ON ALLTOP 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 DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

SEPTEMBER 2017

Approval of the thesis:

ON ALLTOP FUNCTIONS

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

Prof. Dr. Bülent Karasözen _____
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh Özbudak _____
Head of Department, **Cryptography**

Prof. Dr. Ferruh Özbudak _____
Supervisor, **Mathematics/IAM, METU**

Examining Committee Members:

Assoc. Prof. Dr. Ali Doğanaksoy
Mathematics/IAM, METU _____

Prof. Dr. Ersan Akyıldız
Mathematics/IAM, METU _____

Prof. Dr. Ferruh Özbudak
Mathematics/IAM, METU _____

Assist. Prof. Dr. Burcu Gülmez Temür
Mathematics, Atılım University _____

Assist. Prof. Dr. Eda Tekin
Business Administration, Karabuk 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 ALLTOP FUNCTIONS

Hamidli, Fuad
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

September 2017, 53 pages

Let q be a power of an odd prime p and let $\mathbb{F}_q$ be a finite field. A map f is called *planar* on $\mathbb{F}_q$ if for any $a \in \mathbb{F}_q^\star$, the difference map (or derivative of f at a point a) $D_a(x) = f(x+a) - f(x)$ is bijective. The definition of *Alltop function* is that, the difference map at point a in the given field of odd characteristic is itself planar for any $a \in \mathbb{F}_q^*$. Alltop functions have special importance in cryptography and related areas. For example, they are used to construct mutually unbiased bases (MUB) in quantum information theory. The map $x \mapsto x^3$ is an Alltop function in all finite fields found by Alltop in 1980 which is an optimal function with respect to the known bounds on auto and crosscorrelation. Since then it was shown that these kind of functions do not exist when $p = 3$ (Hall, Rao, Donovan). So far, it has been found that x^{q+2} is also an Alltop function over finite field $\mathbb{F}_{q^2}$ where 3 does not divide $q+1$ and this is EA-inequivalent to x^3 whereas its difference function (derivative), which is planar, is EA-equivalent to x^2 (Hall, Rao, Gagola). It is still an open problem whether there exist another EA-inequivalent Alltop functions or any method to construct new Alltop functions.

In this thesis classification of q-cubic Alltop binomials over $\mathbb{F}_{q^2}$ is given. Specifically, $x^3 + ux^{2q+1}$ in $\mathbb{F}_{q^2}$ for $u \in \mathbb{F}_{q^2}^*$ is analyzed and for this case permutation polynomials $L_1(x) = ax + bx^q$ and $L_2(x) = cx + dx^q$ are found that satisfy $L_1 \circ x^3 \circ L_2 = x^3 + ux^{2q+1}$ and $L_1 \circ x^{q+2} \circ L_2 = x^3 + ux^{2q+1}$ for suitable values of u. Hence, by finding suitable values of u, it is shown that this class of functions are EA-equivalent to x^3 and x^{q+2}.

Moreover, except x^3 and the ones in its equivalence class, it is shown that there is no Alltop cubic q-monomials in $\mathbb{F}_{q^3}$. In addition, new notion ”p-ary Alltop functions" are defined from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ and the relation between Alltop functions and p-ary Alltop functions over finite fields is given. Furthermore, some trivial and non-trivial p-ary Alltop functions are found and given.

Keywords: Planar functions, bent functions, Alltop functions, p-ary Alltop functions

ÖZ

ALLTOP FONKSİYONLARI ÜZERİNE

Hamidli, Fuad
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Eylül 2017 , 53 sayfa

q herhangi bir tek asal sayının kuvveti ve $\mathbb{F}_q$ da sonlu cisim olsun. $\mathbb{F}_q$'de tanımlanan f fonksiyonunun bütün $a \in \mathbb{F}_q^*$ noktalarındaki türevi, $D_a f(x) = f(x+a) - f(x)$ birebir ve örtense, f fonksiyonuna düzlemsel fonksiyon denir. Eğer bütün $a \in \mathbb{F}_q^*$ noktalarında türev fonksiyonu kendisi düzlemselse, fonksiyona Alltop fonksiyonu denir. Alltop fonksiyonlarının kriptografi ve ilgili alanlarda özel önemi vardır. Mesela, bu fonksiyonlar kuantum bilgi teorisinde MUB-karşılıklı tarafsız bazlar inşa etmek için kullanılır. x^3 bağıntısı Alltop tarafından 1980'de bulunan bir fonksiyon olup aynı zamanda bilinen oto ve çapraz korelasyon sınırlarına göre ideal ve bütün karakteristiği 3 olmayan sonlu cisimlerde Alltop fonksiyonudur. Daha sonra, bu fonksiyonların p=3'de varolmadığı gösterilmiştir (Hall, Rao, Donovan). Şimdiye kadar x^{q+2} fonksiyonunun da 3-ün $q+1$-i bölmediği durumlarda $\mathbb{F}_{q^2}$ sonlu cismi üzerinde Alltop olduğu ve bunun da x^3-e EA-eşdeğer olmadığı, ama türevinin düzlemsel olup x^2-e EA-eşdeğer olduğu gösterilmiştir. Günümüzde de yeni EA-eşdeğer olmayan Alltop fonksiyonlarının olup olmadığı veya yeni Alltop fonksiyonu üretme yöntemleri bilinmemektedir.
Bu tezde $\mathbb{F}_{q^2}$ sonlu cisminde olan q-kübik Alltop tek terimli ve iki terimli fonksiyonlarının sınıflandırılması yapılmıştır. Özellikle, $\mathbb{F}_{q^2}$ üzerinde ve $u \in \mathbb{F}_{q^2}^*$ için $x^3 + ux^{2q+1}$ fonksiyonu incelenmiş ve bu durum için uygun u değerlerinde $L_1 \circ x^3 \circ L_2 = x^3 + ux^{2q+1}$ ve $L_1 \circ x^{q+2} \circ L_2 = x^3 + ux^{2q+1}$ şartlarını sağlayan $L_1(x) = ax + bx^q$ ve $L_2(x) = cx + dx^q$ lineer permütasyonları bulunmuştur. Böylece, u-nun uygun değerlerinde fonksiyonun x^3 ve x^{q+2}-ye EA-eşdeğer olduğu kanıtlanmıştır. İlaveten, x^3 ve eşdeğer klasları hariç

$\mathbb{F}_{q^3}$'de başka Alltop kübik q-monomialların (tek terimli) varolmadığı kanıtlanmıştır. Ek olarak, $\mathbb{F}_{p^n}$'den $\mathbb{F}_p$'e "p-li Alltop fonksiyonları" kavramı tanımlanmış ve sonlu cisimler üzerinde Alltop fonksiyonları ve p-li Alltop fonkisyonları arasındaki bağlantı verilmiştir. Aynı zamanda bazı bilindik ve bilinmeyen örnekler bulunup verilmiştir.

Anahtar Kelimeler: Düzlemsel fonksiyonlar, bükük fonksiyonlar, Alltop fonksiyonları, p-li Alltop fonksiyonları

to my family

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 family-my mother, father and brother for their supports. In addition, I would like to mention the support extended by my wife Aysel for her motivational role which also helped me achieve my goal.

Finally, I acknowledge the stipend by TUBITAK-BIDEB 2215 program during 2011-2015, which increased my responsibility to finish PhD program.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

FIGURES

CHAPTER 1

INTRODUCTION

In communication systems it has become very often to find new sequences with optimal correlation properties. For example, in the designing process of Code Division Multiple Access systems and similar structures like signal sets, some correlation types such as rms (root mean square) and maximum correlation amplitudes are used. [12]. There are known bounds that are counted as standard for these kinds of correlation types. Welch's bound [33] and Levenstein's bound [16] are the examples of these bounds.

In 1980 W. O. Alltop [1] constructed complex sequences for spread spectrum radar and communication, which met the Welch bound. He used a cubic polynomial over the field $\mathbb{F}_p$ for prime $p > 3$. However, Alltop did not know that this work had results in quantum physics, and his work was not noticed until the appearance of "mutually unbiased bases" notion in quantum information theory.

This construction was extended in [17] for all prime powers ≥ 5 and used to construct MUB (Mutually Unbiased Bases), which is an essential tool in quantum information theory. MUB's were first constructed in 1989 [35] by using quadratic functions over a prime power field. In [12] and in [29] this construction was generalized by using planar functions, the functions that have a wide applications in cryptography. Furthermore, in [12] it was shown that the sequences constructed in this way meet Levenstein's bound.

Although planar functions and Alltop functions are both can also be used to construct MUB's, constructing inequivalent MUB's, from inequivalent functions still remains as one of the difficult problems of quantum information theory.

In 2012 it was shown that Alltop functions do not exist over $\mathbb{F}_{3^n}$ for any positive inte-

ger n [13]. After a while, in 2013 new class of Alltop functions were found and it was shown that this class of function is EA- inequivalent to x^3 which was the only known Alltop function over $\mathbb{F}_{q^2}$ where q is an odd prime power. [14].

It is still an open problem whether there exist another EA-inequivalent Alltop functions or any method to construct new Alltop functions.

This thesis is organized as following manner:

In the first part some basic definitions are given; bent functions, perfectly nonlinear-planar functions, semifields are introduced and some properties, that are also applicable to Alltop functions, are mentioned.

In the second part, definition of Alltop functions and some analogue properties due to the planar functions are given. Moreover, results up to 2013 about Alltop functions are explicitly mentioned.

In the third part, classification of all q-cubic Alltop monomials and binomials over $\mathbb{F}_{q^2}$ is given. Specifically, $x^3 + ux^{2q+1}$ in $\mathbb{F}_{q^2}$ for $u \in \mathbb{F}_{q^2}^*$ is analyzed and for this case permutation polynomials $L_1(x) = ax + bx^q$ and $L_2(x) = cx + dx^q$ are found that satisfy $L_1 \circ x^3 \circ L_2 = x^3 + ux^{2q+1}$ and $L_1 \circ x^{q+2} \circ L_2 = x^3 + ux^{2q+1}$ for suitable values of u. Hence, by finding suitable values of u, it is shown that this class of functions are EA-equivalent to x^3 and x^{q+2}. Moreover, except x^3 and the ones in its equivalence class, it is shown that there is no Alltop cubic q-monomials in $\mathbb{F}_{q^3}$.

In the fourth part, new notion "p-ary Alltop functions" is defined from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ and the relation between Alltop functions and p-ary Alltop functions over finite fields is given. Moreover, cubic p-ary Alltop functions are characterized and some trivial and non-trivial p-ary Alltop functions are found and given.

Finally, in the last part, MUB's are defined and construction method from both-planar functions and Alltop functions is revised. Furthermore, the results of [14] are given.

1.1 Bent Functions

Bent functions were first introduced by Rothaus in 1976 [28] as a combinatorial issue with interesting property; that is these functions have maximum distance to all affine functions. Bent functions are Boolean functions that have extreme nonlinear properties and have a wide applications in cryptography, coding theory, sequence theory,

design theory, combinatorics and other fields.

There is a jubilee survey in [6] and books [25], [32] are also completely devoted to bent functions, especially characterizations, generalizations, variations and applications are mentioned.

In this part it will not be mentioned deeply about bent functions, but will be given a brief introductory definitions and properties, especially in odd characteristic.

In forth part, some characterizations of cubic bent functions are mentioned.

1.1.1 Binary Bent Functions

Definition 1.1.1. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function. Walsh transform of a function f at a point α is defined as*

$$W_f(\alpha) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+x\cdot\alpha}$$

where $x \cdot \alpha = \sum_{i=1}^{n} x_i\alpha_i$ denotes the inner product of binary vectors $\alpha = (\alpha_1, \alpha_2, ...\alpha_n)$ and $x = (x_1, x_2, ..., x_n)$ in $\mathbb{F}_{2^n}$.

Some basic properties of Walsh transform is given as following:

Lemma 1.1.2. *[23]*

$$\sum_{\alpha \in \mathbb{F}_{2^n}} W_f(\alpha)W_f(\alpha+\beta) = \begin{cases} 2^{2n}, & if\, \beta = 0. \\ 0, & if\, \beta \neq 0. \end{cases} \tag{1.1}$$

Corollary of this lemma is Parseval equation:

Corollary 1.1.3.

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

This corollary implies that the average value of the square of the Walsh transforms at point α is 2^n. If Walsh transforms of a function f are the same at all points, then function is called as bent function.

Definition 1.1.4. *The Boolean function $f(x)$ is a bent function if $W_f(\alpha) = \pm 2^{n/2}$ for all $\alpha \in \mathbb{F}_{2^n}$.*

It follows as a consequence that, binary bent functions exist only when n is even. There are several constructions of binary bent functions and there are close connections between bent functions and coding theory.

