-t} - 1)$$

(since $gcd(p^{s(k-1)} + p^{s(k-2)} + ... + 1, p^t) = 1$)

From these equalities we can infer:

$$d' \mid p^{s(k-1)} + p^{s(k-2)} + ... + 1 = \frac{p^{sk} - 1}{p^s - 1} \ \ |p^{sk} - 1 \Rightarrow d' \mid p^{sk} - 1$$

and

$$d' \mid p^{s(k-1)-t} - 1$$

$\Rightarrow d' \mid gcd(p^{sk} - 1, p^{s(k-1)-t} - 1)$

We use Lemma 2.1.1 to see that:

$$gcd(p^{sk} - 1, p^{s(k-1)-t} - 1) = p^{gcd(sk,s(k-1)-t)}$$

which completes the proof. ■

Before proving for $k = 4$ case (which is the new result by Bierbrauer) we will consider the case $k = 3$. But before proving planarity we need to prove the following lemma for this case.

3.0.1 Case k=3

Lemma 3.0.9 *Assume that $k = 3$. Then*

- *i) d' is divisible by $p^{2gcd(s,t)} + p^{gcd(s,t)} + 1$ if $s' + t' \equiv 0(mod\ 3)$*
- *ii) $d' = 3$ if $s' + t' \not\equiv 0(mod\ 3)$ and $q \equiv q' \equiv 1(mod\ 3)$*
- *iii) $d' = 1$ in all other cases.*

where $s' = \frac{s}{gcd(s,t)}$, $t' = \frac{t}{gcd(s,t)}$ and s' is odd.

Proof. Note that in the case $k = 3$, $d' = gcd(p^{2s} + p^s + 1, p^{2s} - p^t) = (p^{2s} + p^s + 1, p^{2s-t} - 1)$ (it is already shown in previous lemma)

- i) Assume that $s' + t' \equiv 0(mod\ 3)$. Then

$\frac{s+t}{gcd(s,t)} \equiv 0(mod\ 3) \Rightarrow s + t \equiv 0(mod\ 3)$

We have to prove two things here:

$p^{2gcd(s,t)} + p^{gcd(s,t)} + 1$ divides $p^{2s-t} - 1$; and $p^{2gcd(s,t)} + p^{gcd(s,t)} + 1$ divides $p^{2s} + p^s + 1$.

Now, observe that

$$gcd(3s, 2s - t) = gcd(3s, 3s - 2s + t) = gcd(3s, s + t) = 3gcd(s, s + t) = 3gcd(s, t)$$

since $s + t \equiv 0(mod\ 3)$.

Hence, we can say that

$$p^{gcd(3s,2s-t)} - 1 = p^{3gcd(s,t)} - 1$$

Again from Lemma 2.1.1,

$$gcd(p^{3s} - 1, p^{2s-t} - 1) = p^{3gcd(s,t)} - 1$$

$$\Rightarrow p^{3gcd(s,t)} - 1 \mid p^{2s-t} - 1$$

$$\Rightarrow p^{2gcd(s,t)} + p^{gcd(s,t)} + 1 \mid p^{2s-t} - 1$$

(because $p^{2gcd(s,t)} + p^{gcd(s,t)} + 1$ divides $p^{3gcd(s,t)} - 1 = (p^{gcd(s,t)} - 1)(p^{2gcd(s,t)} + p^{gcd(s,t)} + 1)$)

Now, it is remained to show that $p^{2gcd(s,t)} + p^{gcd(s,t)} + 1$ divides $p^{2s} + p^s + 1$. We observe that we have a problem: in which cases of a, $T^2 + T + 1$ divides $T^{2a} + T^a + 1$?

By calculating we see that:

$$T^a \equiv \begin{cases} T, & if a \equiv 1(mod 3), \\ -T-1, & if a \equiv 2(mod 3), \\ 1, & if a \equiv 0(mod 3). \end{cases} \tag{3.6}$$

$$T^{2a} \equiv \begin{cases} -T-1, & if a \equiv 1(mod 3), \\ T, & if a \equiv 2(mod 3), \\ 1, & if a \equiv 0(mod 3). \end{cases} \tag{3.7}$$

Hence we obtain that $T^{2a} + T^a + 1 \equiv 0 \pmod{T^2 + T + 1}$ except the case 3 divides a. In fact, if we show that 3 does not divide s' then problem will be done.

Assume that 3 divides s'. Since $s' + t' \equiv 0 \pmod 3 \Rightarrow 3$ divides t'.

$$\frac{s}{gcd(s,t)} = 0(mod 3)$$

$$\frac{t}{gcd(s,t)} = 0(mod 3)$$

$\Rightarrow s = 3m_1 gcd(s,t)$ and $t = 3m_2 gcd(s,t)$ for some m_1 and m_2.

Let

$$gcd(s,t) = a$$

then $s = ap_1$ and $t = ap_2$ where $gcd(p_1, p_2) = 1$. Then we obtain that

$$p_1 = 3m_1$$

and

$$p_2 = 3m_2$$

which implies that $gcd(p_1, p_2) = 3$. Contradiction. Hence, 3 does not divide s' in the case $s' + t' \equiv 0(mod 3)$

• ii) Assume that $s' + t' \not\equiv 0(mod\ 3)$ and $q \equiv q' \equiv 1(mod\ 3)$.

Now consider,

$$gcd(3s, 2s-t) = gcd(3s, 3s-2s+t) = gcd(3s, s+t) = gcd(s, s+t) = gcd(s,t)$$

Observe that, in this case $gcd(3, s+t) = 1$ because of $s' + t' \not\equiv 0(mod\ 3)$.

$$\Rightarrow p^{gcd(3s,2s-t)} - 1 = p^{gcd(s,t)} - 1$$

$$\Rightarrow gcd(p^{3s}-1, p^{2s-t}-1) = p^{gcd(s,t)}-1$$

Now, from definition of d', $d' \mid p^{2s}+p^s+1$.

And since $(p^{2s}+p^s+1) \mid (p^{2s}+p^s+1)(p^s-1) = p^{3s}-1$,

$$\Rightarrow d' \mid p^{3s}-1 \qquad ...(1)$$

Again from definition of d', $d' \mid p^{2s-t}-1$ ...(2)

From (1) and (2)

$$d' \mid gcd(p^{3s}-1, p^{2s-t}-1) = p^{gcd(3s,2s-t)}-1 = p^{gcd(s,t)}-1$$

But since $gcd(s,t) \mid s \Rightarrow p^{gcd(s,t)}-1 \mid p^s-1$

Hence $d' \mid p^s-1$.

$$d' \mid p^{2s}+p^s+1,$$

$$d' \mid p^s-1 \Rightarrow d' \mid gcd(p^{2s}+p^s+1, p^s-1)$$

By doing simple factorization we see that :

$gcd(p^{2s}+p^s+1, p^s-1) = gcd((p^s-1)(p^s+2)+3, p^s-1) = gcd(3, p^s-1)$ $(\star)$

Since $3 \mid p^s-1$,

$gcd(3, p^s-1) = 3 \Rightarrow d' \mid 3$.

