SOME STUDIES ON CCZ-EQUIVALENCE OF THE INVERSE FUNCTION

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

BY

MEHTAP FIDAN

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

SEPTEMBER 2021

Approval of the thesis:

SOME STUDIES ON CCZ-EQUIVALENCE OF THE INVERSE FUNCTION

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

Prof. Dr. A. Sevtap Selçuk Kestel _____
Director, Graduate School of **Applied Mathematics**

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

Prof. Dr. Ferruh Özbudak _____
Supervisor, **Cryptography, METU**

Examining Committee Members:

Assoc. Prof. Dr. Murat Cenk
Institute of Applied Mathematics, METU _____

Prof. Dr. Ferruh Özbudak
Institute of Applied Mathematics, METU _____

Assist. Prof. Dr. Eda Tekin
Department of Mathematics, Karabük 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: MEHTAP FIDAN

Signature :

ABSTRACT

SOME STUDIES ON CCZ-EQUIVALENCE OF THE INVERSE FUNCTION

Fidan, Mehtap
M.S., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

September 2021, 36 pages

Most cryptographic systems, like block ciphers, depend heavily on vectorial Boolean functions. A function with good cryptological properties should have low differential uniformity which is invariant under some equivalence classes. The more general one of these is CCZ-equivalence which is introduced by Carlet, Charpin and Zinoviev in 1998. In cryptography, CCZ-equivalence gained an interest since it preserves many significant properties like differential uniformity. Looking for permutations within the CCZ-class of a function for the construction of S-boxes used in block ciphers is also intriguing. In this thesis, we presented a detailed description on the results of Kölsch's paper about nonexistence of permutation polynomials in the form $L_m(x^{-1}) + L_{m'}(x)$ over binary finite field. This proves that every permutation CCZ-equivalent to the inverse function is also affine equivalent to it. We also gave a criterian to be a permutation polynomial which is verified by using Kloosterman sums.

Keywords: CCZ-equivalence, permutation polynomial, inverse function, kloosterman sum

ÖZ

TERS FONKSİYONUN CCZ-DENKLİĞİ ÜZERİNE BAZI ÇALIŞMALAR

Fidan, Mehtap
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Eylül 2021, 36 sayfa

Vektörel Boolean fonksiyonlar, blok şifreleme gibi çoğu kriptografik sistemin önemli bileşenleridir. İyi kriptolojik özelliklere sahip bir fonksiyon, bazı denklik sınıflarında değişmez olan düşük diferansiyel tekdüzeliğe sahip olmalıdır. Bunlardan daha genel olanı, 1998 yılında Carlet, Charpin ve Zinoviev tarafından tanıtılan CCZ-eşdeğerliğidir. Kriptografide, CCZ-eşdeğerliği, diferansiyel tekdüzelik gibi birçok önemli özelliği koruduğu için ilgi görmeye başlamştır. Blok şifrelemede kullanılan S-kutularının tasarımı için, bir fonksiyonun CCZ-sınıfı içindeki permütasyonlarını aramak da ilgi çekici bir soru olmuştur. Bu tezde, Kölsch'ün $n \geq 5$ için ikili sonlu alanda incelenen $L_m(x^{-1}) + L_{m'}(x)$ formundaki permütasyon polinomların varlığı ile ilgili makalesinin sonuçlarını ayrıntılı bir açıklama ile sunduk. Ayrıca, Kloosterman toplamını kullanarak, bir permütasyon polinomu olma kriteri verdik.

Anahtar Kelimeler: CCZ-denkliği, permütasyon polinomu, ters fonksiyon, kloosterman toplamı

ACKNOWLEDGMENTS

First of all, I would like to express my deep and sincere gratitude to my supervisor Prof. Dr. Ferruh Özbudak for his guidance and advice. His encouragement helped me through difficult times during this thesis and enabled me to fulfill the aimed requirements.

I am so thankful to my thesis defence committee members for taking their valuable time.

I want to express my appreciation and warm thanks to my family for always supporting and standing behind me.

I would also thank to my friends Betül Ünver, who started writing a thesis at the same time as me, for supporting me; Begüm Aydaş and Ardahan F. Yüksel for their endless support throughout the thesis and always.

Finally, I would like to thank The Scientific and Technological Research Coincil of Turkey (TÜBİTAK) for financial support under the program 2210-A.

TABLE OF CONTENTS

ABSTRACT vii

ÖZ ix

ACKNOWLEDGMENTS xi

TABLE OF CONTENTS xiii

LIST OF TABLES xv

LIST OF ABBREVIATIONS xvi

CHAPTERS

1 INTRODUCTION 1

2 NOTION OF CCZ-EQUIVALENCE 3

2.1 Differential and Linear Properties 3

2.2 Concepts of CCZ- and EA-Equivalences 4

2.2.1 Coincidence of EA- and CCZ-equivalence 5

2.2.2 Searching Permutations in a CCZ-class 6

3 PRELIMINARIES TO THE SUBJECT 9

4 SEARCHING EXISTENCE OF PERMUTATIONS 13

4.1 Method to prove 13

4.2 Kloosterman Sum over $\mathbb{F}_{2^n}$ for Permutation Polynomials . . 13

4.3 Proof for Non-existence of Permutation Polynomial 15

5 CRITERIAN FOR THE EXISTENCE OF PERMUTATION IN $\mathbb{F}_{P^N}$. 27

5.1 Kloosterman Sum over $\mathbb{F}_{p^n}$ for Permutation Polynomials . . 27

5.2 Possible Future Works 30

6 CONCLUSION AND OPEN PROBLEMS 33

REFERENCES 35

LIST OF TABLES

Table 2.1 Some APN exponents d to CCZ-equivalence [13] 6

Table 4.1 List of coefficients of x^8 in $\mathcal{Q}((x^2+x)L^*_{m'}(x))$ 25

LIST OF ABBREVIATIONS

CCZ	Carlet Charpin Zinoviev
EA	Extendend Affine
ANF	Algebraic Normal Form
APN	Almost Perfect Nonlinear
DDT	Difference Distribution Table
LAT	Linear Approximation Table
S-box	Substitution Box
Tr	Trace Map

CHAPTER 1

INTRODUCTION

In cryptography, vectorial Boolean functions are essential components of the most crytographic systems, especially, Symmetric Key Cryptography. As design choices of substitution boxes, or shortly S-boxes, they play a vital role in the construction of block ciphers. Against to main attacks on block ciphers which are differential and linear attacks, vectorial Boolean functions should have high resistance. This means that the conditions low differential uniformity [1] and high nonlinearity [16] on these functions are necessary to be secure to linear and differential cryptanalysis, respectively.

There are several equivalence concepts that are invariant under some operations and conditions on vectorial Boolean functions. Three of them which is widely used are affine equivalence, extended affine equivalence, or shortly EA-equivalence and CCZ-equivalence. The most generic one of these equivalence classes is CCZ-equivalence. [5] and since it preserves the differential uniformity it is powerful tool against differential attacks. It was introduced in [7] by Carlet, Charpin and Zinoviev in 1998 and named after [5].

It is important to look for permutatitons within the CCZ-class of a function since they are crucial to design block ciphers. In majority of the thesis, we study on results of the paper of Kölsch [13] about nonexistence permutation polynomials in form $L_m(x^{-1}) + L_{m'}(x)$ over binary finite field for n is greater than or equal to 5, where L_m and $L_{m'}$ are linear mappings. It means that all functions CCZ-equivalent to the inverse function are also extended affine equivalent to it. Furthermore, every permutation that is CCZ-equivalent to the inverse function is also affine equivalent to that.

In this part of the thesis; basic concepts are introduced and a literature review is introduced.

Organization of the thesis is as in the following:

- In Chapter 2, literature review is given to make clear the concepts of equivalence classes.
- In Chapter 3, some definitions, lemmas, corollaries and theorems to be used later are given.
- In Chapter 4, the results of the paper of Kölsch about non-existence of permutation polynomails in the form $L_m(x^{-1}) + L_{m'}(x)$ are studied inclusively.
- In Chapter 5, a criterian to be a permutation polynomial is verified by using Kloosterman sums.
- In Chapter 6, a conclusion is given.

CHAPTER 2

NOTION OF CCZ-EQUIVALENCE

In this part of the thesis; basic definitions are given and literature review is conducted in details.

2.1 Differential and Linear Properties

There are differential and linear properties of functions in S-boxes which measure resistance in the case of linear and differential attacks. For differential and linear cryptanalysis, two main tables that are difference distribution table and linear approximation table, respectively, are powerful tools.

The (DDT) Difference Distribution Table of a S-box is a crucial component to make an estimation about the probabilty of a differential characteristic. The differential uniformity of F can be expressed as the maximum coefficient in the DDT.

Definition 1. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a vectorial Boolean function. The differential uniformity δ of F is follows:*

$$\delta = \max_{c \in \mathbb{F}_{2^n}^*, d \in \mathbb{F}_{2^n}} \{F(x) + F(x+c) = d | x \in \mathbb{F}_{2^n}\}$$

The function is defined APN (almost perfect nonlinear) if it has differential uniformity two.

A vectorial Boolean function which has good cryptological properties should have low differential uniformity to have best resistance to differential attacks. Almost perfect nonlinear functions has the optimal resistance to these attacks, since the differential uniformity has to be always even.

Similarly, Linear Approximation Table, shortly LAT, or Walsh transform of a S-box provide an estimation about its linearity/noninearity characteristics. The *linearity of* F is defined as maximum coefficient in this table.