1.1.2 Generalized Bent Functions

Generalized bent functions or p-ary bent functions were first introduced by Kumar, Scholtz and Welch in 1985 in odd characteristic, similar to binary bent functions.[18]

Definition 1.1.5. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a p-ary function, where p is a prime number and n is a positive integer.*
Then the Walsh transform of a function f at a point α is defined as

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

where $Tr_n : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the absolute trace function and ϵ_p is the complex primitive p-th rooth of unity.

Lemma 1.1.6. *(Parseval equation)*

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

Similar to the binary bent functions, generalized bent functions are defined as following.

Definition 1.1.7. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a p-ary function, where p is a prime number and n is a positive integer.*
Then $f(x)$ is a p-ary bent function (generalized bent) if

$$|W_f(\alpha)| = \pm p^{n/2}$$

for all $\alpha \in \mathbb{F}_{p^n}$.

The bent function f is said to be a *regular bent* function if

$$p^{-n/2} W_f(\alpha) = \epsilon_p^{g(\alpha)}$$

where $g : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $\alpha \in \mathbb{F}_{p^n}$.

The bent function f is said to be a *weakly regular bent* function if

$$\omega p^{-n/2} W_f(\alpha) = \epsilon_p^{g(\alpha)}$$

for some complex number ω where $|\omega| = 1$.

$f(x)$ is called *s-plateaued* if $|W_f(\alpha)| \in \{0, p^{\frac{n+s}{2}}\}$ for all $\alpha \in \mathbb{F}_{p^n}$ and a fixed integer $0 \leq s \leq n$. It is clear that, bent functions are 0-plateaued functions.

Recently new characterizations of p-ary bent functions and plateaued functions by means of the moment of the walsh spectrum in odd characteristics are studied in [24], [27], [26].

In this part, these new characterizations are given and some other characetizations about cubic p-ary bent functions are left to the forth chapter.

Definition 1.1.8. *[24] Let f be a p-ary function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then for any nonnegative integer i, the 2i-th moment of Walsh transform of f is defined as*

$$S_i(f) = \sum_{\alpha \in \mathbb{F}_{p^n}} |W_f(\alpha)|^{2i}$$

with convention that $S_0(f) = p^n$ when $i = 0$.

Theorem 1.1.9. *[24] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then $S_2(f) \geq p^{3n}$ and equality holds if and only if f is bent.*

Proposition 1.1.10. *[24] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then*

$$S_2(f) = p^n \sum_{a,b,x \in \mathbb{F}_{p^n}} \epsilon_p^{D_b D_a f(x)}$$

where $D_b D_a f(x) = f(x + a + b) - f(x + a) - f(x + b) + f(x)$, which is known as the second derivative of a function.

Theorem 1.1.11. *[24] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $\aleph(f)$ be the size of the set $\{(a, b, x) \in \mathbb{F}_{p^n}^3 : D_b D_a f(x) = 0\}$. Then, f is bent if and only if*

$$\aleph(f) = p^{2n} + p^{3n-1} - p^{2n-1}.$$

Corollary 1.1.12. *[24] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. If f is a bent function then*

$$\sum_{\alpha \in \mathbb{F}_{p^n}} |W_f(\alpha)|^{2i} = p^{n(i+1)}$$

for all $i \in \mathbb{N}$.

Corollary 1.1.13. *[24],[27] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then f is bent if and only if*

$$\sum_{a,b,x\in\mathbb{F}_{p^n}} \epsilon_p^{D_b D_a f(x)} = p^{2n}.$$

1.2 Planar Functions

The notion of "Planar functions" was first used by 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 they have some special properties, like an optimal resistance to differential cryptanalysis.
In cryptography, planar functions were first considered in the studies of Nyberg and renamed as "perfect nonlinear" (PN). These functions have been studied intensively and have wide applications in cryptography. There is a detailed survey on perfect nonlinear functions in [3] and some theoretical results of last 25 years are given. In addition, to illustrate the use of perfect nonlinear and almost perfect nonlinear functions some cipher examples are given.
Basic definitions about planar functions are given in the following manner.

Definition 1.2.1. *Let f be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$. Derivative of a function f at a point a is defined as $D_a f(x) = f(x + a) - f(x)$ for every $a \in \mathbb{F}_{p^n}$.*

Definition 1.2.2. *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 the polynomial $f(x)$ is in the shape of the following form:

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

where $a_{ij} \in \mathbb{F}_{p^n}$. Moreover, f is called quadratic if it is a sum of DO polynomial and an affine polynomial.

Definition 1.2.3. *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 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 $0 \neq a \in \mathbb{F}_q$.
Observe that, planar functions do not exist in even characteristic, since in even characteristic $D_a f(x) = D_a f(x+a)$ which contradicts with the definition of planarity. However, recently by changing the definition, new "planar" functions in even characteristic are defined ([30]) and studied.

Example 1.2.4. *Let $\mathbb{F}_{p^n}$ be finite field. Then $f(x) = x^2$ is a planar function over $\mathbb{F}_{p^n}$ (folklore). This is obvious, since $\triangle_a(x) = f(x+a) - f(x) - f(a) = 2ax$ which is one to one function.*

Analogue of perfect nonlinear (planar) functions in even characteristics is APN (almost perfect nonlinear) functions which is defined as below.

Definition 1.2.5. *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 derivative defined, 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 $\boldsymbol{F}$.

Planar functions have also interesting connections between finite commutative semifields and finite geometry (see for example [7], [10], [11]) which is revised in the following subsection.

1.3 Semifields

Definition 1.3.1. *A ring with left and right distributivity with no zero divisors is called a presemifield, and a presemifield with multiplicative identity is called a semifield.*

A semifield need not to be commmutative nor associative. However in the finite case, it was proven that associativity implies commutativity [22].
Any finite presemifield S can be represented as

$$S = (\mathbb{F}_{p^n}, +, \star),$$

where $(\mathbb{F}_{p^n}, +)$ is an additive group and $x \star y = \psi(x, y)$ where $\psi : \mathbb{F}_{p^n}^2 \to \mathbb{F}_{p^n}$.
It is shown in [7], [10] that any finite commutative semifield of odd order can be described by a planar function over a finite field. Moreover, it was also shown that the problem of classifying commutative presemifields of odd order is equivalent to classifying all Dembowski-Ostrom planar functions ([7]). We explicitly revise this result in the following manner.

Definition 1.3.2. *Let $S_1 = (\mathbb{F}_{p^n}, +, \star)$ and $S_2 = (\mathbb{F}_{p^n}, +, *)$ be two presemifields. Then they are called isotopic if there exist three linear permutations L, M and N in $\mathbb{F}_{p^n}$ such that*

$$L(x \star y) = M(x) * N(y)$$

for any $x, y \in \mathbb{F}_{p^n}$. The triple (M,N,L) is called an isotopism between S_1 and S_2.

Every commutative presemifield can be trasformed to a commutative semifield.
Let $S_1 = (\mathbb{F}_{p^n}, +, \star)$ be a commutative presemifield which has no identity element. In order to create a semifield from S_1, pick any $a \in \mathbb{F}_{p^n}^*$ and define a new multiplication $*$ by

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

for all $x, y \in \mathbb{F}_{p^n}$. Then $S_2 = (\mathbb{F}_{p^n}, +, *)$ is a commutative semifield isotopic to S_1 with identity element $a \star a$.
Any commuative presemifield defines a planar Dembowski-Ostrom polynomial and conversely any planar D.O polynomial defines a commutative presemifield. To illustrate, let $f(x)$ be a planar D.O polynomial over $\mathbb{F}_{p^n}$. If $\star$ is defined as

$$x \star y = f(x + y) - f(x) - f(y)$$

for any $x, y \in \mathbb{F}_{p^n}$, then $S = (\mathbb{F}_{p^n}, +, \star)$ is a commutative presemifield.
Conversely, if $S = (\mathbb{F}_{p^n}, +, \star)$ is commutative presemifield with odd order, then a function

$$f(x) = \frac{1}{2}(x \star x)$$

is a planar D.O polynomial. Till now almost all known planar functions are of type Dembowski-Ostrom polynomial except the one in [9] which is not quadratic and power function over $\mathbb{F}_{3^n}$.
There are many intensive studies about commutative semifields for about more than

a hundred years, however, there are only a few number of commutative semifields of odd order found up to now. Some famous examples are Albert's twisted field, Dickson semifields, Coulter-Mathhews and Ding-Yuan semifields, Ganley semifields, Penttila-Williams semifield, and Coulter-Henderson-Kosick semifield (for more see [4]).

1.4 Equivalency criterias

Definition 1.4.1. *Let $\boldsymbol{F} = \mathbb{F}_{p^n}$ be a finite field with p an odd prime.*
A polynomial $L\colon \boldsymbol{F} \to \boldsymbol{F}$ is called a linearized polynomial *(or additive polynomial or p-polynomial) if L is of the shape*

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

In addition, f is called an affine function if it is a sum of a linear function and a constant.

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 $\alpha \in \mathbb{F}_p$. Converse is also the same, that is, any polynomial satisfying this conditions has to be a linearized polynomial.

Definition 1.4.2. *Two functions f and g from $\mathbb{F}_{p^n}$ to itself are called an affine equivalent (linear equivalent) if there are affine (resp.linear) permutations L_1 and L_2 in $\mathbb{F}_{p^n}$ such that*

$$g = L_1 \circ f \circ L_2$$

Definition 1.4.3. *Two functions f and g from $\mathbb{F}_{p^n}$ to itself are EA-equivalent (extended affine equivalent) if there are two affine permutation polynomials L_1 and L_2 and an affine polynomial L_3 in $\mathbb{F}_{p^n}$ such that*

$$g = L_1 \circ f \circ L_2 + L_3$$

Definition 1.4.4. *Two functions f and g from $\mathbb{F}_{p^n}$ to itself are Carlet-Charpin-Zinoviev equivalent (CCZ- equivalent) if for the graphs $G_f = \{(x, f(x)) | x \in \mathbb{F}_{p^n}\}$ and $G_g = \{(x, g(x)) | x \in \mathbb{F}_{p^n}\}$ there exists an affine permutation L in $\mathbb{F}_{p^n}^2$ such that $L(G_f) = G_g$.*

It is obvious that, linear equivalence is a special case of affine equivalence, and an affine equivalence is a special case of EA-equivalence.
In [5] it was shown that EA-equivalence is a particular case of CCZ-equivalence and all permutations are CCZ-equivalent to their inverses.
In fact, CCZ-equivalence is an equivalence relation that preserves PN and APN properties of functions. Hence it is useful to know cases when CCZ and EA-equivalency coincide, as it is difficult to determine whether two functions are CCZ-equivalent or not, when compared with simpler one- EA-equivalency.
In the following lemmas and theorems we revise some basic properties of planar functions. The following lemma in [21] is useful for determining function that whether it is planar or not, in the case that derivative of a function is linearized polynomial.

Lemma 1.4.5. *Let $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a linearized polynomial given as*

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

Then L is a permutation polynomial over $\mathbb{F}_{p^n}$ if and only if L has no non-zero roots in $\mathbb{F}_{p^n}$

It is clear that, if a function f is a planar function and L is an additive function, then $f + L$ is also a planar function.
An analogue of this idea and the folllowing lemma about Alltop functions is given in the next chapter.

Lemma 1.4.6. *[9] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and L is an additive polynomial over the same field. Then the followings are equivalent:*
i) f (L) is a planar polynomial.
ii) L (f) is a planar polynomial
iii) f is a planar polynomial and L is a permutation polynomial.

