ON PERMUTATION POLYNOMIALS OVER FINITE FIELDS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ATILIM UNIVERSITY

BY

MAHA M.M. DABBOOR ASAD

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

MARCH 2017

Approval of the Graduate School of Natural and Applied Sciences, Atılım University.

Prof. Dr. İbrahim Akman
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of **Master of Science in Mathematics Department, Atılım University**.

Prof. Dr. Tanıl Ergenç
Head of Department

This is to certify that we have read the thesis On Permutation Polynomials over Finite Fields submitted by MAHA M.M. DABBOOR ASAD and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Burcu Gülmez Temür
Supervisor

Examining Committee Members:

Prof. Dr. Ferruh Özbudak
Mathematics Department, METU

Assist. Prof. Dr. Fatih Sulak
Mathematics Department, Atılım University

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

Date: March 28, 2017

I declare and guarantee that all data, knowledge and information in this document has been obtained, processed and presented in accordance with academic rules and ethical conduct. Based on these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : MAHA M.M. DABBOOR ASAD

Signature :

ABSTRACT

On Permutation Polynomials over Finite Fields

Dabboor Asad, Maha M.M.
M.S., Department of Mathematics
Supervisor : Assist. Prof. Dr. Burcu Gülmez Temür

March 2017, 90 pages

In this thesis, we study on permutation polynomials defined over finite fields. We have made a survey of some recent research results on constructions and classifications of some types of permutation polynomials over finite fields.

Keywords: Permutation polynomial, finite field, linearized polynomial

ÖZ

Sonlu Cisimler Üzerinde Permutasyon Polinomları

Dabboor Asad, Maha M.M.
Yüksek Lisans, Matematik Bölümü
Tez Yöneticisi : Yrd. Doç. Dr. Burcu Gülmez Temür

28 Mart,2017, 90 sayfa

Bu tezde sonlu cisimlerdeki permutasyon polinomları üzerine çalıştık. Sonlu cisimler üzerinde tanımlanmış bazı permutasyon polinom tiplerinin oluşturulması ve sınıflandırılması ile ilgili son zamanlarda yapılmış birtakım araştırma sonuçlarını derledik.

Anahtar Kelimeler: Permutasyon polinomu, sonlu cisim, doğrusallaştırılmış polinom

To my mother's pure spirit, my father, my husband and all my family

ACKNOWLEDGMENTS

First of all, thanks to Allah for having me finish this work. Especial thanks to my dear father and husband for their continuous encouragement, for their spiritual and moral support.

Deep thanks to math department in Atılım university, and to Dr. Burcu Temür, my supervisor, for her great efforts and constant advice. I shall also thank to Prof. Dr. Ferruh Özbudak from Mathematics Department in METU for his valuable suggestion. All my thanks to the examining committee members, Prof. Dr. Ferruh Özbudak, Assist. Prof. Dr. Fatih Sulak and Assist. Prof. Dr. Burcu Gülmez Temür. Of course I do not forget to thank all my teachers from school and Islamic University of Gaza.

Last but no least, I would like to deeply thank UNRWA management and especially Dr. Bo Schack for supporting me to have a leave permission to complete master degree.

Thank to all those who support me and encourage me and take my hand, friends and loved ones.

TABLE OF CONTENTS

CHAPTERS

CHAPTER 1

INTRODUCTION

Let $\mathbf{F}_q$ denote the finite field of characteristic p with q elements, where $q = p^n, n \in \mathbf{N}$. Let $m > 1$ be an integer and let $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)$ denote the trace function from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$, that is, $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) = x + x^q + ... + x^{q^{m-1}}$. A polynomial of the form $L(x) = \sum_{i=0}^{m-1} a_i x^{q^i} \in \mathbf{F}_{q^m}[x]$ is called a *linearized polynomial* over $\mathbf{F}_{q^m}$. Note that the trace function is a special case of linearized polynomial.
A polynomial $f \in \mathbf{F}_q[x]$ is called a *permutation polynomial* over $\mathbf{F}_q$ if the mapping $x \mapsto f(x)$ induces a bijective map from $\mathbf{F}_q$ to itself. A permutation polynomial $f(x)$ over a finite field $\mathbf{F}_q$ is called a *complete permutation polynomial* if $f(x) + x$ is also a permutation polynomial.

Permutation polynomials over finite fields is an interesting and important topic as they play an essential role in both arithmetical and combinatorial aspects of finite fields. The explicit constructions of permutation polynomials have been a special interest for many applications of finite fields such as cryptography, coding theory, combinatorial design theory, finite geometry and computer science.

In this thesis, our aim is to present some recent studies constructing new classes of permutation polynomials over finite fields. The thesis is organized as follows. In Chapter 2, all definitions and some basic results that will be used throughout the thesis are given.

In Chapter 3, the results of the paper ‘Constructing Permutation Polynomials over Finite Fields’ written by X. Qin and S. Hong are given. In this paper, the authors construct permutation polynomials of the following forms: First they construct $\sum_{i=1}^{k}(L_i(x)+$

$\gamma_i)h_i(B(x))$ over $\mathbf{F}_{q^m}$ where $L_i(x)$ and $B(x)$ are linearized polynomials, next using elementary symmetric polynomials they construct $xh(\lambda_j(x))$ and $xh(\mu_j(x))$ where $\lambda_j(x)$ is the j-th elementary symmetric polynomial of $x, x^q, \ldots .x^{q^{m-1}}$ and $\mu_j(x) = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x^j)$ and finally using linear translators they construct $L_1(x) + L_2(\gamma)h(f(x))$ over $\mathbf{F}_{q^m}$.

In Chapter 4, the results of the paper ‘New Results on Permutation Polynomials over Finite Fields’ written by X. Qin, G. Qian and S. Hong are given, they construct new permutation polynomials of the forms
$L(x) + \sum_{j=1}^{k} \gamma_j h_j(f_j(x))$ and $x + \sum_{j=1}^{k} \gamma_j f_j(x)$ and then using linearized polynomial, permutation polynomials of the form $L(x) + \sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x))$ where $L(x)$ is a linearized polynomial are characterized.

In Chapter 5, the results of the paper ‘On one Class of Permutation Polynomials over Finite Fields of Characteristic Two’ written by L.A. Bassalygo and V.A. Zinoviev are given. In this paper the authors classify all permutation polynomials of type $x^{q^3+q^2+q+2}$ over the field $\mathbf{F}_{q^4}$, where $q = 2^m, m \geq 2$.

In Chapter 6, the results of the paper ‘Permutation and Complete Permutation Polynomials’ written by L.A. Bassalygo and V.A. Zinoviev are given the authors here enumerate all permutation polynomials of the form $x^{q+2} + bx$ over the field $\mathbf{F}_{q^2}$ and $x^{q^2+q+2} + bx$ over the field $\mathbf{F}_{q^3}$.

CHAPTER 2

PRELIMINARIES

In this section we will give all the definitions and some basic results that will be needed throughout the thesis.

Definition 2.0.1 *[8] A* ***field*** *K is a set together with two binary operations, denoted by $+$ and $\cdot$ such that:*

1. *K is an abelian group whith respect to $+$ (with identity element denoted by 0 or 0_K).*

2. *$K \setminus \{0_K\} = K^*$ is an abelian group under $\cdot$.*

3. *The distributive laws hold; that is, for all $a, b, c \in R$ we have $a\cdot(b+c) = a\cdot b+a\cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.*

Definition 2.0.2 *[8] Let E be a field and L a subset of E. L is called a* subfield *of E if L is itself a field under the operations of E. In this context, E is called an* extension field *of K. If $E \neq L$, we say that L is a* proper subfield of E.

Definition 2.0.3 *[8] A field containing no proper subfield is called a prime field.*

Definition 2.0.4 *[8] Let E be an extension field of L. E can be considered as a a vector space over L.* The degree of the extension *E over L denoted by $[E : L]$ is defined to be the dimension of E as a vector space over L, namely $[E : L] = dim_L E$.*

Definition 2.0.5 *[8] Let E be a field , L be a subfield of E and let S be a subset of E. The smallest subfield of E (in the sense of inclusion) containing L and the set subset S is denoted by $L(S)$ and called the extension of L by adjoining the elements of S.*

Remark 2.0.6 *[8] If $S = \{\beta_1, \ldots, \beta_n\}$ then $L(S) = L(\beta_1, \ldots, \beta_n)$. If $S = \{\beta\}$, then $L(\beta)$ is said to be a* simple extension *of L, and β a* defining element *for $L(\beta)$.*

Definition 2.0.7 *[8] Let $p > 0$ be a prime number and $q = p^n$ be a power of p. Then the finite field $\boldsymbol{F}_q$ is a field with q elements.*

Definition 2.0.8 *[8] A polynomial over $\boldsymbol{F}_q$ is an expression of the form*

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

where n is a nonnegative integer, $a_i \in \boldsymbol{F}_q, 0 \leq i \leq n$, and x is an indeterminate over $\boldsymbol{F}_q$, here we say that $f(x) \in \boldsymbol{F}_q[x]$, where $\boldsymbol{F}_q[x]$ is the ring of polynomials over $\boldsymbol{F}_q$.

Theorem 2.0.9 *[8] Let $f \in L[x]$ be an irreducible polynomial over a field L. Then there is a simple algebraic extension $L(\beta)$ where β is a root of f.*

Remark 2.0.10 *[8] If β is a root of the irreducible polynomial f over a field L with $n = degf$. Then $[L(\beta) : L] = n = degf$ and $\{1, \beta, \ldots, \beta^{n-1}\}$ is a basis of $L(\beta)$ as a vector space over L.*

Definition 2.0.11 *[8] If F is an arbitrary field and there exists a positive integer n such that $nr = 0$ for every $r \in F$, then the least such integer n is called the* characteristic *of F and F is said to have (positive) characteristic n. If no such positive integer n exists, F is said to have characteristic 0.*

Corollary 2.0.12 *[8] A finite field has prime characteristic.*

Remark 2.0.13 *[8]*

1. *From here till the end $\boldsymbol{F}_{q^m}$ denotes the finite field of characteristic p with q^m elements where $q = p^n$, p is prime, and $m, n \in \boldsymbol{N}$.*

2. *For the field* $\boldsymbol{F}_{q^m}$ *the prime subfield is the field* $\boldsymbol{F}_p$*, where* p *is the characteristic of* $\boldsymbol{F}_{q^m}$ *with* $q = p^n$*.*

Definition 2.0.14 *[8] Let* E *be a field and* L *a subfield of* E*. An element* $\delta \in E$ *is said to be* algebraic *over* L *if*

$$a_n\delta^n + \cdots + a_1\delta + a_0 = 0,$$

for some $a_i \in L, 1 \leq i \leq n$ *not all zero with* $n > 0$ *is an integer.*

Definition 2.0.15 *[8] Let* E *be a field extension of a field* L*. Then* E *is said to be an* algebraic extension *over* L *if every* $\alpha \in E$ *is algebraic over* L*.*

Proposition 2.0.16 *[8] Every finite extension of a field* L *is algebraic over* L*.*

Theorem 2.0.17 *[8][Existence and Uniqueness of Finite Fields] For every prime number* p *and every positive integer* n*, there exists a finite field with* p^n *elements. Any finite field with* $q = p^n$ *elements it is unique up to isomorphism.*

Remark 2.0.18 *[8] For the finite field* $\boldsymbol{F}_q$*, the extension field* $\boldsymbol{F}_q(\beta)$ *of* $\boldsymbol{F}_q$ *where* β *is a root of the irreducible polynomial* $f \in \boldsymbol{F}_q[x]$*, we have* $\boldsymbol{F}_q(\beta) = \boldsymbol{F}_{q^n}$*, where* $n = degf$*.*

Theorem 2.0.19 *[8][Subfield Criterion] Let* $\boldsymbol{F}_q$ *be the finite field with* $q = p^n$ *elements. Then every subfield of* $\boldsymbol{F}_q$ *has order* p^r *where* r *is a positive divisor of* n*. Conversely, if* r *is a positive divisor of* n*, then there is exactly one subfield of* $\boldsymbol{F}_q$ *with* p^r *elements. Moreover this subfield will be the field* $\boldsymbol{F}_{p^r}$*.*

Theorem 2.0.20 *[8] For every finite field* $\boldsymbol{F}_q$ *the multiplicative group* $\boldsymbol{F}_q^*$ *of nonzero elements of* $\boldsymbol{F}_q$ *is cyclic.*

Definition 2.0.21 *[8] A generator of the cyclic group* $\boldsymbol{F}_q^*$ *is called a* primitive element of $\boldsymbol{F}_q$.

Theorem 2.0.22 *[8] Let* $\boldsymbol{F}_q$ *be a finite field and* $\boldsymbol{F}_s$ *a finite extension field. Then* $\boldsymbol{F}_s$ *is a simple algebraic extension of* $\boldsymbol{F}_q$ *and every primitive element of* $\boldsymbol{F}_s$ *can serve as* *a defining element of $\boldsymbol{F}_s$ over $\boldsymbol{F}_q$. In other word $\boldsymbol{F}_s = \boldsymbol{F}_q(\delta)$ where δ is a primitive element of $\boldsymbol{F}_s$.*

Definition 2.0.23 *[8] Let $f \in K[x]$ be of positive degree and F an extension field of K. Then f is said to* split *in F if f can be written as a product of linear polynomials over F.*

Definition 2.0.24 *[8] Let $f \in K[x]$ and let F be a field extension of K. let $degf = n \geq 1$. F is called a* splitting field of f over *K if f splits in F and $F = K(\alpha_1, \ldots, \alpha_n)$, i.e, F is the smallest extension of K containing all the roots of f.*

Theorem 2.0.25 *[8] If f is an irreducible polynomial in $\boldsymbol{F}_q[x]$ of degree n, then f has a root β in $\boldsymbol{F}_{q^n}$. Furthermore, all the roots of f are simple and are given by the n distinct elements $\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{n-1}}$ of $\boldsymbol{F}_{q^n}$.*

Lemma 2.0.26 *[13] Let $f(x)$ be an irreducible polynomial over $\boldsymbol{F}_q$ of degree m, then $f(x)$ remains irreducible over $\boldsymbol{F}_{q^s}$ if and only if $gcd(s, m) = 1$.*

Corollary 2.0.27 *[8] Let f be an irreducible polynomial in $\boldsymbol{F}_q[x]$ of degree n. Then the splitting field of f over $\boldsymbol{F}_q$ is given by $\boldsymbol{F}_{q^n}$.*

Definition 2.0.28 *[8] Let $\boldsymbol{F}_{q^m}$ be an extension of $\boldsymbol{F}_q$ and let $\beta \in \boldsymbol{F}_{q^m}$. Then the elements $\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{m-1}}$ are called the* conjugates *of β with respect to $\boldsymbol{F}_q$.*

Definition 2.0.29 *[8] Let $m > 1$ be a given integer. By $Tr_{\boldsymbol{F}_{q^m}/\boldsymbol{F}_q}(a)$ we denote the* trace *from $\boldsymbol{F}_{q^m}$ to $\boldsymbol{F}_q$ of a , that is*

$$Tr_{\boldsymbol{F}_{q^m}/\boldsymbol{F}_q}(a) = a + a^q + ... + a^{q^{m-1}}.$$

For $m \geq 1$, $Tr_{\boldsymbol{F}_{q^m}/\boldsymbol{F}_p}(a)$ is called the absolute trace *of a and is denoted as $Tr_{q^m}(a)$, where $\boldsymbol{F}_p$ is the prime subfield of $\boldsymbol{F}_{q^m}$.*

Theorem 2.0.30 *[8] Let $L = \boldsymbol{F}_q$ and $E = \boldsymbol{F}_{q^m}$. Then the trace function $Tr_{E/L}$ satisfies the following properties:*

1. $Tr_{E/L}(a+b) = Tr_{E/L}(a) + Tr_{E/L}(b)$ *for all* $a, b \in E$;

2. $Tr_{E/L}(ca) = cTr_{E/L}(a)$ *for all* $c \in L, a \in E$;

3. $Tr_{E/L}$ *is a linear transformation from* E *onto* L*, where both* E *and* L *are viewed as vector spaces over* L;

4. $Tr_{E/L}(a^q) = Tr_{E/L}(a)$ *for all* $a \in E$*, i.e, all conjugates of* $a \in E$ *with respect to* L *have the same trace.*

Remark 2.0.31 *[8] Note that the trace function* $Tr_{\boldsymbol{F}_{q^m}/\boldsymbol{F}_q} : \boldsymbol{F}_{q^m} \to \boldsymbol{F}_q$ *is a group homomorphism under addition . Let* $K = Ker(Tr_{\boldsymbol{F}_{q^m}/\boldsymbol{F}_q})$*, then since* $Im(Tr_{\boldsymbol{F}_{q^m}/\boldsymbol{F}_q}) = \boldsymbol{F}_q$*, by the first isomorphism theorem* $\boldsymbol{F}_{q^m}/K \cong \boldsymbol{F}_q$*, hence* $|\boldsymbol{F}_{q^m}/K| = |\boldsymbol{F}_q|$*, so* $|K| = q^{m-1}$*, which implies that* $|\{\alpha \in \boldsymbol{F}_{q^m} : Tr_{\boldsymbol{F}_{q^m}/\boldsymbol{F}_q}(\alpha) = 0\}| = q^{m-1}$.

Theorem 2.0.32 *[8][Transitivity of Trace] Let* L *be a finite field ,* E *be a finite extension of* L*, and* F *a finite extension of* E*, then for all* $\alpha \in F$

$$Tr_{F/L}(\alpha) = Tr_{E/L}(Tr_{F/E}(\alpha)).$$

Theorem 2.0.33 *[8] Let* E *be a finite field extension of* $L = \boldsymbol{F}_q$*. Then for* $\alpha \in E$ *we have* $Tr_{E/L}(\alpha) = 0$ *if and only if* $\alpha = \delta^q - \delta$ *for some* $\delta \in E$.

Remark 2.0.34 *Theorem 2.0.33 is special case of Hilbert's Theorem 90 for traces (see [7]).*

Definition 2.0.35 *[8] A polynomial of the form*

$$L(x) = \sum_{i=0}^{m-1} a_i x^{q^i} \in \boldsymbol{F}_{q^m}[x]$$

is called a linearized polynomial *over* $\boldsymbol{F}_{q^m}$.

Lemma 2.0.36 *[10] Let* $B(x), L(x) \in \mathbf{F}_q[x]$ *be linearized polynomials. Then for any* $a \in \mathbf{F}_q$ *and* $x, y \in \mathbf{F}_{q^m}$, $aB(x) = B(ax)$, $B(x+y) = B(x) + B(y)$ *and* $B(L(x)) = L(B(x))$.

Definition 2.0.37 *[8] Let $\boldsymbol{F}_q$ denote the finite field of characteristic p with q elements ($q = p^n, p$ is prime, $n \in \boldsymbol{N}$), and let $\boldsymbol{F}_q^* := \boldsymbol{F}_q \setminus \{0\}$. The polynomial $f \in \boldsymbol{F}_q[x]$ is called a* permutation polynomial *of $\boldsymbol{F}_q$ if and only if for $a \in \boldsymbol{F}_q$:*

1. *the function $f : a \mapsto f(a)$ is onto;*
2. *the function $f : a \mapsto f(a)$ is one-to-one.*

Remark 2.0.38 *For the permutation polynomials over finite fields it is enough to prove that the function $f : a \mapsto f(a)$ is one to one or onto because a one to one mapping over finite set will be onto and vice versa.*

Definition 2.0.39 *[4] A polynomial $f(x) \in \boldsymbol{F}_q[x]$ is called a* complete permutation polynomial *over $\boldsymbol{F}_q$ if and only if the following hold*

1. *$f(x)$ is a permutation polynomial over $\boldsymbol{F}_q$, and*
2. *$f(x) + x$ is a permutation polynomial over $\boldsymbol{F}_q$.*

Definition 2.0.40 *[4] A polynomial $f(x) \in \boldsymbol{F}_q[x]$ is called a* b-complete permutation polynomial *over $\boldsymbol{F}_q$ if and only if:*

1. *$f(x)$ is a permutation polynomial over $\boldsymbol{F}_q$, and*
2. *$f(x) + bx$ is a permutation polynomial over $\boldsymbol{F}_q$, where $b \in \boldsymbol{F}_q^*$*

Remark 2.0.41 *If $f(x)$ is a* b-complete permutation polynomial *over $\boldsymbol{F}_{q^m}$, where $b \in \boldsymbol{F}_{q^m}^*$, then $b^{-1}f(x)$ is* complete permutation polynomial *over $\boldsymbol{F}_{q^m}$.*

Theorem 2.0.42 *[8] The monomial $ax^n \in \boldsymbol{F}_q[x]$ is a permutation polynomial over $\boldsymbol{F}_q$ if and only if $gcd(n, q-1) = 1$.*

Theorem 2.0.43 *[8] Let $\boldsymbol{F}_q$ be of characteristic p. Then the linearized polynomial*

$$L(x) = \sum_{i=0}^{m} a_i x^{p^i} \in \boldsymbol{F}_q[x]$$

is a permutation polynomial of $\boldsymbol{F}_q$ if and only if $L(x)$ only has the root 0 in $\boldsymbol{F}_q$.

Definition 2.0.44 *[8] The* Dickson polynomial *of degree k over a field F, denoted as $D_k(s,r)$, where $r \in F$, is the polynomial defined by*

$$D_k(s,r) = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-i}\binom{k-i}{i}(-r)^i s^{k-2i}.$$

Theorem 2.0.45 *[8] The Dickson polynomial $D_k(s,r), r \in \boldsymbol{F}_q^*$, is a permutation polynomial over $\boldsymbol{F}_q$ if and only if gcd$(k, q^2-1) = 1$.*

Corollary 2.0.46 *[1] Let F be a field of characteristic $p \geq 0$. For $f(x) \in F[x], g(y) \in F[y]$, we have:*

1. *If $p \nmid$ (deg f)(deg g) and $r, s \in F[x,y]$ are non-constant factors of $f(x)+g(y)$ then $(r,s) \neq (1)$ in $F[x,y]$. In particular, if F is algebraically closed, r and s have a common zero.*
2. *If gcd(deg f, deg g) $= 1$ then $f(x)+g(y)$ is irreducible.*

Definition 2.0.47 *[8] Let G be a finite abelian group (written multiplicatively) of order $|G|$ with identity element 1_G. A* character *χ of G is a homomorphism from G into the multiplicative group U of complex numbers of absolute value 1.*

Remark 2.0.48 *[8]*

1. *The character defined by $\chi_0(g) = 1$ for all $g \in G$ is called the* trivial *character χ_0.*
2. *Characters of the additive group of $\boldsymbol{F}_q$ are called* additive characters *of $\boldsymbol{F}_q$. Moreover characters of the multiplicative group $\boldsymbol{F}_q^*$ of $\boldsymbol{F}_q$ are called* multiplicative characters of $\mathbf{F}_q$.

Definition 2.0.49 *[8] Consider the additive group of $\boldsymbol{F}_q$. Let p be the characteristic of $\boldsymbol{F}_q$. Let $Tr : \boldsymbol{F}_q \to \boldsymbol{F}_p$ be the absolute trace function from $\boldsymbol{F}_q$ onto $\boldsymbol{F}_p$. Then the function $\chi_1(a) = e^{2\pi i Tr(a)/p}$ for all $a \in \boldsymbol{F}_q$ is an additive character of $\boldsymbol{F}_q$, and called the* canonical character.

Theorem 2.0.50 (Weil's Theorem) *[8] Let $g \in \boldsymbol{F}_q[x]$ be of degree $m \geq 1$ with gcd$(m, q) = 1$ and let χ be a nontrivial additive character of $\boldsymbol{F}_q$. Then*

$$|\sum_{a \in \boldsymbol{F}_q} \chi\,(g(a))\,| \leq (n-1)\,\sqrt{q}.$$

Definition 2.0.51 *[8] Let χ be a nontrivial additive character of $\boldsymbol{F}_q$ and let $\alpha, \beta \in \boldsymbol{F}_q$. Then the sum*

$$K(\chi; \alpha, \beta) = \sum_{a \in \boldsymbol{F}_q^*} \chi(\alpha a + \beta a^{-1})$$

is called a Kloosterman sum.

Theorem 2.0.52 *[8] If χ is a nontrivial additive character of $\boldsymbol{F}_q$ and $\alpha, \beta \in \boldsymbol{F}_q$ are not both zero, then the Kloosterman sum $K(\chi; \alpha, \beta)$ satisfies*

$$|K(\chi; \alpha, \beta)| \leq 2\,\sqrt{q}.$$

Theorem 2.0.53 (Hasse-Weil bound) *[5] With N the number of $\boldsymbol{F}_q$-rational points of an irreducible non-singular algebraic curve with genus g defined over $\boldsymbol{F}_q$,*

$$|N - q - 1| \leq 2g\,\sqrt{q}.$$

Remark 2.0.54 *[8] the genus g of the curve defined by the equation $f(x, y) = 0$, where f is an absolutely irreducible polynomial $f \in \boldsymbol{F}_q[x, y]$ with deg$(f) = d$, is given by the inequality*

$$g \leq \frac{(d-1)(d-2)}{2}.$$

CHAPTER 3

CONSTRUCTING PERMUTATION POLYNOMIALS OVER FINITE FIELDS

3.1 Permutation polynomials constructed by the linearized polynomials.

In this section we present the results of the paper ”Constructing Permutation Polynomials Over Finite Fields” written by Xiaoer Qin and Shaofang Hong. In this paper, the authors construct several new permutation polynomials over finite fields using linearized polynomials, elementary symmetric polynomials and using linear translators.