Definition 2. *Let* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be a function. Then Walsh transform of* F, $W_{\mathbb{F}} : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{Z}$ *is defined as*

$$W_{\mathbb{F}}(u, v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(uF(x)+vx)}$$

Then *non-linearity of the function* F is the following:

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_{2^n}^*, v \in \mathbb{F}_{2^n}} |W_{\mathbb{F}}(u, v)|$$

To have a better resistance to linear attacks, the function of S-box should have high nonlinearity.

For vectoral Boolean functions, some operations lead to several equivalence concepts which differential and linear properties invariant. In next section, the definitions of these equivalence classes are given. Before that, the graph of a function F mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ is represented as the following.

$$\{x \in \mathbb{F}_{2^n} | (x, F(x))\} = G_F \subset \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$$

2.2 Concepts of CCZ- and EA-Equivalences

Definition 3. *(EA-Equivalence) Let* F_1 *and* F_2 *be two functions mapping from* $\mathbb{F}_{2^n}$ *to* $\mathbb{F}_{2^n}$*, If there exists affine permutations* A_1*,* A_2 *and an affine function* $A_3 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *such as the following*

$$F_2 = A_1 \circ F_1 \circ A_2 + A_3 \tag{2.1}$$

then F_1 *and* F_2 *are extended affine equivalent, or shortly EA-equivalent, where* A_3 *is sum of a constant and a linear function.*
If A_3 *in Eq. (2.1) is zero, then the functions* F_1 *and* F_2 *are called as affine equivalent.*

It can be observed that two functions which are affine equivalent are already EA-equivalent.

CCZ-equivalence, of which EA-equivalence is a special case, is the most general kind of function equivalence known to retain differential uniformity. It can be defined as the fact that if an affine permutation exists that allows us to obtain from one graph of a function to the graph of another function, then these two functions are called CCZ-equivalent.

Definition 4. *(CCZ-Equivalence) Let $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be two vectorial Boolean functions. If an affine, bijective mapping A on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ exists as in the following*

$$\{x \in \mathbb{F}_{2^n} | (x, F(x))\} = A(\{x \in \mathbb{F}_{2^n} | (x, G(x))\})$$

then F, G are CCZ-equivalent.

It can be seen that two vectorial Boolean functions which are EA-equivalent are already CCZ-equivalent.

Generally, the notions of EA-equivalence and CCZ-equivalence differs from each other at some points. For instance, while the compositional inverse of a one-to-one and onto mapping is CCZ-equivalent to itself, this can not be said for EA-equivalence. Note also that EA-equivalence preserves many of cryptologic properties of a function such as its nonlinearity, differential and degree of algebraic normal form (ANF). However, CCZ-equivalence may not invariant under degree of ANF, unlike to EA-equivalence [5].

2.2.1 Coincidence of EA- and CCZ-equivalence

It was shown that in several cases, EA equivalence and CCZ-equivalence coincide [13]. Let the set of every functions which are CCZ-equivalent to F be defined as CCZ-class of F and the set of every functions which are EA-equivalent to F be EA-class of F. EA-classes can be partition to CCZ-class, because EA-equivalence is a specific case of the more general notion CCZ-equivalence. According to experimental results, if F is not permutation then EA- and CCZ-classes of F coincides for most of the vectorial Boolean functions F. Furthermore, in case of being permutation F, CCZ-class of F is composed of exactly two EA-classes of F and its inverse. However, there are some cases which CCZ-class has more than two EA-classes in it, this is possible for Gold APN functions in Table 2.1 in odd dimension [5].

Carlet and Budaghyan [4] proved that CCZ-equivalence and EA-equivalence coincides for Boolean functions and bent functions. Also, another interesting case that was proved in paper [2] is the fact that two APN functions, which are quadratic, are CCZ-equivalent if and only if they are EA-equivalent. By applying Walsh transform of a function F, namely its differential distribution table, Canteaut and Perrin [6] found upper bound for the number of seperate EA-equivalence classes inside the CCZ-equivalence class.

It is not understandable yet how the CCZ-class of F is defined exactly by the inverse

Table 2.1: Some APN exponents d to CCZ-equivalence [13]

	Exponent d	Condition
Kasami	$2^{2s}-2^s+1$	$gcd(s,n)=1$
Gold	2^s+1	$gcd(s,n)=1$
Niho	$2^r-2^{\frac{r}{2}}-1$	$r\ even, n=2r+1$
	$2^r-2^{\frac{3r+1}{2}}-1$	$r\ odd, n=2r+1$
Inverse	2^n-2	$n\ odd$
Welch	2^r+3	$n=2r+1$

transformation (in case of being invertible) and EA-equivalence. This is an open problem for most of the APN monomials in Table 2.1. Only for small values of n by using a computer search; Budaghyan, Calderini and Villa [3] improved the conjecture below.

Conjecture 1. *Assume $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ and $F(x)=x^d$ is inverse function or nonGold APN function. Then all function CCZ-equivalent to F is already EA-equivalent to it or its inverse in case of existing.*

2.2.2 Searching Permutations in a CCZ-class

Here we have an interesting question which is how to analyze every permutations in an APN function's CCZ-class, however searching that problem is still difficult for the APN families. For this question, Güloğlu and Langevin [10] reached the following result by analysing of the Gold and Kasami functions' bent components. If $4|n$, any permutation exists in the CCZ-class of APN Kasami functions in binary finite field.

Lucas Kölsh [13] classified every permutations inside inverse function's CCZ-class

in both odd and even dimensions. The proof method differs from that used in [10], because there are no bent components for the case of inverse function. Let L_m, $L_{m'}$ be nonzero linear mappings. The following proposition is used as the method for the special type of permutation polynomial which has form $L_m(x^{-1}) + L_{m'}(x)$. For a proof see [9].

Proposition 1. *1. Let F be a vectorial Boolean function over $\mathbb{F}_{2^n}$ and L be nonzero linear mapping. All permutation EA-equivalent to F is also affine equivalent to F, if there are no permutatiton in the form $F(x) + L(x)$.*

2. Let F be a vectorial Boolean function over $\mathbb{F}_{2^n}$ and L_m, $L_{m'}$ be nonzero linear mappings. Then all functions CCZ-equivalent to the function are already affine equivalent to it or its inverse if there are no permutation in the form $L_m(F(x)) + L_{m'}(x)$. In addition, every permutation CCZ-equivalent to F is affine equivalent to it and its inverse.

It was found that there exists permutation polynomial in the form $L_m(x^{-1}) + L_{m'}(x)$ for $n \leq 5$, particularly, for $n = 3$ and $n = 4$ over finite field in characteristic 2 with $L_m(x) = x$ by Li and Wang [14].

By Lucas Kölsch [13], it was proven that if n is greater or equal to 5, then no permutation polynomial in the form $L_m(x^{-1}) + L_{m'}(x)$ exists in binary finite field. It means that all functions CCZ-equivalent to the inverse function are affine equivalent to it, which verifies Conjecture 1. In Chapter 4, the result in below will be reached.

Theorem 1. *Let $n \geq 5$, assume F is a inverse function in binary finite field. Then EA-class and CCZ-class of F coincide. In addition, every permutation inside CCZ-class of F is already affine equivalent to it.*

CHAPTER 3

PRELIMINARIES TO THE SUBJECT

In this section, some basic concepts of the subject and notations are introduced.

Definition 5. *Let F be a function such that $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. Then it is called vectiral Boolean function, where $m \in \mathbb{Z}$. The function F is just defined Boolean function for $m = 1$.*

Definition 6. *If the function f in $\mathbb{F}_q[x]$ to itself defined as $x \to f(x)$ is a permutation of $\mathbb{F}_q$, the polynomial f from $\mathbb{F}_q[x]$ is defined a permutation polynomial of $\mathbb{F}_q[x]$.*

Definition 7. *The trace map $Tr : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is defined as*

$$Tr(x) = \sum_{i=0}^{n-1} x^{p^i} = x + x^p + x^{p^2} + ... + x^{p^{n-1}}$$

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

Throughout this chapter and Chapter 3, we will use trace mapping over binary Galois field.

Definition 8. *With respect to the bilinear form, adjoint mapping is denoted by L^* of a linear mapping L*

$$Tr(xy) = \langle x, y \rangle$$

namely, we have the following for each $x, y \in \mathbb{F}_{2^n}$

$$Tr(L(x)y) = Tr(xL^*(y))$$

If we explicitly write linear mapping $L(x) == \sum_{i=0}^{n-1} c_i x^{2^i}$, the adjoint mapping of L is described as $L^*(x) = \sum_{i=0}^{n-1} c_i^{2^{n-i}} x^{2^{n-i}}$

For the proof of the following lemma, see [15].

Lemma 1. *For $s \neq 0$, let $rx^2 + sx + t = 0$ be the quadratic equation in $\mathbb{F}_{2^n}$. Then, $Tr(rt/s^2) = 0$ if and only if the equation has solutions over $\mathbb{F}_{2^n}$.*

The proof of the following lemma can be seen from [9].