Proof. **ii) ⇒ iii)** Let $L(f)$ be a planar function. Then by definition,

$$D_a L(f(x)) = L(f(x + a)) - L(f(x)) = L(D_a f(x))$$

is bijective for any $a \in \mathbb{F}_{p^n}^*$.
Assume f is not planar. Then there exist $b \in \mathbb{F}_{p^n}$ such that $D_b f(x)$ is not bijective that

is,

$$D_b f(x) = D_b f(y)$$

for some $y \in \mathbb{F}_{p^n}$ and $y \neq x$. But in this case

$$D_b L(f(x)) = L(D_b f(x)) = L(D_b f(y)) = D_b L(f(y))$$

which is contradiction that $L(f(x))$ is planar function. Hence $f(x)$ is planar function. Assume $L(x)$ is not a permutation. Then there exists $y \in \mathbb{F}_{p^n}$ such that $y \neq x$ and $L(x) = L(y)$. Then since f is planar over $\mathbb{F}_{p^n}$ then $D_a f(x)$ is bijective over $\mathbb{F}_{p^n}$ for all $a \in \mathbb{F}_{p^n}^*$. This means that, for any $y \in \mathbb{F}_{p^n}$ there exists x_1 such that $D_a f(x_1) = y$ for some nonzero a. And also for any $x \in \mathbb{F}_{p^n}$ there exists x_2 such that $D_a f(x_2) = x$ for the same a, where $x_1 \neq x_2$. Then $L(D_a f(x_1)) = L(D_a f(x_2))$.
On the other hand, $D_a L(f(x_1)) = L(D_a f(x_1)) = L(D_a f(x_2)) = D_a L(f(x_2))$ which is contradiction, since $L(f)$ is planar function.
iii) ⇒ ii) Assume that f is planar and L is a permutation. Since L is a permutation then for $x \neq y$ we have $L(x) \neq L(y)$. Now, assume that $L(f(x))$ is not planar function. Then there exsists $y \in \mathbb{F}_{p^n}$ and $y \neq x$ such that

$$D_a L(f(x)) = D_a L(f(y))$$

Since $D_a L(f(x)) = L(D_a f(x))$ and $D_a L(f(y)) = L(D_a f(y))$, then necessarily $L(D_a f(x)) = L(D_a f(y))$.
But since L is a permutation then $D_a f(x) = D_a f(y)$, which is contradiction, since f is a planar function.
iii) ⇒ i) Assume that f is planar, L is a permutation and $f(L(x))$ is not planar. Then there exists $y \in \mathbb{F}_{p^n}, y \neq x$ such that

$$D_a f(L(x)) = D_a f(L(y))$$

for some $a \in \mathbb{F}_{p^n}^*$. Since $L(x)$ is permutation on $\mathbb{F}_{p^n}$, $L(x) = x_1$ and $L(y) = x_2$ for some $x_1, x_2 \in \mathbb{F}_{p^n}$ and $x_1 \neq x_2$. However, in this case $D_a f(x_1) = D_a f(x_2)$ which is contradiction, since f is planar function.
i) ⇒ iii) Assume that $f(L(x))$ is planar function but $L(x)$ is not permutation. Then there is $y \in \mathbb{F}_{p^n}, y \neq x$ such that $L(x) = L(y)$. This is contradiction, since in this case $D_a f(L(x) = D_a f(L(y))$. Hence $L(x)$ is permutation.
Now, assume that $f(x)$ is not planar, then $D_a f(x) = D_a f(y)$ for some $y \in \mathbb{F}_{p^n}, y \neq x$.

Since L is permutation, $x = L(x_1)$ and $y = L(x_2)$ for some x_1, x_2 such that $x_1 \neq x_2$. Then

$$D_a f(L(x_1)) = D_a f(L(x_2))$$

which is contradiction, since $f(L(x))$ is planar function.

□

In fact, the lemma above leads to the definitions of EA-equivalency for planar functions.

CHAPTER 2

ALLTOP FUNCTIONS

Definition 2.0.1. *A function f is called an Alltop function over $\mathbb{F}_q$, if for any $a \in \mathbb{F}_q^*$, derivative*

$$D_a f(x) = f(x+a) - f(x)$$

is planar function, or equivalently, for any $a, b \in \mathbb{F}_q^*$

$$f(x+a+b) - f(x+a) - f(x+b) + f(x)$$

is a permutation polynomial.

Observe that, linear and quadratic functions over $\mathbb{F}_{p^n}$ can not be an Alltop function since derivative of a function is constant which is not permutation polynomial. So, to find Alltop function we need at least cubic functions to check.

Example 2.0.2. *Let $p > 3$ be an odd prime and $f(x) = x^3$ over $\mathbb{F}_{p^n}$.*
Then

$$D_a D_b f(x) = 6abx$$

which is one-to-one in $\mathbb{F}_{p^n}$.
x^3 is known as the original Alltop function, used in the construction of sequences in 1980 by Alltop to meet cross and auto correlation bounds (Welch bound).

In this thesis we let $q = p^n$, where p is an odd prime and n is a positive integer.

Definition 2.0.3. *A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is an even function if $f(0) = 0$ and $f(x) = f(-x)$ for any $x \in \mathbb{F}_q$.*

Definition 2.0.4. *$f : \mathbb{F}_q \to \mathbb{F}_q$ is called 2-to-1 function if*

- $f(0) = 0$
- $f(x) = f(y)$ *holds if and only if* $x = y$ *or* $x = -y$.

both hold.

In the following theorem [34] there is a criteria to characterize planar functions by means of 2-to-1 functions.

Theorem 2.0.5. *Let f be a Dembowski-Ostrom polynomial from $\mathbb{F}_q$ to itself. Then f is planar if and only if f is 2-to-1.*

For Alltop functions we observe the following proposition by means of even functions:

Proposition 2.0.6. *Let f be an even function from $\mathbb{F}_q$ to itself. Then f can not be an Alltop function.*

Proof. Let $f(x)$ be an even function. Assume that $f(x)$ is an Alltop.
Then necessarily, $D_a f(x) = f(x + a) - f(x)$ is planar for any nonzero a. Equivalently, the second derivative

$$D_b D_a f(x) = f(x + a + b) - f(x + a) - f(x + b) + f(x)$$

has to be permutation for all $a, b \in \mathbb{F}_q^*$. Now take $a = 1, b = 1$. Then

$$D_1 D_1 f(x) = f(x + 2) - 2f(x + 1) + f(x)$$

is also a permutation.
However,

$$D_1 D_1 f(-x - 2) = f(-x) - 2f(-x - 1) + f(x + 2)$$

And since f is an even function,

$$D_1 D_1 f(-x - 2) = D_1 D_1 f(x)$$

i.e., the second derivative is not one to one.
Hence, a function $f(x)$ is not an Alltop function. □

2.1 All known results up to 2013

In this section, some properties and results up to 2013 about Alltop functions are given. Specifically, the results of [14] and [13] are revisited. By using some properties of planar functions, some analogues can be considered also for Alltop functions. Equivalency criterias are all exactly the same with planar functions.

Lemma 2.1.1. *[14] Let $f(x)$ be an Alltop, $P(x)$ a Dembowski-Ostrom planar function and $L(x)$ be a linearized polynomial over $\mathbb{F}_{p^n}$. Then*

$$g(x) = f(x) + P(x) + L(x) + c$$

is also an Alltop function, where $c \in \mathbb{F}_{p^n}$ constant

Proof. It is enough to show that, $D_a g(x)$ is planar for any nonzero a.

$$D_a g(x) = g(x+a) - g(x)$$

$$= f(x+a) + P(x+a) + L(x+a) - f(x) - P(x) - L(x)$$

$$= D_a f(x) + D_a P(x) + L(a)$$

Since f is an Alltop function, then $D_a f(x)$ is planar.
$D_a P(x)$ is an additive polynomial and permutation also, since $P(x)$ is planar D.O polynomial. Obviously, L(a) is a constant.
Hence $D_a g(x)$ is a planar function, because of being the sum of planar, linear and constant functions.

□

Lemma 2.1.2. *Let $L(x)$ be a linearized function in $\mathbb{F}_{p^n}$. Then the following are equivalent:*
i) f (L(x)) is Alltop.
ii) L (f(x)) is Alltop.
iii) f (x) is Alltop and L(x) is invertible.

Proof. Proof is similar to the proof of 1.4.6.
ii) $\iff$ iii) $L(f(x))$ is Alltop $\iff$ $D_a L(f(x)) = L(D_a f(x))$ is planar. By Lemma

1.4.6, L is permutation and $D_a f(x)$ is planar, which means f is Alltop.

i)⇒ iii) Assume that $f(L(x)$ is Alltop function. Then

$$D_b D_a f(L(x))$$

is bijective for any $a, b \in \mathbb{F}_{p^n}^*$.

Assume that $L(x)$ is not permutation, i.e. $L(x) = L(y)$ for some $y \neq x$. But in this case

$$D_b D_a f(L(x)) = D_b D_a f(L(y))$$

which is impossible. Hence L is permutation.

Now assume that, f is not Alltop. Then there exists $y \in \mathbb{F}_{p^n}$ such that

$$D_b D_a f(x) = D_b D_a f(y)$$

Since L is permutation, there exist x_1, x_2 such that $x_1 \neq x_2$ and $L(x_1) = x$ and $L(x_2) = y$. But, in this case

$$D_b D_a f(L(x_1)) = D_b D_a f(L(x_2))$$

which is impossible. Hence f is Alltop.

iii)⇒ i) Assume f is Alltop, L is permutation polynomial and $f(L(x))$ is not an Alltop. Then there exists $y \in \mathbb{F}_{p^n}$ such that $y \neq x$ and

$$D_b D_a f(L(x)) = D_b D_a f(L(y))$$

Since L is permutation, there exist x_1, x_2 such that $x_1 \neq x_2$ and $L(x) = x_1$, $L(y) = x_2$. Then

$$D_b D_a f(x_1) = D_b D_a f(x_2)$$

which is impossible, since f is Alltop.

□

By using the following theorem for planar functions, analogous result was obtained in [14]:

Theorem 2.1.3. *[19] Let $p > 2$ be prime and $L_1(x), L_2(x) \in \mathbb{F}_{p^n}[x]$ be linearized polynomials.*

If $f(x) = L_1(x)L_2(x)$ is planar, then necessarily $L_1(x)$ and $L_2(x)$ are invertible polynomials.

Proof. Let $f(x) = L_1(x)L_2(x)$ as given.
If f is planar then

$$D_a f(x) = L_1(x+a)L_2(x+a) - L_1(x)L_2(x)$$

has to be permutation for any $a \in \mathbb{F}_{p^n}^*$.
By using the linearity property of L_i's we can get

$$D_a f(x) = L_1(x)L_2(a) + L_1(a)L_2(x) + L_1(a)L_2(a)$$

is permutation. Since $D_a f(x)$ is an affine polynomial, it is permutation if and only if it has no nonzero solutions.
Now, assume that $L_1(x)$ is not permutation. Then there exist $b \in \mathbb{F}_{p^n}^*$ such that $L_1(b) = 0$. Then it is easy to see that, $D_b f(x)$ is not permutation since $D_b f(b) = 0$. Hence $L_1(x)$ is permutation.
Since L_1 and L_2 are symmetric, it is easy to see that L_2 is permutation. □

For Alltop functions analogous result is for 3 additive polynomials:

Theorem 2.1.4. *[14] Let $p > 3$ be an odd prime and $L_1(x), L_2(x), L_3(x) \in \mathbb{F}_{p^n}[x]$ be linearized polynomials.*
If $f(x) = L_1(x)L_2(x)L_3(x)$ is Alltop then necessarily $L_1(x), L_2(x), L_3(x)$ are invertible polynomials.

Proof. For $a \in \mathbb{F}_{p^n}^*$, derivative of a function is:

$$D_a f(x) = L_1(x)L_2(x)L_3(a) + L_1(x)L_2(a)L_3(x) + L_1(x)L_2(a)L_3(a) + L_1(a)L_2(x)L_3(x)$$

$$+L_1(a)L_2(x)L_3(a) + L_1(a)L_2(a)L_3(x) + L_1(a)L_2(a)L_3(a) + M_a(x) + C$$

has to be planar, where M is an additive function and C is constant.
Now, take the second derivative to get:

$$D_b D_a f(x) = L_1(x)[L_2(a)L_3(b) + L_2(b)L_3(a)]$$

$$+L_2(x)[L_1(a)L_3(b) + L_1(b)L_3(a)] + L_3(x)[L_1(a)L_2(b) + L_1(b)L_2(a)]$$

is permutation for any $a, b \in \mathbb{F}_{p^n}^*$.

Assume that $L_1(x)$ is not a permuation. Then there exists $c \in \mathbb{F}_{p^n}^*$ such that $L_1(c) = 0$. Then observe that, $D_c D_c f(x) = 0$ has nonzero solution which contradicts that $D_b D_a f(x)$ is permutation for any $a, b \in \mathbb{F}_{p^n}^*$.
Hence $L_1(x)$ is bijective. Same is true for L_2 and L_3.