The following theorem is the first main result of the paper.

Theorem 3.1.1 *For* $1 \leq i \leq k$ *,let* $\gamma_i \in \mathbf{F}_{q^m}$ *and let* $L_i(x), B(x) \in \mathbf{F}_q[x]$ *be linearized polynomials. Let* $h_i(x) \in \mathbf{F}_{q^m}[x]$ *be such that* $h_i(B(\mathbf{F}_{q^m})) \subseteq \mathbf{F}_q$*. Then* $F(x) := \sum_{i=1}^{k}(L_i(x) + \gamma_i)h_i(B(x))$ *is a permutation polynomial over* $\mathbf{F}_{q^m}$ *if and only if each of the following is true:*

1. $\sum_{i=1}^{k}(L_i(x) + B(\gamma_i))h_i(x)$ *permutes* $B(\mathbf{F}_{q^m})$

2. *For any* $y \in B(\mathbf{F}_{q^m})$, $\sum_{i=1}^{k} L_i(x)h_i(y) = 0$ *and* $B(x) = 0$ *with* $x \in \mathbf{F}_{q^m}$ *are both true if and only if* $x = 0$

Proof. We will first prove that the two conditions are sufficient for F(x) to be a permutation polynomial. Assume that the conditions (1) and (2) hold. Now, assume that there exist α and $\beta \in \mathbf{F}_{q^m}$ satisfying $F(\alpha) = F(\beta)$. Since B is a linearized polynomial this will imply that $B(F(\alpha)) = B(F(\beta))$. That is,

$$B(\sum_{i=1}^{k}(L_i(\alpha) + \gamma_i)h_i(B(\alpha))) = B(\sum_{i=1}^{k}(L_i(\beta) + \gamma_i)h_i(B(\beta))). \tag{3.1}$$

By applying Lemma 2.0.36 to both sides of (3.1) it follows that

$$\sum_{i=1}^{k}(L_i(B(\alpha)) + B(\gamma_i))h_i(B(\alpha)) = \sum_{i=1}^{k}(L_i(B(\beta)) + B(\gamma_i))h_i(B(\beta)). \tag{3.2}$$

By condition (1), $\sum_{i=1}^{k}(L_i(x)+B(\gamma_i))h_i(x)$ permutes $B(\mathbf{F}_{q^m})$, then from (3.2) we get that $B(\alpha) = B(\beta)$. Define $t := B(\alpha) = B(\beta)$. We then have $t \in B(\mathbf{F}_{q^m})$ and $B(\alpha - \beta) = 0$. Since $F(\alpha) = F(\beta)$, one has

$$\sum_{i=1}^{k} L_i(\alpha - \beta)h_i(t) = 0.$$

By applying condition (2) to $\alpha - \beta$, it follows that $\alpha - \beta = 0$, hence $\alpha = \beta$. Therefore $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$.

For the converse, suppose that $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$.

We first prove that if $F(x)$ is permutation polynomial then condition(1) holds.
Let $B(x)$ act on $F(x)$ over $x \in \mathbf{F}_{q^m}$, and since $B(x)$ is linearized polynomial by Lemma 2.0.36 it follows that

$$B(F(x)) = \sum_{i=1}^{k}(L_i(B(x)) + B(\gamma_i))h_i(B(x)). \tag{3.3}$$

Since $F(x)$ permutes the elements of the field $\mathbf{F}_{q^m}$, we get the following equalities of cardinalities,

$$\mid \{B(F(x)) : x \in \mathbf{F}_{q^m}\} \mid = \mid \{B(x) : x \in \mathbf{F}_{q^m}\} \mid = \mid B(\mathbf{F}_{q^m}) \mid . \tag{3.4}$$

This concludes that $\sum_{i=1}^{k}(L_i(x) + B(\gamma_i))h_i(x)$ permutes $B(\mathbf{F}_{q^m})$. Therefore condition (1) holds.
Next, we will prove that if $F(x)$ is a permutation polynomial then condition (2) holds. Assume that $\sum_{i=1}^{k} L_i(x)h_i(y) = 0$ and $B(x) = 0$, for some $y \in B(\mathbf{F}_{q^m})$ and $x \in \mathbf{F}_{q^m}$. Since $y \in B(\mathbf{F}_{q^m})$, we can assume that there exist α and $\beta \in \mathbf{F}_{q^m}$ satisfying $B(\alpha) = B(\beta) = y$, which implies $B(\alpha - \beta) = 0$. Therefore $\alpha - \beta$ and x are both in the kernel $ker(B)$ of

$B(x)$. Thus $\alpha-\beta+x = z$, for some $z \in ker(B)$. Substituting $x = \alpha-\beta+z$ in the equation $\sum_{i=1}^{k} L_i(x)h_i(y) = 0$, we get

$$\sum_{i=1}^{k} L_i(\alpha-\beta+z)h_i(y) = 0. \tag{3.5}$$

On the other hand, recall that $z \in ker(B)$, that is $B(z) = 0$, hence $B(\beta - z) = B(\alpha) = y$. Using the discussion above we get the following

$$\begin{aligned} F(\alpha) - F(\beta - z) &= \sum_{i=1}^{k}(L_i(\alpha) + \gamma_i)h_i(B(\alpha)) - \sum_{i=1}^{k}(L_i(\beta - z) + \gamma_i)h_i(B(\beta - z)) \\ &= \sum_{i=1}^{k}(L_i(\alpha) + \gamma_i)h_i(y) - \sum_{i=1}^{k}(L_i(\beta - z) + \gamma_i)h_i(y) \\ &= \sum_{i=1}^{k} L_i(\alpha-\beta+z)h_i(y). \end{aligned} \tag{3.6}$$

Hence from (3.5) and (3.6), it follows that $F(\alpha) = F(\beta - z)$. From the fact that $F(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$, we obtain $\alpha - \beta + z = 0$. Namely, $x = 0$. Thus condition (2) holds.
This completes the proof.

□

The following corollary can be considered as a special case of Theorem 3.1.1.

Corollary 3.1.2 *Let $L_1(x), L_2(x) \in \mathbf{F}_q[x]$ be linearized polynomials. Let $h(x) \in \mathbf{F}_q[x]$ and $\gamma \in \mathbf{F}_{q^m}$. Then $F(x) := L_1(x) + (L_2(x) + \gamma)h(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if each of the following is true:*

1. *$L_1(x) + (L_2(x) + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma))h(x) \in \mathbf{F}_q[x]$ is a permutation polynomial over $\mathbf{F}_q$.*
2. *For any $y \in \mathbf{F}_q, L_1(x) + L_2(x)h(y) = 0$ and $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) = 0$ with $x \in \mathbf{F}_{q^m}$ are both true if and only if $x = 0$.*

Proof. The result follows by theorem3.1.1 if we take $k = 2$, $B(x) = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) \in \mathbf{F}_q[x]$, $\gamma_1 = 0, \gamma_2 = \gamma$, $h_1(x) = 1$ and $h_2(x) = h(x)$. □ In the following examples we will show how to apply Corollary 3.1.2.

Example 3.1.3 *Let $\mathbf{F}_{q^m} = \mathbf{F}_{8^m}$ where m is an odd integer . Let $h(x) = x^3 - ax, L_1(x) = a^2x$ and $L_2(x) = x^2$, with $a \in \mathbf{F}_8^*$. Then $L_1(x) + L_2(x)h(x) = D_5(x, a)$ is a permutation polynomial over $\mathbf{F_8}$ by Theorem 2.0.45 since $gcd(5, q^2 - 1) = 1$, here $D_5(x, a)$ denotes the Dickson polynomial of degree 5 over $\mathbf{F}_8$. Let $y \in \mathbf{F}_8$ be an arbitrary element, $x \in \mathbf{F}_q^m$ with $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_8}(x) = 0$ and $L_1(x) + L_2(x)h(y) = 0$. If $h(y) = 0$, then $L_1(x) = 0$. From $L_1(x) = a^2x = 0$, we drive that $x = 0$. If $h(y) \neq 0$,it then follows from $L_1(x) + L_2(x)h(y) = 0$ that $x = 0$ or $x = \dfrac{a^2}{y^3 - ay} \neq 0$.*

Assume that $x = \dfrac{a^2}{y^3 - ay}$. Since m is odd and $\dfrac{a^2}{y^3 - ay} \neq 0$, implies $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_8}(x) = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_8}(\dfrac{a^2}{y^3 - ay}) = \dfrac{ma^2}{y^3 - ay} \neq 0$.
By Corollary 3.1.2, we get that $L_1(x)+L_2(x)h(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_8}(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$.

Example 3.1.4 *Let $\mathbf{F}_{q^m} = \mathbf{F}_{9^m}$ with $m > 1$ and $gcd(m, 3) = 1$. Let $h(x) = b^2x^2, L_1(x) = x^3, L_2(x) = a^2x$, where $a, b \in \mathbf{F}_9^*, \gamma = 0$.*

Then

- *$L_1(x) + L_2(x)h(x) = x^3 + a^2x(b^2x^2) = x^3 + a^2b^2x^3 = (1 + a^2b^2)x^3$ permutes $\mathbf{F}_9$ because $gcd(3, 9 - 1) = gcd(3, 8) = 1$.*

- *For any $y \in \mathbf{F}_9$, assume that $L_1(x) + L_2(x)h(y) = 0$ and $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_9}(x) = 0$ with $x \in \mathbf{F}_{q^m}$, that is, $x^3 + a^2x(b^2y^2) = 0$, which implies $x(x^2 + a^2(b^2y^2)) = 0$, then either $x = 0$ or $x^2 + a^2b^2y^2 = 0$. If $x \neq 0$, then $x^2 + a^2b^2y^2 = 0$, i.e, $x^2 = -a^2b^2y^2$. Let $\alpha \in \mathbf{F}_9$ be a root of the irreducible polynomial $x^2 + 1$ over $\mathbf{F}_3$.*
  So $x^2 = \alpha^2a^2b^2y^2$ which implies $x = \pm\alpha aby$. Note that $x \in \mathbf{F}_9$ and since $gcd(m, 3) = 1$ then $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_9}(x) = \pm\alpha abym \neq 0$. which gives a contradiction. Hence $x = 0$ and by Corollary 3.1.2 we conclude that
  $L_1(x) + L_2(x)h(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_9}(x)) = x^3 + a^2b^2x(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_9}(x))^2$ is a permutation polynomial over $\mathbf{F}_{q^m}$.

Corollary 3.1.5 *Let $F(x) := L(x) + xh(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x))$ with $L(x) \in \mathbf{F}_q[x]$ being a linearized polynomial and $h(x) \in \mathbf{F}_q[x]$. Then $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if each of the following is true:*

1. *$L(x) + xh(x)$ is a permutation polynomial over $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)$.*

2. *For any $y \in \mathbf{F}_q$, we have that $x \in \mathbf{F}_{q^m}$ satisfies $L(x)+xh(y) = 0$ and $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q)}(x) = 0$ if and only if $x = 0$.*

Proof. Setting $k = 2$, $L_1(x) = L(x), L_2(x) = x$, $\gamma_1 = \gamma_2 = 0$, $h_1(x) = 1, h_2(x) = h(x)$, and $B(x) = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)$, the result follows by Corollary 3.1.2. □

Corollary 3.1.6 *Let $L(x) = a_0x + a_1x^q + ... + a_{m-1}x^{q^{m-1}} \in \mathbf{F}_q[x]$ be a linearized polynomial which permutes $\mathbf{F}_{q^m}$. Let $h(x) \in \mathbf{F}_q[x]$ and $\gamma \in \mathbf{F}_{q^m}$. Then the polynomial $F(x) := L(x) + \gamma h(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x))$ permutes $\mathbf{F}_{q^m}$ if and only if the polynomial $(a_0 + a_1 + ... + a_{m-1})x + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q)}(\gamma)h(x)$ permutes $\mathbf{F}_q$.*

Proof. Setting $k = 2$, $L_1(x) = L(x), L_2(x) = 0$, $\gamma_1 = 0, \gamma_2 = \gamma$, $h_1(x) = 1, h_2(x) = h(x)$ and $B(x) = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma)(x)$, then applying Corollary 3.1.2, the polynomial $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if

1. $L(x)+Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma)h(x)$ is a permutation polynomial over $\mathbf{F}_q$. However, for $x \in \mathbf{F}_q$, we get that $L(x) = a_0x+a_1x+\cdots+a_{m-1}x = (a_0+a_1+...+a_{m-1})x$. The condition becomes $(a_0 + a_1 + ... + a_{m-1})x + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma)h(x)$ permutes $\mathbf{F}_q$.

2. Assume that $L(x) = 0$ and $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) = 0$ with $x \in \mathbf{F}_{q^m}$. Since $L(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$, then $L(x) = 0$ if and only if $x = 0$ for any $x \in \mathbf{F}_{q^m}$. Hence condition (2) in Corollary 3.1.2 already holds.
   It then follows that $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if $(a_0 + a_1 + ... + a_{m-1})x + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma)h(x)$ is a permutation polynomial over $\mathbf{F}_q$ as desired.

□

3.2 Permutation polynomials constructed by the elementary symmetric polynomials

In this section, the authors construct new classes of permutation polynomials using the elementary symmetric polynomials.

Definition 3.2.1 *Let m and j be integers such that* $1 \leq j \leq m-1$.

Let $\sigma_j(x_1, ..., x_m)$ *denote the jth elementary symmetric polynomial in m variables* $x_1, ..., x_m$. *That is,*

$$\sigma_j(x_1, ..., x_m) = \sum_{1 \leq i_1 < ... < i_j \leq m} x_{i_1} ... x_{i_j} \in \boldsymbol{F}_{q^m}[x_1, x_2, ..., x_m].$$

We can define the polynomial $\lambda_j(x)$ *as*

$$\lambda_j(x) := \sigma_j(x, x^q, ..., x^{q^{m-1}}) = \sum_{0 \leq i_1 < ... < i_j \leq m-1} x^{q^{i_1}+...+q^{i_j}} \in \boldsymbol{F}_{q^m}[x].$$

Lemma 3.2.2 *Let* $\alpha \in \mathbf{F}_{q^m}$ *and* $a \in \mathbf{F}_q$. *Then* $\lambda_j(x) \in \mathbf{F}_q[x], \lambda_j(\alpha) \in \mathbf{F}_q, \lambda_j(\alpha^q) = \lambda_j(\alpha)$ *and* $\lambda_j(a\alpha) = a^j \lambda_j(\alpha)$.

Proof. Since all coefficients of the polynomial $\lambda_j(x)$ are 1, then we get that $\lambda_j(x) \in \mathbf{F}_q[x]$. Let $\alpha \in \mathbf{F}_{q^m}$, then $\lambda_j(\alpha) = \sum_{0 \leq i_1 < ... < i_j \leq m-1} \alpha^{q^{i_1}+...+q^{i_j}}$, take the q power of the two sided we get

$$\begin{aligned} \lambda_j(\alpha)^q &= \left(\sum_{0 \leq i_1 < ... < i_j \leq m-1} \alpha^{q^{i_1}+...+q^{i_j}} \right)^q = \sum_{0 \leq i_1 < ... < i_j \leq m-1} \alpha^{q^{i_1+1}+...+q^{i_j+1}} \\ &= \sum_{1 \leq i_1 < ... < i_j \leq m} \alpha^{q^{i_1}+...+q^{i_j}}, \end{aligned}$$

since $\alpha \in \mathbf{F}_{q^m}$, then $\alpha^{q^m} = \alpha = \alpha^{q^0}$, thus we get

$$\lambda_j(\alpha)^q = \sum_{1 \leq i_1 < ... < i_j \leq m} \alpha^{q^{i_1}+...+q^{i_j}} = \sum_{0 \leq i_1 < ... < i_j \leq m-1} \alpha^{q^{i_1}+...+q^{i_j}} = \lambda_j(\alpha),$$

hence $\lambda_j(\alpha) \in \mathbf{F}_q$. Also by the similar argument, one has

$$\lambda_j(\alpha^q) = \sum_{0 \leq i_1 < ... < i_j \leq m-1} \alpha^{q^{i_1+1}+...+q^{i_j+1}} = \lambda_j(\alpha).$$

Now take $a \in \mathbf{F}_q$, since $a^q = a$, then we have

$$\begin{aligned} \lambda_j(a\alpha) &= \sum_{0 \leq i_1 < ... < i_j \leq m-1} (a\alpha)^{q^{i_1}+...+q^{i_j}} = \sum_{0 \leq i_1 < ... < i_j \leq m-1} a^{q^{i_1}+...+q^{i_j}} \alpha^{q^{i_1}+...+q^{i_j}} \\ &= \sum_{0 \leq i_1 < ... < i_j \leq m-1} a^{q^{i_1}} \cdots a^{q^{i_j}} \alpha^{q^{i_1}+...+q^{i_j}} \\ &= \sum_{0 \leq i_1 < ... < i_j \leq m-1} a^j \alpha^{q^{i_1}+...+q^{i_j}} = a^j \sum_{0 \leq i_1 < ... < i_j \leq m-1} \alpha^{q^{i_1}+...+q^{i_j}} \\ &= a^j \lambda_j(\alpha). \end{aligned}$$

□

Lemma 3.2.3 *For any integer j satisfying that $1 \leq j \leq m-1$ and gcd$(j, q-1) = 1$, $\lambda_j : \mathbf{F}_{q^m} \to \mathbf{F}_q$ is onto .*

Proof. First we need to show that there exists $\alpha \in \mathbf{F}_{q^m}$ such that $\lambda_j(\alpha) \neq 0$. From the definition of $\lambda_j(x)$ we observe that the degree of λ_j is

$$deg(\lambda_j(x)) = q^{m-j} + \cdots + q^{m-1} \leq q + \cdots + q^{m-1} = \frac{q^m - 1}{q - 1} - 1 < q^m = |\mathbf{F}_{q^m}|,$$

which implies that the number of roots of $\lambda_j(x)$ in $\mathbf{F}_{q^m}$ is less than q^m, so there exist an element $\alpha \in \mathbf{F}_{q^m}$ such that $\lambda_j(\alpha) \neq 0$. Now choose an $\alpha \in \mathbf{F}_{q^m}$ such that $a := \lambda_j(\alpha) \neq 0$. Let $b \in \mathbf{F}_q$ be arbitrary. Since $gcd(j, q-1) = 1$, by Theorem 2.0.42 the polynomial ax^j is a permutation polynomial over $\mathbf{F}_{q^m}$. It follows that for any $b \in \mathbf{F}_{q^m}$, there exists an element $d \in \mathbf{F}_q$ such that $b = ad^j$. Since $\lambda_j(\alpha) = a$, letting $\delta := d\alpha$ we get

$$\lambda_j(\delta) = \lambda_j(d\alpha) = d^j\lambda_j(\alpha) = ad^j = b$$

Hence $\lambda_j(x)$ is onto . □

We can now characterize permutation polynomials of the form $xh(\lambda_j(x))$ by the following Theorem.

Theorem 3.2.4 *Let m and j be positive integers such that $1 \leq j \leq m-1$ and gcd$(j, q-1) = 1$. Let $h(x) \in \mathbf{F}_q[x]$. Then $xh(\lambda_j(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$ if and only if $h(0) \neq 0$ and $xh(x)^j$ permutes $\mathbf{F}_q$*

Proof. Define $F(x) := xh(\lambda_j(x))$. Assume that $h(0) \neq 0$ and $xh(x)^j$ permutes $\mathbf{F}_q$. Since $xh(x)^j$ permutes $\mathbf{F}_q$, it follows that $\delta h(\delta)^j \neq 0$, for any $\delta \in \mathbf{F}_q^*$. Moreover, $h(\delta) \neq 0$ for $\delta \in \mathbf{F}_q^*$, and since we assumed that $h(0) \neq 0$ we get $h(\delta) \neq 0$ for all $\delta \in \mathbf{F}_q$.
Choose arbitrary elements $\alpha, \beta \in \mathbf{F}_{q^m}$ such that $F(\alpha) = F(\beta)$, that is,

$$\alpha h(\lambda_j(\alpha)) = \beta h(\lambda_j(\beta)). \tag{3.7}$$

Then $\lambda_j(F(\alpha)) = \lambda_j(F(\beta))$, which implies by (3.7) that $\lambda_j(\alpha h(\lambda_j(\alpha))) = \lambda_j(\beta h(\lambda_j(\beta)))$. Using Lemma 3.2.2, and since $h(x) \in \mathbf{F}_q$, $\lambda_j(x) \in \mathbf{F}_q$ we deduce that

$$\lambda_j(\alpha)h(\lambda_j(\alpha))^j = \lambda_j(\beta)h(\lambda_j(\beta))^j. \tag{3.8}$$

Now, since $xh(x)^j$ permutes $\mathbf{F}_q$, it follows from (3.8) that $\lambda_j(\alpha) = \lambda_j(\beta)$. Let $y = \lambda_j(\alpha) = \lambda_j(\beta)$, then the equation (3.7) is equivalent to $(\alpha - \beta)h(y) = 0$, which implies that $\alpha = \beta$ as $h(\delta) \neq 0$ for all $\delta \in \mathbf{F}_q$. Hence $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$.

Conversely, suppose that $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$. We will first prove that $h(0) \neq 0$. By Lemma 3.2.3, the mapping λ_j is onto since $gcd(j, q-1) = 1$. For $1 \leq j \leq m-1$, we have

$$deg\lambda_j(x) = q^{m-j} + \cdots + q^{m-1} \leq q + \cdots + q^{m-1}.$$

Thus for any $a \in \mathbf{F}_q^*$, the equation $\lambda_j(x) = a$ has at most $q + \cdots + q^{m-1}$ roots in $\mathbf{F}_{q^m}$. Then the equation $\lambda_j(x) = 0$ has at least $q^m - (q-1)(q + \cdots + q^{m-1}) = q$ roots in $\mathbf{F}_{q^m}$. Hence $\lambda_j(x) = 0$ has a nonzero root in $\mathbf{F}_{q^m}$. Now, choose $\alpha \in \mathbf{F}_{q^m}^*$ such that $\lambda_j(\alpha) = 0$. Then $\alpha h(0) = \alpha h(\lambda_j(\alpha)) = F(\alpha)$. Since $F(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$ and α is nonzero, then $F(\alpha) \neq 0$, that is , $\alpha h(0) \neq 0$. Thus $h(0) \neq 0$.

We will now prove that $xh(x)^j$ permutes $\mathbf{F}_q$. Let $H(x) := xh(x)^j$. By Lemma 3.2.2 it follows that

$$\lambda_j(F(x)) = \lambda_j(x)h(\lambda_j(x))^j. \tag{3.9}$$

In addition, by Lemma 3.2.3, $\lambda_j(x)$ is a mapping from $\mathbf{F}_{q^m}$ onto $\mathbf{F}_q$, for all integers j with $1 \leq j \leq m-1$ .This means that for all $a \in \mathbf{F}_q$ there exist $b \in \mathbf{F}_{q^m}$ such that $\lambda_j(b) = a$, which implies that

$$\{xh(x)^j : x \in \mathbf{F}_q\} = \{\lambda_j(x)h(\lambda_j(x))^j : x \in \mathbf{F}_{q^m}\}. \tag{3.10}$$

It then follows from (3.9) and (3.10) and the assumption that $F(x)$ permutes $\mathbf{F}_{q^m}$, that

$$\begin{aligned} |\{xh(x)^j : x \in \mathbf{F}_q\}| &= |\{\lambda_j(x)h(\lambda_j(x))^j : x \in \mathbf{F}_{q^m}\}| \\ &= |\{\lambda_j(F(x)) : x \in \mathbf{F}_{q^m}\}| \\ &= |\{\lambda_j(x) : x \in \mathbf{F}_{q^m}\}| = q. \end{aligned}$$

Hence the polynomial $H(x) : \mathbf{F}_q \to \mathbf{F}_q$ is a one-to-one mapping, and since $\mathbf{F}_q$ is finite $H(x)$ is also onto, therefore $H(x) = xh(x)^j$ permutes $\mathbf{F}_q$.

□

Definition 3.2.5 *Define* $\mu_j(x) := \sum_{i=0}^{m-1} x^{jq^i} = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x^j)$, *for* $1 \leq j \leq q^m - 1$. *Then* $\mu_j(x) \in \mathbf{F}_q[x], \mu_j(\alpha) \in \mathbf{F}_q$ *and* $\mu_j(a\alpha) = a^j\mu_j(\alpha)$ *for all* $a \in \mathbf{F}_q$ *and* $\alpha \in \mathbf{F}_{q^m}$.