Lemma 2. *$dim(ker(L)) = dim(ker(L^*))$ and $dim(im(L)) = dim(im(L^*))$, where L is linear mapping over $\mathbb{F}_{2^n}$ and L^* is its adjoint.*

Definition 9. *For each $x \in \mathbb{F}_{2^n}$, quadratic form which is denoted by $\mathcal{Q} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined as follows:*

$$\mathcal{Q}(x) = \sum_{0 \leq s < t < n} x^{2^s + 2^t}$$

Definition 10. *Bilinear form which is denoted by $B(x, y)$ associated to $\mathcal{Q}$ is defined as follows:*

$$B(x, y) = \mathcal{Q}(x + y) + \mathcal{Q}(x) + \mathcal{Q}(y)$$

$B(x, y)$ can be expressed by using absolute trace.

$$\begin{aligned}
B(x, y) &= \sum_{0 \leq s < t < n} (x + y)^{2^s + 2^t} + \sum_{0 \leq s < t < n} x^{2^s + 2^t} + \sum_{0 \leq s < t < n} y^{2^s + 2^t} \\
&= \sum_{s \neq t} x^{2^s} y^{2^t} = \sum_{s} x^{2^s} \sum_{t \neq s} y^{2^s} \\
&= \sum_{s} x^{2^s} (y + y^2 + y^{2^2} + ... + y^{2^{n-1}} + y^{2^s}) \\
&= \sum_{s} x^{2^s} (Tr(y) + y^{2^s}) \\
&= \sum_{s} (xy)^{2^s} + Tr(y) \sum_{s} x^{2^s} \\
&= Tr(xy) + Tr(y)Tr(x)
\end{aligned}$$

Theorem 2. *[17] Let A be a finite subset of the Abelian group $(G, \cdot)$, g be an element in G and H be a subgroup of G. Then $A = gH$ if and only if $|A \cdot A| = |A|$.*

Theorem 3. *[14] Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and L be a nonzero linear function. Define $F(x) = x^{-1} + L(x)$. Then the function F is not a permutation if n is greater than or equal to 5.*

Corollary 1. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ for $n \geq 5$. With non-zero linear mapping L_m and $L_{m'}$ define $F(x) = L_m(x^{-1}) + L_{m'}(x)$. Then the function F is not a permutation if L_m or $L_{m'}$ is bijective.*

Proof. Let $F(x) = L_m(x^{-1}) + L_{m'}(x)$ be a permutation. Firstly, let us choose L_m as bijective. Then by taking the convolution of $F(x)$ from left by L_m^{-1}, we get the following which is also a permutation.

$$L_m^{-1}(F(x)) = x^{-1} + L_m^{-1}(L_{m'}(x))$$

This is a contradiction to Corollary 1. The same proof for the case $L_{m'}$ is bijective can be followed, because $F(x) = L_m(x^{-1}) + L_{m'}(x)$ is a permutation if and only if $F(x^{-1}) = L_m(x) + L_{m'}(x^{-1})$ is a permutation.

□

Definition 11. *Let H be the set of finite subset of $\mathbb{F}_{2^n}$. Then all inverses of the set H is denoted by $\frac{1}{H}$ i.e.*

$$\frac{1}{H} = \{\frac{1}{h} : h \in H \setminus \{0\}\}$$

Moreover, the product set $H \cdot H = \{h_1 h_2 | \quad h_1, h_2 \in H\}$ and $\sqrt{H} = \{\sqrt{h} | \quad h \in H\}$. We have $|\sqrt{H}| = |H|$, since we are in binary finite field the function $x \to x^2$ is bijective.

Definition 12. *Let $\mathcal{H}_c$ is denoted as hyperplanes of $\mathbb{F}_{2^n}$. Then the set $\mathcal{H}_c$ is defined as in the following for $c \in \mathbb{F}_{2^n}^*$.*

$$\mathcal{H}_c = \{Tr(cx) = 0 | x \in \mathbb{F}_{2^n}\}$$

CHAPTER 4

SEARCHING EXISTENCE OF PERMUTATIONS

4.1 Method to prove

In this chapter, the results of Kölsch's paper [13] which prove non-being of permutation polynomial which has the form $L_m(x^{-1}) + L_{m'}(x)$ in binary finite field are studied in details, here L_m, $L_{m'}$ are nonzero linear mapping and $n \geq 5$. To prove it, three stages below will be followed.

- Showing for nonzero r and $k|n$, $kerL_1$ and $kerL_2$ are in the form $r\mathbb{F}_{2^k}$ if F is a permutation
- Showing $dim(kerL_1) = dim(kerL_2) = 1$ for $k = 1$, by using previous stage
- Showing nonexistence of the permutation with the former stage

Before moving on main proof, some concepts which is used in the proof will be constructed.

4.2 Kloosterman Sum over $\mathbb{F}_{2^n}$ for Permutation Polynomials

Definition 13. *Kloosterman sum of c denoted by $K_n(c)$ in $\mathbb{F}_{2^n}$ for $c \in \mathbb{F}_{2^n}$.*

$$K_n(c) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(x^{-1}+cx)}$$

Definition 14. *For an element $c \in \mathbb{F}_{2^n}$, c is defined as Kloosterman zero if $K_n(c) = 0$.*

For the proof of the following proposition, see [9]

Proposition 2. *Assume that $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and L_m & $L_{m'}$ are linear mappings such that L_m, $L_{m'} \neq 0$ in $\mathbb{F}_{2^n}$. For each $u \in \mathbb{F}_{2^n}^*$, the polynomial $L_m(F(x)) + L_{m'}(x)$ is a permutation if and only if*

$$W_{\mathbb{F}}(L_m^*(u), L_{m'}^*(u)) = 0$$

Proof. The fact that a function's all components should be balanced to be a permutation is well-known [15]. In our case, namely, $L_m(F(x)) + L_{m'}(x)$ is a permutation if and only if

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(u(L_m(F(x))+L_m(x)))} = 0, \quad \forall u \in \mathbb{F}_{2^n}^*$$
$$\sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{Tr(L_m^*(u)F(x)+L_m^*(u)x))} = 0$$

from the definiton of Walsh transform we get

$$W_{\mathbb{F}}(L_m^*(u), L_m^*(u)) = 0$$

Here $Tr(L(x)y) = Tr(xL^*(y))$ is used for the computation.

□

Notice that for $F(x) = x^{-1}$, $K_n(u) = W_{\mathbb{F}}(1, u)$.

Case 1: For $u \neq 0$ we obtain the following:

$$W_{\mathbb{F}}(u, v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(ux^{-1}+vx)}$$

by substituting $x \to ux$

$$= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(x^{-1}+uvx)}$$

which is equal to

$$= K_n(uv)$$

Case 2: For $u = 0$ and $v \neq 0$ the following is obtained

$$W_{\mathbb{F}}(u, v) = K_n(uv) = 0$$

Now, by using Kloosterman sums, above Proposition can be written as the following. Proof of this can be found in [9]. Later Proposition 3 will be used to give a criterian to be a permutation for $L_m(x^{-1}) + L_{m'}(x)$.

Proposition 3. *For two linear functions L_m, $L_{m'}$ on binary finite field with n dimension and each $u \in \mathbb{F}_{2^n}$; then $K_n(L_m^*(u)L_{m'}^*(u)) = 0$ and $ker(L_m^*) \cap ker(L_{m'}^*) = \{0\}$ if and only if $L_m(x^{-1}) + L_{m'}(x)$ is a permutation polynomial over $\mathbb{F}_{2^n}$.*

Theorem 4. *[12] Assume n is greater than or equal to 4 and u is a nonzero element in $\mathbb{F}_{2^n}$. If u is a Kloosterman zero of $\mathbb{F}_{2^n}$ in modula 16, then its quadratic and trace functions are zero polynomials, i.e. $\mathcal{Q}(u) = 0$ and $Tr(u) = 0$.*

Vice versa of the theorem is also true. Now, by applying Theorem 4 to Proposition 3, the following corollary is obtained .

Corollary 2. *Let n be greater than or equal to 4 and u be any nonzero element in $\mathbb{F}_{2^n}$. Then $ker(L_m^*) \cap ker(L_{m'}^*) = \{0\}$ and $\mathcal{Q}(L_m^*(u)L_{m'}^*(u)) = Tr(L_m^*(u)L_{m'}^*(u)) = 0$, if $L_m(x^{-1}) + L_{m'}(x)$ is a permutation of $\mathbb{F}_{2^n}$,*

4.3 Proof for Non-existence of Permutation Polynomial

The following theorem is the essential step to obtain the main result.

Theorem 5. *Let L_m and $L_{m'}$ be two linear functions on $\mathbb{F}_{2^n}$ such that L_m, $L_{m'} \neq 0$ for $n \geq 5$. Define $F(x) = L_m(x^{-1}) + L_{m'}(x)$. Then kernels of L_m and $L_{m'}$ are in the form $r\mathbb{F}_{2^k}$ for a non-zero r and $k|n$, namely they are translates of a subfields $\mathbb{F}_{2^k}$ of binary finite field with n dimension if F is a permutation. In addition, $kerL_m = L_{m'}^*(ker(L_m^*))$ and $kerL_{m'} = L_m^*(ker(L_{m'}^*))$*

Proof. Let $F(x) = L_m(x^{-1}) + L_{m'}(x)$ be a permutation of $\mathbb{F}_{2^n}$. By Corollary 2, we have $\mathcal{Q}(L_m^*(u)L_{m'}^*(u)) = Tr(L_m^*(u)L_{m'}^*(u)) = 0$. Let $P(x)$ be equal to $L_m^*(x)L_{m'}^*(x)$. Also, let us take y in $ker(L_m^*)$ and x in $\mathbb{F}_{2^n}$.