□

Note 2.1.5. *It is also noted that, the converse of a theorem is not true in general. To see this explicitly, take $L_1(x) = x^p$, $L_2(x) = x$ and $L_3(x) = x$ in $\mathbb{F}_{q^2}$. In this case $f(x) = x^{q+2}$.*
Then

$$D_a f(x) = 2ax^{q+1} + a^q x^2 + a^2 x^q + 2a^{q+1} x + a^{q+2}$$

has to be planar.
Now, take second derivative at a point b:

$$D_b D_a f(x) = 2axb(x^{q-1} + a^{q-1} + b^{q-1})$$

has to be permutation, ie has no nonzero solution.
Let $q \equiv 2$ (mod 3), then clearly, $q^2 - 1$ is divisible by 3.
Hence there is a subgroup with order 3 in $\mathbb{F}_{q^2}^*$.
If we let ω to be the generator of the subgroup mentioned, then $\omega^{q-2} = 1$.
Now, if $x = \omega^2, a = \omega$ and $b = 1$ then $x^{q-1} + a^{q-1} + b^{q-1} = 0$, i.e. $D_b D_a f(x) = 0$ has nonzero solution, hence is not permutation.

Following theorem shows that Alltop functions in odd characteistics start from characteristic at least 5.

Theorem 2.1.6. *[13] There are no Alltop type polynomial over $\mathbb{F}_{3^n}$.*

Proof. Let f be any function defined over $\mathbb{F}_{3^n}$. Then

$$D_b D_a f(x) = f(x + a + b) - f(x + a) - f(x + b) + f(x)$$

for any $a, b \in \mathbb{F}_{3^n}^*$. Let $a = b = 1$. Then

$$D_1 D_1 f(x) = f(x + 2) - 2f(x + 1) + f(x)$$

Since field has characteristic 3,

$$D_1D_1f(x) = f(x+2) + f(x+1) + f(x).$$

Moreover, one can check that

$$D_1D_1f(x+1) = f(x+2) + f(x+1) + f(x)$$

that is $D_1D_1f(x) = D_1D_1f(x+1)$ is not permutation. Hence, f can not be an Alltop function.

□

In the following theorem new class of Alltop polynomials is given by Hall, Rao and Gagola (2013).

Theorem 2.1.7. *[14] Let $p \geq 5$ be an odd prime, n is a positive integer so that $p^n + 1$ is not divisible by 3.*
Then $f(x) = x^{p^n+2}$ is Alltop over $\mathbb{F}_{p^{2n}}$.

Proof. Let $q = p^n$. To prove, calculate the derivative of a function at any nonzero point:

$$D_af(x) = 2ax^{q+1} + a^qx^2 + a^2x^q + 2a^{q+1}x + a^{q+2}$$

has to be planar for any $a \in \mathbb{F}^*_{q^2}$.
Equivalently, for any $b \in \mathbb{F}^*_{q^2}$

$$D_bD_af(x) = 0$$

has no nontrivial solution. That is,

$$abx^q + ab^qx + a^qbx = 0 \tag{2.1}$$

has $x = 0$ as only root.
Assume that $x \neq 0$. Since a and b are nonzero, divide by a and get:

$$x^qb + xb^q + xba^{q-1} = 0 \tag{2.2}$$

Take q-th power of (2.2) :

$$xb^q + x^qb + x^qb^qa^{1-q} = 0 \tag{2.3}$$

Subtract 2.3 from (2.2), it follows that

$$x(ba^{q-1}) - x^q(b^q a^{1-q}) = 0 \tag{2.4}$$

(2.4) is true if and only if

$$1 - \left(\frac{xb}{a^2}\right)^{q-1} = 0 \tag{2.5}$$

Hence, there exists $c \in \mathbb{F}_q$, such that $xb = ca^2$. Then put this value in (2.2) and use that $c^{q-1} = 1$:

$$\left(\frac{a^2}{b}\right)^{q-1} + b^{q-1} + a^{q-1} = 0 \tag{2.6}$$

$\Longleftrightarrow$

$$\left(\left(\frac{a}{b}\right)^{q-1}\right)^2 + \left(\frac{a}{b}\right)^{q-1} + 1 = 0 \tag{2.7}$$

It can be seen that

$$\left(\frac{a}{b}\right)^{q-1} \neq 1$$

Hence

$$\left(\frac{a}{b}\right)^{3(q-1)} - 1 = 0 \tag{2.8}$$

Since characteristic is different from 3, equation (2.8) has solutions $\Longleftrightarrow$ $3(q-1)$ divides $q^2 - 1 \Longleftrightarrow$ 3 divides $q + 1$.

□

In [14] it is also noted that, $D_a f(x)$ is EA-equivalent to x^2. Moreover, in the following lemma it is shown that this class of functions is EA-inequivalent to x^3.

Lemma 2.1.8. *Let p be an odd prime and n a positive integer. A cubic function $f \in \mathbb{F}_{p^n}$ of the form*

$$f(x) = \sum_{0 \leq k,j,i < n} a_{kji} x^{p^k + p^j + p^i}$$

such that $a_{kkk} = 0$ (for $k = j = i$), is not extended affine equivalent to x^3.

Proof. $f(x)$ is EA-equivalent to x^3 if there exist affine functions $l_1(x), l_2(x)$ and $l_3(x)$ such that

$$l_1 \circ (x^3 \circ (l_2)) + l_3(x) = f(x)$$

Let $l_1(x) = L_1(x) + a$ and $l_2(x) = L_2(x) + b$ where

$$L_1(x) = \sum_{i=0}^{n-1} a_i x^{p^i}$$

$$L_2(x) = \sum_{i=0}^{n-1} b_i x^{p^i}$$

and a, b are constants.

Then

$$l_1 \circ (l_2(x)^3)) + l_3(x) = l_1\Big(\sum_{i=0}^{n-1} b_i^3 x^{3p^i} + N(x)\Big) + l_3(x)$$

$$= L_1\Big(\sum_{i=0}^{n-1} b_i^3 x^{3p^i}\Big) + L_1 \circ N(x) + a + l_3(x) \tag{2.9}$$

where $N(x)$ is a polynomial which does not contain terms in the form of x^{3p^i}.

Since f does not have this term, then necessarily the right hand side of the equation (2.9) has no the term x^{3p^i}.

It is clear that, $L_1 \circ N(x)$ and $l_3(x)$ have no this term, hence necessarily $L_1\Big(\sum_{i=0}^{n-1} b_i^3 x^{3p^i}\Big)$ does not have this term.

This can happen only when, $b_i = 0$ for all $0 \leq i \leq n-1$, that is l_2 is not invertible.

Hence $f(x)$ is not EA-equivalent to x^3.

□

CHAPTER 3

CLASSIFICATION

In this section, cubic Alltop q-monomials and binomials are classified over $\mathbb{F}_{q^2}$. Specifically, $x^3 + ux^{2q+1}$ case over $\mathbb{F}_{q^2}$ explicitly determined. In addition, cubic Alltop q-monomials over $\mathbb{F}_{q^3}$ are classified. It is shown that there is no Alltop cubic q- monomial over this field and some computational results about cubic q binomials over the same field with characteristics 5,7.

3.1 Classification of cubic Alltop q-monomials and q-binomials over $\mathbb{F}_{q^2}$

Over $\mathbb{F}_{q^2}$, all cubic q-monomials are followings:

A_1) x^3

A_2) x^{q+2}

A_3) x^{2q+1} $(= (x^{q+2})^q)$

A_4) x^{3q} $(= (x^3)^q)$

It is clear that, A_1)and A_4) , A_2) and A_3) are EA-equivalent, since they are q-th power of each other.

Hence there are only x^3 and x^{q+2} and they are known to be Alltop over $\mathbb{F}_{q^2}$.

Before classification over $\mathbb{F}_{q^2}$ we have the following fact:

Fact 3.1.1. *Let* $0 \neq a \in \mathbb{F}_{q^2}$. *Then* $x^q + ax$ *is a permutation over* $\mathbb{F}_{q^2}$ *if and only if* a *is not a* $q-1$ *power.*

Let $u \in \mathbb{F}_{q^2}^*$. Then all cubic binomials over $\mathbb{F}_{q^2}$ are in the following forms:

B_1) $x^3 + ux^{2q+1}$

B_2) $x^3 + ux^{q+2}$

B_3) $x^3 + ux^{3q}$

B_4) $x^{q+2} + ux^{2q+1}$

B_5) $x^{q+2} + ux^{3q}$

B_6) $x^{2q+1} + ux^{3q}$

Observe that B_1) and B_6), B_2) and B_5) are EA-equivalent since they are q-th power of each other. After eliminating equivalent functions we get B_1), B_2), B_3) and B_4) as inequivalent cubic binomial functions over $\mathbb{F}_{q^2}$.

Note 3.1.2. *Functions of type B_3) and B_4) above are Alltop if and only if u is not q-1 power over $\mathbb{F}_{q^2}$. That is because, $x^q + ux$ is a permutation polynomial if and only if u is not q-1 power over $\mathbb{F}_{q^2}$. In addition, B_3) and B_4) are the composition of $x^q + ux$ with x^3 and x^{q+2} respectively, which are Alltop functions. By definition of EA-equivalency those types are Alltop.*
(B_3) -in everywhere, B_4) -under the condition 3 does not divide q+1)

Remark 3.1.3. *In case B_2), due to Magma computations done for $q = 5, 7, 11, 13, 17, 19$ there is no suitable u in $\mathbb{F}_{q^2}$ that is $f(x) = x^3 + ux^{q+2}$ is Alltop.*
Hence, it can be conjectured that $f(x) = x^3 + ux^{q+2}$ is not Alltop function for any $u \in \mathbb{F}_{q^2}$.

Here, B_1) case is interesting to determine.

3.1.1 Case B_1) $x^3 + ux^{2q+1}$:

By the help of Magma program we see that in some values of c, these kind of functions are Alltop. Following results are those we get from Magma:

q	u	$f(x)$
5	$\omega^6, \omega^{14}, \omega^{22}$	ALLTOP
7	$\omega^2, \omega^6, \omega^{14}, \omega^{18}, \omega^{26}, \omega^{30}, \omega^{38}, \omega^{42}$	ALLTOP

where ω is a generator of the related field $\mathbb{F}_{q^2}$. For the rest of the values of u, the

function is not an Alltop. In addition, we observe that when $q = 5$ the function is extended affine equivalent to x^3 for the values of the u that makes f Alltop. When $q = 7$, for $u = \omega^2, \omega^{14}, \omega^{26}, \omega^{38}$ function is EA-equivalent to x^3, for $u = \omega^6, \omega^{18}, \omega^{30}, \omega^{42}$ function is EA-equivalent to x^{7+2}.

These results are formulated and generalized in the following lemmas and theorem:

Lemma 3.1.4. *Let $f(x) = x^3 + ux^{2q+1}$ from $\mathbb{F}_{q^2}$ to itself, where $u \in \mathbb{F}_{q^2}^*$ and let ω be a cyclic generator of a field $\mathbb{F}_{q^2}$.*

a) *there exist maps $L_1(x) = ax+bx^q$ and $L_2(x) = cx+dx^q$ in $\mathbb{F}_{q^2}$ such that $L_1 \circ x^3 \circ L_2 = f(x)$ if and only if $N(u) = 9$*

b) *there exist maps $L_1(x) = ax+bx^q$ and $L_2(x) = cx+dx^q$ in $\mathbb{F}_{q^2}$ such that $L_1 \circ x^{q+2} \circ L_2 = f(x)$ if and only if $N(u) = 1$*

where N is the usual Norm function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$.

Proof. *a*) Assume that there exist maps $L_1(x) = ax + bx^q$ and $L_2(x) = cx + dx^q$ in $\mathbb{F}_{q^2}$ such that

$$L_1 \circ (L_2^3 \circ (x)) = x^3 + ux^{2q+1} \tag{3.1}$$

After substitution of $L_1(x), L_2(x)$ and after several calculations we get :

$$x^3(ac^3+bd^{3q})+x^{q+2}(3c^2da+3bc^qd^{2q})+x^{2q+1}(3cd^2a+3c^{2q}d^qb)+x^{3q}(ad^3+bc^{3q}) = x^3+ux^{2q+1} \tag{3.2}$$

From here we get the following set of equations:

$$ac^3 + bd^{3q} = 1 \tag{3.3}$$

$$3cd^2a + 3c^{2q}d^qb = u \tag{3.4}$$

$$3c^2da + 3bc^qd^2 = 0 \tag{3.5}$$

$$ad^3 + bc^{3q} = 0 \tag{3.6}$$

We observe that

Claim 3.1.5. *a, b, c and d are nonzero.*

Proof. Let $a = 0$. Then

$$(3.6) \Rightarrow bc^{3q} = 0$$

$\Rightarrow$ either $b = 0$ or $c = 0$. In both cases (3.3) fails.

Similarly, if $b = 0$ then again from (3.3) either $a = 0$ or $d = 0$ which contradicts with (3.3).

In a same way, it can be shown that c and d are also nonzero.

□

Now, $(3.5) \Leftrightarrow a = -bc^{q-2}d^{2q-1}$.