Remark 3.2.6 *Note that* $\mu_j(x)$ *is a mapping from* $\mathbf{F}_{q^m}$ *onto* $\mathbf{F}_q$ *if* $gcd(j, q^m - 1) = 1$, *that is because* x^j *permutes* $\mathbf{F}_{q^m}$ *if* $gcd(j, q^m - 1) = 1$, *so*

$$\begin{aligned} Im(\mu_j(x)) &= \{Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x^j) : x \in \mathbf{F}_{q^m}\} \\ &= \{Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) : x \in \mathbf{F}_{q^m}\} \\ &= \mathbf{F}_q \end{aligned}$$

Replacing $\lambda_j(x)$ by $\mu_j(x)$ we can characterize a permutation polynomials of the form $xh(\mu_j(x))$ as the following.

Theorem 3.2.7 *Let* m *and* j *be positive integers such that* $1 \leq j \leq q^m - 1$ *and* $gcd(j, q^m - 1) = 1$. *Let* $h(x) \in \mathbf{F}_q[x]$. *Then* $xh(\mu_j(x))$ *is a permutation polynomial over* $\mathbf{F}_{q^m}$ *if and only if* $h(0) \neq 0$ *and* $xh(x)^j$ *permutes* $\mathbf{F}_q$.

Proof. It is enough to prove that if $xh(\mu_j(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$, then $h(0) \neq 0$. The other part of the proof is very similar to that of Theorem 3.2.4. Suppose that $xh(\mu_j(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$. From the fact that $|\{a \in \mathbf{F}_{q^m} : Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(a) = 0\}| = q^{m-1}$, there exist a nonzero element $\delta \in \mathbf{F}_{q^m}$ such that $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\delta) = 0$. Since $gcd(j, q^m - 1) = 1$, x^j permutes $\mathbf{F}_{q^m}$, so there is a nonzero element $c \in \mathbf{F}_{q^m}$ such that $c^j = \delta$. Therefore $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(c^j) = 0$, i.e, $\mu_j(c) = 0$. Then $ch(0) = ch(\mu_j(c))$. Since $xh(\mu_j(x))$ is a permutation polynomial over $\mathbf{F}_{q^m}$ and c is a nonzero, then $ch(0) \neq 0$. Thus $h(0) \neq 0$. So the theorem is proved. □

3.3 Permutation polynomial constructed by linear translators

Definition 3.3.1 *Let* $f : \mathbf{F}_{q^m} \to \mathbf{F}_q$, $a \in \mathbf{F}_q$ *and* α *be a nonzero element in* $\mathbf{F}_{q^m}$. *If* $f(x + u\alpha) - f(x) = ua$ *for all* $x \in \mathbf{F}_{q^m}$ *and* $u \in \mathbf{F}_q$, *then we say that* α *is an* a-linear translator *of the function* f . *In particular,* $a = f(\alpha) - f(0)$.

Theorem 3.3.2 *Let $L_1(x) \in \mathbf{F}_{q^m}[x]$ be a linearized permutation polynomial of $\mathbf{F}_{q^m}$ and $L_2(x) \in \mathbf{F}_{q^m}[x]$ be a linearized polynomial of $\mathbf{F}_{q^m}$.*
Let $b \in \mathbf{F}_q, \gamma \in \mathbf{F}_{q^m}, h : \mathbf{F}_q \to \mathbf{F}_q, f : \mathbf{F}_{q^m} \to \mathbf{F}_q$ be surjective and $L_1^{-1}L_2(\gamma)$ be a b-linear translator of f . Then $L_1(x) + L_2(\gamma)h(f(x))$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if either $L_2(\gamma) = 0$ or $x + bh(x)$ is a permutation polynomial of $\mathbf{F}_q$.

Proof. We define $k(x) := x + bh(x)$ and $K(x) := L_1(x) + L_2(\gamma)h(f(x))$.

Note that if $L_2(\gamma) = 0$, then $K(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$ since $L_1(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$. Assume that $L_2(\gamma) \neq 0$ and $k(x)$ is a permutation polynomial of $\mathbf{F}_q$. In order to show that $K(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$, let x_1, y_1 be arbitrary elements in $\mathbf{F}_{q^m}$ such that $K(x_1) = K(y_1)$, that is,

$$L_1(x_1) + L_2(\gamma)h(f(x_1)) = L_1(y_1) + L_2(\gamma)h(f(y_1)). \tag{3.11}$$

Since $L(x)$ is a linearized polynomial then (3.11) can be written as $L_1(x_1 - y_1) = aL_2(\gamma)$, where $a := h(f(y_1)) - h(f(x_1)) \in \mathbf{F}_q$. As $L_1(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$, there exists a unique element $\alpha \in \mathbf{F}_{q^m}$ such that $L_1(\alpha) = aL_2(\gamma)$. Thus, $\alpha = aL_1^{-1}L_2(\gamma)$ and since $L_1(x_1 - y_1) = aL_2(\gamma)$, we get $L_1(\alpha) = L_1(aL_1^{-1}L_2(\gamma)) = L_1(x_1 - y_1)$. Now, since $L_1(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$ it follows immediately that $\alpha = x_1 - y_1$, i.e.,

$$x_1 = y_1 + aL_1^{-1}L_2(\gamma). \tag{3.12}$$

Substituting the expression of x_1 in (3.11) implies that

$$L_1(aL_1^{-1}L_2(\gamma)) + L_2(\gamma)h(f(y_1 + aL_1^{-1}L_2(\gamma))) = L_2(\gamma)h(f(y_1)), \tag{3.13}$$

which is equivalent to

$$aL_2(\gamma) + L_2(\gamma)h(f(y_1 + aL_1^{-1}L_2(\gamma))) = L_2(\gamma)h(f(y_1)). \tag{3.14}$$

Dividing both sides of (3.14) by $L_2(\gamma)$ we get

$$a + h(f(y_1 + aL_1^{-1}L_2(\gamma))) = h(f(y_1)). \tag{3.15}$$

As $L_1^{-1}L_2(\gamma)$ is the b-linear translator of f, we have $f(y_1 + aL_1^{-1}L_2(\gamma)) - f(y_1) = ab$. Hence we can rewrite (3.15) as

$$a + h(f(y_1) + ab) = h(f(y_1)). \tag{3.16}$$

Now, multiplying (3.16) by b and adding $f(y_1)$ to both sides, we get

$$f(y_1) + ab + bh(f(y_1) + ab) = f(y_1) + bh(f(y_1)). \tag{3.17}$$

Recall that $k(x) = x + bh(x)$, then (3.17) is equivalent to

$$k(f(y_1) + ab) = k(f(y_1)). \tag{3.18}$$

Next, we claim that $a = 0$. In order to prove this claim we will consider the cases where $b = 0$ and $b \neq 0$ separately. If $b = 0$, then by (3.16), one has $a = 0$ as claimed. If $b \neq 0$, then it follows from the assumption that $k(x)$ is a permutation polynomial of $\mathbf{F}_q$ and (3.18) that $a = 0$. The claim is proved. Then by the claim and (3.12), it follows immediately that $x_1 = y_1$. This concludes that $K(x)$ is a permutation polynomialof $\mathbf{F}_{q^m}$.

Conversely, assume that $K(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$. Suppose that $L_2(\gamma) \neq 0$. Here we will also consider the cases where $b = 0$ and $b \neq 0$ separately. If $b = 0$, then $k(x) = x$, is already a permutation polynomial of $\mathbf{F}_q$, then we have done. If $b \neq 0$, then choose arbitrary elements $u_1, u \in \mathbf{F}_q$ such that

$$k(u_1) = k(u_1 + bu). \tag{3.19}$$

Since f is surjective, there exists an element $v_1 \in \mathbf{F}_{q^m}$ such that $u_1 = f(v_1)$. Then (3.19) is equivalent to

$$k(f(v_1)) = k(f(v_1) + bu). \tag{3.20}$$

After replacing y_1 by v_1 and a by u in (3.18) and using the equivalence of (3.18) and (3.13), the equation in (3.20) becomes

$$L_1(v_1) + L_2(\gamma)h(f(v_1)) = L_1(v_1 + uL_1^{-1}L_2(\gamma)) + L_2(\gamma)h(f(v_1 + uL_1^{-1}L_2(\gamma))). \tag{3.21}$$

Recall that $K(x) = L_1(x) + L_2(\gamma)h(f(x))$. It follows from (3.21) that $K(v_1) = K(v_1 + uL_1^{-1}L_2(\gamma))$, but $K(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$, so $v_1 = v_1 + uL_1^{-1}L_2(\gamma)$, which implies $uL_1^{-1}L_2(\gamma) = 0$. Since $L_1(x)$ is a permutation polynomial and $L_2(\gamma) \neq 0$, we have $L_1^{-1}L_2(\gamma) \neq 0$. Hence $u = 0$. Thus $k(x)$ is a permutation polynomial of $\mathbf{F}_q$. This completes the proof of the theorem.

□

Corollary 3.3.3 *Let $L(x) \in \mathbf{F}_{q^m}[x]$ be a linearized permutation polynomial of $\mathbf{F}_{q^m}$. Let $b \in \mathbf{F}_q, \gamma \in \mathbf{F}_{q^m}, h : \mathbf{F}_q \to \mathbf{F}_q, f : \mathbf{F}_{q^m} \to \mathbf{F}_q$ be surjective and γ be a b-linear translator of f. Then $F(x) := L(x) + L(\gamma)h(f(x))$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if $x + bh(x)$ is a permutation polynomial of $\mathbf{F}_q$.*

Proof. If we set $k = 2$ and $L_1(x) = L_2(x)$, then $L_1^{-1}L_2(\gamma) = \gamma$, and apply Theorem 3.3.2 it follows that $F(x) = L(x) + L(\gamma)h(f(x))$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if either $L(\gamma) = 0$ or $x + bh(x)$ is a permutation polynomial of $\mathbf{F}_q$. But since $L(x)$ is a permutation polynomial over $\mathbf{F}_{q^m}$, if $L(\gamma) = 0$ then $\gamma = 0$, but γ is a b-linear translator of f and by definition γ is a nonzero element. Hence $L(\gamma) \neq 0$. Therefore $F(x) = L(x) + L(\gamma)h(f(x))$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if $x + bh(x)$ is a permutation polynomial of $\mathbf{F}_q$ as desired. □

CHAPTER 4

NEW RESULTS OF PERMUTATION POLYNOMIALS OVER FINITE FIELDS

4.1 Permutation polynomial constructed by linear translators

In this section, we will give the results of the paper ”New Result On Permutation Polynomials Over Finite Fields” where the authors construct permutation polynomials of the forms $L(x) + \sum_{j=1}^{k} \gamma_j h_j(f_j(x))$ and $x + \sum_{j=1}^{k} \gamma_j f_j(x)$ using linear translators.

Theorem 4.1.1 *Let k be a positive integer. Let* $L : \mathbf{F}_{q^m} \to \mathbf{F}_{q^m}$ *be a linearized polynomial such that* $dim(Ker(L)) = k$ *and* $Ker(L) \cap Im(L) = \{0\}$ *. Let* $\{\gamma_1, ..., \gamma_k\}$ *be a basis of* $Ker(L)$ *over* $\mathbf{F}_q$ *and* $h_1(x), ..., h_k(x) \in \mathbf{F}_q[x]$ *be permutation polynomials of* $\mathbf{F}_q$*. For any integers i and j with* $1 \leq i, j \leq k$ *let* $b_{ij} \in \mathbf{F}_q$ *and* γ_i *be a* b_{ij}*-linear translator of* $f_j : \mathbf{F}_{q^m}, \to \mathbf{F}_q$*. Then* $F(x) := L(x) + \sum_{j=1}^{k} \gamma_j h_j(f_j(x))$ *is a permutation polynomial of* $\mathbf{F}_{q^m}$ *if and only if* $det(b_{ij})_{1\leq i,j\leq k} \neq 0$ *.*

Proof. Assume that $det(b_{ij})_{1\leq i,j\leq k} \neq 0$, and $F(\alpha) = F(\beta)$, for arbitrary elements $\alpha, \beta \in \mathbf{F}_{q^m}$, which implies that

$$F(\alpha) = L(\alpha) + \sum_{j=1}^{k} \gamma_j h_j(f_j(\alpha)) = L(\beta) + \sum_{j=1}^{k} \gamma_j h_j(f_j(\beta)),$$

since $L(x)$ is linearized polynomial over $\mathbf{F}_{q^m}$, then the equation above is equivalent to

$$L(\alpha - \beta) = \sum_{j=1}^{k} \gamma_j (h_j(f_j(\beta)) - h_j(f_j(\alpha))). \tag{4.1}$$

Note that $h_j(f_j(\beta)) - h_j(f_j(\alpha)) \in \mathbf{F}_q$ for $1 \leq j \leq k$, and since $\gamma_j \in Ker(L)$, we get

$$\begin{aligned} L\left(\sum_{j=1}^{k} \gamma_j(h_j(f_j(\beta)) - h_j(f_j(\alpha)))\right) &= \sum_{j=1}^{k} L\left(\gamma_j(h_j(f_j(\beta)) - h_j(f_j(\alpha)))\right) \\ &= \sum_{j=1}^{k}(h_j(f_j(\beta)) - h_j(f_j(\alpha)))L\left(\gamma_j\right) \\ &= 0, \end{aligned}$$

which implies that $\sum_{j=1}^{k} \gamma_j(h_j(f_j(\beta)) - h_j(f_j(\alpha))) \in Ker(L)$. By equation (4.1) we have $\sum_{j=1}^{k} \gamma_j(h_j(f_j(\beta)) - h_j(f_j(\alpha))) \in Im(L)$, but $Ker(L) \cap Im(L) = \{0\}$. So

$$\sum_{j=1}^{k} \gamma_j(h_j(f_j(\beta)) - h_j(f_j(\alpha))) = 0. \tag{4.2}$$

Hence $L(\alpha - \beta) = 0$, that is, $\alpha - \beta \in Ker(L)$. Now, since $\{\gamma_1, \ldots, \gamma_k\}$ is a basis of $Ker(L)$ over $\mathbf{F}_q$, and $\alpha - \beta \in Ker(L)$, there exist $a_1, \ldots, a_k \in \mathbf{F}_q$ such that

$$\alpha - \beta = a_1\gamma_1 + \cdots + a_k\gamma_k, \tag{4.3}$$

that is,

$$\alpha = \beta + a_1\gamma_1 + \cdots + a_k\gamma_k, \tag{4.4}$$

As $\gamma_1, \ldots, \gamma_k$ are linearly independent over $\mathbf{F}_q$, by (4.2) we have

$$h_j(f_j(\beta)) - h_j(f_j(\alpha)) = 0, \text{ for } 1 \leq j \leq k. \tag{4.5}$$

Substituting $\alpha = \beta + a_1\gamma_1 + \cdots + a_k\gamma_k$ in (4.5) we get

$$h_j(f_j(\beta)) - h_j(f_j(\beta + a_1\gamma_1 + \cdots + a_k\gamma_k)) = 0 \text{ for } 1 \leq j \leq k. \tag{4.6}$$

But $h_j(x)$ is a permutation polynomial of $\mathbf{F}_q$, so (4.6) is equivalent to

$$f_j(\beta + a_1\gamma_1 + \cdots + a_k\gamma_k) - f_j(\beta) = 0 \text{ for } 1 \leq j \leq k. \tag{4.7}$$

On the other hand, from the fact that γ_i is a b_{ij}-linear translator of f_j, for all $1 \leq i, j \leq k$, we get the following equalities,

$$\begin{aligned} &f_j(\beta + a_1\gamma_1 + \cdots + a_{k-1}\gamma_{k-1} + a_k\gamma_k) - f_j(\beta + a_1\gamma_1 + \cdots + a_{k-1}\gamma_{k-1}) = a_k b_{kj}; \\ &f_j(\beta + a_1\gamma_1 + \cdots + a_{k-2}\gamma_{k-2} + a_{k-1}\gamma_{k-1}) - f_j(\beta + a_1\gamma_1 + \cdots + a_{k-2}\gamma_{k-2}) = a_{k-1} b_{k-1j}; \\ &f_j(\beta + a_1\gamma_1 + \cdots + a_{k-3}\gamma_{k-3} + a_{k-2}\gamma_{k-2}) - f_j(\beta + a_1\gamma_1 + \cdots + a_{k-3}\gamma_{k-3}) = a_{k-2} b_{k-2j}; \\ &\vdots \\ &f_j(\beta + a_1\gamma_1) - f_j(\beta) = a_1 b_{1j}. \end{aligned}$$

By summing up the equations above we deduce that

$$f_j(\beta + a_1\gamma_1 + \cdots + a_k\gamma_k) - f_j(\beta) = a_1b_{1j} + a_2b_{2j} + \cdots + a_kb_{kj}.$$

which implies the equation (4.7) is equivalent to

$$a_1b_{1j} + a_2b_{2j} + \cdots + a_kb_{kj} = 0, \text{ for } 1 \leq j \leq k. \tag{4.8}$$

Therefore $(a_1, \ldots, a_k) \in \mathbf{F}_q^k$ is a solution of the following system of linear equations

$$\begin{cases} x_1b_{11} + x_2b_{21} + \cdots + x_kb_{k1} = 0 \\ x_1b_{12} + x_2b_{22} + \cdots + x_kb_{k2} = 0 \\ \vdots \\ x_1b_{1k} + x_2b_{2k} + \cdots + x_kb_{kk} = 0. \end{cases} \tag{4.9}$$

As $det(b_{ij})_{1\leq i,j\leq k} \neq 0$, the rank of the coefficient matrix of (4.9) is equal to k. Thus the system (4.9) of linear equations has only the trivial solution. Namely, $(a_1, \ldots, a_k) = (0, \ldots, 0)$, which implies $\alpha = \beta$ by (4.4). Hence $F(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$.

Conversely, assume that $F(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$, and let $(a_1, \ldots, a_k) \in \mathbf{F}_q^*$ be a solution of the system (4.9), then (4.8) holds. Note that the equation (4.8) is equivalent to (4.6), then (4.6) is also satisfied. That is,

$$h_j(f_j(\beta)) - h_j(f_j(\beta + a_1\gamma_1 + \cdots + a_k\gamma_k)) = 0, \text{ for } 1 \leq j \leq k,$$

where $\beta \in \mathbf{F}_{q^m}$. Choose an element $\alpha \in \mathbf{F}_{q^m}$ such that $\alpha := \beta + a_1\gamma_1 + \cdots + a_k\gamma_k$. Substituting α in the above equation it follows that

$$\sum_{j=1}^{k} \gamma_j(h_j(f_j(\beta)) - h_j(f_j(\alpha))) = 0. \tag{4.10}$$

Recall that $\gamma_1, \ldots, \gamma_k \in Ker(L)$, and since $\alpha - \beta = a_1\gamma_1 + \cdots + a_k\gamma_k$, then

$$L(\alpha - \beta) = L(a_1\gamma_1 + \cdots + a_k\gamma_k) = a_1L(\gamma_1) + \cdots + a_kL(\gamma_k) = 0, \tag{4.11}$$

combining (5.12) and (4.11) we get,

$$L(\alpha - \beta) = \sum_{j=1}^{k} \gamma_j(h_j(f_j(\beta)) - h_j(f_j(\alpha))).$$

Since $L(x)$ is linearized polynomial we have,

$$L(\alpha) + \sum_{j=1}^{k} \gamma_j h_j(f_j(\alpha)) = L(\beta) + \sum_{j=1}^{k} \gamma_j h_j(f_j(\beta)).$$

Note that $F(\alpha) = L(\alpha) + \sum_{j=1}^{k} \gamma_j h_j(f_j(\alpha))$ and $F(\beta) = L(\beta) + \sum_{j=1}^{k} \gamma_j h_j(f_j(\beta))$, therefore $F(\alpha) = F(\beta)$. However, $F(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$, which implies that $\alpha = \beta$, then from the expression of α, it follows that $a_1\gamma_1 + \cdots + a_k\gamma_k = 0$. Since $\{\gamma_1, \ldots, \gamma_k\}$ is a basis of Ker(L) over $\mathbf{F}_q$, we get $a_1 = \cdots = a_k = 0$, which implies the system (4.9) has only the trivial solution. Therefore $det(b_{ij})_{1\leq i,j\leq k} \neq 0$, as desired. □

Corollary 4.1.2 *Let $m \geq 2$ be a positive integer with $gcd(p,m) = 1$, $\gamma_1, ..., \gamma_{m-1} \in \mathbf{F}_{q^m} \setminus \mathbf{F}_q$ be linearly independent over $\mathbf{F}_q$ and $h_1(x), ..., h_{m-1}(x) \in \mathbf{F}_q[x]$ be a permutation polynomial of $\mathbf{F}_q$ .For any integers i and j with $1 \leq i, j \leq m-1$,let $b_{ij} \in \mathbf{F}_q$ and γ_i be a b_{ij}-linear translator of $f_j : \mathbf{F}_{q^m} \to \mathbf{F}_q$ .Then $F(x) := Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) + \sum_{j=1}^{m-1} \gamma_j h_j(f_j(x))$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if $det(b_{ij})_{1\leq i,j\leq m-1} \neq 0$.*

Proof. We will just apply Theorem 4.1.1 by taking $L(x) = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)$. Recall that $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q} : \mathbf{F}_{q^m} \to \mathbf{F}_q$ is onto, so $Im\left(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)\right) = \mathbf{F}_q$. Let a be an element such that $a \in Ker(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}) \cap \mathbf{F}_q$, it follows that $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(a) = 0$, and $a \in \mathbf{F}_q$. Since $a \in \mathbf{F}_q$, then $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(a) = ma$, which implies $ma = 0$, but from the hypothesis that $gcd(p,m) = 1$, it follows that $a = 0$. Hence $Ker(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}) \cap \mathbf{F}_q = \{0\}$. Therefore $Ker(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}) = \mathbf{F}_{q^m} \setminus \mathbf{F}_q^*$. Since $dim(Ker(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q})) = m-1$, and the elements $\gamma_1, ..., \gamma_{m-1}$ are linearly independent, then the set $\{\gamma_1, ..., \gamma_{m-1}\}$ forms a basis of $Ker(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q})$ over $\mathbf{F}_q$. Hence the Corollary is concluded by applying Theorem 4.1.1. □

Corollary 4.1.3 *Let p be an odd prime and k be a positive integer.Let $\{\gamma_1, ..., \gamma_k\}$ be a basis of $\mathbf{F}_{q^k}$ over $\mathbf{F}_q$ and $h_1(x), ..., h_k(x) \in \mathbf{F}_q[x]$ be permutation polynomials of $\mathbf{F}_q$. For any integers i and j with $1 \leq i, j \leq k$, let $b_{ij} \in \mathbf{F}_q$ and γ_i be a b_{ij}-linear translator of $f_j : \mathbf{F}_{q^{2k}} \to \mathbf{F}_q$. Then $F(x) := x - x^{q^k} + \sum_{j=1}^{k} \gamma_j h_j(f_j(x))$ is a permutation polynomial of $\mathbf{F}_{q^{2k}}$ if and only if $det(b_{ij})_{1\leq i,j\leq k} \neq 0$.*

Proof. Setting $m = 2k$ and $L(x) = x - x^{q^k}$ be a linearized polynomial over $\mathbf{F}_{q^{2k}}$, we have $Ker(L) = Ker(x - x^{q^k}) = \mathbf{F}_{q^k}$, hence the set $\{\gamma_1, ..., \gamma_k\}$ is a basis of $Ker(L)$. Now for any $a \in Ker(x - x^{q^k}) \cap Im(x - x^{q^k})$, we get $a = a^{q^k}$ and $a = b - b^{q^k}$ for some $b \in \mathbf{F}_{q^{2k}}$.