By computing the following:

$$\begin{aligned}
0 &= \mathcal{Q}(P(x+y)) \\
&= \mathcal{Q}(L_m^*(x+y)L_{m'}^*(x+y)) \\
&= \mathcal{Q}(L_m^*(x)L_{m'}^*(x) + L_m^*(x)L_2^*(y) + L_m^*(y)L_{m'}^*(x) + L_m^*(y)L_{m'}^*(y)) \\
&= \mathcal{Q}(P(x) + L_m^*(x)L_{m'}^*(y) + L_m^*(y)L_{m'}^*(x) + P(y))
\end{aligned}$$

Since $L_m^*(y) = 0 = P(y)$, we have

$$0 = \mathcal{Q}(P(x) + L_m^*(x)L_{m'}^*(y))$$

By using bilinear form $B(x,y) = \mathcal{Q}(x+y) + \mathcal{Q}(x) + \mathcal{Q}(y) = Tr(xy) + Tr(x)Tr(y)$ in $\mathbb{F}_{2^n}$, in this case

$$\begin{aligned}
B(P(x), L_m^*(x)L_{m'}^*(y)) &= \mathcal{Q}(P(x) + L_m^*(x)L_{m'}^*(y)) + \mathcal{Q}(P(x)) + \mathcal{Q}(L_m^*(x)L_{m'}^*(y)) \\
&= Tr(P(x)L_m^*(x)L_{m'}^*(y)) + Tr(P(x))Tr(L_m^*(x)L_{m'}^*(y))
\end{aligned}$$

the following is obtained.

$$\begin{aligned}
0 &= \mathcal{Q}(P(x)) + \mathcal{Q}(L_m^*(x)L_{m'}^*(y)) + B(P(x) + L_m^*(x)L_{m'}^*(y)) \\
&= \mathcal{Q}(P(x)) + \mathcal{Q}(L_m^*(x)L_{m'}^*(y)) + Tr(P(x)L_m^*(x)L_{m'}^*(y)) + Tr(P(x))Tr(L_m^*(x)L_{m'}^*(y))
\end{aligned}$$

By Corollary 2, $\mathcal{Q}(P(x)) = 0$ and $Tr(P(x)) = 0$, then

$$= \mathcal{Q}(L_m^*(x)L_{m'}^*(y)) + Tr(P(x)L_m^*(x)L_{m'}^*(y)) \tag{4.1}$$

For each z in $ker(L_m^*)$, the Equation 4.1 becomes

$$0 = \mathcal{Q}(L_m^*(x+z)L_{m'}^*(y)) + Tr(P(x+z)L_m^*(x+z)L_{m'}^*(y))$$

Similarly, $L_m^*(z) = 0$, linear and trace mapping properties are used the throghout the following computation.

$$\begin{aligned}
&= \mathcal{Q}(L_m^*(x))L_{m'}^*(y)) + Tr(P(x+z)L_m^*(x)L_{m'}^*(y)) \\
&= \mathcal{Q}(L_m^*(x))L_{m'}^*(y)) + Tr(L_m^*(x)L_{m'}^*(x+z)L_m^*(x)L_{m'}^*(y)) \\
&= \mathcal{Q}(L_m^*(x))L_{m'}^*(y)) + Tr((L_m^*(x)L_{m'}^*(x) + L_m^*(x)L_{m'}^*(z))L_m^*(x)L_{m'}^*(y)) \\
&= \mathcal{Q}(L_m^*(x))L_{m'}^*(y)) + Tr(P(x)L_m^*(x)L_{m'}^*(y) + L_m^*(x)L_{m'}^*(z)L_m^*(x)L_{m'}^*(y))
\end{aligned}$$

The following is obtained.

$$= \mathcal{Q}(L_m^*(x))L_{m'}^*(y)) + Tr(P(x)L_m^*(x)L_{m'}^*(y)) + Tr((L_m^*(x))^2L_{m'}^*(z)L_{m'}^*(y)) \tag{4.2}$$

Let us add Equation 4.1 to Equation 4.2, then for each x in $\mathbb{F}_{2^n}$ and y, z in $ker(L_m^*)$

$$Tr((L_m^*(x))^2 L_{m'}^*(z) L_{m'}^*(y)) = 0 \tag{4.3}$$

Let us take $z = y$ for Equation 4.3, then we have

$$Tr((L_m^*(x))^2 (L_{m'}^*(y))^2) = Tr(L_m^*(x) L_{m'}^*(y)) = 0$$

By Definition 8, $Tr(L(x)y) = Tr(xL^*(y))$, the equation becomes

$$Tr(L_m^*(x) L_{m'}^*(y)) = Tr(x L_m^*(L_{m'}^*(y))) = 0$$

for each $x \in \mathbb{F}_{2^n}$.

From this equation $L_{m'}^*(y) \in ker L_m$ and from the setting $y \in ker(L_m^*)$, $L_2^*(ker(L_m^*)) \subseteq ker(L_m)$. By using Lemma 2 $dim(ker(L_m)) = dim(ker(L_m^*))$ and Corollary 2 $ker(L_m^*) \cap ker(L_{m'}^*) = \{0\}$, we have $L_{m'}^*(ker(L_m^*)) = ker(L_m)$.

Using Definition 8 again,

$$\begin{aligned} Tr((L_m^*(x))^2 L_{m'}^*(z) L_{m'}^*(y)) &= Tr(L_m^*(x) \sqrt{L_{m'}^*(z) L_{m'}^*(y)}) \\ &= Tr(x L_m(\sqrt{L_{m'}^*(z) L_{m'}^*(y)})). \end{aligned}$$

Similarly, since $y, z \in ker(L_m^*)$ and $\sqrt{L_{m'}^*(z) L_{m'}^*(y)}$ is in $ker(L_m)$, we get the following $\sqrt{L_{m'}^*(ker(L_m^*)) L_{m'}^*(ker(L_m^*))} \subseteq ker(L_m)$. By previous result $L_{m'}^*(ker(L_m^*)) = ker(L_m)$, we obtained $\sqrt{ker(L_m) ker(L_m)} = ker(L_m)$.

From here, we can obtain $|(ker(L_m) \setminus \{0\}) \cdot (ker(L_m) \setminus \{0\})| = |(ker(L_m) \setminus \{0\})|$. Then by Theorem 2, for subgroup H of $\mathbb{F}_{2^n}^*$ and $r \in \mathbb{F}_{2^n}$, we have the following $ker(L_m) \setminus \{0\} = rH$, or equivalently, $ker(L_m) = rH \cup \{0\}$. Since cardinality of $ker(L_m)$ is 2^k for an element k in $\mathbb{N}$, $2^k - 1$ is the cardinality of H. Also, since H is the multiplicative subgroup of $\mathbb{F}_{2^k}$, for $k|n$ and $r \in \mathbb{F}_{2^n}^*$, we have $ker(L_m) = r\mathbb{F}_{2^k}$. Similary, the same results can be obtained for $ker(L_2)$ since $F(x^{-1}) = L_m(x) + L_{m'}(x^{-1})$ is a permutation if and only if $F(x) = L_m(x^{-1}) + L_{m'}(x)$ is a permutation.

□

Proposition 4. *Let L_m and $L_{m'}$ be two linear functions on $\mathbb{F}_{2^n}$ such that L_m, $L_{m'} \neq 0$. Define $F(x) = L_m(x^{-1}) + L_{m'}(x)$. Then for each nonzero u in $\mathbb{F}_{2^n}$, $L_{m'}(u)$ is not in $L_m(\frac{1}{\mathcal{H}_{\frac{1}{u}}})$ and F has one solution if and only if F is a permutation.*

Proof. For u in $\mathbb{F}_{2^n}^*$ and each x in $\mathbb{F}_{2^n}$, $F(x+u)+F(x) \neq 0$ if and only if F is a permutation. Namely,

$$\begin{aligned} &L_m((x+u)^{-1}) + L_{m'}(x+u) + L_m(x^{-1}) + L_{m'}(x) \neq 0 \\ &L_m(x^{-1} + (x+u)^{-1}) + L_{m'}(x + (x+u)) \neq 0 \\ &L_{m'}(u) \neq L_m(x^{-1} + (x+u)^{-1}) \end{aligned} \tag{4.4}$$

Let the set be $A_u = \{a \in \mathbb{F}_{2^n} : (x+u)^{-1} + x^{-1} = a \textit{ for some } x \textit{ in } \mathbb{F}_{2^n}\}$

Case 1: Let us choose $x = u$ and $x = 0$ for the equation $(x+u)^{-1} + x^{-1} = a$. Then we get $u^{-1} = a$.

Case 2: If we choose x other than u and 0, by multiplying the equation $(x+u)^{-1} + x^{-1} = a$ by $x(x+u)$, we obtain the following equation

$$ax^2 + uax + u = 0$$

The equation has solutions if and only if $Tr(\frac{ua}{u^2a^2}) = Tr(\frac{1}{ua}) = 0$ with $a \neq 0$, from Lemma 1.

By combining the cases, we get

$$(x+u)^{-1} + x^{-1} = a \iff u^{-1} = a \quad \text{or} \quad Tr(\frac{1}{ua}) = 0$$

From Definition 12,

$$\begin{aligned} \mathcal{H}_{\frac{1}{u}} &= \{Tr(\frac{x}{u}) = 0 : x \in \mathbb{F}_{2^n}\} \\ \frac{1}{\mathcal{H}_{\frac{1}{u}}} &= \{Tr(\frac{1}{ux}) = 0 : x^{-1} \in \mathbb{F}_{2^n}\}, \forall u \in \mathbb{F}_{2^n}^* \end{aligned}$$

We can say that $u^{-1} \in A_u$ and $\frac{1}{\mathcal{H}_{\frac{1}{u}}} \in A_u$.
Equation 4.4 implies $L_{m'}(u) \notin L_m(A_u)$, and so $L_{m'}(u) \notin L_m(\frac{1}{\mathcal{H}_{\frac{1}{u}}})$.
If u is a solution for F, i.e. $F(u) = 0$, then we have $L_m(a^{-1}) = L_{m'}(a)$.