Put this value in (3.6) to get:

$$(c^{q-1} - d^{q-1})(c^{q-1} + d^{q-1}) = 0 \tag{3.7}$$

Now put the value of a from (3.5) to (3.3):

(3.3) $\Leftrightarrow$

$$bd^{2q-1}(d^{q-1} - c^{q-1}) = 1 \tag{3.8}$$

(3.7) and (3.8) $\Leftrightarrow c^{q+1} + d^{q+1} = 0$ and $c^{q+1} - d^{q+1} \neq 0$

Now putting the value of a in (3.4) and then using $c^{q+1} = -d^{q+1}$ we get:

$$(3.4) \Leftrightarrow \psi = -3\frac{c^{q-1}}{d^{q-1}} \Leftrightarrow N(u) = 9$$

b) Proof is similar to part *a*).

Assume that there exist maps $L_1(x) = ax + bx^q$ and $L_2(x) = cx + dx^q$ in $\mathbb{F}_{q^2}$ such that

$$L_1 \circ (L_2^{q+2} \circ (x)) = x^3 + ux^{2q+1} \tag{3.9}$$

After substitution of $L_1(x), L_2(x)$ and several calculations we get:

$$(ac^2d^q + bcd^{2q})x^3 + (2c^{q+1}da + d^{q+2}a + c^{2q+1}b + 2c^qd^{q+1}b)x^{2q+1} + (ac^{q+2} + 2cd^{q+1}a$$

$$+2c^{q+1}d^q b + d^{2q+1}b)x^{q+2} + (ac^2d^q + bcd^{2q})x^{3q} = x^3 + ux^{2q+1} \tag{3.10}$$

We get the following set of equations:

$$ac^2d^q + bcd^{2q} = 1 \tag{3.11}$$

$$2c^{q+1}da + d^{q+2}a + c^{2q+1}b + 2c^q d^{q+1}b = u \tag{3.12}$$

$$ac^{q+2} + 2cd^{q+1}a + 2c^{q+1}d^q b + d^{2q+1}b = 0 \tag{3.13}$$

$$ac^q d^2 + bdc^{2q} = 0 \tag{3.14}$$

Claim 3.1.6. *a, b, c and d are nonzero.*

Proof. If $a = 0$ then (3.14) $\Rightarrow bdc^{2q} = 0$ which contradicts with (3.11).
If $b = 0$, similarly (3.14) $\Rightarrow ad^2c^q = 0$, contradicts with (3.11).
From (3.11), $c \neq 0$ and $d \neq 0$. □

Now (3.14) $\iff a = \frac{-bc^q}{d}$. Put this value in (3.13) to get:

$$(d^{q+1} - c^{q+1})(d^{q+1} + c^{q+1}) = 0 \tag{3.15}$$

(3.11) $\iff$

$$d^{q-1}bc(d^{q+1} - c^{q+1}) = 1 \tag{3.16}$$

Now take q-th power of both side

$$d^{1-q}b^q c^q(d^{q+1} - c^{q+1}) = 1 \tag{3.17}$$

By multiplying (3.16) and (3.17)

$$b^{q+1}c^{q+1}(d^{q+1} - c^{q+1})^2 = 1 \tag{3.18}$$

(3.15) and (3.18) $\iff d^{q+1} + c^{q+1} = 0$ and $d^{q+1} - c^{q+1} \neq 0$.

(3.12) $\iff u = bc^q d^{q+1} - c^{2q+1}b.$

So,

$$N(u) = b^{q+1}c^{q+1}(d^{q+1} - c^{q+1})^2 = 1$$

holds.

□

Lemma 3.1.7. *Let q be an odd power and $\mathbb{F}_q$ be a finite field and n be an odd integer in* $[0, 1, .., q+1]$. *Let* $L_1(x) = \omega^{\frac{-3n(q-1)}{2}}x + x^q$, $L_2(x) = \omega^{\frac{n(q-1)}{2}}x + x^q$ *and* $L_3(x) = \omega^{n(1-q)/2}x^q - x$ *be functions from $\mathbb{F}_{q^2}$ to itself where ω is a generator of $\mathbb{F}_{q^2}$. Then L_1,L_2 and L_3 are permutations over $\mathbb{F}_{q^2}$.*

Proof. To show that $L_1(x)$ is a permutation, we have to show that $L_1(x)$ has the only trivial root over $\mathbb{F}_{q^2}$. Assume that $L_1(x)$ is not permutation that is ,

$$L_1(x) = 0$$

has nontrivial roots. Assuming that $x \neq 0$,

$$x^{q-1} = -\omega^{\frac{-3n(q-1)}{2}}$$

However, right hand side is not a q-1 power in $\mathbb{F}_{q^2}$ because n is an odd number, this is contradiction. Hence $L_1(x)$ is an invertible polynomial.

Similarly, if $L_2(x)$ is not one to one, then it must have nontrivial solutions:

$$L_2(x) = \omega^{\frac{n(q-1)}{2}}x + x^q$$

$$x^{q-1} = -\omega^{(n/2)(1-q)}$$

However, since n is odd, right hand-side is not q-1 power and hence this equation has no nontrivial solution.

In a similar way, assume $L_3(x) = 0$ is not a permutation that is it has a non trivial solution. Then

$$\omega^{n(1-q)/2}x^q = x \Rightarrow$$

$$x^{q-1} = \omega^{n(q-1)/2}$$

Since n, q are odd numbers, right hand side is not $q-1$ power, hence there is no nontrivial solution.

□

The following theorem helps us to prove that the functions of type B_1) are EA-equivalent to x^3 and x^{q+2} for the suitable values of u and hence can be considered as an Alltop function under certain conditions. (when EA-equivalent to x^3 no any condition, when EA-equivalent to x^{q+2} the condition is that 3 does not divide $q+1$)

Theorem 3.1.8. *Let $f(x) = x^3 + ux^{2q+1}$ from $\mathbb{F}_{q^2}$ to itself, where $u \in \mathbb{F}_{q^2}^*$ and let ω be a cyclic generator of a field $\mathbb{F}_{q^2}$.*
a) *there exist maps $L_1(x) = ax+bx^q$ and $L_2(x) = cx+dx^q$ in $\mathbb{F}_{q^2}$ such that $L_1 \circ x^3 \circ L_2 = f(x)$ if and only if $u = 3\omega^{n(1-q)}$ for any odd integer $n \in [1, 2, 3, ..., q+1]$*
b) *there exist maps $L_1(x) = ax+bx^q$ and $L_2(x) = cx+dx^q$ in $\mathbb{F}_{q^2}$ such that $L_1 \circ x^{q+2} \circ L_2 = f(x)$ if and only if $u = \omega^{n(1-q)}$ for any odd integer $n \in [1, 2, 3, ..., q+1]$*

Proof. **a)** Use arguments of part a) in Lemma 1 and try to solve equations (3.3), (3.4), (3.5), (3.6). Since $c^{q-1} = -d^{q-1}$, let $c = \omega^i, d = \omega^j$ where ω is the given generator of a field $\mathbb{F}_{q^2}$ and $i, j \in [0, 1, ..., q^2-1]$. Obviously, $\omega^{(q+1)(i-j)} = -1$. This is possible if and only if $i - j = \frac{n(q-1)}{2}$ for any odd integer n in $[1, .., q+1]$.

$$(3.3) \iff -2bd^{2q-1}c^{q+1} = 1 \iff b = \frac{\omega^{-3qj}}{2}$$

$$(3.5) \iff a = \frac{\omega^{-3j-\frac{3n(q-1)}{2}}}{2}$$

$$(3.4) \iff u = -3\omega^{(i-j)(q-1)} \iff u = 3\omega^{n(q-1)}$$

b) Use equations of part b) of Lemma 1 (3.11), (3.12), (3.13), (3.14). As in part a) let $c = \omega^i, d = \omega^j$ for some $i, j \in [0, 1, ..q^2-1]$. Since $c^{q+1} = -d^{q+1}$,

$$\omega^{(i-j)(q+1)} = -1 \iff i - j = n(\frac{q-1}{2})$$

where n is any odd integer in $[1, 2, ..., q+1]$.

$$(3.11) \iff 2b\omega^{(2q+1)j} = \omega^{n(1-q)/2} \iff b = \frac{\omega^{\frac{n(1-q)}{2}-j(2q+1)}}{2}$$

$$(3.14) \iff a = \frac{-bc^q}{d} = \frac{-\omega^{(q+2)j}}{2}$$

We have $c = \omega^{n(q-1)/2+j}, d = \omega^j$. □

Corollary 3.1.9. *Let $f(x) = x^3 + ux^{2q+1}$ from $\mathbb{F}_{q^2}$ to itself, where $u \in \mathbb{F}_{q^2}^*$ and let ω be a cyclic generator of a field $\mathbb{F}_{q^2}$.*
a) If $u = 3\omega^{n(1-q)}$ for any odd integer $n \in [1, 2, 3, ..., q+1]$ then f is an Alltop function, i.e f is EA-equivalent to x^3.
b) If $u = \omega^{n(1-q)}$ for any odd integer $n \in [1, 2, 3, ..., q+1]$ and 3 does not divide $q+1$ then f is an Alltop function, i.e f is EA-equivalent to x^{q+2}.

Proof. a) It is enough to find suitable i, j such that $L_1(x) = ax + bx^q$ and $L_2(x) = cx + dx^q$ are permutations.
Choose $j = 0$ to get

$$L_1(x) = \frac{1}{2}\omega^{\frac{-3n(q-1)}{2}}x + \frac{1}{2}x^q$$

and

$$L_2(x) = \omega^{\frac{n(q-1)}{2}}x + x^q$$

By Lemma 3.0.6 they are permutation polynomials.
b) It is enough to show that there exists j that makes $L_1(x) = ax + bx^q$ and $L_2(x) = cx + dx^q$ permutation. Let $j = 0$. Then

$$L_1(x) = \frac{-1}{2}x + \frac{1}{2}\omega^{n(1-q)/2}x^q$$

and

$$L_2(x) = \omega^{n(q-1)/2}x + x^q$$

by Lemma 3.1.7, $L_1(x)$ and $L_2(x)$ are both permutations.

□

3.2 Classification of cubic Alltop q-monomials over $\mathbb{F}_{q^3}$

Before classification over $\mathbb{F}_{q^3}$ we give some results of paper [15] in order to determine a planarity of a derivative of our functions.
For further details about all q-quadratic binomial classification of planar functions can be found in [20] explicitly.

Lemma 3.2.1. *[15](Lem 5.1) Let p be an odd prime and n be a positive integer.*
Let $f(x) = x^{p^m+1} + \beta x^2 \in \mathbb{F}_{p^n}[x]$ where $m > 0$ and $\beta \in \mathbb{F}_{p^n}^*$.

Put $t = \frac{n}{gcd(m,n)}$ *and* $q = p^{gcd(m,n)}$*(so* $p^n = q^t$*). Then* f *is a planar function over* $\mathbb{F}_{q^t}$ *if and only if the equation*

$$x^{q-1} + y^{q-1} = -2\beta$$

has no solution $(x, y) \in \mathbb{F}_{q^t}^* \times \mathbb{F}_{q^t}^*$.

It is also noted that in [15], when $t \geq 3$, Lemma 3.2.1 does not produce any planar function.

Over $\mathbb{F}_{q^3}$ all different cubic q-monomials are given below:

$A_1)$ x^3

$A_2)$ x^{q+2}

$A_3)$ x^{q^2+2}

$A_4)$ x^{2q+1}

$A_5)$ x^{q^2+q+1}

$A_6)$ x^{2q^2+1}

$A_7)$ x^{3q}

$A_8)$ x^{q^2+2q}

$A_9)$ x^{2q^2+q}

$A_{10})$ x^{3q^2}

Observe that, $A_1)$, $A_7)$ and $A_{10})$ are EA-equivalent to each other since they are q-th, q^2-th power of each other.

Similarly, $A_2), A_6)$ and $A_8)$ and $A_3), A_4)$ and $A_9)$ are q-th power of each other.

Hence after ommiting equivalent class, we have the following different inequivalent monomials:

$B_1)$ x^3

$B_2)$ x^{q+2}

$B_3)$ x^{q^2+2}

$B_4)$ x^{q^2+q+1}

Case $B_1)$ is clear.

We look for the other cases:

Case $B_2) f(x) = x^{q+2}$:

By using definition, for any $a \in \mathbb{F}_{q^3}^*$, $f(x + a) - f(x) = (x + a)^{q+2} - x^{q+2}$ has to be planar.