It follows that $a = (b - b^{q^k})^{q^k} = b^{q^k} - b^{q^{2k}} = b^{q^k} - b = -a$, which implies that $2a = 0$, but since p is an odd prime, then $a = 0$. Therefore $Ker(x - x^{q^k}) \cap Im(x - x^{q^k}) = \{0\}$. By Theorem 4.1.1 the Corollary is concluded. □

Corollary 4.1.4 *Let $m \geq 2$ be a positive integer with $gcd(p, m) = 1$, $\gamma_1, ..., \gamma_{m-1} \in \mathbf{F}_{q^m} \setminus \mathbf{F}_q$ be linearly independent over $\mathbf{F}_q$. Let $h_j : \mathbf{F}_q \longrightarrow \mathbf{F}_q$ be a permutation of $\mathbf{F}_q$ and $H_j : \mathbf{F}_{q^m} \longrightarrow \mathbf{F}_{q^m}$,$\beta_j \in \mathbf{F}_{q^m}$ for $1 \leq j \leq m-1$. Then $F(x) := Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) + \sum_{j=1}^{m-1} \gamma_j h_j(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)) + \beta_j x))$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if $det(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_i\beta_j))_{1\leq i,j\leq m-1} \neq 0$.*

Proof. We will apply Corollary 4.1.2 by setting $f_j(x) = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x))+\beta_j x)$, $1 \leq j \leq m-1$. Then for all $x \in \mathbf{F}_{q^m}$ and all $a \in \mathbf{F}_q$

$$\begin{aligned} f_j(x + a\gamma_i) - f_j(x) =& Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x + a\gamma_i)) + \beta_j(x + a\gamma_i)) \\ & - Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)) + \beta_j x) \\ & = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) + aTr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_i)) + \beta_j(x + a\gamma_i)) \\ & - Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)) + \beta_j x), \end{aligned}$$

but $\gamma_i \in Ker(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q})$, for $1 \leq i \leq m-1$, then $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_i) = 0$, which implies

$$f_j(x + a\gamma_i) - f_j(x) = aTr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_i\beta_j).$$

Therefore γ_i is a $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_i\beta_j)$- linear translator of $f_j(x)$ for $1 \leq i, j \leq m-1$. Hence by Corollary 4.1.2 $F(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if $det(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_i\beta_j))_{1\leq i,j\leq m-1} \neq 0$, as desired. □

Corollary 4.1.5 *Let p be an odd prime and k be a positive integer. Let $\alpha \in \mathbf{F}_{q^k}$ be a primitive element of $\mathbf{F}_{q^k}$. Let $h_1(x), ..., h_k(x) \in \mathbf{F}_q[x]$ be permutation polynomials of $\mathbf{F}_q, H_1(x), ..., H_k(x) \in \mathbf{F}_{q^{2k}}[x]$ and $\beta_1, ..., \beta_k \in \mathbf{F}_{q^{2k}}$. Then $F(x) := x - x^{q^k} + \sum_{j=1}^{k} \alpha^{j-1} h_j(Tr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(H_j(x - x^q) + \beta_j x))$ is a permutation polynomial of $\mathbf{F}_{q^{2k}}$ if and only if $det(Tr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(\alpha^{i-1}\beta_j))_{1\leq i,j\leq k} \neq 0$.*

Proof. From the fact that α is a primitive element of $\mathbf{F}_{q^k}$, by Theorem 2.10 [8] it follows that $\mathbf{F}_{q^k} = \mathbf{F}_q(\alpha)$, hence the set $\{1, \alpha, \ldots, \alpha^{k-1}\}$ forms a basis of $\mathbf{F}_{q^k}$ over $\mathbf{F}_q$.

Set $f_j(x) = Tr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(H_j(x - x^q) + \beta_j x), f_j : \mathbf{F}_{q^{2k}} \to \mathbf{F}_q, 1 \leq j \leq k$, then for all $x \in \mathbf{F}_{q^{2k}}$ and all $a \in \mathbf{F}_q$,

$$\begin{aligned} f_j(x + a\alpha^{i-1}) - f_j(x) =& Tr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(H_j(x + a\alpha^{i-1} - (x + a\alpha^{i-1})^q) + \beta_j(x + a\alpha^{i-1}))- \\ & Tr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(H_j(x - x^q) + \beta_j x) \\ =& Tr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(H_j(x - x^q) + a\beta_j\alpha^{i-1} + \beta_j x)- \\ & Tr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(H_j(x - x^q) + \beta_j x) \\ =& aTr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(\beta_j\alpha^{i-1}). \end{aligned}$$

So α^{i-1} is a $Tr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(\beta_j\alpha^{i-1})$-linear translator of f_j, for $1 \leq i, j \leq k$. Applying Corollary 4.1.3 for f_j and $\gamma_j = \alpha^{j-1}$ for $1 \leq j \leq k$, gives that the polynomial $F(x)$ is a permutation polynomial of $\mathbf{F}_{q^{2k}}$ if and only if $det(Tr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(\alpha^{i-1}\beta_j))_{1\leq i,j\leq k} \neq 0$. □

Example 4.1.6 *Let p be an odd prime and t_1, t_2 be positive integers satisfying that $gcd(t_i, q - 1) = 1$ for $i = 1, 2$. Let $\alpha \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$, then $1, \alpha$ are linearly independent,otherwise there is $r, s \in \boldsymbol{F}_q$ such that $r \cdot 1 + s\alpha = 0$ which implies $\alpha = -rs^{-1} \in \boldsymbol{F}_q$, but $\alpha \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$, hence the set $\{1, \alpha\}$ is a basis of $\mathbf{F}_{q^2}$ over $\mathbf{F}_q$. Let $\beta_1, \beta_2 \in \mathbf{F}_{q^4}$ and $H_1(x), H_2(x) \in \mathbf{F}_{q^4}[x]$. Then it follows immediately from Corollary 4.1.5 that the polynomial $F(x) := x^{q^2} - x + (Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(H_1(x^{q^2} - x) + \beta_1 x))^{t_1} + \alpha(Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(H_2(x^{q^2} - x) + \beta_2 x))^{t_2}$ is a permutation polynomial of $\mathbf{F}_{q^4}$ if and only if*

$$\det\begin{pmatrix} Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\beta_1) & Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\beta_2) \\ Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\alpha\beta_1) & Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\alpha\beta_2) \end{pmatrix} \neq 0.$$

Example 4.1.7 *Let p be an odd prime and let $\alpha \in \boldsymbol{F}_{q^4}$ be a primitive element of $\boldsymbol{F}_{q^4}$ and $D_{t_i}(x, 1)$ be a Dickson polynomial where $i = 1, 2, 3$ and t_1, t_2, t_3 be positive integers such that $gcd(t_i, q^2 - 1) = 1$, hence $D_{t_i}(x, 1)$ is a permutation polynomial over $\boldsymbol{F}_{q^2}$. Let $\beta_1, \beta_2\beta_3 \in \boldsymbol{F}_{q^4}$ and $H_1(x), H_2(x), H_3(x) \in \boldsymbol{F}_{q^4}[x]$. Then by applying Corollary 4.1.4 the polynomial $F(x) := x^{q^3} + x^{q^2} + x^q + x + \sum_{i=1}^{3} \alpha^i D_{t_i}\left(Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(H_i(x^{q^3} + x^{q^2} + x^q + x) + \beta_i x), 1\right)$ is a permutation polynomial of $\mathbf{F}_{q^4}$ if and only if*

$$\det\begin{pmatrix} Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\alpha\beta_1) & Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\alpha\beta_2) & Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\alpha\beta_3) \\ Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\alpha^2\beta_1) & Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\alpha^2\beta_2) & Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\alpha^2\beta_3) \\ Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\alpha^3\beta_1) & Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\alpha^3\beta_2) & Tr_{\mathbf{F}_{q^4}/\mathbf{F}_q}(\alpha^3\beta_3) \end{pmatrix} \neq 0.$$

Theorem 4.1.8 *Let k and l be positive integers with $l \leq k$. For any integers i and j with $1 \leq i, j \leq k$ let $\gamma_i \in \mathbf{F}_{q^m}, b_{ij} \in \mathbf{F}_q$ and γ_i be a b_{ij}-linear translator of $f_j : \mathbf{F}_{q^m} \to \mathbf{F}_q$ such that $\gamma_1, ..., \gamma_k$ are linearly independent over $\mathbf{F}_q$. Let $A = (b_{ij})_{1 \leq i,j \leq k}$ be a $k \times k$ matrix over $\mathbf{F}_q$ and I be the $k \times k$ identity matrix over $\mathbf{F}_q$. Then each of the following is true :*

1. *$F(x) := x + \sum_{j=1}^{k} \gamma_j f_j(x)$* is a permutation polynomial of $\mathbf{F}_{q^m}$ *if and only if rank$(I + A) = k$.*
2. *$F(x) := x + \sum_{j=1}^{k} \gamma_j f_j(x)$ is a q^l-to-1 mapping of $\mathbf{F}_{q^m}$ if rank$(I + A) = k - l$.*

Proof.

1. Assume that *rank*$(I + A) = k$. Choose arbitrary elements $\alpha, \beta \in \mathbf{F}_{q^m}$, such that $F(\alpha) = F(\beta)$, that is

$$\alpha + \sum_{j=1}^{k} \gamma_j f_j(\alpha) = \beta + \sum_{j=1}^{k} \gamma_j f_j(\beta), \tag{4.12}$$

which implies

$$\alpha - \beta = \sum_{j=1}^{k} \gamma_j \left(f_j(\beta) - f_j(\alpha) \right). \tag{4.13}$$

Set $a_j := f_j(\beta) - f_j(\alpha) \in \mathbf{F}_q$, then it follows from (4.13) that $\alpha = \beta + \sum_{j=1}^{k} \gamma_j a_j$. In (4.12) if we substitute $\alpha = \beta + \sum_{j=1}^{k} \gamma_j a_j$, then it follows that

$$\beta + \sum_{j=1}^{k} \gamma_j a_j + \sum_{j=1}^{k} \gamma_j f_j(\beta + \sum_{j=1}^{k} \gamma_j a_j) = \beta + \sum_{j=1}^{k} \gamma_j f_j(\beta), \tag{4.14}$$

which is equivalent to

$$\sum_{j=1}^{k} \gamma_j \left(a_j + f_j(\beta + \sum_{i=1}^{k} \gamma_i a_i) - f_j(\beta) \right) = 0. \tag{4.15}$$

From the hypothesis γ_i be a b_{ij}-linear translator of f_j for $1 \leq i, j \leq k$,

$$f_j(\beta + \gamma_1 a_1 + \cdots + \gamma_{k-1} a_{k-1} + \gamma_k a_k) - f_j(\beta + \gamma_1 a_1 + \cdots + \gamma_{k-1} a_{k-1}) = a_k b_{kj}$$

$$f_j(\beta + \gamma_1 a_1 + \cdots + \gamma_{k-2} a_{k-2} + \gamma_{k-1} a_{k-1}) - f_j(\beta + \gamma_1 a_1 + \cdots + \gamma_{k-2} a_{k-2}) = a_{k-1} b_{k-1j}$$

$$\vdots$$

$$f_j(\beta + \gamma_1 a_1) - f_j(\beta) = a_1 b_{1j},$$

by summing up the equations it follows that $f_j(\beta+\sum_{j=1}^{k}\gamma_j a_j)-f_j(\beta)=\sum_{i=1}^{k}a_i b_{ij}$. Hence equation (4.15) becomes the following

$$\sum_{j=1}^{k}\gamma_j\left(a_j+\sum_{i=1}^{k}a_i b_{ij}\right)=0. \tag{4.16}$$

But from the hypothesis the elements $\gamma_1, ..., \gamma_k$ are linearly independent over $\mathbf{F}_q$, which implies that the equation (4.16) equivalent to

$$a_j+\sum_{i=1}^{k}a_i b_{ij}=0, \text{ for } 1\le j\le k. \tag{4.17}$$

It follows that $(a_1,\dots,a_k)^T\in\mathbf{F}_q$ be a solution of the system of linear equations

$$\begin{cases} x_1+x_1b_{11}+x_2b_{21}+\cdots+x_kb_{k1}=0\\ x_1b_{12}+x_2+x_2b_{22}+\cdots+x_kb_{k2}=0\\ \vdots\\ x_1b_{1k}+x_2b_{2k}+\cdots+x_k+x_kb_{kk}=0\end{cases}$$

which is equivalent to the system

$$(I+A)^TX=0, \tag{4.18}$$

where $X=(x_1,\dots,x_k)^T$. By using the fact that $rank(I+A)=k$, the system (4.18) has only the trivial solution. Therefore $a_1=a_2=\cdots=a_k=0$. Recall $\alpha=\beta+\sum_{j=1}^{k}\gamma_j a_j$, then it follows that $\alpha=\beta$. Hence the polynomial $F(x)$ is a permutation polynomial if $rank(I+A)=k$.

Conversely, assume that $F(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$. In order to show that $rank(I+A)=k$, suppose $(a_1,a_2,\dots,a_k)^T\in\mathbf{F}_q^k$ is a solution of the system (4.18) of linear equations, it follows that (4.17) is satisfied. Since (4.17) and (4.14) are equivalent, then we have

$$\beta+\sum_{j=1}^{k}\gamma_j a_j+\sum_{j=1}^{k}\gamma_j f_j(\beta+\sum_{j=1}^{k}\gamma_j a_j)=\beta+\sum_{j=1}^{k}\gamma_j f_j(\beta),$$

where $\beta\in\mathbf{F}_{q^m}$. Setting

$$\alpha:=\beta+\sum_{j=1}^{k}\gamma_j a_j, \tag{4.19}$$

we get

$$\alpha + \sum_{j=1}^{k} \gamma_j f_j(\alpha) = \beta + \sum_{j=1}^{k} \gamma_j f_j(\beta), \tag{4.20}$$

that is, $F(\alpha) = F(\beta)$. Since $F(x)$ is a permutation polynomial, we get $\alpha = \beta$. From (4.19) it follows that $\sum_{j=1}^{k} \gamma_j a_j = 0$. From the hypothesis $\gamma_1, \ldots, \gamma_k$ are linearly independent over $\mathbf{F}_q$, which implies $a_1 = a_2 = \cdots = a_k = 0$, that is $(a_1, a_2, \ldots, a_k)^T = (0, 0, \ldots, 0)^T$. Therefore the system of linear equations (4.18) has only the trivial solutions. Thus $rank(I + A) = k$.

2. Suppose that $rank(I + A) = k - l$. Let $(r_1, \ldots, r_k)^T \in \mathbf{F}_q^k$ be an arbitrary solution of the system of linear equations (4.18), then $r_j + \sum_{i=1}^{k} r_i b_{ij} = 0,$ for $1 \leq j \leq k$. and let $\beta \in \mathbf{F}_{q^m}$. By using the definition of $F(x)$ we get

$$F(\beta + \sum_{j=1}^{k} \gamma_j r_j) = \beta + \sum_{j=1}^{k} \gamma_j r_j + \sum_{j=1}^{k} \gamma_j f_j(\beta + \sum_{j=1}^{k} \gamma_j r_j),$$

Since γ_i is a $b_{ij}-$ linear translator of f_j, for $1 \leq i, j \leq k$, then $f_j(\beta + \sum_{j=1}^{k} \gamma_j r_j) - f_j(\beta) = \sum_{i=1}^{k} r_i b_{ij}$, thus $f_j(\beta + \sum_{j=1}^{k} \gamma_j r_j) = f_j(\beta) + \sum_{i=1}^{k} r_i b_{ij}$. Hence

$$\begin{aligned} F(\beta + \sum_{j=1}^{k} \gamma_j r_j) &= \beta + \sum_{j=1}^{k} \gamma_j r_j + \sum_{j=1}^{k} \gamma_j (f_j(\beta) + \sum_{i=1}^{k} r_i b_{ij}) \\ &= \beta + \sum_{j=1}^{k} \gamma_j f_j(\beta) + \sum_{j=1}^{k} \gamma_j (r_j + \sum_{i=1}^{k} r_i b_{ij}) \\ &- \beta + \sum_{j=1}^{k} \gamma_j f_j(\beta) + \sum_{j=1}^{k} \gamma_j (0) \\ &= \beta + \sum_{j=1}^{k} \gamma_j f_j(\beta) \\ &= F(\beta). \end{aligned} \tag{4.21}$$

On the other hand, since $rank(I+A) = k-l$, the dimension of the solution space of the system of linear equations over $\mathbf{F}_q$ (4.18), is l, hence there are exactly q^l solutions of (4.18). Since $\gamma_1, \ldots, \gamma_k$ are linearly independent over $\mathbf{F}_q$, also the number of elements in the set

$$|\{\sum_{j=1}^{k} \gamma_j r_j : (r_1, \ldots, r_k)^T \text{ solutions of (4.18) }\}| = q^l.$$

By the discussion above and (4.21) we see that $F(x)$ is a q^l−to-1 mapping of $\mathbf{F}_{q^m}$. So part (2) is proved.

□

Corollary 4.1.9 *[6] Let $\gamma \in \mathbf{F}_{q^m}$ be a b-linear translator of $f : \mathbf{F}_{q^m} \to \mathbf{F}_q$. Then each of the following is true :*

1. *$F(x) := x + \gamma f(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$, if $b \neq -1$.*
2. *$F(x) := x + \gamma f(x)$ is a $q - to - 1$ mapping of $\mathbf{F}_{q^m}$, if $b = -1$.*

Proof. This corollary follows immediately from Theorem 4.1.8 since if $b \neq -1$, the linear equation $(1 + b)x = 0$ has only the trivial solution over $\mathbf{F}_q$, on the other hand, if $b = -1$, then the number of solutions of the linear equation $(1 + b)x = 0$ over $\mathbf{F}_q$ is q and in this case $F(x)$ is q−to-1 mapping of $\mathbf{F}_{q^m}$. □

Corollary 4.1.10 *[6] Let $\gamma, \delta \in \mathbf{F}_{q^m}$ be linearly independent over $\mathbf{F}_q$. Suppose γ is a b_1-linear translator of $f_1 : \mathbf{F}_{q^m} \to \mathbf{F}_q$ and a b_2-linear translator of $f_2 : \mathbf{F}_{q^m} \to \mathbf{F}_q$ and moreover δ is a d_1-linear translator of $f_1 : \mathbf{F}_{q^m} \to \mathbf{F}_q$ and a d_2-linear translator of $f_2 : \mathbf{F}_{q^m} \to \mathbf{F}_q$. Then $F(x) := x + \gamma f_1(x) + \delta f_2(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$, if $b_1 \neq -1$ and $d_2 - \dfrac{d_1 b_2}{1 + b_1} \neq -1$ or by symmetry, if $d_2 \neq -1$ and $b_1 - \dfrac{d_1 b_2}{1 + d_2} \neq -1$.*

Proof. By applying Theorem 4.1.8, the polynomial $F(x)$ is permutation polynomial if and only if $rank(I + A) = 2$ where

$$A = \begin{pmatrix} b_1 & d_1 \\ b_2 & d_2 \end{pmatrix}$$

which means that if and only if

$$det \begin{pmatrix} 1 + b_1 & d_1 \\ b_2 & 1 + d_2 \end{pmatrix} \neq 0,$$

that is if and only if $b_1 \neq -1$ and $d_2 - \dfrac{d_1 b_2}{1 + b_1} \neq -1$ or by symmetry, if $d_2 \neq -1$ and $b_1 - \dfrac{d_1 b_2}{1 + d_2} \neq -1$, as desired. □

Corollary 4.1.11 *[6] Let $\gamma \in \mathbf{F}_{q^m} \backslash \mathbf{F}_q$ and $M(x) := x^{q^2} - (1+(\gamma^q-\gamma)^{q-1})x^q + (\gamma^q-\gamma)^{q-1}x$. Let $H_1, H_2 : \mathbf{F}_{q^m} \to \mathbf{F}_{q^m}$ and $\beta_1, \beta_2 \in \mathbf{F}_{q^m}$. Then $F(x) := x + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_1(M(x)) + \beta_1 x) + \gamma Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_2(M(x)) + \beta_2 x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if $(1 + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\beta_1))(1 + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma\beta_2)) \neq Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma\beta_1)Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\beta_2)$.*

Proof. We will get the result by applying Theorem 4.1.8 by setting $k = 2$, $f_1 = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_1(M(x)) + \beta_1 x)$, $f_2 = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_2(M(x)) + \beta_2 x)$, since from the hypothesis $\gamma \in \mathbf{F}_{q^m} \setminus \mathbf{F}_q$ it follows that $1, \gamma$ are linearly independent over $\mathbf{F}_q$. Note that the polynomial $M(x)$ is a linearized polynomial and $M(s) = 0$, for any $s \in \mathbf{F}_q$. Then 1 is a $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\beta_1)-$linear translator of f_1 because, for all $x \in \mathbf{F}_{q^m}$ and all $s \in \mathbf{F}_q$ we have

$$\begin{aligned} f_1(x+s) - f_1(x) =& Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_1(M(x+s)) + \beta_1(x+s)) - Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_1(M(x)) + \beta_1 x), \\ =& sTr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\beta_1). \end{aligned}$$

Analogously 1 is a $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\beta_2)-$linear translator of f_2, γ is a $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma\beta_1)-$linear translator of f_1, and a $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma\beta_2)-$linear translator of f_2. Thus by Theorem 4.1.8 the polynomial $F(x)$ is permutation polynomial of $\mathbf{F}_{q^m}$ if and only if

$$det \begin{pmatrix} 1 + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\beta_1) & Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma\beta_1) \\ Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\beta_2) & 1 + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma\beta_2) \end{pmatrix} \neq 0,$$

which is equivalent to the condition
$(1 + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\beta_1))(1 + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma\beta_2)) \neq Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma\beta_1)Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\beta_2)$, as desired. □

Corollary 4.1.12 *Let k be a positive integer . Let $L : \mathbf{F}_{q^m} \to \mathbf{F}_{q^m}$ be a linearized polynomial with kernel $Ker(L)$ and $\{\delta_1, ..., \delta_k\}$ be a basis of $Ker(L)$ over $\mathbf{F}_q$. Let $H_j : \mathbf{F}_{q^m} \to \mathbf{F}_{q^m}$ and $\beta_j \in \mathbf{F}_{q^m}$ for $1 \leq j \leq k$. Then $F(x) := x + \sum_{j=1}^{k} \delta_j Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(L(x)) + \beta_j x)$ is a* permutation polynomial *of $\mathbf{F}_{q^m}$ if and only if $det(I + (Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\delta_j\beta_j)))_{1 \leq i,j \leq k} \neq 0$*

.

Proof. Set $f_j = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(L(x)) + \beta_j x)$. Note that $\{\delta_1, ..., \delta_k\}$ is linearly independent over $\mathbf{F}_q$ because it is a basis of $Ker(L)$ over $\mathbf{F}_q$. Let $x \in \mathbf{F}_{q^m}$ and $s \in \mathbf{F}_q$, and since

$\delta_j \in Ker(L)$ for all $1 \leq i, j \leq k$, we have

$$\begin{aligned}
f_j(x + s\delta_i) - f_j(x) =& Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(L(x + s\delta_i)) + \beta_j(x + s\delta_i)) - Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(L(x)) + \beta_j x)\\
=& Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(L(x) + L(s\delta_i)) + \beta_j x + s\delta_i\beta_j) -\\
& Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(L(x)) + \beta_j x)\\
=& Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(L(x)) + \beta_j x) - Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(L(x)) + \beta_j x) +\\
& Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(s\delta_i\beta_j)\\
=& sTr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\delta_i\beta_j),
\end{aligned}$$

hence δ_i is a $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\delta_i\beta_j)$−linear translator of f_j for $1 \leq i, j \leq k$. Now applying Theorem 4.1.8 by taking $\gamma_j = \delta_j$, the desired result follows immediately.

□

Corollary 4.1.13 *Let $\theta \in \mathbf{F}_{q^m}$ be a primitive element of $\mathbf{F}_{q^m}$ and $m > 3$ be integer. Let $a = \dfrac{(\theta - \theta^{q^3})(\theta^{q^2} - \theta)^{q-1}}{\theta^{q^2} - \theta^q}, b = \dfrac{(\theta^{q^3} - \theta)(\theta - \theta^q)^{q^2-1}}{\theta^{q^2} - \theta^q}, c = -1 - a - b$, and $N(x) := x^{q^3} + ax^{q^2} + bx^q + cx$. Let $H_1(x), H_2(x), H_3(x) \in \mathbf{F}_{q^m}[x]$ and $\gamma_1, \gamma_2, \gamma_3 \in \mathbf{F}_{q^m}$. Then*

$$\begin{aligned}
F(x) :=& x + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_1(N(x)) + \gamma_1 x) + \theta Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_2(N(x)) + \gamma_2 x) +\\
& \theta^2 Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_3(N(x)) + \gamma_3 x)
\end{aligned}$$

is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if

$$det\begin{pmatrix} 1 + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_1) & Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_2) & Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_3)\\ Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\theta\gamma_1) & 1 + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\theta\gamma_2) & Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\theta\gamma_3)\\ Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\theta^2\gamma_1) & Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\theta^2\gamma_2) & 1 + Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\theta^2\gamma_3) \end{pmatrix} \neq 0.$$

Proof. Set $k = 3$, and $f_j = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(N(x)) + \gamma_j x)$ for $1 \leq j \leq 3$. Since $\theta \in \mathbf{F}_{q^m}$ is a primitive element of $\mathbf{F}_{q^m}$, we know that $\mathbf{F}_{q^m} = \mathbf{F}_q(\theta)$, so the set $\{1, \theta, \theta^2, \ldots, \theta^{m-1}\}$ forms a basis of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$, so $1, \theta, \theta^2$ are linearly independent over $\mathbf{F}_q$. Note that

$$\begin{aligned}
N(1) =& 1 + a + b + c = 0, \text{ and}\\
N(\theta) =& \theta^{q^3} + a\theta^{q^2} + b\theta^{q} + c\theta\\
=& \theta^{q^3} + a\theta^{q^2} + b\theta^{q} - (1 + a + b)\theta\\
=& \theta^{q^3} + a(\theta^{q^2} - \theta) + b(\theta^{q} - \theta) - \theta\\
=& \theta^{q^3} + \frac{(\theta - \theta^{q^3})(\theta^{q^2} - \theta)^{q-1}}{\theta^{q^2} - \theta^{q}}(\theta^{q^2} - \theta) + \frac{(\theta^{q^3} - \theta)(\theta - \theta^{q})^{q^2-1}}{\theta^{q^2} - \theta^{q}}(\theta^{q} - \theta) - \theta\\
=& \theta^{q^3} + \frac{(\theta - \theta^{q^3})(\theta^{q^2} - \theta)^{q}}{\theta^{q^2} - \theta^{q}} - \frac{(\theta^{q^3} - \theta)(\theta - \theta^{q})^{q^2}}{\theta^{q^2} - \theta^{q}} - \theta\\
=& \theta^{q^3} - \theta + \frac{\theta - \theta^{q^3}}{\theta^{q^2} - \theta^{q}}(\theta^{q^3} - \theta^{q} + \theta^{q^2} - \theta^{q^3})\\
=& 0,
\end{aligned}$$

similarly for θ^2 we get $N(\theta^2) = 0$; hence $1, \theta, \theta^2$ are roots of $N(x)$. Take $x \in \mathbf{F}_{q^m}$ and $s \in \mathbf{F}_q$, for $i = 0, 1, 2$, since $N(x)$ is linearized polynomial we have

$$\begin{aligned}
f_j(x + s\theta^i) - f_j(x) =& Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(N(x + s\theta^i)) + \gamma_j(x + s\theta^i)) - Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(N(x)) + \gamma_j x)\\
=& Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(N(x)) + \gamma_j x) - Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(H_j(N(x)) + \gamma_j x) +\\
& sTr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_j\theta^i)\\
=& sTr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_j\theta^i);
\end{aligned}$$

therefore for all $1 \leq j \leq 3$ and $0 \leq i \leq 2$, θ^i is a $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\gamma_j\theta^i)$−linear translator of f_j. Thus applying Theorem 4.1.8 concludes the result immediately. □ The next Corollary describes an application of Theorem 4.1.8, which gives a large family of complete permutation polynomials of $\mathbf{F}_{q^m}$.