In addition, since $p^s \equiv p^t \equiv 1 \pmod 3$ and

$d' = gcd(p^{2s}+p^s+1, p^{2s-t}-1) = gcd(p^{2s}+p^s+1, p^{2s}-p^t)$,

$\Rightarrow 3 \mid d'$.

Hence, $d' = 3$.

• iii) In this case up to $(\star)$ everything is the same in case ii) since we dont use any condition except $s'+t' \not\equiv 0 \pmod 3$ which is the case of iii) also.

We get that $d' \mid gcd(3, p^s-1)$. It is obvious that $gcd(3, p^s-1)$ is either, 3 or 1. Hence $d' \mid 3$ or $d' \mid 1$ implies d' is either 3 or 1.

If we are in the situation that $p^s \equiv 1 \pmod 3$ and $p^t \not\equiv 1 \pmod 3$ then $gcd(3, p^s-1) = 3$ and $d' = gcd(p^{2s}+p^s+1, p^{2s}-p^t)$ can not be 3 because 3 does not divide $p^{2s}-p^t$.So $d' = 1$.

If we are in the situation that $p^s \not\equiv 1 \pmod 3$ and $p^t \equiv 1 \pmod 3$ then $gcd(3, p^s-1) = 1$ and since d' divides $gcd(3, p^s-1)$ we get $d' = 1$. ■

Now, by using the lemma above, for the condition $k = 3$ we will prove that new family of functions defined in the Definition 3.0.3 are planar for some conditions.

Theorem 3.0.10 *Let p be an odd prime, $q = p^s$, $q' = p^t$, for some positive integers s and t, $\boldsymbol{F} = \mathbb{F}_{q^3}$ (ie. $k = 3$), $s' = \frac{s}{gcd(s,t)}$, $t' = \frac{t}{gcd(s,t)}$ and s' is odd. Let $f : \boldsymbol{F} \to \boldsymbol{F}$ be defined as:*

$$f(x) = x^{1+q'} - vx^{q^2+qq'}$$

where $ord(v) = q^2 + q + 1$.

Then f is a planar function in each of the following cases:

• $s' + t' \equiv 0$(*mod 3)*

and

• $q \equiv q' \equiv 1$(*mod 3)*

Proof. Observe that, we are in the situation of Definition 2.0.1. To prove the theorem we proceed as the method defined for $k = 3$ and $k = 4$ in the paper of Bierbrauer (see [1]).
Assume that $\triangle_a(ax) = 0$. Our aim is to show that $\triangle(x)$ is one to one. Since $\triangle_a(ax) = 0$,

$$x + x^{q'} - u(x^{q^2} + x^{qq'}) = 0 \tag{3.8}$$

where $u = va^m = va^{q^2+qq'-q'-1} \in (\mathbb{F}^*_{q^3})^{q-1}$. In this case it is proved in Lemma 3.0.5 we have two conditions, and when $k = 3$ we get:

$$T((\frac{1}{w^{q^2}} + \frac{1}{w^q})x^{q'}) = 0$$

$$T((w^{q'} - w^{q'q^2})x^{q'}) = 0$$

Now, assume that these two equations are linearly dependent over $\mathbb{F}_q$. Then by Lemma 3.0.7:

$$\frac{1}{u^{q+q'}} = (1 - u^{1+q^2})^{(q-1)(qq'-1)} \tag{3.9}$$

For the proof of theorem we will look 2 cases given in the theorem:

• **Case1**: $s' + t' \equiv 0$(mod 3)
In the equation (3.9), right hand side (RHS), ie, $(1 - u^{1+q^2})^{(q-1)(qq'-1)}$ has the exponent:

$$qq' - 1 = p^s p^t - 1 = p^{s+t} - 1 = p^{s'gcd(s,t)+t'gcd(s,t)} - 1 = p^{(s'+t')gcd(s,t)} - 1$$

Now, since $3 \mid s' + t'$ (our case)

$$\Rightarrow p^{3gcd(s,t)} - 1 \mid p^{(s'+t')gcd(s,t)} - 1 = qq' - 1$$

$$\Rightarrow (p^{gcd(s,t)} - 1)(p^{2gcd(s,t)} + p^{gcd(s,t)} + 1) = p^{3gcd(s,t)} - 1 \mid qq' - 1$$

Hence we conclude that

$$(1-u^{1+q^2})^{(q-1)(qq'-1)} \in (\mathbb{F}^*_{q^k})^{(q-1)(p^{2gcd(s,t)}+p^{gcd(s,t)}+1)}$$

(Recall from Lemma 3.0.4 that,
$u = va^m$, where $a \in \mathbb{F}_{q^3}$, $v \in (\mathbb{F}^*_{q^3})^{q-1}$ and $m = q^2 + qq' - q' - 1 = (q-1)(q+q'+1)$.
Furthermore, $d' = gcd(q^2+q+1, q'+q+1)$ in this case)
Now, by Lemma 3.0.9,

$$p^{2gcd(s,t)} + p^{gcd(s,t)} + 1 \mid d' = gcd(q^2+q+1, q'+q+1)$$

Since $d' \mid q'+q+1$,
$\Rightarrow p^{2gcd(s,t)} + p^{gcd(s,t)} + 1 \mid q'+q+1$ holds.

$$\Rightarrow (1-u^{q^2+1})^{(q-1)(qq'-1)} \in (\mathbb{F}^*_{q^3})^{(q-1)(p^{2gcd(s,t)}+p^{gcd(s,t)}+1)}$$

Since

$$\frac{1}{u^{q+q'}} = (1-u^{q^2+1})^{(q-1)(qq'-1)}$$

$$\Rightarrow \frac{1}{u^{q+q'}} \in (\mathbb{F}^*_{q^3})^{(q-1)(p^{2gcd(s,t)}+p^{gcd(s,t)}+1)}$$
$$\Rightarrow u^{q+q'} \in (\mathbb{F}^*_{q^3})^{(q-1)(p^{2gcd(s,t)}+p^{gcd(s,t)}+1)}$$