In other words,

$$x^{q+2} + 2ax^{q+1} + a^2x^q + a^qx^2 + 2a^{q+1}x + a^{q+2} - x^{q+2}$$

has to be planar. Equivalently,

$$2ax^{q+1} + a^qx^2$$

has to be planar for any $a \in \mathbb{F}_{q^3}^*$ since ommiting linear terms does not affect planarity. However, due to the Lemma 3.2.1, such functions do not produce any planar function over $\mathbb{F}_{q^3}$.

Case $B_3) f(x) = x^{2q+1}$:

Similarly,

$$f(x+a) - f(x) = ax^{2q} + 2x^{q+1}a^q + 2x^qa^{q+1} + a^{2q}x + a^{2q+1}$$

has to be planar for any $a \in \mathbb{F}_{q^3}^*$.

Equivalently,

$$ax^{2q} + 2a^qx^{q+1}$$

has to be planar.

Similar to the second case, such functions are not planar.

Case $B_4) f(x) = x^{q^2+q+1}$:

We show that this function is not an Alltop function.

$$f(x+a) - f(x) = ax^{q^2+q} + a^qx^{q^2+1} + a^{q+1}x^{q^2} + a^{q^2}x^{q+1} + a^{q^2+1}x^q + a^{q^2+q}x + a^{q^2+q+1}$$

Eliminate linear terms and check planarity of

$$g(x) = ax^{q^2+q} + a^qx^{q^2+1} + a^{q^2}x^{q+1}$$

in $\mathbb{F}_{q^3}$. Observe that, it is a Dembowski-Ostrom polynomial.

Apply Lemma 2.0.5 and get that the function $g(x)$ has to be 2-to-1 for any $a \in \mathbb{F}_{q^3}^*$.

Let $a = 1$.

Then

$$g(x) = x^{q^2+q} + x^{q^2+1} + x^{q+1}$$

has to be 2-to-1.

However, observe that

$$g(\omega) = g(-\omega) = g(\omega^q)$$

holds, where ω is a cyclic generator of $\mathbb{F}_{q^3}$. Hence it cannot be 2-to-1.

By combining all these cases, we get the following theorem:

Theorem 3.2.2. *Except x^3 and its EA-equivalence class, there is no Alltop cubic q-monomials in $\mathbb{F}_{q^3}$.*

3.3 Classification of cubic Alltop q-binomials over $\mathbb{F}_{q^3}$

In this part, Magma calculations of cubic q-binomials over $\mathbb{F}_{q^3}$ are done for $q = 5, 7$ (and for some cases $q = 11$) and it is found that except one of the cases there is no $c \in \mathbb{F}_{q^3}$ that makes function Alltop.
Due to the calculations done in MAGMA, the following results are obtained for cubic q-binomials in $\mathbb{F}_{q^3}$.
After eliminating equivalent functions as before, all remaining inequivalent cubic q-binomials over $\mathbb{F}_{q^3}$ are following:

- 1) $x^3 + cx^{q+2}$ - Not Alltop for $q = 5, 7$
- 2) $x^3 + cx^{q^2+2}$ - Not Alltop for $q = 5, 7$
- 3) $x^3 + cx^{2q+1}$ - Not Alltop for $q = 5, 7$
- 4) $x^3 + cx^{q^2+q+1}$ - Not Alltop for $q = 5, 7$
- 5) $x^3 + cx^{2q^2+1}$ - Not Alltop for $q = 5, 7$
- 6) $x^3 + cx^{3q}$ - Alltop, since $f(x) = (x + cx^q) \circ x^3$, and f is Alltop if and only if c is not a $q - 1$st power, since in this case $x + cx^q$ is linearized permutation.
- 7) $x^3 + cx^{q^2+2q}$ - Not Alltop for $q = 5, 7$
- 8) $x^3 + cx^{2q^2+q}$ - Not Alltop for $q = 5, 7$
- 9) $x^{q+2} + cx^{q^2+2}$ - Not Alltop for $q = 5, 7$
- 10) $x^{q+2} + cx^{2q+1}$ - Not Alltop for $q = 5, 7$
- 11) $x^{q+2} + cx^{q^2+q+1}$ - Not Alltop for $q = 5, 7$
- 12) $x^{q+2} + cx^{2q^2+1}$ - Not Alltop for $q = 5, 7$
- 13) $x^{q+2} + cx^{2q^2+q}$ - Not Alltop for $q = 5, 7$

- 14) $x^{q^2+2} + cx^{2q+1}$ - Not Alltop for $q = 5, 7$
- 15) $x^{q^2+2} + cx^{q^2+q+1}$ - Not Alltop for $q = 5, 7$

Remark 3.3.1. *Observe that, when $q = 5$ and $q = 7$ over $\mathbb{F}_{q^3}$, only $x^3 + cx^{3q}$ is an Alltop function and in this case the function is EA-equivalent to x^3.*
It is still an open problem to find an Alltop function from this class of functions in $\mathbb{F}_{q^3}$. In the case that new Alltop functions are found from the class of any cubic q-binomial over $\mathbb{F}_{q^3}$, this will be EA-inequivalent all previous Alltop functions found before.

CHAPTER 4

P-ARY ALLTOP FUNCTIONS

In this part we define "p-ary Alltop" functions by using gneeralized (p-ary) bent functions and then relate this notion with Alltop functions.
It is known that when p is an odd prime and $q = p^n$ for some n, then a function f defined over $\mathbb{F}_q$ is p-ary bent if and only if it is perfect-nonlinear.
Since in this case perfect-nonlinear functions have balanced derivatives, we can define p-ary bent functions also in different way as following:

Definition 4.0.1. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ where p is an odd prime, $n \geq 1$ integer. Then f is called p-ary bent function if $D_a f(x) = f(x+a) - f(x)$ is balanced for any $a \in \mathbb{F}_{p^n}^*$.*

Definition 4.0.2. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ where p is an odd prime, $n \geq 1$ integer. Then f is called "p-ary Alltop function" if $D_a f(x) = f(x+a) - f(x)$ is p-ary bent for any $a \in \mathbb{F}_{p^n}^*$.*
Equivalently, for any $a, b \in \mathbb{F}_{p^n}^*$, $D_b D_a f(x)$ is balanced.

Observation 4.0.3. *Let be any p-ary function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then f is p-ary Alltop*
$\iff$

$$\sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{D_b D_a f(x)} = 0,$$

for all $a, b \in \mathbb{F}_{p^n}^*$, where ϵ_p is a p-th root of unity in $\mathbb{F}_{p^n}$.

4.1 Characterization of cubic p-ary Alltop functions

In this part, by using the results in [26] characterization of cubic p-ary Alltop functions over $\mathbb{F}_{p^n}$ is given. Before characterization of p-ary Alltop functions, explicit

results about cubic p-ary bent functions in [26] are revised.

Let f be an arbitrary cubic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then f can be written as

$$f(x) = Tr^n(xD(x)) + Tr^n(xA(x)) + \alpha(x),$$

where $D(x)$ is Dembowski-Ostrom polynomial,

$A(x)$ is a linearized polynomial given by

$$A(x) = \sum_{0 \le i \le n-1} a_i x^{p^i}$$

with $a_i \in \mathbb{F}_{p^n}$,

$\alpha(x)$ is an affine polynomial for $x \in \mathbb{F}_{p^n}$,

and Tr^n is a usual trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.

Let $B : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{F}_p$ be the quadratic map depending on D defined as

$$B(x, y) = D(x + y) - D(x) - D(y)$$

for $x, y \in \mathbb{F}_{p^n}$.

For $a, b \in \mathbb{F}_{p^n}$, let

$$L_{a,b,B}f(x) = Tr^n(xB(a, b)) + Tr^n(aB(x, b)) + Tr^n(bB(x, a))$$

for every $x \in \mathbb{F}_{p^n}$.

For $a, b \in \mathbb{F}_{p^n}$, let $C_{a,b,d}$ and $C_{a,b,A}$ be the constant functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ defined as

$$C_{a,b,D} = Tr^n(aB(a, b)) + Tr^n(bB(a, b)) + Tr^n(aD(b)) + Tr^n(bD(a))$$

$$C_{a,b,A} = Tr^n(aA(b)) + Tr^n(bA(a))$$

For simplicity, lets use $Tr()$ notation instead of $Tr^n()$.

Lemma 4.1.1. *[26] Let f be an arbitrary cubic function in the form*

$$f(x) = Tr(xD(x)) + Tr(xA(x)) + \alpha(x)$$

The second derivative of f at point $(a, b) \in \mathbb{F}_{p^n}^2$ is an affine function defined as

$$D_b D_a f(x) = L_{a,b,B}f(x) + C_{a,b,D} + C_{a,b,A}$$

for $x \in \mathbb{F}_{p^n}$.

Proof. By direct calculations it is clear that

$$D_b D_a \alpha(x) = 0.$$

Hence,

$$D_b D_a f(x) = D_b D_a \{Tr(xD(x)) + Tr(xA(x))\}$$

First, calculate first derivative at point a:

$$D_a Tr(xD(x)) = Tr((x+a)D(x+a)) - Tr(xD(x))$$

$$= Tr((x+a)(B(x,a) + D(x) + D(a))) - Tr(xD(x))$$

$$= Tr(xB(x,a)) + Tr(xD(a)) + Tr(aB(x,a)) + Tr(aD(x)) + Tr(aD(a))$$

and

$$D_a Tr(xA(x)) = Tr((x+a)A(x+a)) - Tr(xA(x)$$

$$= Tr(xA(a)) + Tr(aA(x)) + Tr(aA(a))$$

And now take the second derivarive at point b:

$$D_b D_a Tr(xD(x)) = Tr((x+b)B(x+b,a)) + Tr((x+b)D(a)) + Tr(aB(x+b,a)) + Tr(aD(x+b))$$

$$-Tr(xB(x,a)) + Tr(xD(a)) + Tr(aB(x,a)) + Tr(aD(x)) + Tr(aD(a))$$

$$= Tr(xB(a,b)) + Tr(aB(x,a)) + Tr(bB(x,a)) + Tr(aB(a,b)) + Tr(bB(a,b)) + Tr(aD(b)) + Tr(bD(a))$$

and

$$D_b D_a Tr(xA(x)) = Tr(aA(b)) + Tr(bA(a)))$$

Observe that,

$$D_b D_a Tr(xD(x)) = L_{a,b,B} f(x) + C_{a,b,D}$$

and

$$D_b D_a Tr(xA(x)) = C_{a,b,A}$$

□

Let $S = \{(a,b) : L_{a,b,B}(x) = 0, \text{ for any } x \in \mathbb{F}_{p^n}\}$ and $S_a = \{b \in \mathbb{F}_{p^n} : L_{a,b,B}(x) = 0, \text{ for any } x \in \mathbb{F}_{p^n}\}$.

Observe that, S_a is an $\mathbb{F}_p$ - linear subspace of $\mathbb{F}_{p^n}$ and it is clear that $S_0 = \mathbb{F}_{p^n}$.

The notation above results in following proposition :

Proposition 4.1.2. *[26] Let p be an odd prime, and f be any cubic function defined as above. If*

$$\sum_{a\in\mathbb{F}_{p^n}^*}\sum_{b\in S_a}\epsilon_p^{C_{a,b,D}+C_{a,b,A}}=0$$

then f is bent.

By using the above notations and arguments, we have following results for p-ary Alltop functions.

Theorem 4.1.3. *Let $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ is any cubic p-ary function. Then f is p-ary Alltop function if and only if*

$$\sum_{x\in\mathbb{F}_{p^n}}\epsilon_p^{L_{a,b,B}f(x)}=0$$

for any $a,b\in\mathbb{F}_{p^n}^*$.

Theorem 4.1.4. *$f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ is any cubic p-ary function. Then f is p-ary Alltop function if and only if*

$$S=\{(o,y):y\in\mathbb{F}_{p^n}\}\cup\{(x,0):x\in\mathbb{F}_{p^n}\}$$

4.2 Some trivial and non-trivial examples

Let $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ so that $f(x)=Tr(F(x))$, where $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ is a cubic function. It is clear that, if we choose F as Alltop function, then f will be a p-ary Alltop function. To see this explicitly, we use the characterization that we get in Theorem 4.1.3 and give the following trivial examples.

Example 4.2.1. *Let $F(x)=x^3, f(x)=Tr(x^3)$.*

Then $D(x)=x^2, B(x,y)=2xy$ and

$L_{a,b,B}f(x)=Tr(x2ab)+Tr(a2bx)+Tr(b2ax)=6Tr(abx)$

Since p is odd, when $p\neq 3$, f is a p-ary Alltop function.

It is trivial example, since x^3 is an Alltop function.