Corollary 4.1.14 *Let p be an odd prime and k be a positive integer . For any integers i and j with $1 \leq i, j \leq k$, let $\gamma_i \in \mathbf{F}_{q^m}, b_{ij} \in \mathbf{F}_q, \gamma_i$ be a b_{ij}-linear translator of $f_j : \mathbf{F}_{q^m} \to \mathbf{F}_q$ such that $\gamma_1, ..., \gamma_k$ are linearly independent over $\mathbf{F}_q$. Let $A = (b_{ij})_{1\leq i,j\leq k}$ be a $k \times k$ matrix over $\mathbf{F}_q$ and I be the $k \times k$ identity matrix over $\mathbf{F}_q$. Then*

$$F(x) := x + \sum_{j=1}^{k} \gamma_j f_j(x)$$

is a complete permutation polynomial of $\mathbf{F}_{q^m}$ if and only if $rank(I + A) = k$ and $rank(2I + A) = k$.

Proof.

Let $g(x) := F(x) + x := 2x + \sum_{j=1}^{k} \gamma_j f_j(x)$. We are going to prove that $g(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if $rank(2I + A) = k$.

Assume that $rank(2I + A) = k$. To show that $g(x)$ is a permutation polynomial choose arbitrary elements $\alpha, \beta \in \mathbf{F}_{q^m}$, such that $g(\alpha) = g(\beta)$, that is

$$2\alpha + \sum_{j=1}^{k} \gamma_j f_j(\alpha) = 2\beta + \sum_{j=1}^{k} \gamma_j f_j(\beta), \tag{4.22}$$

which implies

$$2\alpha - 2\beta = \sum_{j=1}^{k} \gamma_j \left(f_j(\beta) - f_j(\alpha) \right). \tag{4.23}$$

Set $a_j := f_j(\beta) - f_j(\alpha) \in \mathbf{F}_q$, then it follows from (4.23) that $2\alpha = 2\beta + \sum_{j=1}^{k} \gamma_j a_j$. In (4.22) if we substitute $2\alpha = 2\beta + \sum_{j=1}^{k} \gamma_j a_j$, then it follows that

$$2\beta + \sum_{j=1}^{k} \gamma_j a_j + \sum_{j=1}^{k} \gamma_j f_j(\beta + \frac{1}{2} \sum_{j=1}^{k} \gamma_j a_j) = 2\beta + \sum_{j=1}^{k} \gamma_j f_j(\beta), \tag{4.24}$$

let $r_j = \frac{1}{2} a_j$, for $1 \leq j \leq k$, equation (4.24) is equivalent to

$$\sum_{j=1}^{k} \gamma_j \left(2r_j + f_j(\beta + \sum_{i=1}^{k} \gamma_i r_i) - f_j(\beta) \right) = 0. \tag{4.25}$$

From the hypothesis γ_i be a b_{ij}-linear translator of f_j for $1 \leq i, j \leq k$,

$$f_j(\beta + \gamma_1 r_1 + \cdots + \gamma_{k-1} r_{k-1} + \gamma_k r_k) - f_j(\beta + \gamma_1 r_1 + \cdots + \gamma_{k-1} r_{k-1}) = r_k b_{kj}$$

$$f_j(\beta + \gamma_1 r_1 + \cdots + \gamma_{k-2} r_{k-2} + \gamma_{k-1} r_{k-1}) - f_j(\beta + \gamma_1 r_1 + \cdots + \gamma_{k-2} r_{k-2}) = r_{k-1} b_{k-1j}$$

$$\vdots$$

$$f_j(\beta + \gamma_1 r_1) - f_j(\beta) = r_1 b_{1j},$$

by summing up the equations it follows that $f_j(\beta + \sum_{j=1}^{k} \gamma_j r_j) - f_j(\beta) = \sum_{i=1}^{k} r_i b_{ij}$. Hence equation (4.25) becomes the following

$$\sum_{j=1}^{k} \gamma_j \left(2r_j + \sum_{i=1}^{k} r_i b_{ij} \right) = 0. \tag{4.26}$$

But from the hypothesis the elements $\gamma_1, ..., \gamma_k$ are linearly independent over $\mathbf{F}_q$, which implies that the equation (4.26) equivalent to

$$2r_j + \sum_{i=1}^{k} r_i b_{ij} = 0, \text{ for } 1 \leq j \leq k. \tag{4.27}$$

It follows that $(r_1, \ldots, r_k)^T \in \mathbf{F}_q$ be a solution of the system of linear equations

$$\begin{cases} 2x_1 + x_1 b_{11} + x_2 b_{21} + \cdots + x_k b_{k1} = 0 \\ x_1 b_{12} + 2x_2 + x_2 b_{22} + \cdots + x_k b_{k2} = 0 \\ \vdots \\ x_1 b_{1k} + x_2 b_{2k} + \cdots + x_k b_{kk} + 2x_k = 0 \end{cases}$$

which is equivalent to the system

$$(2I + A)^T X = 0, \tag{4.28}$$

where $X = (x_1, \ldots, x_k)^T$. By using the fact that $rank(2I + A) = k$, the system (4.28) has only the trivial solution. Therefore $r_1 = r_2 = \cdots = r_k = 0$, which implies that $a_1 = a_2 = \cdots = a_k = 0$. Recall $2\alpha = 2\beta + \sum_{j=1}^{k} \gamma_j a_j$, then we get $2\alpha = 2\beta$, since p is odd, it follows that $\alpha = \beta$. Hence the polynomial $F(x)$ is a permutation polynomial if $rank(I + A) = k$.

Conversely, assume that $g(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$. In order to show that $rank(2I + A) = k$, suppose $(r_1, r_2, \ldots, r_k)^T \in \mathbf{F}_q^k$ is a solution of the system (4.28) of linear equations, it follows that (4.27) is satisfied. Replace r_j by $\frac{1}{2}a_j$ for $1 \le j \le k$, and using the equivalence of (4.27) and (4.24), then we have

$$2\beta + \sum_{j=1}^{k} \gamma_j a_j + \sum_{j=1}^{k} \gamma_j f_j(\beta + \frac{1}{2} \sum_{j=1}^{k} \gamma_j a_j) = 2\beta + \sum_{j=1}^{k} \gamma_j f_j(\beta),$$

where $\beta \in \mathbf{F}_{q^m}$. Setting

$$2\alpha := 2\beta + \sum_{j=1}^{k} \gamma_j a_j, \tag{4.29}$$

we get

$$2\alpha + \sum_{j=1}^{k} \gamma_j f_j(\alpha) = 2\beta + \sum_{j=1}^{k} \gamma_j f_j(\beta), \tag{4.30}$$

that is, $F(\alpha) = F(\beta)$. Since $F(x)$ is a permutation polynomial, we get $\alpha = \beta$. From (4.29) it follows that $\sum_{j=1}^{k} \gamma_j a_j = 0$. From the hypothesis $\gamma_1, \ldots, \gamma_k$ are linearly independent over $\mathbf{F}_q$, which implies $a_1 = a_2 = \cdots = a_k = 0$, it follows that $r_1 = r_2 = \cdots = r_k = 0$, that is $(r_1, r_2, \ldots, r_k)^T = (0, 0, \ldots, 0)^T$. Therefore the system of linear equations (4.28) has only the trivial solutions. Thus $rank(2I + A) = k$.

Therefore from Theorem 4.1.8, $F(x) = x + \sum_{j=1}^{k} \gamma_j f_j(x)$ is a complete permutation polynomial of $\mathbf{F}_{q^m}$ if and only if $rank(I + A) = k$ and $rank(2I + A) = k$, as desired. □

4.2 Permutation polynomials of the form $L(x) + \sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x))$.

Theorem 4.2.1 *Let l and k be positive integers with $l \leq k$. Let $L(x) \in \mathbf{F}_{q^m}[x]$ be a linearized polynomial such that $dim(Ker(L)) = k$ and $Ker(L) \cap Im(L) = \{0\}$. Let $\gamma_1, ..., \gamma_l \in Ker(L)$ be linearly independent over $\mathbf{F}_q$ and $h_1(x), ..., h_l(x) \in \mathbf{F}_{q^m}[x]$. Then $F(x) := L(x) + \sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x))$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if there exists an integer i with $1 \leq i \leq l$ such that $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x + \upsilon) - h_i(x)) \neq 0$ for any $x \in \mathbf{F}_{q^m}$ and any $\upsilon \in Ker(L) \setminus \{0\}$.*

Proof. Suppose that there exists an integer i with $1 \leq i \leq l$ such that $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x + \varepsilon) - h_i(x)) \neq 0$ for any $x \in \mathbf{F}_{q^m}$ and any $\varepsilon \in Ker(L) \setminus \{0\}$. Choose arbitrary elements α and β such that $F(\alpha) = F(\beta)$, then

$$L(\alpha) + \sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(\alpha)) = L(\beta) + \sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(\beta)).$$

Since $L(x)$ and $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)$ are linearized polynomials, the equation above is equivalent to

$$L(\alpha - \beta) = \sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(\beta) - h_i(\alpha)), \tag{4.31}$$

thus

$$\sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(\beta) - h_i(\alpha)) \in Im(L)$$

However, note that $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(\beta) - h_i(\alpha)) \in \mathbf{F}_q$ and since $\gamma_i \in Ker(L)$ for $1 \leq i \leq l$, we get

$$L(\sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(\beta) - h_i(\alpha))) = \sum_{i=1}^{l} Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(\beta) - h_i(\alpha))L(\gamma_i) = 0,$$

hence $\sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(\beta) - h_i(\alpha)) \in Ker(L)$ for $1 \leq i \leq l$. But from the hypothesis $Ker(L) \cap Im(L) = \{0\}$ it follows that

$$\sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(\beta) - h_i(\alpha)) = 0. \tag{4.32}$$

We can conclude from (4.31) and (4.32) that $L(\alpha - \beta) = 0$, hence $\alpha - \beta \in Ker(L)$. Therefore there exist $\upsilon \in Ker(L)$ such that $\alpha = \beta + \upsilon$.

Claim: The element $\upsilon \in Ker(L)$ is 0.

Proof the claim: Assume that $\upsilon \neq 0$. Since $\gamma_1, \ldots, \gamma_l$ are linearly independent over $\mathbf{F}_q$, then it follows from (4.32) that $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_j(\beta) - h_j(\alpha)) = 0$ for all $1 \leq j \leq l$, which implies $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_j(\beta + \upsilon) - h_j(\beta)) = 0$ since $\alpha = \beta + \upsilon$. But from the hypothesis, there exist i_0 with $1 \leq i_0 \leq l$ such that $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_{i_0}(x + \upsilon) - h_{i_0}(x)) \neq 0$, let $x = \beta$, then $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_{i_0}(\beta + \upsilon) - h_{i_0}(\beta)) \neq 0$, for some $1 \leq i_0 \leq l$, this gives a contradiction. Thus $\upsilon = 0$. Now, since $\upsilon = 0$, we get $\alpha = \beta$, therefore $F(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$.

Conversely, suppose that $F(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$. Let $x \in \mathbf{F}_{q^m}$ and $\upsilon \in Ker(L) \setminus \{0\}$, then

$$\begin{aligned} F(x+\upsilon) - F(x) =& L(x+\upsilon) + \sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x+\upsilon)) - L(x) + \sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x)) \\ =& \sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x+\upsilon) - h_i(x)) \end{aligned} \tag{4.33}$$

Since $\upsilon \neq 0$, and $F(x)$ is a permutation polynomial, it follows from (4.33) that

$$\sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x+\upsilon) - h_i(x)) \neq 0.$$

Thus there exists an integer i with $1 \leq i \leq l$ such that $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x + \upsilon) - h_i(x)) \neq 0$ for any $x \in \mathbf{F}_{q^m}$ and any $\upsilon \in Ker(L) \setminus \{0\}$. □

Corollary 4.2.2 *Let l and $m \geq 2$ be positive integers with $gcd(p, m) = 1$ and $l < m$. Let $\gamma_1, ..., \gamma_l \in \mathbf{F}_{q^m} \setminus \mathbf{F}_q$ be linearly independent over $\mathbf{F}_q$ and $h_1(x), ..., h_l(x) \in \mathbf{F}_{q^m}[x]$. Then $F(x) := Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) + \sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x))$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if there exists an integer i with $1 \leq i \leq l$ such that $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(h_i(x+\varepsilon) - h_i(x)) \neq 0$ for any $x \in \mathbf{F}_{q^m}$ and any $\varepsilon \in \mathbf{F}_{q^m} \setminus \mathbf{F}_q$.*

Proof. We will apply Theorem 4.2.1 by setting the linearized polynomial $L(x) = Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)$. Since $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q} : \mathbf{F}_{q^m} \to \mathbf{F}_q$ is surjective, $Im(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}) = \mathbf{F}_q$. Let $s \in Ker(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}) \cap \mathbf{F}_q$, then $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(s) = 0$ and $Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}(s) = ms$, hence $ms = 0$, but $gcd(p, m) = 1$ this implies $s = 0$, therefore $Ker(L) \cap Im(L) = Ker(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}) \cap \mathbf{F}_q = \{0\}$, and hence $Ker(Tr_{\mathbf{F}_{q^m}/\mathbf{F}_q}) = \mathbf{F}_{q^m} \setminus \mathbf{F}_q^*$. Then the Corollary follows immediately from Theorem 4.2.1. □

Corollary 4.2.3 *Let p be an odd prime , l and k be positive integers with $l \leq k$. Let $\{\gamma_1, ..., \gamma_k\}$ be a basis of $\mathbf{F}_{q^k}$ over $\mathbf{F}_q$ and $h_1(x), ..., h_l(x) \in \mathbf{F}_{q^{2k}}[x]$. Then $F(x) := x - x^{q^k} + \sum_{i=1}^{l} \gamma_i Tr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(h_i(x))$ is a permutation polynomial of $\mathbf{F}_{q^{2k}}$ if and only if there exists an integer i with $1 \leq i \leq l$ such that $Tr_{\mathbf{F}_{q^{2k}}/\mathbf{F}_q}(h_i(x+\varepsilon) - h_i(x)) \neq 0$ for any $x \in \mathbf{F}_{q^{2k}}$ and any $\varepsilon \in \mathbf{F}_{q^k}^*$.*

Proof. Let $m = 2k$, and $L(x) = x - x^{q^k}$ be a linearized polynomial over $\mathbf{F}_{q^{2k}}$, then as in the proof of Corollary 4.1.3 it follows that $Ker(x - x^{q^k}) = \mathbf{F}_{q^k}$, and $Ker(x - x^{q^k}) \cap Im(x - x^{q^k}) = \{0\}$, the desired result follows from Theorem 4.2.1. □

CHAPTER 5

ON ONE CLASS OF PERMUTATION POLYNOMIALS OVER FINITE FIELDS OF CHARACTERISTIC TWO

In this paper the authors classified all permutation polynomials of type

$$x^{1+\frac{q^4-1}{q-1}} + bx$$

over the field $\mathbf{F}_{q^4}$, where $q = 2^m, m \geq 2$.

In particular, for odd m, such polynomials were considered in the paper [13], were the anthers proved the following theorem (the proof is based on the Dickson polynomials).

Theorem 5.0.4 *[13] Let $q = 2^m, m \geq 3$ is odd . A polynomial of the type*

$$f(x) = x^{1+\frac{q^4-1}{q-1}} + bx \tag{5.1}$$

over $\mathbf{F}_{q^4}$ is a P.P over $\mathbf{F}_{q^4}$ if the element b looks as follows:

$$\left.\begin{aligned} 1)\ b &= u(1+\beta+\beta^2) + v\beta^3; \\ 2)\ b &= u(1+\beta+\beta^3) + v(\beta+\beta^2) \\ 3)\ b &= u(1+\beta^3) + v(1+\beta+\beta^2); \\ 4)\ b &= u(\beta+\beta^3) + v(\beta^2+\beta^3), \end{aligned}\right\} \tag{5.2}$$

where u, v run through $\mathbf{F}_q, (u, v) \neq (0, 0)$, and where β is a root of $x^4 + x + 1$.

Remark 5.0.5 *The proof of this theorem in [13] depends on the following fact that is for $b \in \boldsymbol{F}_{q^s} \setminus \boldsymbol{F}_q,\ d = \frac{q^s-1}{q-1} + 1$, where s is a positive integer and $gcd(d-1, q-1) =$*

$gcd(s, q-1) = 1$, then the polynomial $x^d + bx \in \boldsymbol{F}_{q^s}[x]$ is a permutation polynomial over $\boldsymbol{F}_{q^s}$ if and only if $h_b(y) \in \boldsymbol{F}_q$ is a permutation polynomial over $\boldsymbol{F}_q$, where $h_b(y)$ is defined as

$$h_b(y) = y\sum_{i=0}^{s} \lambda_i y^{s-i},$$

where $\lambda_0 = 1$, and $\lambda_i = \sum_{0\le j_1<j_2<\cdots<j_i\le s-1} b_{j_1}b_{j_2}\dots b_{j_i}$ for $1 \le i \le s$, and $b_i = b^{q^i}$. The idea of the proof is to reach $h_b(y)$ in some conditions of b, when $s = 4$, to the Dickson polynomial $D_5(y, \lambda_2)$, and verify that all $b's$ listed in Theorem 5.0.4 satisfy the conditions. Since $D_5(y, \lambda_2)$ is a permutation polynomial over $\boldsymbol{F}_q$ due to Theorem 2.0.45, then so $h_b(y)$. By the fact, this implies that for $b's$ in Theorem 5.0.4 the polynomial $x^d + bx \in \boldsymbol{F}_{q^4}[x]$ is a permutation polynomial over $\boldsymbol{F}_{q^4}$, where $d = \frac{q^4-1}{q-1} + 1$, as illustrated.

In this paper the proof is different, it depends on a following lemma from [9]. However in [13] , it was not proved that there do not exist other elements b for which polynomials $x^{1+\frac{q^4-1}{q-1}} + bx$ are permutation polynomials. In this paper, the authors fill this gap and prove , firstly, these sufficient conditions are also necessary ; secondly, these sufficient and necessary conditions are fulfilled only for b satisfying (5.2) ; and thirdly , permutation polynomials in the form $x^{1+\frac{q^4-1}{q-1}} + bx$ do not exist for the even integers $m \geq 4$ but for $m = 2$ such polynomials exist.

In this chapter we need the following result from [9].

Lemma 5.0.6 *[9] The polynomial*

$$f(x) = x^{1+\frac{q-1}{n}} + bx, \quad n \mid (q-1), n > 1,$$

over $\boldsymbol{F}_q$ is a permutation polynomial if and only if the following conditions are satisfied:

1. *the element b is such that $(-b)^n \neq 1$;*
2. *the inequality*

$$\left(\left(b + w^i\right)\left(b + w^j\right)^{-1}\right)^{\frac{q-1}{n}} \neq w^{j-i} \tag{5.3}$$

holds for all i, j such that $0 \leq i < j < n$, *where w is a fixed primitive root of the nth degree of* 1 *in the field* $\boldsymbol{F}_q$.

Proof.

We will first prove that the conditions in the Lemma are sufficient. Let $f(x) = x^{1+\frac{q-1}{n}} + bx,\ \ n \mid (q-1), n > 1$, assuming that $((b+w^i)(b+w^j)^{-1})^{\frac{q-1}{n}} \neq w^{j-i}$ and $(-b)^n \neq 1$. Here w is a fixed primitive nth root of unity in the field $\mathbf{F}_q$, that is $w^n = 1$.
Assume that $f(c) = 0$, for some $c \in \mathbf{F}_q^*$, then for some $0 \leq i \leq n$ we have

$$0 = bc + c^{\frac{q+n-1}{n}} = (b + c^{\frac{q-1}{n}})c = (b + w^i)c.$$

Now $(-b)^n \neq 1$ means that $-b$ is not an n-th root of unity which implies that $b + w^i \neq 0$ for any $0 \leq i \leq n$, hence $c = 0$, a contradiction. Now take two elements $c_1, c_2 \in \mathbf{F}_q^*$ such that $f(c_1) = f(c_2)$, then $(b + c_1^{\frac{q-1}{n}})c_1 = (b + c_2^{\frac{q-1}{n}})c_2$, thus for some $0 \leq i, j < n$ we have $(b + w^i)c_1 = (b + w^j)c_2$. Without loss of generality we may assume $i \leq j$. Thus $(b + w^i)(b + w^j)^{-1} = c_2 c_1^{-1}$, hence $((b + w^i)(b + w^j)^{-1})^{\frac{q-1}{n}} = c_2^{\frac{q-1}{n}}(c_1^{-1})^{\frac{q-1}{n}} = w^{j-i}$, which is a contradiction unless $i = j$. In this case $c_2 c_1^{-1} = (b + w^i)(b + w^j)^{-1} = 1$, thus $c_1 = c_2$. Therefore $f(x)$ is a permutation polynomial over $\mathbf{F}_q$.

Next, we will show that the conditions are necessary . Assume that $f(x)$ is permutation polynomial. Assume $(-b)^n = 1$, which means that $-b$ is one of the n-th roots of unity in the field $\mathbf{F}_q$, so $b + w^i = 0$ for some $0 \leq i < n$. Let $c \in \mathbf{F}_q$ such that $c^{\frac{q-1}{n}} = w^i$, then $c \neq 0$, and $f(c) = c(c^{\frac{q-1}{n}} + b) = c(w^i + b) = 0 = f(0)$, which contradicts with the fact that $f(x)$ is a permutation polynomial over $\mathbf{F}_q$. Hence $(-b)^n \neq 1$. Suppose that $((b + w^i)(b + w^j)^{-1})^{\frac{q-1}{n}} = w^{j-i}$ for some $0 \leq i, j < n$. Let $a = (b + w^i)(b + w^j)^{-1}$, and let $d \in \mathbf{F}_q^*$ such that $d^{\frac{q-1}{n}} = w^j$. Then $(b + w^i)(b + w^j)^{-1} = a = dd^{-1}a$. Thus $(da^{-1})^{\frac{q-1}{n}} = (d(b + w^i)^{-1}(b + w^j))^{\frac{q-1}{n}} = d^{\frac{q-1}{n}}.w^{i-j} = w^j w^{i-j} = w^i$. On the other hand $(b + w^i)da^{-1} = (b + w^j)d$, and since $(da^{-1})^{\frac{q-1}{n}} = w^i$, we get $f(da^{-1}) = f(d)$, thus $f(x)$ fails to be a permutation polynomial over $\mathbf{F}_q$ since $a \neq 1$. Hence $((b + w^i)(b + w^j)^{-1})^{\frac{q-1}{n}} \neq w^{j-i}$ for some $0 \leq i, j < n$.