From Lemma 3.0.4 it is known that $u = va^m$ holds.By using this equality we get

$$u^{q+q'} = (va^m)^{q+q'} = v^{q+q'}a^{(q+q')m}$$

Now, see that

$$a^m = a^{(q-1)(q'+q+1)} \in (\mathbb{F}^*_{q^3})^{(q-1)(p^{2gcd(s,t)}+p^{gcd(s,t)}+1)}$$
$$\Rightarrow a^{(q+q')m} \in (\mathbb{F}^*_{q^3})^{(q-1)(p^{2gcd(s,t)}+p^{gcd(s,t)}+1)}$$
$$\Rightarrow v^{q+q'} \in (\mathbb{F}^*_{q^3})^{(q-1)(p^{2gcd(s,t)}+p^{gcd(s,t)}+1)}$$

By definitions of q and q' (and also s' and t') we get:

$$q+q' = p^{s'gcd(s,t)} + p^{t'gcd(s,t)}$$

It is obvious that, since $ord(v) = q^2+q+1$, v generates $(\mathbb{F}^*_{q^3})^{(q-1)(p^{2gcd(s,t)}+p^{gcd(s,t)}+1)}$.

$$\Rightarrow (p^{2gcd(s,t)} + p^{gcd(s,t)} + 1) \mid q+q' = p^{s'gcd(s,t)} + p^{t'gcd(s,t)}$$

But this is impossible we showed it in the proof of previous lemma part i). Hence, in this case 2 equations given in the beginning can not be linearly dependent.

• **Case2**: $q \equiv q' \equiv 1 (\text{mod } 3)$

For this case, we proved in Lemma 3.0.9 that $d' = gcd(q^2 + q + 1, q' + q + 1) = 3$

Since $3 \mid qq' - 1$ (RHS) of the equation (3.9) satisfies:

$$(1 - u^{q^2+1})^{(q-1)qq'-1)} \in (\mathbb{F}^*_{q^3})^{3(q-1)}$$

Hence (LHS) of the equation (3.9) must satisfy:

$$u^{q+q'} \in (\mathbb{F}^*_{q^3})^{3(q-1)}$$

$$\Rightarrow 3 \mid q + q'$$

On the other hand, $q + q' \equiv 2(mod\ 3)$, ie, not divisible by 3. Contradiction.

As a result, we can conclude that 2 equations are not linearly dependent, so they are linearly independent.

Following the method, it is time to assume that $0 \neq x \in \mathbb{F}_q$.

$x \in \mathbb{F}_q \Rightarrow x^q = x$. Using these identity simplify the equation (3.8) to get:

$$\triangle_a(ax) = (1 - u)(x + x^{q'}) = 0$$

Now, look whether $1 - u = 0$ can hold or not. Remember that, $d' = |(\mathbf{F}^*)^{q-1}/(\mathbf{F}^*)^m|$ where, $(\mathbf{F}^*) = \mathbb{F}_{q^3}$. Since in our both cases, $d' > 1$ and $ord(v) = q^2 + q + 1$ we can say that:

$$v \notin (\mathbf{F}^*)^m$$

And since, $u = va^m$ and $a^m \in (\mathbf{F}^*)^m$ then $u = va^m = 1$ can not hold.

Now, lets look whether $x + x^{q'} = 0$ holds or not. But we already know from Claim 2.1.2 that it can happen if and only if $s' = s/gcd(s, t)$ is even. However, we are given that s' is odd.

We get contradiction to the fact that $x \neq 0$.

Hence we can say that, $\triangle_a(ax) = 0$ if and only if $x = 0$. This means that, $\triangle_a$ is one to one.

Hence , $f(x)$ is planar function in the above conditions given.

■

Up to this point, we used nothing but the proof method of Bierbrauer [1] for $k = 3$. But for $k = 3$ it had already been proven by other scientists also [10]. The new result of Bierbrauer comes when $k = 4$. In this case, we still proceed the same method. In the proof of the following theorem we often refer to the previous definitions and lemmas.

3.0.2 New result: Case k=4

Theorem 3.0.11 *Let p be an odd prime, $q = p^s$, $q' = p^t$, for some positive integers s and t, $\boldsymbol{K} = \mathbb{F}_q$, $\boldsymbol{F} = \mathbb{F}_{q^4}$, $(2s)/gcd(2s, t)$ is odd and $q \equiv q' \equiv 1(mod\ 4)$.*
Let $f : \boldsymbol{F} \to \boldsymbol{F}$ be defined as:

$$f(x) = x^{1+q'} - vx^{q^3+q'q}$$

where $ord(v) = q^3 + q^2 + q + 1$. Then f is a planar function.

But before proving the theorem we need to prove the following claim.

Claim 3.0.12 $d' = gcd(q^3 + q^2 + q + 1, q' + q^2 + q + 1) = 4$ *under the conditions above in the theorem.*

Proof. (of Claim 3.0.12)
Since we are given that $(2s)/gcd(2s, t)$ is odd, it is easy to see that

$$s = 2^{\alpha-1}s', \quad t = 2^{\alpha}t'$$

where α is positive integer and s' and t' are positive odd integers. Before proving the claim, consider $\alpha = 1$ and see what happens in this case.
• $\alpha = 1 \Rightarrow s = s'$ and $t = 2t'$
$\Rightarrow d' = gcd((q + 1)(q^2 + 1), q^3 - q') = gcd((p^s + 1)(p^{2s} + 1), p^{3s} - p^t)$

$$= gcd((p^{s'} + 1)(p^{2s'} + 1), p^{3s'} - p^{2t'})$$

$$= gcd((p^{s'} + 1)(p^{2s'} + 1), p^{2t'}(p^{3s'-2t'} - 1))$$

$$= gcd((p^{s'} + 1)(p^{2s'} + 1), p^{3s'-2t'} - 1)$$

Obviously, $3s' - 2t'$ is an odd number since s' and t' are odd. Call $z = 3s' - 2t'$ and obtain:

$$d' = gcd((p^{s'} + 1)(p^{2s'} + 1), p^z - 1)$$

Let p' be an odd prime divisor of d'. Then, $p' \mid (p^z - 1)$ and $p' \mid (p^{s'} + 1)(p^{2s'} + 1)$. Since p' is prime number, either $p' \mid (p^{s'} + 1)$ or $p' \mid (p^{2s'} + 1)$.
First assume that $p' \mid (p^{s'} + 1)$. Then

$$p^{s'} \equiv -1(mod\ p')$$

Since z is an odd number :

$$p^{s'z} \equiv -1(mod\ p')$$

On the other hand, since $p' \mid (p^z - 1)$:

$$p^z \equiv 1(mod\ p')$$

And since s' is odd, raise the power to get:

$$p^{s'z} \equiv 1(mod\ p')$$

which is the contradiction.