□

Lemma 3. *For three distinct nonzero elements r, s, t from $\mathbb{F}_{2^n}^*$, $r + s = t$ if ad only if $\mathbb{F}_{2^n} = \mathcal{H}_r \cup \mathcal{H}_s \cup \mathcal{H}_t$. Particularly, nonzero three elements r, s, t always can be found in $A \setminus \{0\}$ s.t. $\mathcal{H}_{\frac{1}{r}} \cup \mathcal{H}_{\frac{1}{s}} \cup \mathcal{H}_{\frac{1}{t}} = \mathbb{F}_{2^n}$ if $A = a\mathbb{F}_{2^k}$ where $k > 1$, $k|n$ and $a \in \mathbb{F}_{2^n}^*$.*

Proof. Since a hyperplane's dimension is one less than that of its ambient space, in our binary finite field $\mathbb{F}_{2^n}$ case whose dimension is n, a hyperplane's dimension is $n-1$. Thus, a hyperpane has 2^{n-1} elements. Similarly, intersection of two distinct hyperplanes has one less dimension than one's dimension, and has 2^{n-2} elements. Based on these, we can write the following:

$$
\begin{aligned}
&= |\mathcal{H}_r \cup \mathcal{H}_s \cup \mathcal{H}_t| \\
&= |\mathcal{H}_r \cap \mathcal{H}_s \cap \mathcal{H}_t| - |\mathcal{H}_r \cap \mathcal{H}_s| - |\mathcal{H}_r \cap \mathcal{H}_t| - |\mathcal{H}_s \cap \mathcal{H}_t| + |\mathcal{H}_r| + |\mathcal{H}_s| + |\mathcal{H}_t| \\
&= |\mathcal{H}_r \cap \mathcal{H}_s \cap \mathcal{H}_t| - 3 \cdot 2^{n-2} + 3 \cdot 2^{n-1} \\
&= |\mathcal{H}_r \cap \mathcal{H}_s \cap \mathcal{H}_t| + 2^{n-2} + 2^{n-1}
\end{aligned}
$$

This implies that $2^{n-2} = |\mathcal{H}_r \cap \mathcal{H}_s \cap \mathcal{H}_t|$ if and only if $\mathcal{H}_r \cup \mathcal{H}_s \cup \mathcal{H}_t = \mathbb{F}_{2^n}$. Also, since having 2^{n-2} elements two hyperplanes which do not coincide, one of the hyperplanes contains the elements of intersection of the other two distinct hyperplanes, let $\mathcal{H}_t$ be the hyperplane. Namely, $\mathcal{H}_r \cap \mathcal{H}_s \subseteq \mathcal{H}_t$, which implies that $r + s = t$.
Particularly, for two elements $r = ab_1$, $s = ab_2$ from $A = a\mathbb{F}_{2^k}$, $b_1, b_2 \in \mathbb{F}_{2^k}^*$.

$$\frac{1}{r} + \frac{1}{s} = \frac{1}{a}(\frac{1}{b_1} + \frac{1}{b_2})$$

Also, $\frac{1}{b_1} + \frac{1}{b_2} = \frac{1}{b} \in \mathbb{F}_{2^k}^*$. Now we have three distinct elements r, s, ab such that $\frac{1}{r} + \frac{1}{s} = \frac{1}{ab}$. By above part of the proof, we can conclude that $\mathcal{H}_{\frac{1}{r}} \cup \mathcal{H}_{\frac{1}{s}} \cup \mathcal{H}_{\frac{1}{ab}}$ is equal to binary finite field with n dimension.

□

Theorem 6. *Let $n \geq 5$. For $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and two linear functions L_m and $L_{m'}$ on $\mathbb{F}_{2^n}$ such that L_m, $L_{m'} \neq 0$, define $F(x) = L_m(x^{-1}) + L_{m'}(x)$, Then $|ker(L_m)| = |ker(L_{m'})| = 2$, if F is a permutation.*

Proof. To prove $|ker(L_{m'})| = 2$, we should show $k = 1$ for $ker(L_m) = r\mathbb{F}_{2^k}$ and $ker(L_{m'}) = r\mathbb{F}_{2^k}$ which we get from Theorem 5.

Let us assume that $k \geq 2$. Then by Lemma 3, three nonzero distinct elements $r, s, t \in ker L_{m'}$ s.t $\mathcal{H}_{\frac{1}{r}} \cup \mathcal{H}_{\frac{1}{s}} \cup \mathcal{H}_{\frac{1}{t}} = \mathbb{F}_{2^n}$ and $\frac{1}{\mathcal{H}_{\frac{1}{r}}} \cup \frac{1}{\mathcal{H}_{\frac{1}{s}}} \cup \frac{1}{\mathcal{H}_{\frac{1}{t}}} = \mathbb{F}_{2^n}^*$ can be found.
Recall Proposition 4 which says $L_{m'}(a) \notin L_m(\frac{1}{\mathcal{H}_{\frac{1}{u}}})$ for all $u \in \mathbb{F}_{2^n}^*$.

Since $ker(L_{m'}) = r\mathbb{F}_{2^k}$ and $k \geq 2$, there exist an element in $\mathbb{F}_{2^n}^*$ such that $L_{m'}(x) = 0$, so we can write the following by using Proposition 4 for three elements $r, s, t \in \mathbb{F}_{2^n}^*$.

$$0 \notin L_m(\mathbb{F}_{2^n}^*) = L_m(\frac{1}{\mathcal{H}_{\frac{1}{r}}}) \cup L_m(\frac{1}{\mathcal{H}_{\frac{1}{s}}}) \cup L_m(\frac{1}{\mathcal{H}_{\frac{1}{t}}})$$

We know that $kerL_1$ has more than one element by Corollary 1, so we have a contradiction to above equation. $|ker(L_{m'})| = 2$, since $k = 1$.
Similarly, we can prove it for $kerL_1$ since $F(x^{-1}) = L_m(x) + L_{m'}(x^{-1})$ is a permutation if and only if $F(x) = L_m(x^{-1}) + L_{m'}(x)$ is so.

□

By using Theorem 6, assume $L_m(x) = x^2 + ux$ for an element $u \neq 0$ (after we will take $u = 1$, so $|ker(L_m)| = 2$ by Theorem 6). Let us examine the following for $L_m(x^{-1}) + L_{m'}(x) = a$:

$$a = x^{-2} + ux^{-1} + L_{m'}(x) \tag{4.5}$$

By multiplying this with u^{-2}

$$u^{-2}a = c^{-2}x^{-2} + u^{-1}x^{-1} + u^{-2}L_{m'}(x)$$

and substituting $x \to \frac{x}{u}$, we have

$$u^{-2}a = x^{-2} + x^{-1} + u^{-2}L_{m'}(\frac{x}{u})$$

which has one solution if and only if for each $a \in \mathbb{F}_{2^n}$ Equation 4.5 has only a zero. Since $u^{-2}L_{m'}(\frac{x}{u})$ is linear map, we can take $L_m(x) = x^2 + x$, or equivalent case $L_m(x) = (x^2 + x)^{2n-1} = x^{2^n} + x^{2^{n-1}} = x + x^{2^{n-1}}$. Since adjoint mapping of L is $L^* = \sum_{j=0}^{n-1} c_j^{2^{n-j}} x^{2^{n-j}}$, when we take $L_m(x) = x + x^{2^{n-1}}$, the adjoint mapping of L is $L_m^*(x) = x^2 + x$. Notice $ker(L_m) = ker(L_m^*) = \{0, 1\}$. From this and Theorem 5 $kerL_m = L_{m'}^*(kerm'(L_m^*))$, we can conclude $L_{m'}^*(1) = 1$.

Theorem 7. *For $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and two linear functions L_m and $L_{m'}$ on $\mathbb{F}_{2^n}$ s.t. L_m, $L_{m'} \neq 0$, define $F(x) = L_m(x^{-1}) + L_{m'}(x)$. For $n \geq 5$, permutation polynomial in the form of the function F does not exist.*

Proof. From above, we have $L_{m'}^*(1) = 1$, $L_m^*(x) = x^2 + x$, and $\sum_{j=0}^{n-1} c_j x^{2^j} = L_{m'}^*$. Also, let F permutes binary finite field with n . Then we should get contradiction to

conditions above which we obtain from Corollary 2 and Equation 4.1. Notice that for $y = 1$, $L^*_{m'}(y) = 1$ since $L^*_{m'}(1) = 1$. For each x in $\mathbb{F}_{2^n}$,

$$0 = Tr(L^*_m(x)L^*_{m'}(x)) = Tr((x^2 + x)L^*_{m'}(x)) \tag{4.6}$$

$$0 = \mathcal{Q}(L^*_m(x)L^*_{m'}(x)) = Q((x^2 + x)L^*_{m'}(x)) \tag{4.7}$$

$$0 = \mathcal{Q}(L^*_m(x)L^*_{m'}(y)) + Tr(P(x)L^*_m(x)L^*_{m'}(y))$$

$$0 = \mathcal{Q}(x^2 + x) + Tr((x^2 + x)(x^2 + x)L^*_{m'}(x)) = \mathcal{Q}(x^2 + x) + Tr((x^4 + x^2)L^*_{m'}(x)) \tag{4.8}$$

Let us look at condition (4.6).

$$0 = Tr((x^2 + x)\sum_{j=0}^{n-1} c_j x^{2^j}) = Tr(x^2 \sum_{j=0}^{n-1} c_j x^{2^j}) + Tr(x \sum_{j=0}^{n-1} c_j x^{2^j})$$

$$0 = \sum_{s=0}^{n-1}(x^2 \sum_{j=0}^{n-1} c_j x^{2^j})^{2^s} + \sum_{s=0}^{n-1}(x \sum_{j=0}^{n-1} c_j x^{2^j})^{2^s}$$

$$0 = \sum_{s=0}^{n-1}\sum_{j=0}^{n-1} c_j^{2^s} x^{2^{j+s}+2^{s+1}} + \sum_{s=0}^{n-1}\sum_{j=0}^{n-1} c_j^{2^s} x^{2^{j+s}+2^s}$$

By substituting $j \to j - s$, we get

$$0 = \sum_{s=0}^{n-1}\sum_{j=0}^{n-1} c_{j-s}^{2^s} x^{2^j+2^{s+1}} + \sum_{s=0}^{n-1}\sum_{j=0}^{n-1} c_{j-s}^{2^s} x^{2^j+2^s}$$

Again, by substituting $s \to s - 1$ in the left sum, then the following:

$$\sum_{s=0}^{n-1}\sum_{j=0}^{n-1} c_{j-s+1}^{2^{s-1}} x^{2^j+2^s} + \sum_{s=0}^{n-1}\sum_{i=0}^{n-1} c_{j-s}^{2^s} x^{2^j+2^s} = 0$$

$$\sum_{s=0}^{n-1}\sum_{j=0}^{n-1}(c_{j-s+1}^{2^{s-1}} + c_{j-s}^{2^s}) x^{2^j+2^s} = 0$$

When we take $j = s = 1$, the coefficient of x^4 becomes $c_1 + c_0^2 = 0$.