□

5.1 Polynomials of the form $x^{1+\frac{q^4-1}{q-1}} + bx$, $q = 2^m$, $m \geq 2$

Lemma 5.1.1 *The polynomial*

$$f(x) = x^{1+\frac{q^4-1}{q-1}} + bx$$

over $\mathbf{F}_{q^4}$ *is a* permutation polynomial *if and only if* $b \in \mathbf{F}_{q^4} \setminus \mathbf{F}_q$ *and the following inequality:*

$$x(b+x)^{q^3+q^2+q+1} \neq y(b+y)^{q^3+q^2+q+1} \tag{5.4}$$

holds for all $x, y \in \mathbf{F}_q$ *, such that* $x \neq 0, y \neq 0, x \neq y$ *.*

Proof. Consider the field $\mathbf{F}_{q^4}$ and set $n = q-1$. Then the condition $(-b)^n \neq 1$ of lemma 5.0.6 implies that $b^{q-1} \neq 1$, i.e., $b \in \mathbf{F}_{q^4} \setminus \mathbf{F}_q$. Set $x = w^i$ and $y = w^j$, and then inequality (5.3) becomes the following inequality:

$$\left((b+x)(b+y)^{-1}\right)^{\frac{q^4-1}{q-1}} \neq yx^{-1}$$

or equivalently

$$x(b+x)^{q^3+q^2+q+1} \neq y(b+y)^{q^3+q^2+q+1}$$

for all $x, y \in \mathbf{F}_q$, such that $x \neq 0, y \neq 0, x \neq y$. □

Remark 5.1.2 *By lemma 5.1.1 the polynomial* $x^{1+\frac{q^4-1}{q-1}} + bx$ *is a permutation polynomial if and only if* $b \in \mathbf{F}_{q^4} \setminus \mathbf{F}_q$ *and the equation over* $\boldsymbol{F}_q$

$$x(b+x)^{q^3+q^2+q+1} + y(b+y)^{q^3+q^2+q+1} = 0 \tag{5.5}$$

has no solutions $x, y \in \boldsymbol{F}_q, x \neq 0, y \neq 0, x \neq y$*. By direct calculations equation(5.5) is equivalent to*

$$\begin{aligned}
&b^{1+q+q^2+q^3}(x+y) + (b^{1+q+q^2} + b^{1+q+q^3} + b^{1+q^2+q^3} + b^{q+q^2+q^3})(x^2+y^2)+ \\
&(b^{1+q} + b^{1+q^2} + b^{1+q^3} + b^{q+q^2} + b^{q+q^3} + b^{q^2+q^3})(x^3+y^3)+ \\
&(b + b^q + b^{q^2} + b^{q^3})(x^4+y^4) + x^5 + y^5 = 0.
\end{aligned} \tag{5.6}$$

Now let $z = x + y$ *and*

$$\left.\begin{aligned}
B_1 &= b + b^q + b^{q^2} + b^{q^3}, \\
B_2 &= b^{1+q} + b^{1+q^2} + b^{1+q^3} + b^{q+q^2} + b^{q+q^3} + b^{q^2+q^3}, \\
B_3 &= b^{1+q+q^2} + b^{1+q+q^3} + b^{1+q^2+q^3} + b^{q+q^2+q^3}, \\
B_4 &= b^{1+q+q^2+q^3}.
\end{aligned}\right\} \tag{5.7}$$

by substituting z and the expressions (5.7) in (5.6), equation (5.6) reduces to the following equation over x and z:

$$z(x^4 + B_2x^2 + (z^3 + B_2z)x + z^4 + B_1z^3 + B_2z^2 + B_3z + B_4) = 0. \tag{5.8}$$

Hence, using lemma 5.1.1 instead of (5.4) one can write

$$z(x^4 + B_2x^2 + (z^3 + B_2z)x + z^4 + B_1z^3 + B_2z^2 + B_3z + B_4) = 0$$

has no solutions $x, y \in \mathbf{F}_q, x \neq 0, y \neq 0, x \neq y$, which implies that either $z = 0$ or $x^4 + B_2x^2 + (z^3 + B_2z)x + z^4 + B_1z^3 + B_2z^2 + B_3z + B_4 = 0$, but $z = x + y$ and $x \neq 0, y \neq 0$ and $x \neq y$, so $z \neq 0$, hence

$$x^4 + B_2x^2 + (z^3 + B_2z)x + z^4 + B_1z^3 + B_2z^2 + B_3z + B_4 = 0$$

Note that the conditions $x, y \in \mathbf{F}_q, x \neq 0, y \neq 0, x \neq y$ implies that $x \neq 0$, $z \neq 0$, and more exactly to the condition $z \neq 0$ alone, as the equality $x = 0$ and and the equality $y = 0$, i.e., $z = x$ implies

$$z^4 + B_1z^3 + B_2z^2 + B_3z + B_4 = (z + b)^{q^3+q^2+q+1} = 0$$

which is impossible as $z \in \mathbf{F}_q$ and $b \in \mathbf{F}_{q^4} \setminus \mathbf{F}_q$.

Using Remark 5.1.2, lemma 5.1.1 can be written as follows:

Lemma 5.1.3 *Let $q = 2^m$. The polynomial $f(x) = x^{1+\frac{q^4-1}{q-1}} + bx$, over $\mathbf{F}_{q^4}$ is a* permutation polynomial *if and only if $b \in \mathbf{F}_{q^4} \setminus \mathbf{F}_q$ and the equation*

$$x^4 + B_2x^2 + (z^3 + B_2z)x + z^4 + B_1z^3 + B_2z^2 + B_3z + B_4 = 0 \tag{5.9}$$

has no solutions $x, z \in \mathbf{F}_q$ such that $z \neq 0$ (for $x = 0$ and $x = z$, i.e., $y = 0$, this equation has no solutions).

Substituting a new variable $w = x + B_1$ in the equation (5.9) we obtain

$$\begin{aligned}(w+B_1)^4 &+ B_2(w + B_1)^2 + (z^3 + B_2z)(w + B_1) + z^4 + B_1z^3 + B_2z^2 + B_3z + B_4\\ &= w^4 + B_1^4 + B_2w^2 + B_2B_1^2 + z^3w + z^3B_1 + B_2zw + B_2B_1z + z^4 + B_1z^3 + B_2z^2 +\\ &\quad B_3z + B_4\\ &= w^4 + B_2w^2 + (z^3 + zB_2)w + z^4 + B_2z^2 + Dz + E\end{aligned}$$

where

$$D = B_1B_2 + B_3 \quad \text{and} \quad E = B_1^4 + B_1^2B_2 + B_4. \tag{5.10}$$

Then equation(5.9) becomes:

$$w^4 + B_2w^2 + (z^3 + zB_2)w + z^4 + B_2z^2 + Dz + E = 0 \tag{5.11}$$

Now substituting $\gamma = \dfrac{w}{z}$, we get the following equation (recall that $z \neq 0$):

$$\gamma^4 + \gamma + \frac{B_2}{z^2}(\gamma^2 + \gamma + 1) + 1 + \frac{D}{z^3} + \frac{E}{z^4} = 0 \tag{5.12}$$

The cases $B_2 \neq 0$ and $B_2 = 0$ will be considered separately .

Case 1 : $B_2 \neq 0$

One can rewrite the equation (5.12) as:

$$\begin{aligned} &\gamma^4 + \gamma + \frac{B_2}{z^2}(\gamma^2 + \gamma + 1) + 1 + \frac{D}{z^3} + \frac{E}{z^4} \\ &= (\gamma^2 + \gamma + 1)^2 + (\gamma^2 + \gamma + 1)(1 + \frac{B_2}{z^2}) + 1 + \frac{D}{z^3} + \frac{E}{z^4} \end{aligned} \tag{5.13}$$

Let $\gamma^2 + \gamma + 1 = \xi$. The existence of a solution to the equation (5.12) now reduced to the existence of solutions of the following two equations :

$$\xi^2 + \xi(1 + \frac{B_2}{z^2}) + 1 + \frac{D}{z^3} + \frac{E}{z^4} = 0 \tag{5.14}$$

and

$$\gamma^2 + \gamma + 1 = \xi \tag{5.15}$$

When $z \neq \sqrt{B_2}$, dividing both sides of (5.14) by $(1 + \frac{B_2}{z^2})^2$, we get

$$\left(\frac{\xi}{(1 + \frac{B_2}{z^2})}\right)^2 + \frac{\xi}{(1 + \frac{B_2}{z^2})} + \frac{1 + \frac{D}{z^3} + \frac{E}{z^4}}{(1 + \frac{B_2}{z^2})^2} = 0$$

By using Theorem 2.0.33, we obtain that equation (5.14) has a solution if and only if

$$
\begin{aligned}
0 = Tr_q\left(\frac{1+\frac{D}{z^3}+\frac{E}{z^4}}{(1+\frac{B_2}{z^2})^2}\right) &= Tr_q\left(\frac{\frac{z^4+Dz+E}{z^4}}{\frac{(z^2+B_2)^2}{z^4}}\right) \\
&= Tr_q\left(\frac{z^4+Dz+E}{(z^2+B_2)^2}\right) = Tr_q\left(\frac{z^4+Dz+E}{(z^2+(\sqrt{B_2})^2)^2})\right) \\
&= Tr_q\left(\frac{z^4+B_2^2+B_2^2+zD+E}{z^4+B_2^2}\right) = Tr_q\left(1+\frac{B_2^2+E+zD}{z^4+B_2^2}\right) \\
&= Tr_q\left(1+\frac{B_2^2+E+zD+D\sqrt{B_2}+D\sqrt{B_2}}{z^4+B_2^2}\right) \\
&= Tr_q\left(1+\frac{B_2^2+E+D\sqrt{B_2}}{z^4+B_2^2}+\frac{D(z+\sqrt{B_2})}{z^4+B_2^2}\right) \\
&= Tr_q\left(1+\frac{B_2^2+E+D\sqrt{B_2}}{(z+\sqrt{B_2})^4}+\frac{D}{(z+\sqrt{B_2})^3}\right) \qquad (5.16)
\end{aligned}
$$

Fact: If F is a finite field with characteristic two, then every element $a \in \mathbf{F}$ is a square.

Proof the fact: Take the multiplicative group $F^* = F \setminus \{0\}$, the map $f : F^* \to F^*$ given by $f(x) = x^2$ is a group automorphism , because:

- $f(ab) = (ab)^2 = a^2b^2$ for all $a, b \in F^*$
- Assume that $f(a) = f(b)$, then $a^2 - b^2 = 0$, but the characteristic of F is 2, which implies that $(a-b)^2 = 0$, thus $a = b$.

hence F is one to one and onto. Therefore every element in F is a square (note that $0 = 0^2$).

Let $v = \frac{1}{z+\sqrt{B_2}}$ and $t = B_2^2 + E + D\sqrt{B_2}, v, t \in \mathbf{F}_q$. Since $q = 2^m$, by the fact we proved, every element in $\mathbf{F}_q$ is a square, so $t = s^2$ for some $s \in \mathbf{F}_q$, and also $s = C^2$ for some $C \in \mathbf{F}_q$, it follows that $B_2^2 + E + D\sqrt{B_2} = t = s^2 = (C^2)^2 = C^4$, then instead of (5.16) one can write:

$$
\begin{aligned}
Tr_q\left(\frac{1+\frac{D}{z^3}+\frac{E}{z^4}}{(1+\frac{B_2}{z^2})^2}\right) &= Tr_q(1+C^4v^4+Dv^3) = Tr_q(1+(Cv)^4+Dv^3) \\
&= Tr_q(1+Cv+Dv^3) = 0,
\end{aligned}
$$

(since Cv and $(Cv)^4$ are conjugates, so they have the same trace). Hence, equation (5.14) has a solution if and only if

$$Tr_q(1+Cv+Dv^3) = 0$$

where $C^4 = B_2^2 + E + D\sqrt{B_2}$ and $v = \frac{1}{z+\sqrt{B_2}}$.

The subcase (C,D)=(0,0).

For this subcase equation (5.14) becomes

$$\xi^2 + \xi\left(1 + \frac{B_2}{z^2}\right) + \left(1 + \frac{B_2}{z^2}\right)^2 = 0.$$

Proposition 5.1.4 *Let $q = 2^m$ and $m \geq 3$ be odd . Let $b \in \mathbf{F}_{q^4} \setminus \mathbf{F}_q, B_2 \neq 0$ and the following two conditions be satisfied :*

$$B_3 = B_1 B_2, \tag{5.17}$$

$$B_4 = B_1^4 + B_1^2 B_2 + B_2^2. \tag{5.18}$$

Then the polynomial $f(x) = x^{1+\frac{q^4-1}{q-1}} + bx$ is a permutation polynomial over $\mathbf{F}_{q^4}$.

Proof. Consider the following two cases for z :

- when $z \neq \sqrt{B_2}$
  $Tr_q(1 + Cv + Dv^3) = Tr_q(1) = m.1 \neq 0$, since m is odd. Hence for odd m there are no solutions for equation (5.14).
- when $z = \sqrt{B_2}$
  equation (5.14) becomes $\xi^2 = 0$, thus $\xi = 0$,
  which implies that
  $$\gamma^2 + \gamma + 1 = 0 \tag{5.19}$$
  So equation (5.12) has a solution if and only if $\gamma \in \mathbf{F}_q$ is a root of the polynomial $x^2 + x + 1$. But, since the $x^2 + x + 1$ is an irreducible polynomial over $\mathbf{F}_2$, by Lemma 2.0.26 it is remains irreducible over $\mathbf{F}_{2^m} = \mathbf{F}_q$ since m is odd. So there is no $\gamma \in \mathbf{F}_q$ such that $\gamma^2 + \gamma + 1 = 0$.
  Therefore the equations (5.14) and (5.15) have no solutions in $\mathbf{F}_q$.

□

Proposition 5.1.5 *Let $q = 2^m$ and $m \geq 2$ be even . Let $b \in \mathbf{F}_{q^4} \setminus \mathbf{F}_q, B_2 \neq 0$ and the conditions (5.17) and (5.18) be satisfied. Then the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is not a permutation polynomial over $\mathbf{F}_{q^4}$.*

Proof. Consider the two cases for z :

- When $z \neq \sqrt{B_2}$
  Equation(5.14) has a solution if and only if $Tr_q(1) = 0$, and since m is even, we have $Tr_q(1) = m.1 = 0$
  So there is no permutation polynomial when m is even and $z \neq \sqrt{B_2}$.

- When $z = \sqrt{B_2}$
  Equation(5.14) becomes $\xi^2 = 0 \implies \xi = 0$, then from equation(5.15)we get $\gamma^2 + \gamma + 1 = 0$.
  We are going to find $\gamma \in \mathbf{F}_q$ such that $\gamma^2 + \gamma + 1 = 0$.
  By Lemma 2.0.26, the irreducible polynomial x^2+x+1 over $\mathbf{F}_2$ will be reducible over $\mathbf{F}_{2^m}$ when m is even. So it has a root in $\mathbf{F}_{2^m} = \mathbf{F}_q$ since the degree of the polynomial is two.
  Hence , there is no permutation polynomial when m is even and $z = \sqrt{B_2}$.

□

The subcase $(C, D) \neq (0, 0)$**.**

Proposition 5.1.6 *Let $q = 2^m, B_2 \neq 0$ and $(C, D) \neq (0, 0)$. Then the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is* not a permutation polynomial over $\mathbf{F}_{q^4}$ *for all $m \geq 6$.*

Proof. Note that proving $x^{1+\frac{q^4-1}{q-1}} + bx$ is not permutation polynomial is equivalent to prove that the equations (5.14) and (5.15) have a solution. We already observe that equation (5.14) has a solution if and only if

$$Tr_q(1 + Cv + Dv^3) = 0$$

where $v \neq 0$ and $v \neq \frac{1}{\sqrt{B_2}}$. Now again by Theorem 2.0.33 equation (5.15) has a solution if and only if $Tr_q(\xi + 1) = 0$, which is if and only if $Tr_q(\xi) = Tr_q(1)$.

Claim: If

$$Tr_q(1 + \frac{B_2}{z^2}) = 1$$

then one of solutions of equation (5.14) will coincide with $Tr_q(1)$.

Proof the Claim: If $Tr_q(1+Cv+Dv^3) = 0$ then equation (5.14) has two solutions ξ_0 and ξ_1, the sum of these solutions is equal to the coefficient $1 + \frac{B_2}{z^2}$, that is $\xi_0 + \xi_1 = 1 + \frac{B_2}{z^2}$, thus the solutions of (5.14) are ξ_0 and $\xi_1 = \xi_0 + 1 + \frac{B_2}{z^2}$.

Recall that $Tr_q : \mathbf{F}_q \to \mathbf{F}_2$, so $Tr_q(1) = 0$ or 1, then we get:

- if $Tr_q(\xi_0) = 0$ and since $Tr_q(1 + \frac{B_2}{z^2}) = 1$ then $Tr_q(\xi_0 + 1 + \frac{B_2}{z^2}) = 1$.
- if $Tr_q(\xi_0) = 1$ and since $Tr_q(1 + \frac{B_2}{z^2}) = 1$ then $Tr_q(\xi_0 + 1 + \frac{B_2}{z^2}) = 0$.

In both cases, either $Tr_q(\xi_0) = Tr_q(1)$ or $Tr_q(\xi_0 + 1 + \frac{B_2}{z^2}) = Tr_q(1)$, which implies that $\gamma^2 + \gamma + \xi = 1$ has a solution either for $\xi = \xi_0$ or $\xi = \xi_0 + 1 + \frac{B_2}{z^2}$.

Consequently, the purpose is to prove the existence of $v, v \neq 0$ and $v \neq \frac{1}{\sqrt{B_2}}$ such that

$$Tr_q(1 + Cv + Dv^3) = 0$$

and

$$Tr_q(1 + \frac{B_2}{z^2}) = 1$$

Recall that $v = \frac{1}{z+\sqrt{B_2}}$ then $z = \frac{1}{v} + \sqrt{B_2}$, thus

$$Tr_q(1 + \frac{B_2}{z^2}) = Tr_q(1 + \frac{\sqrt{B_2}}{z}) = Tr_q(\frac{1}{1 + v\sqrt{B_2}}) = 1.$$

Define the functions $k : \mathbf{F}_q \to \mathbf{F}_q$ and $l : \mathbf{F}_q \to \mathbf{F}_q$, with

$$k(v) = 1 + Cv + Dv^3, \quad l(v) = \frac{1}{1 + v\sqrt{B_2}}, \quad \text{where} \quad l(\frac{1}{\sqrt{B_2}}) = 0,$$

and define the function $s(v) = k(v) + l(v)$. Now define the following sets for the three functions $k(v), l(v)$ and $s(v)$

$$K_0 = \{v \in \mathbf{F}_q : Tr_q(k(v)) = 0\} \quad \text{and} \quad K_1 = \{v \in \mathbf{F}_q : Tr_q(k(v)) = 1\},$$

$$L_0 = \{v \in \mathbf{F}_q : Tr_q(l(v)) = 0\} \quad \text{and} \quad L_1 = \{v \in \mathbf{F}_q : Tr_q(l(v)) = 1\},$$

$$S_0 = \{v \in \mathbf{F}_q : Tr_q(s(v)) = 0\} \quad \text{and} \quad S_1 = \{v \in \mathbf{F}_q : Tr_q(s(v)) = 1\}.$$

Since $k(0) = 1$ and $l(0) = 1$, and $Tr_q(1) = 0$ or 1, then the point $v = 0$ does not belong to the set $K_0 \cap L_1$, and $Tr_q(l(\frac{1}{\sqrt{B_2}})) = Tr_q(0) = 0$, then also the point $v = \frac{1}{\sqrt{B_2}}$ does not belong to the set $K_0 \cap L_1$, that is to reach the purpose it is enough to prove that $|K_0 \cap L_1| > 0$. Consider the canonical additive character χ_1 over the elements of a function $f(v)$ from $\mathbf{F}_q$ to $\mathbf{F}_q, q = 2^m$ defined by $\chi_1(f(v)) = (-1)^{Tr(f(v))}$ for all $v \in \mathbf{F}_q$, thus

$$\sum \chi_1(f(v)) = \sum_{v \in \mathbf{F}_q} (-1)^{Tr(f(v))} = |F_0| - |F_1| \tag{5.20}$$

where

$$F_0 = \{v \in \mathbf{F}_q : Tr_q(f(v)) = 0\} \text{ and } F_1 = \{v \in \mathbf{F}_q : Tr_q(f(v)) = 1\},$$

Recall that $|\{c \in \mathbf{F}_{2^m} : Tr_{\mathbf{F}_{2^m}/\mathbf{F}_2}(c) = 0\}| = 2^{m-1}$, and since the images of $Tr_{\mathbf{F}_{2^m}/\mathbf{F}_2}$ is $\mathbf{F}_2$ then $|\{c \in \mathbf{F}_{2^m} : Tr_{\mathbf{F}_{2^m}/\mathbf{F}_2}(c) = 1\}| = 2^{m-1}$, apply this fact for $l(v)$, we get

$$|L_0| = |L_1| = 2^{m-1} = \frac{q}{2}. \tag{5.21}$$

Now by bounds for exponential sums Theorem 2.0.50 follows that

$$|\sum \chi_1(k(v))| \leq 2\sqrt{q},$$

so $||K_0| - |K_1|| \leq 2\sqrt{q}$, which implies $|K_0| - |K_1| \geq -2\sqrt{q}$, and since $|K_0| + |K_1| = q$, then $|K_0| - q + |K_0| \geq -2\sqrt{q}$, thus

$$|K_0| \geq \frac{q}{2} - \sqrt{q}. \tag{5.22}$$

Also from bounds for exponential sums (Theorem 6,[2]) it follows that $|\sum \chi_1(s(v))| \leq 4\sqrt{q} + 1$, so $||S_0| - |S_1|| \leq 4\sqrt{q} + 1$, which implies $|S_0| - |S_1| \leq 4\sqrt{q} + 1$, and since $|S_0| + |S_1| = q$, then $|S_0| - q + |S_0| \leq 4\sqrt{q} + 1$, thus

$$|S_0| \leq \frac{4\sqrt{q} + q}{2} + \frac{1}{2}. \tag{5.23}$$

Now as

$$2|K_0 \cap L_1| + |K_0 \cap L_0| + |K_1 \cap L_1| = |K_0| + |L_1|,$$

and

$$|K_0 \cap L_0| + |K_1 \cap L_1| = |S_0|,$$

one can deduce that

$$2|K_0 \cap L_1| = |K_0| + |L_1| - |S_0|,$$

hence from the inequalities (5.21), (5.22), and (5.23) we get

$$\begin{aligned} 2|K_0 \cap L_1| &\geq \frac{q}{2} - \sqrt{q} + \frac{q}{2} - \frac{q+1}{2} - 2\sqrt{q} \\ &= \frac{q-1}{2} - 3\sqrt{q}. \end{aligned}$$

Therefore

$$\begin{aligned} |K_0 \cap L_1| &\geq \frac{q-1}{4} - \frac{3\sqrt{q}}{2} \\ &= \frac{q-1-6\sqrt{q}}{4}. \end{aligned}$$

Now we observe that $\dfrac{q-1-6\sqrt{q}}{4} > 0, q = 2^m$ holds for $m \geq 6$, which implies that for $m \geq 6, B_2 \neq 0$ and $(C, D) \neq (0, 0)$, the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is not a permutation polynomial.

□

The case $B_2 = 0$

The subcase $D \neq 0$.

Proposition 5.1.7 *Let* $q = 2^m, b \in \mathbf{F}_{q^4} \setminus \mathbf{F}_q$ *and*

$$B_2 = 0, \quad B_3 \neq 0.$$

Then the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ *is not a permutation polynomial over* $\mathbf{F}_{q^4}$ *for* $m \geq 6$.

Proof. Since $z \neq 0$ we can set $u = \frac{1}{z}$, then for $B_2 = 0$ equation (5.12) becomes,

$$f(\gamma, u) = \gamma^4 + \gamma + 1 + Du^3 + Eu^4 = 0.$$

Define a plane curve $\mathcal{P}$ over $\mathbf{F}_q$ as

$$\mathcal{P} = \{(\gamma, u) : f(\gamma, u) = \gamma^4 + \gamma + 1 + Du^3 + Eu^4 = 0\}.$$

By applying the Hasse-Wiel bound Theorem 2.0.53, the number N of $\mathbf{F}_q$-rational points of $\mathcal{P}$ given by

$$|N - q - 1| \leq 2g\sqrt{q}.$$

Since $deg(f) = 4$, from Remark 2.0.54 we have $g \leq 3$, which implies that $N \geq q - 6\sqrt{q}$. Recall that $u = \frac{1}{z} \neq 0$, and since the number of points with $u = 0$ does not exceed 4. We get that, when $q - 6\sqrt{q} > 4$ there exist an $\mathbf{F}_q$-rational point (γ, u) with $u \neq 0$ such that $f(\gamma, u) = 0$, which implies that there exists a solution $\gamma, z \in \mathbf{F}_q, z \neq 0$ for the equation (5.12). By simple calculations when $m \geq 6$ we have $q - 6\sqrt{q} > 4$. Therefore for $B_2 = 0, D \neq 0$ and $m \geq 6$ there is no permutation polynomial over $\mathbf{F}_{q^4}$ of the type $x^{1+\frac{q^4-1}{q-1}} + bx$.

□

The subcase $D = 0$.

Here it is obliged to consider the cases of odd and even m separately. First we need the following remark for the proof of the next proposition.

Remark 5.1.8 *1. Note that if $f(x) \in \mathbf{F}_{2^m}[x]$, defined as*

$$f : \mathbf{F}_{2^m} \to \mathbf{F}_{2^m}, \quad f(x) = x^4$$

then f is an automorphism of the field $\mathbf{F}_{2^m}$, because

(a) $f(a + b) = (a + b)^4 = a^4 + b^4$ for all $a, b \in \mathbf{F}_{2^m}$ since the characteristic of the field is 2.