Now we can assume that $p' \mid (p^{2s'} + 1)$. Similarly,

$$p^{2s'} \equiv -1(mod\ p')$$

$$\Rightarrow p^{2s'z} \equiv -1(mod\ p')$$

$$p^z \equiv 1(mod\ p')$$

$$\Rightarrow p^{2s'z} \equiv 1(mod\ p')$$

Contradiction. Hence , there can not be an odd prime divisor of d'.This means that, d' is of the form 2^e for some positive integer e. Now, since it is given, $(p^s + 1) \equiv 2(mod\ 4)$ and $(p^{2s} + 1) \equiv 2(mod\ 4)$. Then, $4 \mid (p^s + 1)(p^{2s} + 1)$ but $8 \nmid (p^s + 1)(p^{2s} + 1)$.

And obviously $4 \mid (p^{3s} - p^t)$ by the same reason. Hence, $4 \mid d' = gcd((p^s+1)(p^{2s}+1)), p^{3s} - p^{2t})$ but $8 \nmid d'$. We can conclude that $d' = 4$ since d' is of the form 2^e and $4 \mid d'$.

• $\alpha \geq 2 \Rightarrow p^s \equiv p^{2^{\alpha-1}s'} \equiv (p^{s'})^{2^{\alpha-1}} \equiv 1(mod\ 8)$,(Since square of an od number gives 1 mod 8)

Similarly, $p^t \equiv p^{2^\alpha t'} \equiv (p^{t'})^{2^\alpha} \equiv 1(mod\ 8)$ by the same reason.Then $(q+1)(q^2+1) \equiv 4(mod\ 8)$.

The rest is the same as the case $\alpha = 1$:

$d' = gcd((p^{2^{\alpha-1}s'}+1)(p^{2^\alpha s'}+1), p^z-1)$ where z is the same z in the first part (odd). Now, assume that p' is an any odd prime divisor of d'.Then $p' \mid (p^{2^{\alpha-1}s'}+1)(p^{2^\alpha s'}+1)$ and $p' \mid (p^{2^{\alpha-1}s'}(p^z-1)$

$\Rightarrow$ either $p' \mid (p^{2^{\alpha-1}s'} + 1)$ or $p' \mid (p^{2^\alpha s'} + 1)$

If $p' \mid (p^{2^{\alpha-1}s'} + 1)$, then $p^{2^{\alpha-1}s'} \equiv -1(mod\ p') \Rightarrow p^{2^{\alpha-1}s'z} \equiv -1(mod\ p')$ (since z is odd).On the other hand, $p^z \equiv 1(mod\ p') \Rightarrow p^{2^{\alpha-1}s'z} \equiv 1(mod\ p')$.Contradiction.

If $p' \mid (p^{2^\alpha s'} + 1)$, then $p^{2^\alpha s'} \equiv -1(mod\ p') \Rightarrow p^{2^\alpha s'z} \equiv -1(mod\ p')$. But, $p^z \equiv 1(mod\ p') \Rightarrow p^{2^\alpha s'z} \equiv 1(mod\ p')$. Contradiction.

Hence d' is of the form 2^e for some positive integer e. Observe that, $4 \mid d'$ but $8 \nmid d'$

$$\Rightarrow d' = 4$$

■

Claim 3.0.13 *Let Z be a subgroup of order $q+1$, then $|(\boldsymbol{F}^*)^{q-1}/Z(\boldsymbol{F}^*)^m| = 2$. In particular, $u \notin Z$ and $u \notin (\boldsymbol{F}^*)^m$.*

Proof. (of Claim 3.0.13) From previous claim we get

$$|(\mathbf{F}^*)^{q-1}| = 4|(\mathbf{F}^*)^m|$$

We have left to prove that

$$|Z(\mathbf{F}^*)^m| = 2|(\mathbf{F}^*)^m|$$

To calculate $|Z(\mathbf{F}^*)^m| = lcm(|Z|, |(\mathbf{F}^*)^m|)$ we first find $|(\mathbf{F}^*)^m|$:

$$\begin{aligned}
|(\mathbf{F}^*)^m| &= \frac{q^4-1}{gcd(q^4-1,(q-1)(q^2+q+1+q'))} \\
&= \frac{q^3+q^2+q+1}{gcd(q^3+q^2+q+1, q^2+q+1+q')} \\
&= \frac{q^3+q^2+q+1}{d'} = \frac{q^3+q^2+q+1}{4}
\end{aligned}$$

Using this equality we find

$$\begin{aligned}
|Z(\mathbf{F}^*)^m| &= lcm(q+1, \frac{q^3+q^2+q+1}{4}) \\
&= lcm(q+1, \frac{(q+1)(q^2+1)}{4}) \\
&= \frac{(q+1)(q^2+1)}{2}) \\
&= 2|(\mathbf{F}^*)^m|
\end{aligned}$$

Now, lets show that $u \notin Z$. Assume to the contrary that $u \in Z$. Since $|Z| = q+1$, $u^{q+1} = 1$ holds.We already know that $u = va^m$ where v is the $(q-1)$-st power, $m = (q-1)(q'+q^2+q+1)$ and $v, a \in (\mathbf{F}^*)^{q-1} = \mathbb{F}_{q^4}$. Raise the power to $(q+1)$ in both sides to get:

$$u^{q+1} = v^{q+1}a^{m(q+1)}$$

$$\Rightarrow 1 = v^{q+1}a^{m(q+1)}$$

$$\Rightarrow v = a^{-m}$$

$$\Rightarrow v \in (\mathbf{F}^*)^m$$

Hence, $ord(v) = (q^3+q^2+q+1)$ must divide $|(\mathbf{F}^*)^m|$. But this is impossible since we have found that $|(\mathbf{F}^*)^m| = (q^3+q^2+q+1)/4 < q^3+q^2+q+1$. We get contradiction, so $u \notin Z$.