For $i = 0$, $s = r$, the coefficient of x^{2^r+1} is $c_{-r+1}^{2^{r-1}} + c_{-r}^{2^r} = 0$.
Similarly, for $i = r$, $s = 0$, the coefficient of x^{2^r+1} is $c_{r+1}^{2^{-1}} + c_r = 0$. For each $1 \leq r \leq n-1$, we can write the following for the coefficients of x^{2^r+1}.

$$c_{-r+1}^{2^{r-1}} + c_{-r}^{2^r} + c_{r+1}^{2^{-1}} + c_r = 0 \tag{4.9}$$

Now, let us look at the condition 4.8.

$$\begin{aligned} 0 &= Tr((x^4 + x^2)L_2^*(x)) + \mathcal{Q}(x^2 + x) \\ &= Tr(x^3) + Tr(x) + Tr((x^4 + x^2)\sum_{i=0}^{n-1} c_j x^{2^j}) + \mathcal{Q}(x^2) + \mathcal{Q}(x) \end{aligned}$$

Since $\mathcal{Q}(x) = \mathcal{Q}(x^2)$, we get

$$\begin{aligned} 0 &= Tr(x^3) + Tr(x) + \sum_{s=0}^{n-1}(x^4 \sum_{j=0}^{n-1} c_j x^{2^j})^{2^s} + \sum_{s=0}^{n-1}(x^2 \sum_{j=0}^{n-1} c_j x^{2^j})^{2^s} \\ &= \sum_{j=0}^{n-1}(x^{2+1})^{2^j} + \sum_{j=0}^{n-1} x^{2^j} + \sum_{s=0}^{n-1}\sum_{j=0}^{n-1} c_j^{2^s} x^{2^{j+s}+2^{s+2}} + \sum_{s=0}^{n-1}\sum_{j=0}^{n-1} c_j^{2^s} x^{2^{j+s}+2^{s+1}} \end{aligned}$$

Again by substituting $j \to j - s$ for right and left double sum, we have

$$\sum_{j=0}^{n-1} x^{2^{j+1}+2^j} + \sum_{j=0}^{n-1} x^{2^j} + \sum_{s=0}^{n-1}\sum_{j=0}^{n-1} c_{j-s}^{2^s} x^{2^j+2^{s+2}} + \sum_{s=0}^{n-1}\sum_{j=0}^{n-1} c_{j-s}^{2^s} x^{2^j+2^{s+1}} = 0$$

By substituting $s \to s - 2$ for left double summation

$$\sum_{j=0}^{n-1} x^{2^{j+1}+2^j} + \sum_{j=0}^{n-1} x^{2^j} + \sum_{s=0}^{n-1}\sum_{i=0}^{n-1} c_{j-s+2}^{2^{s-2}} x^{2^j+2^s} + \sum_{s=0}^{n-1}\sum_{j=0}^{n-1} c_{j-s+1}^{2^{s-1}} x^{2^j+2^s} = 0$$

$$\sum_{j=0}^{n-1} x^{2^{j+1}+2^j} + \sum_{i=0}^{n-1} x^{2^j} + \sum_{s=0}^{n-1}\sum_{j=0}^{n-1} (c_{j-s+2}^{2^{s-2}} + c_{j-s+1}^{2^{s-1}}) x^{2^j+2^s} = 0$$

When we look at the coefficient of x^8 for $i = s = 2$, we get $1 + c_2 + c_1^2 = 0$.

For $j = r$, $s = 0$, the coefficient of x^{2^r+1} is $c_{r+2}^{2^{-2}} + c_{r+1}^{2^{-1}} = 0$.
Also, notice that when $r = 1$ and $r = n - 1$, we have coefficient 1 from $Tr(x^3)$.
Similarly, for $i = 0$, $s = r$, the coefficient of x^{2^r+1} is $c_{-r+2}^{2^{r-2}} + c_{-r+1}^{2^{r-1}} = 0$. By writing these together, we get

$$c_{r+2}^{2^{-2}} + c_{r+1}^{2^{-1}} + c_{-r+2}^{2^{r-2}} + c_{-r+1}^{2^{r-1}} = \begin{cases} 0, & r \in \{2, ..., n-2\} \\ 1, & r \in \{1, n-1\} \end{cases} \tag{4.10}$$

Let us substitute $r \to r-1$ and square it, then we have

$$c_{r+1}^{2^{-1}} + c_r^+ c_{-r+3}^{2^{r-2}} + c_{-r+2}^{2^{r-1}} = \begin{cases} 0, & r \in \{3, ..., n-1\} \\ 1, & r \in \{0, 2\} \end{cases}$$

When we add that to Equation 4.9, we get the following. Notice that $r \geq 1$ for Equation 4.9.

$$c_{-r+3}^{2^{r-2}} + c_{-r+2}^{2^{r-1}} + c_{-r+1}^{2^{r-1}} + c_{-r}^{2^r} = \begin{cases} 1, & r = 2 \\ 0, & r \in \{3, ..., n-1\} \end{cases}$$

Again, substitute $r \to -r$

$$c_{r+3}^{2^{-r-2}} + c_{r+2}^{2^{-r-1}} + c_{r+1}^{2^{-r-1}} + c_r^{2^{-r}} = \begin{cases} 0, & r \in \{3, ..., n-1\} \\ 1, & r = 2 \end{cases}$$

and take the exponent 2^{r+2}.

$$c_{r+3} + c_{r+2}^2 + c_{r+1}^2 + c_r^{2^2} = \begin{cases} 0, & r \in \{1, ..., n-3\} \\ 1, & r = n-2 \end{cases} \tag{4.11}$$

Before, it has found that the equations $c_1 + c_0^2 = 0$ for coefficient of x^4 and $c_1^2 + c_2 + 1 = 0$ for coefficient x^8. Based on these, we have a claim.

Claim: For all i, where $1 \leq i \leq n-1$

$$c_i = \begin{cases} c_0^{2^i}, & \text{if i is odd} \\ c_0^{2^i} + 1, & \text{if i is even} \end{cases} \tag{4.12}$$

Proof of Claim: Claim is proved by induction.

The case $i = 1$ is done, we know that $c_1 = c_0^2$.

For the case $i = 2$, we have $c_2 = c_1^2 + 1 = c_0^{2^2} + 1$.

For the case $i = 3$, we use Equation 4.10 for $r = 1$, and we get.

$$\begin{aligned} & c_{r+2}^{2^{-2}} + c_{r+1}^{2^{-1}} + c_{-r+2}^{2^{r-2}} + c_{-r+1}^{2^{r-1}} = 1 \\ & c_3^{2^{-2}} + c_2^{2^{-1}} + c_1^{2^{-1}} + c_0 = 1 \\ & c_3^{2^{-2}} + (c_0^4 + 1)^{2^{-1}} + (c_0^2)^{2^{-1}} + c_0 = 1 \\ & c_3^{2^{-2}} + c_0^2 + 1 + c_0 + c_0 = 1 \\ & c_3^{2^{-2}} = c_0^2 \to c_3 = c_0^8 \end{aligned}$$

Now let us look at for the case $k \geq 3$ by using Equation 4.11 for r is other than $n-2$.

$$c_{k+1} + c_k^2 + c_{k-1}^2 + c_{k-2}^4 = 0$$

By claim Equation 4.13, we get the following if k is odd.

$$\begin{aligned} c_{k+1} &= (c_0^{2^k})^2 + (c_0^{2^{k-1}} + 1)^2 + (c_0^{2^{k-2}})^4 \\ &= c_0^{2^{k+1}} + c_0^{2^k} + 1 + c_0^{2^k} \\ &= c_0^{2^{k+1}} + 1 \end{aligned}$$

Similarly, in case of k is even, we have the following result.

$$\begin{aligned} c_{k+1} &= (c_0^{2^k} + 1)^2 + (c_0^{2^{k-1}})^2 + (c_0^{2^{k-2}} + 1)^4 \\ &= c_0^{2^{k+1}} + 1 + c_0^{2^k} + c_0^{2^k} + 1 \\ &= c_0^{2^{k+1}} \end{aligned}$$

For the case c_{n-1} we will use the Equation 4.9 for $r = 1$.

$$\begin{aligned} c_{-r+1}^{2^{r-1}} + c_{-r}^{2^r} + c_{r+1}^{2^{-1}} + c_r &= 0 \\ c_0 + c_{-1}^2 + c_2^{2^{-1}} + c_1 &= 0 \end{aligned}$$

Since $c_n = c_0$, and so $c_{n-1} = c_{-1}$, we have

$$\begin{aligned} c_{n-1}^2 &= c_0 + (c_0^{2^2} + 1)^{2^{-1}} + c_0^2 \\ c_{n-1}^2 &= c_0 + c_0^2 + 1 + c_0^2 \\ c_{n-1}^2 &= c_0 + 1 \\ c_{n-1} &= c_0^{2^{-1}} + 1 \end{aligned}$$

Since $c_0 = c_0^{2^n}$, and so $c_0^{2^{-1}} = c_0^{2^{n-1}}$, we get $c_{n-1} = c_0^{2^{n-1}} + 1$ which concludes that n is odd. Therefore, the proof of the claim is done.