(b) $f(ab) = (ab)^4 = a^4b^4$ for all $a, b \in \mathbf{F}_{2^m}$

(c) If $f(a) = f(b) \Longrightarrow a^4 = b^4 \Longrightarrow a^4 - b^4 = 0 \Longrightarrow (a - b)^4 = 0 \Longrightarrow a - b = 0 \Longrightarrow a = b$. Thus f is one to one and since the field is finite , it is also onto, therefore f is an automorphism of the field $\mathbf{F}_{2^m}$.

2. The polynomial $x^4 + x + 1$ is irreducible over $\boldsymbol{F}_2$, and it is remains irreducible over $\boldsymbol{F}_{2^m}$ for odd m, so there is no $\gamma \in \boldsymbol{F}_{2^m}$ such that $\gamma^4 + \gamma + 1 = 0$.

Proposition 5.1.9 *Let $q = 2^m, m \geq 3$ be odd . Let $b \in \mathbf{F}_{q^4} \setminus \mathbf{F}_q$ and*

$$B_2 = 0, \quad B_3 = 0,$$

then the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is a P.P over $\mathbf{F}_{q^4}$ if and only if $B_4 = B_1^4$.

Proof. Consider the following two cases for E :

- $E \neq 0$

  For $E \neq 0, D = 0$ and $B_2 = 0$, eq(5.12), becomes $\gamma^4 + \gamma + 1 + \frac{E}{z^4} = 0$, now since z^4 is an automorphism of the field $\mathbf{F}_{2^m}$, and for odd m, $\gamma^4 + \gamma + 1 \neq 0$ for any $\gamma \in \mathbf{F}_{2^m}$, thus for the element $\frac{\gamma^4+\gamma+1}{E}$ in $\mathbf{F}_{2^m}$, there exist $a \in \mathbf{F}_{2^m}$ such that $\frac{\gamma^4+\gamma+1}{E} = \frac{1}{a^4}$.

  Hence for any $\gamma \in \mathbf{F}_{2^m}$ there is a solution for eq(5.12), so for this case there is no such permutation polynomial.

- $E = 0$

  By previous Remark 5.1.8 number 2 , the solution of eq(5.12) does not exist,thus when $B_2 = 0$, and $D = 0$, the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is a permutation polynomial if and only if $E = 0$. Since the conditions $B_2 = 0, D = 0$, are equivalent to the conditions $B_2 = 0, B_3 = 0$, and when $E = 0$ then $B_4 = B_1^4$, the proposition is holds.

□

Remark 5.1.10 *For even m , the equation $f(x) = x^4 + x + 1$ has no solutions in $\mathbf{F}_{2^m}$ when $m \equiv 2 \ (mod 4)$, that is because the irreducible polynomial $x^4 + x + 1$ over $\boldsymbol{F}_2$ of degree 4 has a root α in the extension field $\mathbf{F}_{2^4}$ of $\mathbf{F}_2$, and moreover by Theorem 2.14 [8] all roots of $f(x)$ are in $\mathbf{F}_{2^4}$, hence all roots of $f(x)$ are in $\mathbf{F}_{2^4}$ or any extension of it. Since 4 not divides m when $m \equiv 2 \ (mod 4)$, so $\mathbf{F}_{2^4}$ is not a subfield of $\mathbf{F}_{2^m}$, therefore $f(x)$ has not any root in $\mathbf{F}_{2^m}$ when $m \equiv 2 \ (mod 4)$. However such an element b does not exist for even m by the following Lemma.*

Lemma 5.1.11 *Let $b \in \mathbf{F}_{q^4}$ where $q = 2^m$ and let B_2 and B_3 obtained from b according to (5.7). Then for even m, $B_2 = B_3 = 0$ if and only if b is an element of $\mathbf{F}_q$.*

Proof. Assume that $B_2 = B_3 = 0$. In the intermediate field $\mathbf{F}_q \subseteq \mathbf{F}_{q^2} \subseteq \mathbf{F}_{q^4}$, the polynomial $x^2 + x + \alpha$ where α is a fixed element in $\mathbf{F}_{q^2}$ such that $Tr_{q^2}(\alpha) = 1$, has no roots in $\mathbf{F}_{q^2}$ by Theorem 2.0.33 because $Tr_{q^2}(\alpha) \neq 0$, so it is irreducible polynomial over $\mathbf{F}_{q^2}$. Let δ be a root of the polynomial $x^2 + x + \alpha$, then δ will be in $\mathbf{F}_{q^4}$, thus the set $\{1, \delta\}$ is a basis of the field $\mathbf{F}_{q^4}$ as a vector space over $\mathbf{F}_{q^2}$. Therefore any element $b \in \mathbf{F}_{q^4}$ can be written in the form

$$b = r + t\delta, \ \text{ for some } r, t \in \mathbf{F}_{q^2} \ \text{ and } \ \delta^2 + \delta + \alpha = 0.$$

Denote

$$R = \alpha + \alpha^2 + \alpha^4 + \cdots + \alpha^{2^{m-1}},$$

then

$$R^q = \alpha^q + \alpha^{2q} + \alpha^{4q} + \cdots + \alpha^{2^{2m-1}},$$

it follows that

$$\begin{aligned} R + R^q &= \alpha + \alpha^2 + \alpha^4 + \cdots + \alpha^{2^{m-1}} + \alpha^{2^m} + \alpha^{2^{m+1}} + \alpha^{2^{m+2}} + \cdots + \alpha^{2^{2m-1}} \\ &= Tr_{q^2}(\alpha) = 1. \end{aligned}$$

Since $\delta^2 + \delta + \alpha = 0$, we get $\delta^2 = \delta + \alpha$, and

$$\begin{aligned} \delta^4 &= \delta^2 + \alpha^2 = \delta + \alpha + \alpha^2; \\ \delta^8 &= \delta^2 + \alpha^2 + \alpha^4 = \delta + \alpha + \alpha^2 + \alpha^4; \\ \delta^{16} &= \delta^2 + \alpha^2 + \alpha^4 + \alpha^8 = \delta + \alpha + \alpha^2 + \alpha^4 + \alpha^8; \end{aligned}$$

hence by induction we deduce that

$$\delta^{2^m} = \delta + \alpha + \alpha^2 + \alpha^4 + \cdots + \alpha^{2^{m-1}}$$

Therefore

$$\delta^q = \delta + R, \ \ \delta^{q^2} = \delta + 1, \ \ \delta^{q^3} = \delta + R + 1. \tag{5.24}$$

Rewriting B_2 and B_3 from (5.7) in terms of r and t, by using $b = r + t\delta$ and (5.24) we obtain

$$\begin{aligned} B_2 = {} & t^{q+1}(\delta^{q+1} + \delta^{q^3+1} + \delta^{q+q^2} + \delta^{q^2+q^3}) + r^2 + rt(\delta^{q^2} + \delta) + t^2\delta^{q^2+1} + r^{2q} \\ & + r^q t^q(\delta^{q^3} + \delta^q) + t^{2q}\delta^{q+q^3} \\ = {} & t^{q+1}(\delta^q(\delta + \delta^{q^2}) + \delta^{q^3}(\delta + \delta^{q^2})) + r^2 + rt(\delta + 1 + \delta) + t^2((\delta + 1)\delta) + r^{2q} \\ & + r^q t^q(\delta + R + 1 + \delta + R) + t^{2q}(\delta + R)(\delta + R + 1) \\ = {} & t^{q+1} + r^2 + rt + \alpha t^2 + r^{2q} + r^q t^q + \alpha^q t^{2q}. \end{aligned}$$

Let

$$s = r^2 + rt + \alpha t^2, \tag{5.25}$$

and by similar computation for B_3, we obtain

$$B_2 = t^{q+1} + s + s^q \ , \quad \text{and} \quad B_3 = st^q + s^q t. \tag{5.26}$$

From the condition $B_2 = 0$, we get $tB_2 = t^{q+2} + st + s^q t = 0$, and since $B_3 = 0$, then $s^q t = st^q$, which implies $t^{q+2} + st + st^q = 0$, thus

$$s(t + t^q) = t^{q+2}. \tag{5.27}$$

First, when $t + t^q = 0$, i.e, $t = t^q$ and since $B_2 = 0$, follows that $t = 0$ or $s = s^q$, if $t = 0$, then from $B_3 = 0$, we get that $s = s^q$. Hence, if $t + t^q = 0$ we have $t = 0$ and $s = s^q$, i.e, $s \in \mathbf{F}_q$, and therefore from (5.25), $r = \sqrt{s} \in \mathbf{F}_q$, thus the element $b = r + t\delta = \sqrt{s} + 0 = \sqrt{s} \in \mathbf{F}_q$.

Next, when $t + t^q \neq 0$, from the expression (5.27), one concludes that

$$s = \frac{t^{q+2}}{t + t^q}.$$

Substituting this expression for s in (5.25), we obtain a quadratic equation over r :

$$r^2 + rt + \alpha t^2 + \frac{t^{q+2}}{t + t^q} = 0. \tag{5.28}$$

By Theorem 2.0.33 this quadratic equation has a solution in $\mathbf{F}_{q^2}$ if and only if

$$Tr_{q^2}(\alpha + \frac{t^q}{t + t^q}) = 0,$$

Recall $Tr_{q^2}(\alpha) = 1$, and since $Tr_{q^2}(\alpha + \frac{t^q}{t + t^q}) = Tr_{q^2}(\alpha) + Tr_{q^2}(\frac{t^q}{t + t^q})$, then the condition is equivalent to

$$Tr_{q^2}(\frac{t^q}{t + t^q}) = 1.$$

But by transitivity property of trace we have

$$\begin{aligned} Tr_{q^2}\left(\frac{t^q}{t + t^q}\right) &= Tr_q\left(Tr_{\mathbf{F}_{q^2}/\mathbf{F}_q}\left(\frac{t^q}{t + t^q}\right)\right) \\ &= Tr_q\left(\frac{t^q}{t + t^q} + \left(\frac{t^q}{t + t^q}\right)^q\right) \\ &= Tr_q\left(\frac{t^q}{t + t^q} + \frac{t}{t + t^q}\right) \\ &= Tr_q(1) = 0 \ \text{ for even } m, \end{aligned}$$

which implies that the equation (5.28) over r, when $t + t^q \neq 0$, i.e, for any $t \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$, has no solutions in $\mathbf{F}_{q^2}$, that is when $B_2 = B_3 = 0$, we have $b \in \mathbf{F}_q$.

□

5.2 The main results

After proving Proposition 5.1.6 and Proposition 5.1.7, it remains to consider the cases when $m = 2, 3, 4$ and 5.

The direct calculations show that for $m = 4$, there are no permutation polynomials of the type $x^{1+\frac{q^4-1}{q-1}} + bx$ over $\mathbf{F}_{q^4}$ for $q = 2^4$.

But for $m = 2$ there are 48 such polynomials (for $b = \alpha^i, i = 3, 11, 37, 61, 63, 91$ and their cyclotomic classes $C_i = \{i, 2i, 2^2i, ..., 2^8i\}$ modulo $255 = 4^4 - 1$, where α is a primitive element of $\mathbf{F}_{4^4}$).

From here , Propositions 5.1.5,5.1.6,5.1.7 and Lemma 5.1.11 , the following theorem is valid.

Theorem 5.2.1 *Let $q = 2^m, m \geq 4$ be even. The polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ over $\mathbf{F}_{q^4}$ is not a permutation polynomial for any $b \in \mathbf{F}^*_{q^4}$.*

For $m = 3$ and $m = 5$, the direct calculations show that the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is a permutation polynomial over $\mathbf{F}_{q^4}$ if and only if the conditions of Proposition 5.1.4 are satisfied.

From here , Propositions 5.1.4, 5.1.6, 5.1.7 and 6.2.1, and since the conditions of Proposition 6.2.1 represent a special case of the conditions in Propositions 5.1.4, the following theorem is valid.

Theorem 5.2.2 *Let $q = 2^m$ and $m \geq 3$ be odd. The polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ over $\mathbf{F}_{q^4}$ is a permutation polynomial if and only if the following conditions are satisfied*

$$b \in \mathbf{F}_{q^4} \setminus \mathbf{F}_q, B_3 + B_1B_2 = 0 \ \textit{and} \ B_4 + B_1^4 + B_1^2B_2 + B_2^2 = 0.$$

In [13] these conditions for $B_i's$ in Theorem 5.2.2 were proved in a different way to be sufficient conditions.

For odd m, in order to find all b for which the polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is a permutation polynomial we need the following remark .

Remark 5.2.3 *Recall that the polynomial* $x^4 + x + 1$ *is irreducible over* $\boldsymbol{F}_2$, *then it remains irreducible over* $\boldsymbol{F}_{2^m}$ *when* $gcd(m, 4) = 1$. *Let* β *be a root of* $x^4 + x + 1$, *then* β *is a primitive element in* $\boldsymbol{F}_{2^4}$. *Hence as* $\boldsymbol{F}_{q^4}$ *is a finite extension of* $\boldsymbol{F}_q$ *with degree 4, the set* $\{1, \beta, \beta^2, \beta^3\}$ *present a base of* $\boldsymbol{F}_{q^4}$ *over* $\boldsymbol{F}_q$.

Therefore for the element b of $\mathbf{F}_{q^4}$, *one can present b as a polynomial of degree 3 over* $\mathbf{F}_q$ *:*

$$b = x_0 + x_1\beta + x_2\beta^2 + x_3\beta^3, \quad x_i \in \mathbf{F}_q$$

where β *is a primitive element of* $\mathbf{F}_{2^4}$, *i.e, it is a root of the polynomial* $1 + \beta + \beta^4 = 0$. *Then*

$$\begin{aligned} b^q &= x_0 + x_1\beta^q + x_2\beta^{2q} + x_3\beta^{3q}, \\ b^{q^2} &= x_0 + x_1\beta^{q^2} + x_2\beta^{2q^2} + x_3\beta^{3q^2}, \\ b^{q^3} &= x_0 + x_1\beta^{q^3} + x_2\beta^{2q^3} + x_3\beta^{3q^3}. \end{aligned}$$

Note that m is odd , then $m \equiv 1\ (mod 4)$ *or* $m \equiv 3\ (mod 4)$, *from the fact* β *is a primitive root in* $\boldsymbol{F}_{q^4}$, *i.e,* $\beta^{2^4} = 1$, *we have the following*

$$\beta^{2^m} = \begin{cases} \beta^2 & \textit{if } m \equiv 1\ (mod 4), \\ \beta^8 & \textit{if } m \equiv 3\ (mod 4), \end{cases} \qquad \beta^{2^{2m}} = \begin{cases} \beta^4 & \textit{if } m \equiv 1\ (mod 4), \\ \beta^4 & \textit{if } m \equiv 3\ (mod 4), \end{cases}$$

$$\beta^{2^{3m}} = \begin{cases} \beta^8 & \textit{if } m \equiv 1\ (mod 4). \\ \beta^2 & \textit{if } m \equiv 3\ (mod 4). \end{cases}$$

Now write B_1 *from expression (5.7) in terms of* x_i, *in both cases* $m \equiv 1\ (mod 4)$ *and* $m \equiv 3\ (mod 4)$ *we get*

$$\begin{aligned} B_1 =& 4x_0 + x_1(\beta + \beta^q + \beta^{q^2} + \beta^{q^3}) + x_2(\beta^2 + \beta^{2q} + \beta^{2q^2} + \beta^{2q^3}) + x_3(\beta^3 + \beta^{3q} + \beta^{3q^2} + \beta^{3q^3}) \\ =& x_1(\beta + \beta^2 + \beta^4 + \beta^8) + x_2(\beta^2 + \beta^4 + \beta^8 + \beta^{16}) + x_3(\beta^3 + \beta^6 + \beta^{12} + \beta^{24}). \end{aligned}$$

Recall that β is a root of $x^4 + x + 1$, then
$\beta^4 = 1 + \beta,\ \beta^6 = \beta^2 + \beta^3,$
$\beta^{12} = \beta^4 + \beta^6 = 1 + \beta + \beta^2 + \beta^3,\ \beta^{24} = 1 + \beta^2 + \beta^4 + \beta^6 = 1 + \beta^2 + 1 + \beta + \beta^2 + \beta^3 = \beta + \beta^3.$
from here follows that
$B_1 = x_3$. *By similar calculations one also gets:*

$$\begin{aligned}
&B_2 = x_0x_3 + x_1x_2 + x_3^2,\\
&B_3 = x_0^2x_3 + x_1^3 + x_1x_2x_3 + x_1x_3^2 + x_2^3 + x_2^2x_3 + x_3^3,\\
&B_4 = x_0^4 + x_0^3x_3 + x_0^2x_1x_2 + x_0^2x_3^2 + x_0x_1^3 + x_0x_1x_2x_3 + x_0x_1x_3^2 + x_0x_2^3\\
&\quad + x_0x_2^2x_3 + x_0x_3^3 + x_1^4 + x_1^2x_2x_3 + x_1x_2^3 + x_2^4 + x_2x_3^3 + x_3^4.
\end{aligned}$$

Using these expressions of B_1, B_2, B_3 and B_4 we obtain the following :
the condition $B_1B_2 = B_3$ is equivalent to the condition:

$$x_0x_3(x_0 + x_3) + x_1(x_1 + x_3)^2 + x_2^2(x_2 + x_3) = 0 \tag{5.29}$$

and the condition $B_4 = B_1^4 + B_1^2B_2 + B_2^2$ is equivalent to :

$$\begin{aligned}
&x_0^4 + x_0^3x_3 + x_0^2x_1x_2 + x_0x_1^3 + x_0x_2^3 + x_0x_2^2x_3 + x_0x_1x_3^2 +\\
&+ x_0x_1x_2x_3 + x_1^4 + x_1^2x_2^2 + x_1^2x_2x_3 + x_1x_2x_3^2 + x_1x_3^3 + x_2^4 + x_2x_3^3 = 0
\end{aligned} \tag{5.30}$$

By the following Theorem we can find all solutions to this system of equations and the number of all solutions.

Theorem 5.2.4 *All solutions of the system of two equations(5.29) and (5.30) for odd m are :*

$$\begin{array}{lll}
(x_0 = x_2, & x_1 = x_2, & x_2, x_3),\\
(x_0 = x_2 + x_3, & x_1 = x_2, & x_2, x_3),\\
(x_0 = 0, & x_1 = x_2 + x_3, & x_2, x_3),\\
(x_0 = x_3, & x_1 = x_2 + x_3, & x_2, x_3),
\end{array}$$

where x_2, x_3 run over $\boldsymbol{F}_q$ and $(x_2, x_3) \neq (0, 0)$. The number of all solutions is $2(2q + 1)(q - 1)$.

Proof. Assume that $x_3 \neq 0$ and define new variables:

$$r = \frac{x_0}{x_3},\quad ,t = \frac{x_1}{x_3},\quad a = \frac{x_2}{x_3}.$$

Rewriting the equations (5.29) and (5.30) in terms of r, t and a we get the following equations :

$$r^2 + r + t^3 + t + a^3 + a^2 = 0 \tag{5.31}$$

and

$$r^4+r^3+r^2ta+rt^3+rta+rt+ra^3+ra^2+t^4+t^2a^2+t^2a+ta^3+ta+t+a^4+a = 0, \tag{5.32}$$

respectively. Now, solving the system of the equations (5.31) and (5.32) will give us all solutions of the system of equations (5.29) and (5.30).

Multiplying equation (5.31) by r^2 and adding the result to equation (5.32) we get:

$$(r^2 + r)(t^3 + t + a^3 + a^2 + ta) + t^4 + t^2a^2 + t^2a + ta^3 + ta + t + a^4 + a = 0. \tag{5.33}$$

Substituting $r^2 + r = t^3 + t + a^3 + a^2$ in (5.33) we get the following equation in terms of t and a :

$$(t^3 + t + a^3 + a^2)(t^3 + t + a^3 + a^2 + ta) + t^4 + t^2a^2 + t^2a + ta^3 + ta + t + a^4 + a = 0$$

which is equivalent to

$$(t^2 + t + a^2 + a)(t^4 + t^3 + t^2a^2 + ta + a^4 + a^3 + a^2 + a + 1) = 0, \tag{5.34}$$

Thus we have either $t^2 + t + a^2 + a = 0$ or $t^4 + t^3 + t^2a^2 + ta + a^4 + a^3 + a^2 + a + 1 = 0.$ Hence the equations (5.31) and (5.34) can be considered as two different systems of equations. We first consider the system of the following equations:

$$\begin{aligned} &r^2 + r + t^3 + t + a^3 + a^2 = 0 \\ &t^4 + t^3 + t^2a^2 + ta + a^4 + a^3 + a^2 + a + 1 = 0. \end{aligned} \tag{5.35}$$

By applying the trace function to both equations in (5.35) we get

$$Tr_q(r^2 + r + t^3 + t + a^3 + a^2) = Tr_q(t^3 + t) + Tr_q(a^3 + a^2) = 0,$$

and from the second equation in (5.35) we get

$$\begin{aligned} &Tr_q(t^4 + t^3) + Tr_q(t^2a^2 + ta) + Tr_q(a^4 + a^3 + a^2 + a) = Tr_q(1); \\ &Tr_q(t + t^3) + Tr_q(a^3 + a^2) = Tr_q(1), \end{aligned}$$

but since m is odd, $Tr_q(1) = 1 \neq 0$, this gives a contradiction, thus the system (5.35) has no solutions. Hence all solutions for $x_3 \neq 0$, of the system of two equations (5.31) and (5.32) are the solutions of the second system.

Now consider the second system

$$\begin{aligned} &r^2 + r + t^3 + t + a^3 + a^2 = 0 \\ &t^2 + t + a^2 + a = 0, \end{aligned} \tag{5.36}$$

By solving the second equation in (5.36) for t, we get

$$(t + a)^2 + t + a = 0, \quad \text{which implies either } \ t = a \text{ or } t = a + 1,$$

and it follows from the first equation of (5.36) that:
if $t = a$, then

$$r = a \text{ or } r = a + 1,$$

if $t = a + 1$ then

$$r = 0 \text{ or } r = 1.$$

Evidently the system (5.36) has the following solutions:

$$\begin{array}{ll} (r = a, & t = a), \\ (r = a + 1, & t = a), \\ (r = 0, & t = a + 1), \\ (r = 1, & t = a + 1), \end{array} \tag{5.37}$$

which is equivalent to

$$\begin{array}{lll} (x_0 = x_2, & x_1 = x_2, & x_2, x_3), \\ (x_0 = x_2 + x_3, & x_1 = x_2, & x_2, x_3), \\ (x_0 = 0, & x_1 = x_2 + x_3, & x_2, x_3), \\ (x_0 = x_3, & x_1 = x_2 + x_3, & x_2, x_3). \end{array}$$

Moreover, the number of distinct solutions for $x_3 \neq 0$ equals $4q(q - 1)$. If $x_3 = 0$ then from equation (5.29) it follows that

$$x_1^3 + x_2^3 = 0,$$

which is equivalent to

$$(x_1 + x_2)(x_1^2 + x_1 x_2 + x_2^2) = 0,$$

therefore either $x_1 + x_2 = 0$ or $x_1^2 + x_1x_2 + x_2^2 = 0$, but if we consider the equation $x_1^2 + x_1x_2 + x_2^2 = 0$ as a quadratic equation in the variable x_1, then by Theorem 2.0.33 this equation has no solutions for any x_2 in $\mathbf{F}_{2^m}$ because $Tr_q(\frac{x_2^2}{x_2^2}) = Tr_q(1) = 1 \neq 0$ (since m is odd). Thus $x_1 + x_2 = 0$, i.e, $x_1 = x_2$. Substituting $x_3 = 0$ and $x_1 = x_2$ in (5.30) we get $x_0(x_0 + x_2) = 0$ which implies that $x_0 = 0$ or $x_0 = x_2$. Therefore all solutions when $x_3 = 0$ are the following

$$\begin{array}{lll} (x_0 = 0, & x_1 = x_2, & x_2, x_3), \\ (x_0 = x_3, & x_1 = x_2, & x_2, x_3). \end{array}$$

Moreover, the number of distinct solutions for $x_3 = 0$ equals $2(q-1)$. Therefore the number of all solutions which is the sum of the number of solutions for $x_3 \neq 0$ and for $x_3 = 0$, is equal to $4q(q-1) + 2(q-1) = 2(2q+1)(q-1)$. □

Remark 5.2.5 *All these solutions are the same with the solutions in [13], however the authers did not proved in [13] that there are no other solutions. Here in this paper the authors fill this gap and prove there are no other solutions for b foe which a polynomial $x^{1+\frac{q^4-1}{q-1}} + bx$ is a permutation polynomial over $\mathbf{F}_{q^4}$. Hence the suffecient conditions for b from Theorem 5.0.4 are also necessary. In [13] the number of their distinct solutions is given as:* $2(2q+1)(q-1)$, *which coincides with the result here.*

From the fact that the sufficient conditions for b from Theorem 5.0.4 are also necessary the following corollary is satisfied.