Similarly, assume that $u \in (\mathbf{F}^*)^m$. This means that $va^m \in (\mathbf{F}^*)^m$. Impossible since $v \notin (\mathbf{F}^*)^m$ and $a^m \in (\mathbf{F}^*)^m$. ■

Proof.(of Theorem 3.0.11) We follow the method described before and use the Lemma 3.0.4, Lemma 3.0.5 and Lemma 3.0.7 and assume that two $\mathbb{F}_q$-linear conditions are dependent. Then by Lemma 3.0.7 :

$$\frac{1}{u^{q+q'}} = (1-u^{1+q^3})^{(q-1)(qq'-1)}$$

Since it is given, $4 \mid qq'-1$, (RHS) $\in (\mathbf{F}^*)^{4(q-1)}$. On the other hand, (LHS) $\notin (\mathbf{F}^*)^{4(q-1)}$ because $q+q' \equiv 2(mod\ 4)$. We get contradiction, so the equations are linearly independent. It has been proved that $x \in \mathbb{F}_{q^2}$ satisfies both equations. We simplify the equation in Lemma 3.0.5 and get:

$$x + x^{q'} = u(x^q + x^{q'q}) = u(x + x^{q'})^q$$

Assume $x \neq 0$. Recall that, since $2s/gcd(2s,t)$ is odd we have found that $s = 2^{\alpha-1}s'$ and $t = 2^{\alpha}t'$ where s' and t' are odd numbers. Now see that

$$\frac{s}{gcd(s,t)} = \frac{2^{\alpha-1}s'}{gcd(2^{\alpha-1}s', 2^{\alpha}t')} = \frac{s'}{gcd(s', 2t')} = \frac{s'}{gcd(s', t')}$$

Since s' and t' are odd, $s/gcd(s,t)$ is an odd number. Then by Claim 2.1.2, $x + x^{q'} \neq 0$. Then

$$u = (x + x^{q'})^{1-q}$$

We see that u is the $q-1$-st power in $\mathbb{F}_{q^2}$, say $u = n^{q-1} \in \mathbb{F}_{q^2}$. Then by raising power to $q+1$ we get:

$$u^{q+1} = n^{q^2-1} = 1$$

This implies that $u \in Z$, however we showed that this is impossible. Contradiction to the assumption $x \neq 0$.We conclude that, $\triangle_a(ax)$ has the dimension 0, implies that f is planar.

■

3.0.3 About the nuclei

In this part, we estimate the left nucleus and the middle nucleus for the last planar function defined in the Theorem 3.0.11.

Theorem 3.0.14 *Assume that all the conditions in Theorem 3.0.11 are satisfied and f is a planar function. Let $(\boldsymbol{F}, +, \star)$ be a semifield isotopic to a presemifield $(\boldsymbol{F}, +, *)$ determined by f. Then $(\boldsymbol{F}, +, \star)$ has a left nucleus and middle nucleus of dimensions a multiple of $gcd(s,t)$ and $gcd(2s,t)$ respectively.*

Proof. Recall that, we have in the Theorem 3.0.11 that $(2s)/gcd(2s,t)$ is an odd and $s = 2^{\alpha-1}s'$ and $t = 2^{\alpha}t'$ where α is positive integer and s' , t' are odd numbers. These identities help us to see the followings:

$$gcd(2s,t) = gcd(2^{\alpha}s', 2^{\alpha}t') = 2^{\alpha}gcd(s',t')$$

$$gcd(s,t) = gcd(2^{\alpha-1}s', 2^{\alpha}t') = 2^{\alpha-1}gcd(s',2t') = 2^{\alpha-1}gcd(s',t')$$

Hence we can say that, $\mathbb{F}_{q^2} = \mathbb{F}_{p^{2s}}$ has an odd degree over $\mathbb{F}_{p^{gcd(2s,t)}}$ (because $2s = 2^{\alpha}s'$ and $s'/gcd(s',t')$ is also odd). In addition, $\mathbb{F}_{p^{gcd(2s,t)}}$ has a degree 2 over $\mathbb{F}_{p^{gcd(s,t)}}$.
To prove the theorem, we will show that $\mathbb{F}_{p^{gcd(s,t)}}$ is in the left nucleus and $\mathbb{F}_{p^{gcd(2s,t)}}$ is in the middle nucleus of the semifield $(\mathbf{F}, +, \star)$. Now define our corresponding presemifield product as following:

$$x * a = \frac{\triangle_a(x)}{4-4v} = \frac{f(x+a) - f(x) - f(a)}{4-4v}$$
$$= \frac{xa^{q'} + x^{q'}a - vx^{q^3}a^{q'q} - va^{q^3}x^{q'q}}{2-2v}$$

Observe that, 1 is an identity element due to this multiplication and in particular $1 * 1 = 1$. It is already mentioned the way of producing semifield from presemifiled in introduction part,so we apply the procedure : choose our favorite element 1 and define our new semifield multiplication $\star$ as:

$$(x * 1) \star (a * 1) = x * a$$

Now to show that $\mathbb{F}_{p^{gcd(s,t)}}$ is in $N_l(\mathbf{F})$, take any element $b \in \mathbb{F}_{p^{gcd(s,t)}} \subset \mathbb{F}_{p^t}$. Then obviously, b satisfies

$$b^{p^{gcd(s,t)}} = b, \quad b^{p^t} = b, \quad b^{p^s} = b$$

Using these identities we observe the followings:

$$b * 1 = \frac{b + b^{q'} - vb^{q^3} - vb^{q'q}}{2-2v}$$

$$= \frac{b + b - vb - vb}{2-2v} = b = 1 * b$$

$$b * a = \frac{ba^{q'} + ab^{q'} - vb^{q^3}a^{q'q} - va^{q^3}b^{q'q}}{2 - 2v}$$
$$= \frac{ba + ab - vba - vab}{2 - 2v} = ba$$
$$= b(1 * a) = (ba) * 1$$

By definition of $\star$ we have :

$$(b * 1) \star ((x * 1) \star (a * 1)) = (b * 1) \star (x * a)$$

Now,

$$((b * 1) \star (x * 1)) \star (a * 1) = (b * x) \star (a * 1) \quad (\textit{definition})$$
$$= (bx * 1) \star (a * 1) \quad (\textit{identity above})$$
$$= (bx) * a = (b * 1) \star (x * a)$$

Hence, $b * 1 \in N_l(\mathbf{F})$ implies that $\mathbb{F}_{p^{gcd(s,t)}}$ is in $N_l(\mathbf{F})$.