Still, we do not verify a contradiction to the coefficients from the conditions 4.6 and 4.8. Thus, we look at condition 4.7.

$$\begin{aligned} 0 &= \mathcal{Q}((x^2+x)L_{m'}^*(x)) = \mathcal{Q}((x^2+x)\sum_{j=0}^{n-1} c_j x^{2^j}) \\ &= \mathcal{Q}(\sum_{j=0}^{n-1} c_j x^{2^j+2} + \sum_{j=0}^{n-1} c_j x^{2^j+1}) \\ &= \sum_{0\leq t<s<n} (\sum_{j=0}^{n-1} c_j x^{2^j+2} + \sum_{j=0}^{n-1} c_j x^{2^j+1})^{2^r} (\sum_{i=0}^{n-1} c_i x^{2^i+2} + \sum_{i=0}^{n-1} c_i x^{2^i+1})^{2^s} \\ &= \sum_{0\leq t<s<n} (\sum_{j=0}^{n-1} c_j^{2^t} x^{2^{j+t}+2^{t+1}} + \sum_{j=0}^{n-1} c_j^{2^t} x^{2^{j+t}+2^t})(\sum_{i=0}^{n-1} c_i^{2^s} x^{2^{i+s}+2^s+1} + \sum_{i=0}^{n-1} c_j^{2^s} x^{2^{i+s}+2^s}) \end{aligned}$$

By substituting $j \to j-t$ and $i \to i-s$, we have

$$= \sum_{0\le t<s<n} (\sum_{j=0}^{n-1} c_{j-t}^{2^t} x^{2^j+2^{t+1}} + \sum_{j=0}^{n-1} c_{j-t}^{2^t} x^{2^j+2^t})(\sum_{i=0}^{n-1} c_{i-s}^{2^s} x^{2^i+2^s+1} + \sum_{i=0}^{n-1} c_{i-s}^{2^s} x^{2^i+2^s})$$

Again, by substituting $t \to t-1$ into left sum of left parentheses and $s \to s-1$ into left sum of right parentheses, we have

$$= \sum_{0\le t<s<n} (\sum_{j=0}^{n-1} c_{j-r+1}^{2^{t-1}} x^{2^j+2^t} + \sum_{j=0}^{n-1} c_{j-t}^{2^t} x^{2^j+2^t})(\sum_{i=0}^{n-1} c_{i-s+1}^{2^{s-1}} x^{2^i+2^s} + \sum_{i=0}^{n-1} c_{i-s}^{2^s} x^{2^i+2^s})$$

$$= \sum_{0\le t<s<n} (\sum_{j=0}^{n-1} (c_{j-t+1}^{2^{t-1}} + c_{j-t}^{2^t}) x^{2^j+2^t})(\sum_{i=0}^{n-1} (c_{i-s+1}^{2^{s-1}} + c_{i-s}^{2^s}) x^{2^i+2^s})$$

$$= \sum_{0\le t<s<n} \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} (c_{j-t+1}^{2^{t-1}} + c_{j-t}^{2^t})(c_{i-s+1}^{2^{s-1}} + c_{i-s}^{2^s}) x^{2^j+2^r+2^i+2^s}$$

Let us check the coefficients of x^8 in this polynomial to get a contradiction to condition 4.8 which is a zero polynomial. The possible choices for i, r, j, s are given in the following. Let $d_{j,t,i,s} = (c_{j-t+1}^{2^{t-1}} + c_{j-t}^{2^t})(c_{i-s+1}^{2^{s-1}} + c_{i-s}^{2^s})$.

Table 4.1: List of coefficients of x^8 in $\mathcal{Q}((x^2+x)L_{m'}^*(x))$

i	r	j	s	$d_{j,t,i,s}$
0	1	0	2	1
0	0	2	1	0
0	0	1	2	0
1	0	0	2	1
2	0	0	1	1

Now ,we can see the following from Table 4.1:

$$d_{j,t,i,s} = \begin{cases} 1, & \text{otherwise} \\ 0, & \text{if } j = t \text{ or } i = s \end{cases} \tag{4.13}$$

Since sum of coefficients $d_{j,t,i,s}$ is 1, $\mathcal{Q}((x^2+x)L_{m'}^*(x))$ is not a zero polynomial, so a contradiction is obtained. Thus, Theorem 7 is proved.

By Theorem 7 and Proposition 1, we reached the main result which is mentioned in Chapter 1. □

CHAPTER 5

CRITERIAN FOR THE EXISTENCE OF PERMUTATION IN $\mathbb{F}_{P^N}$

In this part of the thesis, a proposition is verified on $\mathbb{F}_{p^n}$, which gives a criterian to be a permutation polynomial in the special type $L_m(x^{-1}) + L_{m'}(x)$ by using the general form of Kloosterman sum. Later, it is planned to be used for future work mentioned on next section. Recall the general form of Kloosterman sums:

$$K_{p^n}(a) = \sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(x^{p^n-2}+ax)}$$

where ζ is the primitive $p-th$ rooth of unity.

5.1 Kloosterman Sum over $\mathbb{F}_{p^n}$ for Permutation Polynomials

Proposition 5. *For two linear functions L_m, $L_{m'}$ on $\mathbb{F}_{p^n}$ and each $u \in \mathbb{F}_{p^n}$; then $K_{p^n}(L_m^*(u)L_{m'}^*(u)) = 0$ and $ker(L_m^*) \cap ker(L_{m'}^*) = \{0\}$ if and only if $L_m(x^{-1}) + L_{m'}(x)$ is a permutation polynomial over $\mathbb{F}_{p^n}$.*

Proof. A function's all components should be balanced to be a permutation [15]. Namely, $F(x) = L_m(x^{-1}) + L_{m'}(x)$ is a permutation if and only if

$$\begin{aligned} 0 &= \sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(u(L_m(x^{-1})+L_{m'}(x)))}, \forall u \in \mathbb{F}_{p^n}^* \\ &= \sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(L_m^*(u)x^{-1}+L_{m'}^*(u)x))} \\ &= W_{\mathbb{F}}(L_m^*(u), L_{m'}^*(u)) \end{aligned}$$

Let's examine the cases of $L_m^*(b)$ and $L_{m'}^*(b)$.

Case 1: Let $L_m^*(u) = 0$ and $L_{m'}^*(u) \neq 0$. Then we have the following

$$\sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(L_{m'}^*(u)x)}$$

For simplicity, let's call $L_{m'}^*(u)$ as β.

Claim: If $\beta \neq 0$, then $\sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(\beta x)} = 0$.

Proof of Claim: There exists an element $x_0 \in$F$_{p^n}$ such that $Tr(\beta x_0) \neq 0$. Since $\{x : \mathbb{F}_{p^n}\} = \{x + x_0 : \mathbb{F}_{p^n}\}$,

$$\sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(\beta x)} = \sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(\beta(x+x_0)}$$

$$= \sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(\beta x)} \sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(\beta(x_0)}$$

Let $S = \sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(\beta x)}$ and $u = \sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(\beta x_0)}$, then we have the following

$$S = vS$$

$$S(1 - v) = 0$$

Since $Tr(\beta x_0) \neq 0$, v can not be equal to 1, so S has to be 0. Thus, our claim is hold. In addition, since we choose $L_{m'}^*(u)$ is different from 0 for all u in $\mathbb{F}_{p^n}^*$, $ker(L_{m'}^*) = 0$. Then we get $ker(L_m^*) \cap ker(L_{m'}^*) = 0$.

Case 2: Let $L_m^*(u) = 0$ and $L_{m'}^*(u) = 0$. Then we have the following

$$\sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(L_m^*(u)x^{-1} + L_{m'}^*(u)x)} = p^n$$

Case 3: Let $L_m^*(u) \neq 0$ and $L_{m'}^*(u) = 0$. Then we get the following

$$\sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(L_m^*(u)x^{-1})}$$

For simplicity, let's call $L_m^*(u)$ as β.

Claim: If $\beta \neq 0$, then $\sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(\beta x)} = 0$.

Proof of Claim:

$$\sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(\beta \frac{1}{x})} = \sum_{x \neq 0} \zeta^{Tr(\beta \frac{1}{x})} + \sum_{x=0} \zeta^{Tr(\beta \frac{1}{x})}$$

Since $\{x \in \mathbb{F}_{p^n}^* : x\} = \{x \in \mathbb{F}_{p^n} : \frac{1}{x}\}$,

$$\begin{aligned} &= \sum_{x \neq 0} \zeta^{Tr(\beta x)} + \sum_{x=0} \zeta^{Tr(\beta .0)} \\ &= \sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(\beta x)} \end{aligned}$$

Similarly in *Case 1*, $ker(L_m^*) = 0$ since we choose $L_m^*(u)$ is different from 0 for all u in $\mathbb{F}_{p^n}^*$, $ker(L_{m'}^*) = 0$.Then, again we obtain $ker(L_m^*) \cap ker(L_{m'}^*) = 0$.