Example 4.2.2. *Let $n=2, F(x)=x^{p+2}$ and $f(x)=Tr(x^{p+2})$. Then*

$$D(x)=x^{p+1}, B(x,y)=xy^p+x^py$$

and

$$L_{a,b,B}f(x) = Tr(x(a^p b + ab^p)) + Tr(a(x^p b + xb^p))) + Tr(b(a^p x + ax^p))$$

After simplifications,

$$L_{a,b,B}f(x) = Tr(2x(ab^p + a^p b + a^{1/p}b^{1/p}))$$

(Here we used that $Tr(x) = Tr(x^p) = Tr(x^{1/p})$ and additive property of trace function) f is p-ary Alltop if and only if $ay^p + a^p y + ay$ has no nonzero solution y in $\mathbb{F}_{p^2}$.

Claim 4.2.3. *If 3 does not divide $p + 1$, then condition is satisfied and f is p-ary Alltop.*

Proof. Proof is similar to the proof of Theorem 2.1.7 Assume

$$ay^p + a^p y + ay = 0$$

then raise the p-th power and subtract :

$$a^p y + ay^p + a^p y^p = 0$$

We get

$$(ay)^{p-1} = 1.$$

This is if and only if

$$(ay)^{p-1} = \omega^{p+1}$$

where ω is a cyclic generator of a field $\mathbb{F}_{p^2}$.
Then $a = \frac{\omega^{p+1}}{y}$. Put this value instead of a in the above equation to get:

$$\frac{1}{y^{p-1}} + y^{p-1} + 1 = 0$$

$$\Rightarrow 1 + y^{p-1} + y^{2(p-1)} = 0$$

Multiply both sides by $(y^{p-1} - 1)$ and get

$$y^{3(p-1)} - 1 = 0$$

This can happen if and only if $3(p-1)$ divides $p^2 - 1$, that is 3 divides $p + 1$. So, if 3 does not divide $p + 1$ there is no non trivial solution. □

In fact, with these conditions F will be Alltop in $\mathbb{F}_{p^2}$ which we already know from second chapter.

The above examples are trivial examples since F is an Alltop function. It is interesting to find p-ary Alltop functions f so that F is not an Alltop.
Does there exist p-ary Alltop functions that are not trivial? The answer is yes and there are a lot of such functions.
Due to the computations in Magma we have following examples:

Example 4.2.4. *Let $F(x) = x^3 + cx^{2p+1}$, $f(x) = Tr(F(x))$ where $c \in \mathbb{F}_{p^n}$ and ω is a cyclic generator of a field $\mathbb{F}_{p^n}$*

- *If $n = 2$, $p = 5$, $c = \omega^{13}$ then $f(x)$ is p-ary Alltop but $F(x)$ is not Alltop.*
- *If $n = 3$, $p = 7$, $c = \omega^{49}$ then $f(x)$ is p-ary Alltop but $F(x)$ is not Alltop.*

At the end of this chapter, we give our main theorem not only for cubic but any p-ary Alltop functions to show relation between Alltop functions and p-ary Alltop functions. But before we give some other definitions and theorems from [21] that we used in our proof of theorem.

Definition 4.2.5. *Let G be a finite Abelian group of order $|G|$ with identity element 1_G. A character χ of G is a homomorphism from G to U where U is a multiplicatie group of a complex numbers that have absolute value 1.*

Equivalently, if χ is a character then for any $g_1, g_2 \in G$:

$$\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$$

And since

$$\chi(1_G) = \chi(1_G)\chi(1_G)$$

$$\chi(1_G) = 1$$

Moreover, for every $g \in G$,

$$\chi(g)^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1$$

Hence the values of χ are the $|G|$ -th roots of unity. And

$$\chi(g^{-1})\chi(g) = \chi(g^{-1}g) = 1$$

So,

$$\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$$

where the bar denotes complex conjugation of $\chi(g)$.
A character χ_0 is trivial if $\chi_0(g) = 1$ for all $g \in G$. The rest of the characters are known as nontrivial characters.

Theorem 4.2.6. *[21] If χ is a nontrivial character of a finite Abelian group G then*

$$\sum_{g\in G}\chi(g) = 0$$

If $g \in G$ with $g \neq 1_G$, then

$$\sum_{\chi}\chi(g) = 0$$

In addition to theorem, we have an additional orthogonality relations for characters. Let χ and ψ be characters of G. Then

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} = \begin{cases} 0 & \text{if } \chi \neq \psi \\ 1 & \text{if } \chi = \psi \end{cases} \tag{4.1}$$

Character theory is sometimes useful to get expressions about the number of solutions of equations in finite Abelian group G. The argument is as folllowing:

Lemma 4.2.7. *Let G be a finite Abelian group and let f be an arbitrary map, $f : G^n \to G$, where G^n is a cartesian product.*
Then for given $y \in G$ the number of solutions $N(y)$ of

$$f(x_1, x_2, ..., x_n) = y$$

is

$$N(y) = \frac{1}{|G|}\sum_{x_1\in G}\sum_{x_2\in G}...\sum_{x_n\in G}\sum_{\chi\in G}\chi(f(x_1, x_2, .., x_n))\overline{\chi(y)} \tag{4.2}$$

In the case of finite fields, for $\mathbb{F}_q$ there are additive character for additive group $\mathbb{F}_q$ and multiplicative character for multiplicative group $\mathbb{F}_q^*$.

In this part, for finite fields only additive characters of a finite field $\mathbb{F}_q$ are considered and some properties that will be helpful to prove our theorem are mentioned from [21].

Let $\mathbb{F}_q$ be a finite field with characteristic p, where p is an odd prime and let $Tr : \mathbb{F}_q \to \mathbb{F}_p$ be the absolute trace function.

Then the function χ_1 defined as

$$\chi_1(x) = \epsilon_p^{Tr(x)}$$

where ϵ_p is a p-th root of unity, for all $x \in \mathbb{F}_q$ is a character of the additive group of $\mathbb{F}_q$.

To see this explicitly, check that

$$\chi_1(x_1 + x_2) = \epsilon_p^{Tr(x_1+x_2)}$$

$$= \epsilon_p^{Tr(x_1)}\epsilon_p^{Tr(x_2)}$$

$$= \chi(x_1)\chi(x_2)$$

All additive characters of $\mathbb{F}_q$ can be expressed in terms of χ_1, which is given in the following theorem.

Theorem 4.2.8. *[21] For $b \in \mathbb{F}_q$, the function χ_b satisfying*

$$\chi_b(x) = \chi_1(bx)$$

for all $x \in \mathbb{F}_q$ is an additive character of $\mathbb{F}_q$, and each additive character of $\mathbb{F}_q$ is obtained in this way.

Lemma 4.2.9. *[21] Let χ_a and χ_b be given as additive characters of $\mathbb{F}_q$ as in Theorem 4.2.8. Then*

$$\sum_{x\in\mathbb{F}_q} \chi_a(x)\overline{\chi_b(x)} = \begin{cases} 0 & \text{if } a \neq b \\ q & \text{if } a = b \end{cases} \tag{4.3}$$

In particular,

$$\sum_{x\in\mathbb{F}_q} \chi_a(x) = 0$$

for $a \neq 0$.

The knowledge above about additive characters over a finite Abelian groups, especially over a finite field $\mathbb{F}_q$, is used to prove the following theorem ([21] Theorem 7.7) about permutation polynomials.

Theorem 4.2.10. *Let f be a polynomial from $\mathbb{F}_q$ to itself. Then polynomial f is a permutation polynomial of $\mathbb{F}_q$ if and only if*

$$\sum_{x\in\mathbb{F}_q}\chi(f(x)) = 0$$

for all nontrivial additive characters χ of $\mathbb{F}_q$.

Proof. Assume that f is a permutation polynomial of $\mathbb{F}_q$. Then,

$$\sum_{x\in\mathbb{F}_q}\chi(f(x)) = \sum_{x\in\mathbb{F}_q}\chi(x)$$

Hence, by Theorem 4.2.8

$$\sum_{x\in\mathbb{F}_q}\chi(x) = 0$$

Conversely, assume that

$$\sum_{x\in\mathbb{F}_q}\chi(f(x)) = 0$$

for any nontrivial character χ.

Then by Lemma 4.2.7, we can count $N(y)$ for any $y \in \mathbb{F}_q$, where $N(y)$ denotes the number of solutions of $f(x) = y$ in $\mathbb{F}_q$.

$$N(y) = \frac{1}{q}\sum_{x\in\mathbb{F}_q}\sum_{\chi}\chi(f(x))\overline{\chi(y)}$$

$$= 1 + \frac{1}{q}\sum_{\chi\neq\chi_0}\overline{\chi(x)}\sum_{x\in\mathbb{F}_q}\chi(f(x))$$

$$= 1$$

by equation (4.1).

Hence, f is a permutation polynomial of $\mathbb{F}_q$. □

Immediate trivial corollary follows:

Corollary 4.2.11. *Let f be a function from $\mathbb{F}_q$ to itself. Then f is a permutation polynomial of $\mathbb{F}_q$ if and only if*

$$\sum_{x\in\mathbb{F}_q} \epsilon_p^{Tr(\alpha x)} = 0$$

for any $\alpha \in \mathbb{F}_q^*$.

At the end of this section we give our main theorem about p-ary Alltop functions and Alltop functions.

Theorem 4.2.12. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be any function and $f_\alpha : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a p-ary function defined as*

$$f_\alpha(x) = Tr(\alpha F(x))$$

for any $\alpha \in \mathbb{F}_{p^n}^*$, where Tr is the usual trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.
Then F is Alltop if and only if f_α is p-ary Alltop for any $\alpha \in \mathbb{F}_{p^n}^*$.

Proof. Let f_α is given as above. Then by Observation 4.0.3, f_α is p-ary Alltop if and only if

$$\sum_{x\in\mathbb{F}_{p^n}} \epsilon_p^{D_bD_af_\alpha(x)} = 0,$$

for all $a, b \in \mathbb{F}_{p^n}^*$, where ϵ_p is a p-th root of unity in $\mathbb{F}_{p^n}$.
Since

$$D_bD_af_\alpha(x) = D_bD_aTr(\alpha F(x)) = Tr(\alpha D_bD_aF(x))$$

Then f_α is p-ary Alltop if and only if

$$\sum_{x\in\mathbb{F}_{p^n}} \epsilon_p^{Tr(\alpha D_bD_a(F(x)))} = 0$$

for any nonzero $a, b \in \mathbb{F}_{p^n}$.
Since α is also nonzero, by Corollary 4.2.11, the sum is zero if and only if $D_bD_aF(x)$ is permutation for any $a, b \in \mathbb{F}_{p^n}$, which means that F is an Alltop function.

□

CHAPTER 5

APPLICATIONS TO CRYPTOGRAPHY

This part is about applications of Alltop functions to cryptography-especially to construction of mutually unbiased bases which is an essential part of quantum cryptography.

5.1 Mutually Unbiased Bases

"Mutually Unbiased Bases" notion in quantum mechanics first appeared in the studies of Schwinger [31] in 1960. By using planar functions and Alltop functions, construction of complete mutually unbiased bases is possible as mentioned in the first chapter. But before we start with some basic definitions related to mutually unbiased bases.

Definition 5.1.1. *A subset* $\{v_1, v_2, .., v_n\}$ *of a vector space V with inner product* $<,>$ *is called orthonormal if*

$$< v_i, v_j >= \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{otherwise} \end{cases} \tag{5.1}$$

Definition 5.1.2. *Let A and B be two orthonormal basis in* $\mathbb{C}^d$*. A and B are said to be unbiased if*

$$< a, b >= \frac{1}{\sqrt{d}}$$

for all $a \in A$ *and* $b \in B$*. Moreover, a set of bases which are pairwise unbiased is known as a set of mutually unbiased bases (MUB).*

Schwinger's observation was that, for two mutually unbiased bases A and B, information can not be gathered when a quantum system in a basis state from A, is measured

with respect to the basis B.
Explicitly, if a quantum state is prepared in an eigenstate of basis A and measured in basis B, then probability of outcome k with known a is

$$P(k|a) = | < b, a > |^2 = \frac{1}{d}$$

for any output k, where $a \in A$ and $b \in B$. That is, all outcomes have equal probability. In quantum cryptography, this property of MUB's was used to bind a protocol BB84 [2], which is used in sharing secret keys between users in a secure way.
It is known that [35] in $\mathbb{C}^d$ there can be at most $d + 1$ MUB's and in this case, such sets are called complete.