For the $N_m(\mathbf{F})$, we take an element $b \in \mathbb{F}_{p^{gcd(2s,t)}}$ and show that $b * 1$ is in the middle nucleus. Since $b \in \mathbb{F}_{p^{gcd(2s,t)}} \subset \mathbb{F}_{p^t}$, it satisfies:

$$b^{p^{gcd(2s,t)}} = b \quad \textit{and} \quad b^{p^t} = b$$

Similar to the left nucleus case using these identities we get:

$$b * 1 = \frac{b - vb^q}{1 - v}$$

and

$$x * b = \frac{bx + xb - vx^q b^q - vb^q x^q}{2 - 2v} = \frac{2bx - 2vx^q b^q}{2 - 2v}$$
$$(bx) * 1 = \frac{2bx - 2vx^q b^q}{2 - 2v}$$
$$\Rightarrow x * b = (bx) * 1$$
$$\Rightarrow x * (ba) = (bx) * a$$

for any x. Now it follows that

$$((x * 1) \star (b * 1)) \star (a * 1) = (x * b) \star (a * 1)$$
$$= (bx * 1) \star (a * 1)$$
$$= (bx) * a$$
$$(x * 1) \star ((b * 1) \star (a * 1)) = (x * 1) \star (b * a)$$

$$= (x * 1) \star (ba * 1)$$

$$= x * (ba)$$

And we already know that $x * (ba) = (bx) * a$, hence $\mathbb{F}_{p^{gcd(2s,t)}}$ is in middle nucleus, that completes the proof.

■

CHAPTER 4

Some APN polynomials

In this chapter some APN functions that are constructed in the way of definition in Chapter 2 are illustrated. Note that, now we are in even characteristic, namely in characteristic 2. We have two theorems for the cases $k = 2$ and $k = 3$ respectively.[1] Proof idea is the same as the method described in Chapter 2, we will proceed the same steps. Our aim is to show that, the kernel of $\triangle_a(x)$ has the dimension 1.

Theorem 4.0.15 *Let s be odd and t be an even number satisfying $t < 2s$ and $gcd(s,t) = 1$. Let $q = 2^s$, $q' = 2^t$, $\boldsymbol{F} = \mathbb{F}_{q^2}$, $v \in \boldsymbol{F}\backslash\mathbb{F}_q$ and $u \notin (\boldsymbol{F}^*)^3$. Then the function*

$$f(x) = ux^{1+qq'} + u^q x^{q+q'} + vx^{q'(1+q)}$$

is an APN.

Proof. By looking Chapter 2 for the new family of functions defined, we see that the function in the theorem satisfies the properties of these new family. Here we have

$$p = 2, k = 2, \mathbf{K} = \mathbb{F}_q, \mathbf{F} = \mathbb{F}_{q^2}$$

and the quadratic polynomial is defined as

$$P(X_0, X_1, Y_0, Y_1) = uX_0Y_1 + u^qX_1Y_0 + vY_0Y_1$$

Now to proceed, we have to calculate $\triangle_a(ax)$ where $0 \neq a \in \mathbf{F}$. Remember that, $\triangle_a(x) = f(x+a) - f(x) - f(a)$

$$f(x+a) = u(x+a)^{1+qq'} + u^q(x+a)^{qq'+1} + v(x+a)^{q'(1+q)}$$

$$f(x) = ux^{1+qq'} + u^q x^{q+q'} + vx^{q'(1+q)}$$

$$f(a) = ua^{1+qq'} + u^q a^{q+q'} + va^{q'(1+q)}$$

By substituting in the equation and by doing simplifications we get:

$$\triangle_a(x) = u(xa^{qq'} + ax^{qq'}) + u^q(x^q a^{q'} + a^q x^{q'}) + v(x^{q'} a^{q'q} + a^{q'} x^{q'q})$$

Now we find $\triangle_a(ax)$, by putting ax instead of x:

$$\triangle_a(ax) = ua^{1+qq'}(x + x^{qq'}) + u^q a^{q'+q}(x^q + x^{q'}) + va^{q'(1+q)}(x^{q'} + x^{q'q})$$

We have to prove that the kernel of $\triangle_a(ax)$ has dimension 1. Since $k = 2$ we need only one **K**-linear equation. To get equation, take trace of each side and equalize to 0, $\mathbf{T}(c\triangle_a(ax)) = 0$ (Separation step- collect the terms involving $x^{q'}$ to one side) and use the elementary properties of trace function. In this case we take $c = 1$.

$$\mathbf{T}(u^q a^{q'+q} x^{q'}) + \mathbf{T}(va^{q'q+q} x^{q'}) = \mathbf{T}(ua^{q'q+1} x) + \mathbf{T}(ua^{qq'+1} x^{qq'}) + \mathbf{T}(u^q a^{q'+q} x^q) + \mathbf{T}(va^{q'q+q} x^{q'q})$$

To simplify, use the property that $\mathbf{T}(x) = \mathbf{T}(x^q)$:

$$= \mathbf{T}(ua^{q'q+1} x) + \mathbf{T}(u^q a^{q'+q} x^{q'}) + \mathbf{T}(u^q a^{q'+q} x^q) + \mathbf{T}(v^q a^{q'+1} x^{q'})$$

Since we are in characteristic 2 we obtain the following equation:

$$\mathbf{T}((v + v^q)a^{q'+qq'} x^{q'}) = 0$$

Observe that, $v + v^q \neq 0$ since given that $v \notin \mathbb{F}_q$. The solution is non-trivial, so it follows that $x \in \mathbb{F}_q$. Hence we can substitute, $x^q = x$ in the main equation and simplify:

$$\triangle_a(ax) = (ua^{1+q'q} + u^q a^{q'+q})(x + x^{q'}) = 0$$

Claim 4.0.16 $ua^{1+q'q} + u^q a^{q'+q} \neq 0$

Proof. (of Claim 4.0.16): Assume that $ua^{1+q'q} + u^q a^{q'+q} = 0$. Then it follows that

$$ua^{1+q'q} = u^q a^{q'+q} = (ua^{1+q'q})^q$$

This means that $ua^{1+q'q} \in \mathbb{F}_q$. Since, $q = 2^s$ the elements of $\mathbb{F}_q$ are third powers. Observe that, $3 \mid 1 + qq' = 1 + 2^{s+t}$ since $s + t$ is odd. Hence, $a^{1+q'q}$ is also third power. It follows that u has to be third power but this is not true. Contradiction. ■

Now, using the claim above we see that $x + x^{q'} = 0$. But this can happen only if $x \in \mathbb{F}_q$ since $gcd(s,t) = 1$. Hence, the dimension of the kernel of linear mapping $\triangle_a(x)$ has the dimension 1 in characteristic 2, implying that f is an APN.