Case 4: Let $L_m^*(u) \neq 0$ and $L_{m'}^*(u) \neq 0$. Then we have the following

$$\sum_{x \in \mathbb{F}_{p^n}} \zeta^{Tr(L_m^*(u)x^{-1} + L_{m'}^*(u)x)}$$

Let $y^{-1} = L_m^*(u)x^{-1}$, then $x = yL_m^*(u)$. Substituting these to the equation above yields

$$\sum_{y} \zeta^{Tr(y^{-1} + L_m^*(u)L_2^*(u)y)}$$

which is equal to Kloosterman sum for $\mathbb{F}_{p^n}$ which we want to obtain $K_{p^n}(L_m^*(u)L_{m'}^*(u))$.

We get $u \notin ker(L_m^*) \cap ker(L_{m'}^*)$, thus

$$W_{\mathbb{F}}(L_m^*(u), L_{m'}^*(u)) = K_{p^n}(L_m^*(u)L_{m'}^*(u))$$

□

5.2 Possible Future Works

As future work, our main aim is to examine the existence of permutation polynomial in specal type $L_m(x^{-1}) + L_{m'}(x)$ in characteristic 3 finite field. In particular, as a first stage, we want to search the accuracy of the statement if $F(x) = L_m(x^{-1}) + L_{m'}(x)$ is a permutation over $\mathbb{F}_{3^n}$ then for $r \neq 0$ kernels of L_m and $L_{m'}$ are in the form $r\mathbb{F}_{3^k}$, namely they are translates of $\mathbb{F}_{3^k}$. This statement is based on Theorem 5.

To prove that, the steps below should be followed.

1. Defining an appropriate form $\mathcal{Q}$ over $\mathbb{F}_{3^n}$
2. Defining an appropriate bilinear form $B(x, y)$ associated to Q over $\mathbb{F}_{3^n}$
3. Determining for which modula we can derive a condition on ternary Kloosterman zeros over $\mathbb{F}_{3^n}$ such that $K_{3^n}(a) \equiv 0$ by using trace mapping Tr and suitable form Q.

Step 3 is based on Theorem 4.

Moreover, for step 3, there are some results to characterize ternary Kloosterman sums modula 9 and 27 which are conducted in [8].

The result for ternary Kloosterman sums in modula 9 using the trace mapping by using Stickelberger's theorem is the following:

Theorem 8. *[8]*

$$K_{3^n}(a) = \begin{cases} 0 \quad \textit{(mod9)}, \quad \textit{if} \quad Tr(a) = 0 \\ 3 \quad \textit{(mod9)}, \quad \textit{if} \quad Tr(a) = 1 \\ 6 \quad \textit{(mod9)}, \quad \textit{if} \quad Tr(a) = 2 \end{cases}$$

for $u \in \mathbb{F}_{3^n}$.

The result for ternary Kloosterman sums in modula 27 using the trace mapping by using Gross-Koblitz formula is the following:

Theorem 9. *[8] For $p = 3$ and $n \geq 3$, the following:*

$$K_{3^n}(u) = \begin{cases} 0 \pmod{27}, & \text{if } \tau_B(u) + 2\tau_A(u) = 0 \text{ and } Tr(u) = 0 \\ 3 \pmod{27}, & \text{if } \tau_B(u) = 2 \text{ and } Tr(u) = 1 \\ 6 \pmod{27}, & \text{if } \tau_B(a) + \tau_A(a) = 2 \text{ and } Tr(u) = 2 \\ 9 \pmod{27}, & \text{if } \tau_B(u) + 2\tau_A(u) = 1 \text{ and } Tr(u) = 0 \\ 12 \pmod{27}, & \text{if } \tau_B(u) = 0 \text{ and } Tr(u) = 1 \\ 15 \pmod{27}, & \text{if } \tau_B(u) + \tau_A(u) = 0 \text{ and } Tr(u) = 2 \\ 18 \pmod{27}, & \text{if } \tau_B(u) + 2\tau_A(u) = 2 \text{ and } Tr(u) = 0 \\ 21 \pmod{27}, & \text{if } \tau_B(u) = 1 \text{ and } Tr(u) = 1 \\ 24 \pmod{27}, & \text{if } \tau_B(u) + \tau_A(u) = 1 \text{ and } Tr(u) = 2 \end{cases}$$

,where the sets:

$$A := \{k \in \{0, ..., 3^n - 2\} | k = 3^s + 3^t\}, (s, t \text{ not necesserily distinct})$$

$$B := \{k \in \{0, ..., 3^n - 2\} | k = 3^r + 3^t + 3^k\}, (r, s\ t \text{ distinct})$$

and $\tau_S : \mathbb{F}_{p^n} \to \mathbb{F}_p$ generalised trace is defined as

$$\tau_S(a) = \sum_{i \in S} a^i$$

where S is any subset of $\{0, ..., p^n - 2\}$ such that $S^p := \{s^p \mod (p^n - 1) | s \in S\} = S$.

In our case, we used generalised trace as $\tau_Q : \mathbb{F}_{2^n} \to \mathbb{F}_2$

$$\tau_Q(a) = \sum_{i \in Q} a^{2^i + 2^j}$$

where $\mathcal{Q} := \{k \in \{0, ..., 2^n - 2\} | k = 2^s + 2^t\}, (s, t \text{ distinct})$.

CHAPTER 6

CONCLUSION AND OPEN PROBLEMS

S-boxes which vectorial Boolean functions are used in their design are one of the block buildings of symmetric key cryptography systems. It is important to have high resistance of these functions on some cryptographic attacks. Differential and linear attacks are the main attacks widely used in cryptography. These properties remains invariant under several equivalence classes such as EA-equivalence and CCZ-equivalence. Moreover, since permutations have a significant role in design of block ciphers, it is beneficial to search permutations inside CCZ-class of a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

In the first and second chapter, we have given basic definitions and concepts in order to make the subject explicit. Also, to clarify the questioning process about coincidence of EA-equivalence & CCZ-equivalence and permutations inside CCZ-equivalence, some literaure review is conducted.

In Chapter 3, we have presented on detailed description CCZ-equivalence of the inverse function. We have presented in $\mathbb{F}_{2^n}$ non-existence of permutation polynomials of the form $L_m(x^{-1}) + L_{m'}(x)$ for $n \geq 5$. Main result which is reached by Lucas Kölsch, is that the CCZ-class of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ coincides with the EA-class of F. In addition to that, all permutations in the CCZ-class of F are affine equivalent to it. It is an open question for other functions which have desirable differetial uniformity and nonlinearity properties. Same question would also be researched for odd characteristic. Non-existence of permutation polynomials of the form $L_m(x^{-1}) + L_{m'}(x)$ for characteristic ≥ 5 is shown in [11] based on non-existence of Kloosterman zeros. However, it can be search for charactestic 3.

In Chapter 4, a criterian which is about being permutation polynomial of the form $L_m(x^{-1}) + L_{m'}(x)$ over $\mathbb{F}_{p^n}$ is delivered by using Kloosterman sums and Walsh transforms. This criterian can be applied for all charactaristics p. Therefore, it can be used to search the problem mentioned above for characteristic 3.

REFERENCES

[1] E. Biham and A. Shamir, Differential cryptanalysis of des-like cryptosystems, Journal of Cryptology, 4, pp. 3–72, 2004.

[2] C. Bracken, E. Byrne, G. McGuire, and G. Nebe, On the equivalence of quadratic apn functions, Designs, Codes and Cryptography, 61, pp. 261–272, 2011.

[3] L. Budaghyan, M. Calderini, and I. Villa, On relations between ccz- and ea-equivalences, Cryptography and Communications, 12, pp. 85–100, 2019.

[4] L. Budaghyan and C. Carlet, Ccz-equivalence and boolean functions, IACR Cryptol. ePrint Arch., 2009, p. 63, 2009.

[5] L. Budaghyan, C. Carlet, and A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, IEEE Transactions on Information Theory, 52, pp. 1141–1152, 2006.

[6] A. Canteaut and L. Perrin, On ccz-equivalence, extended-affine equivalence, and function twisting, IACR Cryptol. ePrint Arch., 2018, p. 713, 2018.

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

[8] F. Gologlu, G. McGuire, and R. Moloney, Ternary kloosterman sums using stickelberger's theorem and the gross-koblitz formula, arXiv: Number Theory, 2010.

[9] F. Göloğlu, L. Kölsch, G. M. M. Kyureghyan, and L. Perrin, On subspaces of kloosterman zeros and permutations of the form $l_1(x^{-1}) + l_2(x)$, ArXiv, abs/2003.14068, 2020.

[10] F. Göloğlu and P. Langevin, Almost perfect nonlinear families which are not equivalent to permutations, Finite Fields Their Appl., 67, p. 101707, 2020.

[11] F. Göloğlu and G. McGuire, On theorems of carlitz and payne on permutation polynomials over finite fields with an application to $x^{-1} + l(x)$, Finite Fields Their Appl., 27, pp. 130–142, 2014.

[12] F. Göloğlu, G. McGuire, and R. Moloney, Binary kloosterman sums using stickelberger's theorem and the gross-koblitz formula, Acta Arithmetica, 148(3), pp. 269–279, 2011.

[13] L. Kölsch, On ccz-equivalence of the inverse function, arXiv:2008.08398, 2020.

[14] Y. Li and M. Wang, Permutation polynomials ea-equivalent to the inverse function over gf (2n), Cryptography and Communications, 3, pp. 175–186, 2011.

[15] R. Lidl and H. Niederreiter, Finite fields: Encyclopedia of mathematics and its applications., Computers & Mathematics With Applications, 7, p. 136, 1997.

[16] M. Matsui, Linear cryptanalysis method for des cipher, in T. Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, pp. 386–397, Springer Berlin Heidelberg, Berlin, Heidelberg, 1994, ISBN 978-3-540-48285-7.

[17] T. Tao and V. Vu, Additive combinatorics, in *Cambridge studies in advanced mathematics*, 2007.