In addition, when d is any prime power, there are several constructions of complete MUB's ([35],[17]), however, when d is not a prime power it is still an open problem to construct complete MUB's. Although Schwinger did not construct an extremal sets of MUBs in 1960, Alltop constructed a complex sequences for radar and telecommunication systems, which have optimal properties. Alltop's construction is for only dimension prime p, which produces $p + 1$ mutually unbiased bases. In [17] this construction is generalized to all prime powers.
To illustrate, the following example is given about MUB's:

Example 5.1.3. *In a 2 dimensional Hilbert space $\mathbb{C}^2$:*

$$\{(1,0),(0,1)\},$$
$$\left\{\frac{(1,0)+(0,1)}{\sqrt{2}}, \frac{(1,0)-(0,1)}{\sqrt{2}}\right\},$$
$$\left\{\frac{(1,0)+i(0,1)}{\sqrt{2}}, \frac{(1,0)-i(0,1)}{\sqrt{2}}\right\}$$

are basis such that, each of them is orthonormal. Since they are orthonormal and pairwise unbiased, a set of these bases is MUB. In addition, it is a complete set of MUB over $\mathbb{C}^2$.

5.1.1 Constructions

Before construction of complete MUB's from both planar and Alltop functions, we need the following theorem ([8], [21]) (which is also known as Weil sums):

Theorem 5.1.4. *Let $f(x)$ be any function from $\mathbb{F}_q$ to itself where $q = p^n$, ϵ_p is a p-th root of unity and $\chi(x)$ is an additive character of $\mathbb{F}_q$ (which is $\chi(x) = \epsilon_p^{Tr(x)}$). Then f is perfect nonlinear (planar) if and only if*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(af(x) + bx) \right| = \sqrt{q}$$

Theorem 5.1.5. *(Construction from planar functions)[29][12] Let $\mathbb{F}_q$ be a finite field with characteristic p, where p is an odd prime and f be a planar function over $\mathbb{F}_q$. Denote*

$$B_a = \{v_{ab} \quad | \quad b \in \mathbb{F}_q\}$$

the set of vectors given by

$$v_{ab} = \frac{1}{\sqrt{q}} \left(\epsilon_p^{Tr(af(x)+bx)} \right)_{x \in \mathbb{F}_q}$$

with $a, b \in \mathbb{F}_q$. The standard basis E with the sets B_a, $a \in \mathbb{F}_q$, form a complete set of $q + 1$ MUBs in $\mathbb{C}^q$.

Example 5.1.6. *Let $q = p = 3$ in the theorem above and $f(x) = x^2$. Then*

$$B_o = \{v_{00}, v_{01}, v_{02}\} = \left\{ \frac{1}{\sqrt{3}}(1,1,1), \frac{1}{\sqrt{3}}(1, \epsilon_3, \epsilon_3^2), \frac{1}{\sqrt{3}}(1, \epsilon_3^2, \epsilon_3) \right\},$$

$$B_1 = \{v_{10}, v_{11}, v_{12}\} = \left\{ \frac{1}{\sqrt{3}}(1, \epsilon_3, \epsilon_3), \frac{1}{\sqrt{3}}(1, \epsilon_3^2, 1), \frac{1}{\sqrt{3}}(1, 1, \epsilon_3^2) \right\},$$

$$B_2 = \{v_{20}, v_{21}, v_{22}\} = \left\{ \frac{1}{\sqrt{3}}(1, \epsilon_3^2, \epsilon_3^2), \frac{1}{\sqrt{3}}(1, \epsilon_3, 1), \frac{1}{\sqrt{3}}(1, 1, \epsilon_3) \right\},$$

With standard basis $E = \{(0,0,1), (0,1,0), (1,0,0)\}$, in dimension 3, these bases form four mutually unbiased bases, which is maximal.

Note that Alltop's original function (x^3) was only for $\mathbb{C}^p$, where $p > 3$. A generalization to all prime powers is given in the following theorem (Klappeneker, Rötteler)

Theorem 5.1.7. *(Alltop's construction) [17] Let $\mathbb{F}_q$ be a finite field with characteristic odd prime $p \geq 5$. Let B_a be a set of vectors*

$$B_a = \{v_{ab} \quad | \quad a \in \mathbb{F}_q\}$$

given by

$$v_{ab} = \frac{1}{\sqrt{q}} \left(\epsilon_p^{Tr((x+b)^3 + a(x+b))} \right)_{x \in \mathbb{F}_q}$$

The standard basis and the sets B_a with $a \in \mathbb{F}_q$ forms a complete set of $q + 1$ mutually unbiased bases of $\mathbb{C}^q$.

In [14] it was proven that the above theorem holds not only for x^3, it holds for any Alltop functions over $\mathbb{F}_q$.

Theorem 5.1.8. *Let $\mathbb{F}_q$ be a finite field with characteristic odd prime $p \geq 5$ and $f(x)$ be an Alltop function over $\mathbb{F}_q$. Let*

$$B_a = \{v_{ab} \quad | \quad b \in \mathbb{F}_q\}$$

be the set of vectors given by

$$v_{ab} = \frac{1}{\sqrt{q}}\left(\epsilon_p^{Tr(f(x+a)+b(x+a))}\right)_{x\in\mathbb{F}_q}$$

with $a, b \in \mathbb{F}_q$. The standard basis with the sets B_a, $a \in \mathbb{F}_q$ form a complete set of $q+1$ MUBs in $\mathbb{C}^q$.

Proof. Observe that, for any $a, b \in \mathbb{F}_q$

$$v_{ab} = \frac{1}{\sqrt{q}}\left(\chi(f(x+a)+b(x+a))\right)_{x\in\mathbb{F}_q}$$

Now,

$$< v_{ab}|v_{cd} >= \frac{1}{q}\sum_{x\in\mathbb{F}_q}\chi\Big(f(x+a)-f(x+c)+b(x+a)-d(x+c)\Big)$$

(Note that, this notation is called cat-bra notation in quantum information theory, and have some special properties like

$$< v_{ab}|v_{cd} >= v^*_{a_1b_1}v_{c_1d_1} + ... + v^*_{a_nb_n}v_{c_nd_n}$$

where $v^*_{a_ib_i}$ is complex conjugate of $v_{a_ib_i}$)
Substitute $y = x + c$ and $\beta = a - c$:

$$< v_{ab}|v_{cd} >= \frac{1}{q}\sum_{x\in\mathbb{F}_q}\chi\Big(f(y+\beta)-f(y)+(b-d)y+b\beta\Big)$$

$$= \frac{1}{q}\sum_{x\in\mathbb{F}_q}\chi\Big(D_\beta f(y)+(b-d)y+\beta\Big)$$

Since f is Alltop, then necessarily $D_\beta f(y)$ is planar, and so $D_\beta f(y) + (b-d)y + \beta$ is also planar for $\beta \in \mathbb{F}_q^*$. Then by 5.1.5,

$$< v_{ab}|v_{cd} >= \frac{1}{\sqrt{q}}$$

for $a \neq c$. If $a = c$ then

$$< v_{ab}|v_{cd} >= \frac{1}{q} \sum_{x \in \mathbb{F}_q} \chi\Big((b-d)(x+c)\Big).$$

If $b \neq d$ then,

$$< v_{ab}|v_{cd} >= 0$$

Finally, if $b = d$, then

$$< v_{ab}|v_{ab} >= \frac{1}{q} \sum_{x \in \mathbb{F}_q} \chi(0) = 1$$

Hence, orthonormal property holds. Moreover, since each vector is unbiased pairwise, complete set of MUBs in $\mathbb{C}^q$ is constructed.

□

REFERENCES

[1] W. Alltop, Complex sequences with low periodic correlations (corresp.), IEEE Transactions on Information Theory, 26(3), pp. 350–354, 1980.

[2] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and con tos5, 1984.

[3] C. Blondeau and K. Nyberg, Perfect nonlinear functions and cryptography, Finite fields and their applications, 32, pp. 120–147, 2015.

[4] L. Budaghyan and T. Helleseth, Planar functions and commutative semifields, Tatra Mountains Mathematical Publications, 45(1), pp. 15–25, 2010.

[5] C. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions and permutations suitable for des-like cryptosystems, Designs, Codes and Cryptography, 15(2), pp. 125–156, 1998.

[6] C. Carlet and S. Mesnager, Four decades of research on bent functions, Designs, Codes and Cryptography, 78(1), pp. 5–50, 2016.

[7] R. S. Coulter and M. Henderson, Commutative presemifields and semifields, Advances in Mathematics, 217(1), pp. 282–304, 2008.

[8] R. S. Coulter and R. W. Matthews, Bent polynomials over finite fields, Bulletin of the Australian Mathematical Society, 56(3), pp. 429–437, 1997.

[9] R. S. Coulter and R. W. Matthews, Planar functions and planes of lenz-barlotti class ii, Designs, Codes and Cryptography, 10(2), pp. 167–184, 1997.

[10] P. Dembowski and T. G. Ostrom, Planes of ordern with collineation groups of ordern 2, Mathematische Zeitschrift, 103(3), pp. 239–258, 1968.

[11] L. E. Dickson, On commutative linear algebras in which division is always uniquely possible, Transactions of the American Mathematical Society, 7(4), pp. 514–522, 1906.

[12] C. Ding and J. Yin, Signal sets from functions with optimum nonlinearity, IEEE transactions on communications, 55(5), pp. 936–940, 2007.

[13] J. L. Hall, A. Rao, and D. Donovan, Planar difference functions, in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pp. 1082–1086, IEEE, 2012.

[14] J. L. Hall, A. Rao, and S. M. Gagola, A family of alltop functions that are ea-inequivalent to the cubic function, IEEE Transactions on Communications, 61(11), pp. 4722–4727, 2013.

[15] X.-D. Hou and C. Sze, On certain diagonal equations over finite fields, Finite Fields and Their Applications, 15(6), pp. 633–643, 2009.

[16] G. A. Kabatiansky and V. I. Levenshtein, On bounds for packings on a sphere and in space, Problemy Peredachi Informatsii, 14(1), pp. 3–25, 1978.

[17] A. Klappenecker and M. Rötteler, Constructions of mutually unbiased bases, in *Finite fields and applications*, pp. 137–144, Springer, 2004.

[18] P. V. Kumar, R. A. Scholtz, and L. R. Welch, Generalized bent functions and their properties, Journal of Combinatorial Theory, Series A, 40(1), pp. 90–107, 1985.

[19] G. Kyureghyan and F. Ozbudak, Planar products of linearized polynomials, in *WCC 2011-Workshop on coding and cryptography*, pp. 351–360, 2011.

[20] M. Kyuregyan, F. Özbudak, and A. Pott, Some planar maps and related function fields, Arithmetic, Geometry, Cryptography and Coding Theory, 574, pp. 87–114, 2012.

[21] R. Lidl and H. Niederreiter, Finite fields: Encyclopedia of mathematics and its applications., Computers & Mathematics with Applications, 33(7), pp. 136–136, 1997.

[22] J. Maclagan-Wedderburn, A theorem on finite algebras, Transactions of the American Mathematical Society, 6(3), pp. 349–352, 1905.

[23] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, Elsevier, 1977.

[24] S. Mesnager, Characterizations of plateaued and bent functions in characteristic p, in *International Conference on Sequences and Their Applications*, pp. 72–82, Springer, 2014.

[25] S. Mesnager, *Bent functions*, Springer, 2016.

[26] S. Mesnager, F. Özbudak, and A. Sınak, On the p-ary (cubic) bent and plateaued (vectorial) functions, Designs, Codes and Cryptography/submitted.

[27] S. Mesnager, F. Özbudak, and A. Sınak, Results on characterizations of plateaued functions in arbitrary characteristic, in *International Conference on Cryptography and Information Security in the Balkans*, pp. 17–30, Springer, 2015.

[28] O. S. Rothaus, On “bent” functions, Journal of Combinatorial Theory, Series A, 20(3), pp. 300–305, 1976.

[29] A. Roy and A. Scott, Weighted complex projective 2-designs from bases: optimal state determination by orthogonal measurements, Journal of mathematical physics, 48(7), p. 072110, 2007.

[30] K.-U. Schmidt and Y. Zhou, Planar functions over fields of characteristic two, Journal of Algebraic Combinatorics, 40(2), pp. 503–526, 2014.

[31] J. Schwinger, Unitary operator bases, Proceedings of the National Academy of Sciences, 46(4), pp. 570–579, 1960.

[32] N. Tokareva, *Bent functions: results and applications to cryptography*, Academic Press, 2015.

[33] L. Welch, Lower bounds on the maximum cross correlation of signals (corresp.), IEEE Transactions on Information theory, 20(3), pp. 397–399, 1974.

[34] G. Weng and X. Zeng, Further results on planar do functions and commutative semifields, Designs, Codes and Cryptography, 63(3), pp. 413–423, 2012.

[35] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, Annals of Physics, 191(2), pp. 363–381, 1989.