■

Theorem 4.0.17 *Let $gcd(s,3) = 1$, $gcd(t,3) = 1$, $gcd(s,t) = 1$, $t < 3s$ and 3 divides $s + t$. Let $q = 2^s$, $q' = 2^t$, $\boldsymbol{F} = \mathbb{F}_{q^3}$, $v \in \mathbb{F}_q$ and $u \in \boldsymbol{F} \backslash (\boldsymbol{F}^*)^7$. Then the function*

$$f(x) = ux^{q^2+qq'} + u^q x^{1+q'} + vx^{q'(1+q)}$$

is an APN.

Proof. Function f satisfies the properties of the new family of functions defined before: $p = 2, k = 3$ and $P(X,Y) = uX_2Y_1 + u^qX_0Y_0 + vY_0Y_1$. Then we follow the steps, let $0 \neq a \in \mathbf{F}$:

$$f(x+a) = u(x^{q^2+qq'} + x^{q^2}a^{qq'} + a^{q^2}x^{qq'} + a^{q^2+qq}) + u^q(x^{q'+1} + xa^{q'} + ax^{q'} + a^{q'+1})$$

$$+v(x^{q'+qq'} + x^{q'}a^{q'q} + a^{q'}x^{q'q} + a^{q'+qq'})$$

$$f(a) = ua^{q^2+qq'} + u^q a^{1+q'} + va^{q'(1+q)}$$

Then

$$\triangle_a(x) = u(x^{q^2}a^{qq'} + a^{q^2}x^{qq'}) + u^q(xa^{q'} + ax^{q'}) + v(x^{q'}a^{q'q} + a^{q'}x^{q'q})$$

$$\Rightarrow \triangle_a(ax) = ua^{qq'+q^2}(x^{q^2} + x^{qq'}) + u^q a^{q'+1}(x + x^{q'}) + va^{q'q+q'}(x^{q'} + x^{q'q})$$

The separation step yields the equation $\mathbf{T}(c\triangle_a(ax)) = 0$ for some c. Collect the terms involving $x^{q'}$ to the right side:

$$\mathbf{T}(cua^{q^2+qq'}x^{q^2}) + \mathbf{T}(cu^q a^{1+q'}x) = \mathbf{T}(cu^q a^{1+q'}x^{q'}) + \mathbf{T}(cva^{q'+qq'}x^{q'}) + \mathbf{T}(cua^{q^2+qq'}x^{q'q}) + \mathbf{T}(cva^{q'+qq'}x^{q'q})$$

Use the facts that $\mathbf{T}(x) = \mathbf{T}(x^q)$, $v^q = v$ and $x^{q^3} = x$ to get:

$$\mathbf{T}((c^q u^q a^{1+q'q^2} + cu^q a^{1+q'})x) = \mathbf{T}((cu^q a^{1+q'} + cva^{q'+qq'} + c^{q^2}u^{q^2}a^{q+q'} + c^{q^2}va^{q'q^2+q'})x^{q'}) \quad (4.1)$$

Now we want to find a value of c that makes left side 0:

$$c^q u^q a^{1+q'q^2} + cu^q a^{1+q'} = 0$$

$$\Rightarrow c^q u^q a^{1+q'q^2} = cu^q a^{1+q'}$$

$$\Rightarrow c^{q-1} = a^{q'(1-q^2)}$$

$$\Rightarrow c = a^{-q'(q+1)}$$

$$\Rightarrow c = a^{q'q^2}$$

Last equality comes from the fact that $a \in \mathbb{F}_{q^3}$. Now when $c = a^{q'q^2}$, left side of the equation (4.1) vanishes and the right side becomes:

$$\mathbf{T}((a^{q'q^2}u^q a^{1+q'} + \cancel{a^{q'q^2}va^{q'+qq'}} + a^{q'q}u^{q^2}a^{q+q'} + \cancel{a^{q'q}va^{q'q^2+q'}})x^{q'}) = 0$$

$$\Rightarrow \mathbf{T}((a^{q'q^2+1+q'}u^q + a^{q'q+q+q'}u^{q^2})x^{q'}) = 0$$

Observe that, $(a^{q'q^2+1+q'}u^q)^q = a^{q'q+q+q'}u^{q^2}$. Then call $\alpha = u^q a^{q'q^2+1+q'}$. Hence we get our first condition as :

$$\mathbf{T}((\alpha + \alpha^q)x^{q'}) = 0$$

Now we want to find c so that the right hand side of the equation (4.1) vanishes. That means

$$cu^q a^{1+q'} + cva^{q'+qq'} + c^{q^2}u^{q^2}a^{q+q'} + c^{q^2}va^{q'q^2+q'} = 0$$

$$\Rightarrow c\cancel{a^{q'}}(u^q a + va^{qq'}) = c^{q^2}\cancel{a^{q'}}(u^{q^2}a^q + va^{q'q^2})$$

Observe that, $(u^q a + va^{qq'})^q = u^{q^2}a^q + va^{q'q^2}$

$$\Rightarrow c(u^q a + va^{qq'}) = c^{q^2}(u^q a + va^{qq'})^q$$

$$\Rightarrow c = u^{q^2}a^q + va^{q'q^2}$$

This value of c makes right side of the equation (4.1) 0 and left side is the required second equation.

$$\mathbf{T}(((u^{q^2}a^q + va^{q'q^2})^q u^q a^{1+q'q^2} + (u^{q^2}a^q + va^{q'q^2})u^q a^{1+q'})x) = 0$$

$$\Rightarrow \mathbf{T}((u^{q+1}a^{q^2+q'q^2+1} + \cancel{yu^q a^{q'+q'q^2+1}} + u^{q^2+q}a^{q'+q+1} + \cancel{yu^q a^{q'+q'q^2+1}})x) = 0$$

$$\Rightarrow \mathbf{T}(u^{q+1}a^{q^2+q'q^2+1} + u^{q^2+q}a^{q'+q+1})x) = 0$$

Note that, since we are in characteristic 2, $\mathbf{T}(x) = \mathbf{T}(x^{q'})$. Furthermore,

$$(u^{q+1}a^{q^2+q'q^2+1})^q = u^{q^2+q}a^{q'+q+1}$$

So let $\beta = u^{q+1}a^{q^2+q'q^2+1}$. Then equation becomes:

$$\mathbf{T}((\beta + \beta^q)x) = 0$$

$$\Rightarrow \mathbf{T}((\beta+\beta^q)^{q'}x^{q'})=0$$

This equation is our second $\mathbb{F}_q$-linear equation. Recall that ,

$$\alpha+\alpha^q=a^{q'q^2+1+q'}u^q+a^{q'q+q+q'}u^{q^2}=a^{q'}(a^{q'q^2+1}u^q+a^{q'q+q}u^{q^2})$$

Now let, $\phi=a^{q'q^2+1}u^q+a^{q'q+q}u^{q^2}$. Then

$$\alpha+\alpha^q=a^{q'}\phi$$

Observe also that,

$$\beta+\beta^q=u^qa(a^{q'q^2+1}u^q+a^{q'q+q}u^{q^2})^q=u^qa\phi^q$$

Claim 4.0.18 *$\alpha\notin\mathbb{F}_q$ and $\beta\notin\mathbb{F}_q$. In particular, $\phi\neq 0$.*

Proof.(of Claim 4.0.18) Assume to the contrary that $\alpha\in\mathbb{F}_q$. Then $\alpha=\alpha^q$ holds. Put the value of α instead to get:

$$u^qa^{1+q'+q'q^2}=u^{q^2}a^{q+q'q+q'}$$

$$\Rightarrow u^{q^2-q}=a^{1+q'q^2-q-q'q}$$

$$\Rightarrow u^{q(q-1)}=a^{(q-1)(qq'-1)}$$

$$\Rightarrow u^q=a^{qq'-1}$$

Now since, $3\mid s+t$, then $qq'-1=2^{s+t}-1$ is divisible by 7. Hence right hand side satisfies:

$$a^{qq'-1}\in(\mathbf{F}^*)^7$$

$$\Rightarrow u^q\in(\mathbf{F}^*)^7$$

$$\Rightarrow u\in(\mathbf{F}^*)^7 \qquad (since\ \ 7\not| q)$$

But this is impossible, since given that $u\notin(\mathbf{F}^*)^7$. Contradiction.
Now since $0\neq\alpha+\alpha^q=a^{q'}\phi$, it follows that $\phi\neq 0$. Similarly, since $\phi\neq 0$ and
$0\neq u^qa\phi^q=\beta+\beta^q$ then, $\beta\notin\mathbb{F}_q$. ■

Claim 4.0.19 $\mathbb{F}_q^*\subseteq(\boldsymbol{F}^*)^7=(\mathbb{F}_{q^3}^*)^7$.

Proof.(of Claim 4.0.19) Our aim is to show that there exists $\beta\in(\mathbb{F}_{q^3}^*)^7$ such that β is a primitive element of $\mathbb{F}_q^*$. Since $\mathbb{F}_q^*$ is a cyclic group it has a generator, say α. Obviously,

$\alpha \in \mathbb{F}^*_{q^3}$.

Observe that, when $gcd(s, 3) = 1$ then $gcd(7, 2^s - 1) = 1$ holds. Then we can say that α^7 is also a primitive element of $\mathbb{F}^*_q$. Note that

$$\alpha^7 \in (\mathbb{F}^*_{q^3})^7$$

That helps us to prove that $\mathbb{F}^*_q \subseteq (\mathbf{F}^*)^7 = (\mathbb{F}^*_{q^3})^7$. ■

Assume that two $\mathbb{F}_q$-linear conditions are dependent. Then this is equivalent to saying that

$$\frac{(\beta + \beta^q)^{q'}}{\alpha + \alpha^q} \in \mathbb{F}_q$$

$$\Rightarrow u^{q'q}\phi^{qq'-1} \in \mathbb{F}_q \subseteq (\mathbf{F}^*)^7$$

Obviously, $\phi^{qq'-1} \in (\mathbf{F}^*)^7$ because $7 \mid qq' - 1$.

$$\Rightarrow u^{q'q} \in (\mathbf{F}^*)^7$$

$$\Rightarrow u \in (\mathbf{F}^*)^7$$

Contradiction. Hence two equations are linearly independent and it is known that $x \in \mathbb{F}_q$ satisfies both equation. Now, $\triangle_a(ax) = 0$ simplifies to:

$$(ua^{q^2+q'q} + u^q a^{1+q'})(x + x^{q'}) = 0$$

Show that

$$ua^{q^2+q'q} + u^q a^{1+q'} \neq 0$$

Otherwise,

$$u^{q-1} = a^{(q-1)(q'+q+1)}$$

$$\Rightarrow u = a^{q'+q+1}$$

Now turn to the conditions on s and t. There are only two possibilities:

i)$s = 3m + 1$ and $t = 3n + 2$ or,

ii)$s = 3m + 2$ and $t = 3n + 1$

Observe that, in both cases $q' + q + 1$ is divisible by 7. Hence,

$$u = a^{q'+q+1} \in (\mathbf{F}^*)^7$$

But this is impossible. So $ua^{q^2+q'q} + u^q a^{1+q'} \neq 0$. It follows that

$$x + x^{q'} = 0$$

Since $gcd(s,t) = 1$, this can happen only when $x \in \mathbb{F}_2$. This means that the kernel of $\triangle_a(x)$ has the dimension 1 in characteristic 2, equivalent to saying that f is an APN function.
(For another proof way for this theorem see [9])

■

REFERENCES

[1] J. Bierbrauer. *New semifields, PN and APN functions.* Designs, Codes and Cryptography, v. 54, pp. 189 - 200, 2010.

[2] Coulter, R.S., Henderson, M. *Commutative presemifields and semifields.* Adv.Math. 217, 282-304 (2008)

[3] M.Lavrauw, O.Polverino. *Finite semifields and Galois geometry*, available from *http://cage.ugent.be/ ml*, 2011.

[4] L.E.Dickson. *On commutative linear algebras in which division is always uniquely possible*, Trans.Amer.Math.Soc.,7(1906), pp.514-522.

[5] A.A. Albert, On non-associative division algebras, Trans. Amer. Math. Soc. 72 (1952), 296-309.

[6] S.D. Cohen and M.J. Ganley, Commutative semifields, two-dimensional over their middle nuclei, J. Algebra 75 (1982), 373-385

[7] M.J. Ganley, Central weak nucleus semifields, European J. Combin. 2 (1981), 339-347.

[8] T. Penttila and B. Williams, Ovoids of parabolic spaces, Geom. Dedicata 82 (2000), 1-19.

[9] C.Bracken, E.Byrne, N.Markin, G.McGuire: *New families of quadratic almost perfect nonlinear trinomials and multinomials*, Finite Fields and Their Applications, 2008.

[10] Z. Zha, G. M. Kyureghyan, and X. Wang, *A new family of perfect nonlinear binomials.* Finite Fields and Their Applications, 2009.