Corollary 5.2.6 *Let $q = 2^m$, where $m \geq 3$. The polynomial $b^{-1}x^{\frac{q^4-1}{q-1}+1}$ is a complete permutation polynomial over the field $\mathbf{F}_{q^4}$, if and only if the number m is odd and b satisfies the conditions of Theorem 5.0.4.*

Proof. The polynomial $b^{-1}x^{\frac{q^4-1}{q-1}+1}$ is a complete permutation polynomial if and only if $b^{-1}x^{\frac{q^4-1}{q-1}+1}$ and $b^{-1}x^{\frac{q^4-1}{q-1}+1} + x$ are permutation polynomials over the field $\mathbf{F}_{q^4}$. Let $d = \frac{q^4-1}{q-1} + 1 = q^3 + q^2 + q + 2$. Note that $gcd(d, \frac{q^4-1}{q-1}) = gcd(d, d-1) = 1$. By long division we have $gcd(d, q-1) = gcd(d, 2^m - 1) = gcd(2^{3m} + 2^{2m} + 2^m + 2, 2^m - 1) = gcd(5, 2^m - 1) = 1$ (since m is odd).

Hence $gcd(d, q^4 - 1) = 1$, we deduce from Theorem 2.0.42 that $b^{-1}x^{\frac{q^4-1}{q-1}+1}$ is a permutation polynomial over the field $\mathbf{F}_{q^4}$. For b satisfies the condition of Theorem 5.0.4, then by Note 2.0.41, the polynomial $b^{-1}x^{\frac{q^4-1}{q-1}+1} + x$ is a permutation polynomial over the field $\mathbf{F}_{q^4}$. Thus for such $b's$, the polynomial $b^{-1}x^{\frac{q^4-1}{q-1}+1}$ is a complete permutation polynomial over the field $\mathbf{F}_{q^4}$. □

CHAPTER 6

PERMUTATION AND COMPLETE PERMUTATION POLYNOMIALS

In this paper the authors classify all permutation polynomials of type $x^{q+2}+bx$ over the field $\mathbf{F}_{q^2}$ and of type $x^{q^2+q+2}+bx$ over $\mathbf{F}_{q^3}$, where $q = p^m > 2, p$ prime. Therefore, all cases when the polynomials $b^{-1}x^{q+2}$ over $\mathbf{F}_{q^2}$ and $b^{-1}x^{q^2+q+2}$ over $\mathbf{F}_{q^3}$ are the complete permutation polynomial are enumerated.

6.1 The case of polynomial $x^{q+2}+bx$

In this section we will consider the field $\mathbf{F}_{q^2}$, and set $n = q-1$.

Proposition 6.1.1 *The polynomial $x^{q+2}+bx$ is a permutation polynomial over the field $\boldsymbol{F}_{q^2}$ if and only if $b \in \boldsymbol{F}_{q^2} \setminus \boldsymbol{F}_q$ and the equation*

$$(x+y)^2+(x+y)(b+b^q)+b^{q+1}-xy=0, \tag{6.1}$$

has no solutions $x, y \in \boldsymbol{F}_q, x \neq 0, y \neq 0, x \neq y$.

Proof. Since the field is $\mathbf{F}_{q^2}$, and $n = q-1$, we have

$$1+\frac{q^2-1}{n}=1+\frac{q^2-1}{q-1}=1+q+1=q+2.$$

Applying Lemma5.0.6 to the polynomial $x^{q+2}+bx$ we get
The polynomial $x^{q+2}+bx$ is a permutation polynomial over the field $\mathbf{F}_{q^2}$ if and only if

1. $(-b)^n \neq 1$;

2. $((b+w^i)(b+w^j)^{-1})^{q+1} \neq w^{j-i}$ holds for all i, j, such that $0 \leq i < j < n$, where w is a fixed primitive n-th root of unity in the field $\mathbf{F}_{q^2}$.

The condition $(-b)^n \neq 1$ implies that $-b$ is not in $\mathbf{F}_q$, so $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$. For the second condition, setting $x = w^i$ and $y = w^j$, the inequality in condition (2) becomes the following

$$((b+x)(b+y)^{-1})^{q+1} \neq yx^{-1}$$

which is equivalent to

$$x(b+x)^{q+1} \neq y(b+y)^{q+1},$$

for all $x, y \in \mathbf{F}_q$, such that $x \neq 0, y \neq 0, x \neq y$. Thus the $x^{q+2} + bx$ is a permutation polynomial over the field $\mathbf{F}_{q^2}$ if and only if $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ and the equation over $\mathbf{F}_q$

$$x(b+x)^{q+1} = y(b+y)^{q+1},$$

has no solutions $x, y \in \mathbf{F}_q, x \neq 0, y \neq 0, x \neq y$. However this equation may be written as

$$x(b+x)(b+x)^q - y(b+y)(b+y)^q = 0,$$

moreover since $\text{char}(\mathbf{F}_{q^2}) = p$ and $x, y \in \mathbf{F}_q$, the equation is equivalent to

$$x(b^q+x)(b+x) - y(b^q+y)(b+y) = 0.$$

By simple calculations we get the following

$$(x^3 - y^3) + (x^2 - y^2)(b^q + b) + (x-y)b^{q+1} = 0$$

which is equivalent to

$$(x-y)(x^2 + xy + y^2 + (x+y)(b+b^q) + b^{q+1}) = 0,$$

but $x \neq y$, so conclude that

$$x^2 + xy + y^2 + (x+y)(b+b^q) + b^{q+1} = 0,$$

or equivalently

$$(x+y)^2 + (x+y)(b+b^q) + b^{q+1} - xy = 0.$$

Hence the second condition of this proposition is satisfied.

□

Now, it is more convenient to consider the cases of fields of even and odd characteristics separately.

6.1.1 Fields of even characteristic

Proposition 6.1.2 *Let $q = 2^m, m > 1$. The polynomial $x^{q+2} + bx$ is a permutation polynomial over the field $\boldsymbol{F}_{q^2}$ if and only if $b \in \boldsymbol{F}_{q^2} \setminus \boldsymbol{F}_q$ and*

$$x^2 + xz + z^2 + z(b + b^q) + b^{q+1} = 0 \tag{6.2}$$

has no solutions in the field $\boldsymbol{F}_q$ for all $z \in \boldsymbol{F}_q^*$.

Proof. Since the field has even characteristic , using the identity $xy = x^2 + x(x + y)$ and setting $x + y = z$, from Eq.(6.1) we arrive to the equation

$$x^2 + xz + z^2 + z(b + b^q) + b^{q+1} = 0.$$

Note that the conditions $x, y \in \mathbf{F}_q, x \neq y$ are equivalent to the condition $z \in \mathbf{F}_q, z \neq 0$, and when $z \in \mathbf{F}_q$, then $x \neq 0, y \neq 0$ because of

$$xy = z^2 + z(b + b^q) + b^{q+1} = (z + b)^{q+1} \neq 0$$

for $z \in \mathbf{F}_q, b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$. Hence from Proposition 6.1.1 the result is obtained. □

Theorem 6.1.3 *Let $q = 2^m, m > 1$. The polynomial $x^{q+2} + bx$ is a permutation polynomial over $\boldsymbol{F}_{q^2}$ if and only if $b \in \boldsymbol{F}_{q^2} \setminus \boldsymbol{F}_q$, the number m is odd, and $b^{3(q-1)} = 1$. The number of such different elements b is equal to $2(q - 1)$. All these elements can be written in one of the following forms:*

$$b = \alpha^{(q+1)(3t+1)/3} \quad or \quad b = \alpha^{(q+1)(3t+2)/3}, \quad t = 0, 1, \ldots, 2^m - 2,$$

where α is a primitive element of the field $\boldsymbol{F}_{q^2}$.

Proof. In the field $\mathbf{F}_q, q = 2^m$, by Theorem 2.0.33 the equation (6.2) has a solution for a fixed $z \in \mathbf{F}_q^*$ if and only if

$$Tr_q\left(\frac{z^2 + z(b + b^q) + b^{q+1}}{z^2}\right) = 0,$$

where

$$Tr_q(a) = a + a^2 + a^4 + \cdots + a^{2^{m-1}}, \quad a \in \mathbf{F}_q,$$

is the trace function from $\mathbf{F}_q$ into $\mathbf{F}_2$. We have

$$\frac{z^2 + z(b + b^q) + b^{q+1}}{z^2} = \frac{z^2 + z(b + b^q) + b^{q+1} + b^2 + b^2 + b^{2q} + b^{2q}}{z^2}$$
$$= 1 + \frac{b + b^q}{z} + \left(\frac{b + b^q}{z}\right)^2 + \frac{b^2 + b^{q+1} + b^{2q}}{z^2},$$

since $\frac{b + b^q}{z}$ and $\left(\frac{b + b^q}{z}\right)^2$ are conjugates in $\mathbf{F}_q$ with respect to $\mathbf{F}_2$, they have the same trace, thus

$$Tr_q\left(\frac{z^2 + z(b + b^q) + b^{q+1}}{z^2}\right) = Tr_q(1) + Tr_q\left(\frac{b^2(1 + b^{q-1} + b^{2(q-1)})}{z^2}\right).$$

If $1 + b^{q-1} + b^{2(q-1)} \neq 0$, let $c = b^2(1 + b^{q-1} + b^{2(q-1)})$ be a nonzero element, then by direct computation we observe that $c^q = c$, so $c \in \mathbf{F}_q^*$. Note that the mapping $z \mapsto z^2$ is an automorphism of the field $\mathbf{F}_q, q = 2^m$, there exists a nonzero element $z \in \mathbf{F}_q$ such that $z^2 = b^2(1 + b^{q-1} + b^{2(q-1)})$, for such z the following equality is valid

$$Tr_q\left(\frac{b^2(1 + b^{q-1} + b^{2(q-1)})}{z^2}\right) = Tr_q(1).$$

Hence

$$Tr_q\left(\frac{z^2 + z(b + b^q) + b^{q+1}}{z^2}\right) = 0.$$

Thus if $1 + b^{q-1} + b^{2(q-1)} \neq 0$, equation (6.2) has a solution in $\mathbf{F}_q^*$, we deduce that by Proposition 6.1.2 , the polynomial $x^{q+2} + bx$ is not a permutation polynomial over $\mathbf{F}_{q^2}$.

If $1 + b^{q-1} + b^{2(q-1)} = 0$, then $Tr_q\left(\frac{b^2(1 + b^{q-1} + b^{2(q-1)})}{z^2}\right) = 0$, thus the solution of equation (6.2) does not exist if and only if $Tr_q(1) = 1$, but $Tr_q(1) = m.1$, then $Tr_q(1) = 1$ if and only if m is odd. Now since

$$(b^{q-1} + 1)(1 + b^{q-1} + b^{2(q-1)}) = b^{3(q-1)} + 1,$$

if $1 + b^{q-1} + b^{2(q-1)} = 0$, then $b^{3(q-1)} + 1 = 0$, hence the polynomial $x^{q+2} + bx$ is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $b \in \mathbf{F}_{q^2} \backslash \mathbf{F}_q$, m is odd, and $b^{3(q-1)}+1 = 0$. Now let's find the possible forms of such b's.

Claim: If $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ and $b^{3(q-1)} = 1$, then b in the following form

$$b = \alpha^{(q+1)(3t+1)/3} \quad \text{or} \quad b = \alpha^{(q+1)(3t+2)/3}, \quad t = 0, 1, \ldots, 2^m - 2,$$

where α is a primitive element of the field $\mathbf{F}_{q^2}$.

proof the claim: The multiplicative group of $\mathbf{F}_{q^2}$ is cyclic. Since α is a primitive element of the field $\mathbf{F}_{q^2}$, then $\alpha^{q^2-1} = 1$. For an element b of the group, $b^{3(q-1)} = 1$ holds if and only if $b = \alpha^m$ for some $m \in \mathbf{Z}$ such that $(q^2 - 1)$ divides $3(q-1)m$, which implies that $m = \frac{(q+1)k}{3}$ for some $k \in \mathbf{Z}$. It is enough to check $k \in \mathbf{Z}$ satisfies this for k modulo 3. When $k = 1$ and $k = 2$, we get $b^{3(q-1)} = 1$, the condition is satisfy. But when $k = 3$ we get that $b^{(q-1)} = 1$, this contradicts with $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$. Therefore $b = \alpha^{\frac{q+1}{3}}$ or $b = \alpha^{\frac{2(q+1)}{3}}$.

Now we are on the position to find the possible structure of such $b's$. Let r denotes a third root of unity in $\mathbf{F}_{q^2}$ with $r \neq 1$.

Claim: $r^2 + r + 1 = 0$ if $r \neq 1$.

proof the claim: Since $r^3 = 1$ and $r \neq 1$, we have $0 = r^3 - 1 = (r-1)(r^2 + r + 1)$, which gives us $r^2 + r + 1 = 0$ when $r \neq 1$.

Let's analyze all of the b's in three cases by consider the powers $3t + 1, 3t + 2$ and $3t + 3$ where $t = 0, 1, \ldots, 2^m - 2$.

Case 1: Say b is of the form $b = \alpha^{\frac{q+1}{3}(3t+1)}$ where $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$.

Then $b^{q-1} = \alpha^{\frac{q+1}{3}(q-1)(3t+1)} = \alpha^{(q^2-1)\frac{(3t+1)}{3}} = 1^{\frac{3t+1}{3}} = 1^{\frac{1}{3}} = r \neq 1$, so

$$b^{2(q-1)} + b^{q-1} + 1 = r^2 + r + 1 = 0.$$

Thus this case will be included in the forms of b.

Case 2: Say b is of the form $b = \alpha^{\frac{q+1}{3}(3t+2)}$ where $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$.

Then $b^{q-1} = \alpha^{\frac{q+1}{3}(q-1)(3t+2)} = \alpha^{(q^2-1)\frac{(3t+2)}{3}} = 1^{\frac{3t+2}{3}} = 1^{\frac{1}{3}} = r \neq 1$, so

$$b^{2(q-1)} + b^{q-1} + 1 = r^2 + r + 1 = 0.$$

Thus also this case will be included in the forms of b.

Case 3: Say b is of the form $b = \alpha^{\frac{q+1}{3}(3t+3)}$ where $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$.

Then $b^{q-1} = \alpha^{\frac{q+1}{3}(q-1)(3t+3)} = \alpha^{(q^2-1)(t+1)} = 1$, contradicts with $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$.

Thus this case will not included in the forms of b.

Therefore all elements of $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$, such that $b^{3(q-1)} = 1$ can be written in one of the following forms

$$b = \alpha^{(q+1)(3t+1)/3} \quad \text{or} \quad b = \alpha^{(q+1)(3t+2)/3}, \quad t = 0, 1, \ldots, 2^m - 2,$$

where α is a primitive element of the field $\mathbf{F}_{q^2}$. Note that there is $2^m - 1$ elements b for each Case 1 and Case 2 , hence the number of all different elements b is equal to

$(2^m - 1) + (2^m - 1) = 2(2^m - 1) = 2(q - 1)$.

The proof of the theorem is complete. □

Corollary 6.1.4 *Let $q = 2^m$, where $m > 1$. The polynomial $b^{-1}x^{q+2}$ is a complete permutation polynomial over the field $\boldsymbol{F}_{q^2}$, if and only if the number m is odd and b satisfies the condition of Theorem(6.1.3).*

Proof. The polynomial $b^{-1}x^{q+2}$ is a complete permutation polynomial if and only if $b^{-1}x^{q+2}$ and $b^{-1}x^{q+2} + x$ are permutation polynomials over the field $\mathbf{F}_{q^2}$. Since the integers 2^m+2 and $2^{2m}-1$ are relatively prime when m is odd, i.e, $gcd(q+2, q^2-1) = 1$, we deduce from Theorem 2.0.42 that $b^{-1}x^{q+2}$ is a permutation polynomial over the field $\mathbf{F}_{q^2}$. If b satisfies the conditions of Theorem 6.1.3, the polynomial $x^{q+2} + bx$ is a permutation polynomial over the field $\mathbf{F}_{q^2}$. Which implies by Remark 2.0.41, the polynomial $b^{-1}x^{q+2} + x$ is a permutation polynomial over the field $\mathbf{F}_{q^2}$. Thus for such bs, the polynomial $b^{-1}x^{q+2}$ is a complete permutation polynomial over the field $\mathbf{F}_{q^2}$. □

6.1.2 Fields of odd characteristic

Proposition 6.1.5 *Let $q = p^m$ and $p \geq 3$ prime. The polynomial $x^{q+2} + bx$ is a permutation polynomial over $\boldsymbol{F}_{q^2}$ if and only if $b \in \boldsymbol{F}_{q^2} \setminus \boldsymbol{F}_q$ and the equation*

$$3(x + y)^2 + 4(x + y)(b + b^q) + 4b^{q+1} + (x - y)^2 = 0,$$

has no solutions $x, y \in \boldsymbol{F}_q, x \neq 0, y \neq 0, x \neq y$.

Proof. Since $q = p^m, p \geq 3$, for this case we can use the equation $4xy = (x + y)^2 - (x - y)^2$. Eq.(6.1) is equivalent to

$$4(x + y)^2 + 4(x + y)(b + b^q) + 4b^{q+1} - 4xy = 0$$

or

$$4(x + y)^2 + 4(x + y)(b + b^q) + 4b^{q+1} - (x + y)^2 + (x - y)^2 = 0,$$

which becomes

$$3(x + y)^2 + 4(x + y)(b + b^q) + 4b^{q+1} + (x - y)^2 = 0,$$

then the result comes immediately from Proposition 6.1.1 . □

Proposition 6.1.6 *Let $q = p^m$ and $p \geq 3$. The polynomial $x^{q+2} + bx$ is a permutation polynomial over $\boldsymbol{F}_{q^2}$ if and only if $b \in \boldsymbol{F}_{q^2} \setminus \boldsymbol{F}_q$ and the equation*

$$3z^2 + 4z(b + b^q) + 4b^{q+1} + u^2 = 0, \tag{6.3}$$

has no solutions $u, z \in \boldsymbol{F}_q, u \neq 0$.

Proof. Set $x + y = z, x - y = u$. Then the equality in Proposition 6.1.5

$$3(x + y)^2 + 4(x + y)(b + b^q) + 4b^{q+1} + (x - y)^2 = 0$$

is equivalent to

$$3z^2 + 4z(b + b^q) + 4b^{q+1} + u^2 = 0$$

and the conditions $x, y \in \mathbf{F}_q, x \neq 0, y \neq 0, x \neq y$ are equivalent to the conditions $u \neq 0, z, -z$, more specifically only to the condition $u \neq 0$, since when $u = \pm z$ the last equation becomes

$$z^2 + z(b + b^q) + b^{q+1} = (z + b)^{q+1} = 0$$

which is not possible since $z \in \mathbf{F}_q$ and $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$. Therefore, Proposition 6.1.5 adopted to this case will be as follows : The polynomial $x^{q+2} + bx$ is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ and the equation

$$3z^2 + 4z(b + b^q) + 4b^{q+1} + u^2 = 0,$$

has no solutions $u, z \in \mathbf{F}_q, u \neq 0$. □

We will first consider the case when $p = 3$.

Theorem 6.1.7 *Let $q = 3^m$. The polynomial $x^{q+2} + bx$ is a permutation polynomial over the field $\boldsymbol{F}_{q^2}$ if and only if $b \in \boldsymbol{F}_{q^2} \setminus \boldsymbol{F}_q$ and $b^{q-1} = -1$. The number of such different elements b equals $q - 1$, and all these elements can be presented in the following form:*

$$b = \alpha^{\frac{q+1}{2}(2t+1)}, \quad t = 0, 1, \ldots, q - 2,$$

where α is a primitive elements of the field $\boldsymbol{F}_{q^2}$.

Proof. From the fact that the characteristic of the field $\mathbf{F}_q$ is 3, that is $q = 3^m$, Eq.(6.3) becomes

$$z(b + b^q) + b^{q+1} + u^2 = 0. \tag{6.4}$$

Consider the following two cases:

- If $b+b^q \neq 0$, then for any $u \in \mathbf{F}_q, u \neq 0$, Eq(6.4) has a solution $z = \frac{-u^2-b^{q+1}}{b+b^q}$, hence by Proposition 6.1.6, the polynomial $x^{q+2} + bx$ is not a permutation polynomial over $\mathbf{F}_{q^2}$ in this case.
- If $b + b^q = 0$, then $b^q = -b$ and $b^{q+1} = -b^2$, Eq.(6.4) implies that $u^2 - b^2 = 0$, thus $(u - b)(u + b) = 0$, which implies $u = \pm b$, but this impossible for $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ and $u \in \mathbf{F}_q$, so Eq.(6.4) has no solutions, therefore by Proposition 6.1.6 the polynomial $x^{q+2} + bx$ is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ and $b^{q-1} = -1$.

Now let's find the possible structure of b with $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q, b^{q-1} = -1$. let α be a primitive element of the field $\mathbf{F}_{q^2}$, then $ord(\alpha) = q^2 - 1$. Note that $q^2 - 1$ is an even integer , then one has $\alpha^{\frac{q^2-1}{2}} = -1$. For an element b of the multiplicative group of $\mathbf{F}_{q^2}$, $b^{q-1} = -1$ so $b^{2(q-1)} = 1$ holds if and only if $b = \alpha^m$ for some $m \in \mathbf{Z}$ such that $(q^2 - 1)$ divides $2(q-1)m$, thus $m = \frac{(q+1)k}{2}$ for some $k \in \mathbf{Z}$. It is enough to check $k \in \mathbf{Z}$ satisfies this for k modulo 2. When $k = 1$, we get $b = \alpha^{\frac{(q+1)}{2}}$, and $b^{q-1} = -1$, the condition for b is satisfy. But when $k = 2, b = \alpha^{q+1}$ implies that $b^{q-1} = 1 \neq -1$, the condition for b fails for $k = 2$. Therefore $b = \alpha^{\frac{q+1}{2}}$.

Let's analyze all of the b's in two cases by consider the powers $2t+1$, and $2t+2$ where $t = 0, 1, \ldots, q-2$.

Case 1: If $b = \alpha^{\frac{q+1}{2}(2t+1)}, t = 0, 1, \ldots, q-2$, then $b^{q-1} = \alpha^{\frac{q+1}{2}(q-1)(2t+1)} = (-1)^{2t+1} = -1$. Thus this case included in the form of b because $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$, and $b^{q-1} = -1.$, Case 2: If $b = \alpha^{\frac{q+1}{2}(2t+2)}, t = 0, 1, \ldots, q-2$, then $b^{q-1} = \alpha^{(q+1)(q-1)(t+1)} = 1$, this implies that $b \in \mathbf{F}_q$. this case will not be included in the forms of b.

Hence all elements of b such that $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$, and $b^{q-1} = -1$, can be presented in the form:

$$b = \alpha^{\frac{q+1}{2}(2t+1)}, \quad t = 0, 1, \ldots, q-2,$$

where α is a primitive element of the field $\mathbf{F}_{q^2}$. Therefore the number of distinct elements b is $q-1$.
The proof of the theorem is complete.

□

Corollary 6.1.8 *Let $q = 3^m$. The polynomial $b^{-1}x^{q+2}$ is a complete permutation polynomial over the field $\boldsymbol{F}_{q^2}$ if and only if b satisfies the condition of Theorem6.1.7.*

Proof. The polynomial $b^{-1}x^{q+2}$ is a complete permutation polynomial over the field $\mathbf{F}_{q^2}$ if and only if $b^{-1}x^{q+2}$ and $b^{-1}x^{q+2} + x$ are permutation polynomials over the field $\mathbf{F}_{q^2}$. Since the integers 3^m+2 and $3^{2m}-1$ are mutually prime, i.e, $gcd(q+2, q^2-1) = 1$, then by Theorem 2.0.42 the polynomial $b^{-1}x^{q+2}$ is a permutation polynomial over $\mathbf{F}_{q^2}$. If b satisfies the conditions of Theorem 6.1.7, the polynomial $x^{q+2}+bx$ is a permutation polynomial over the field $\mathbf{F}_{q^2}$. Which implies by Remark 2.0.41, $b^{-1}x^{q+2} + x$ is a permutation polynomial over $\mathbf{F}_{q^2}$. Hence for such $b's$, the polynomial $b^{-1}x^{q+2}$ is a complete permutation polynomial over the field $\mathbf{F}_{q^2}$. □

Next, we will consider the case when $p > 3$.

Proposition 6.1.9 *Let $q = p^m$ and $p > 3$. The polynomial $x^{q+2} + bx$ is a permutation polynomial over $\boldsymbol{F}_{q^2}$ if and only if $b \in \boldsymbol{F}_{q^2} \setminus \boldsymbol{F}_q$ and the equation*

$$4b^2 - 4b^{q+1} + 4b^{2q} - 3u^2 = v^2 \tag{6.5}$$

has no solutions $u, v \in \boldsymbol{F}_q, u \neq 0$.

Proof. For the case $p > 3$, taking into account that the discriminant of the quadratic equation (6.3) over z is equal to

$$\begin{aligned}\Delta = 4^2(b + b^q)^2 - 4.3(4b^{q+1} + u^2) &= 4(4b^2 + 4b^{2q} + 8b^{q+1} - 12b^{q+1} - 3u^2)\\ &= 4(4b^2 + 4b^{2q} - 4b^{q+1} - 3u^2)\\ &= 2^2(4b^2 - 4b^{q+1} + 4b^{2q} - 3u^2)\end{aligned}$$

Eq.(6.3) in Proposition 6.1.6 has no solution if and only if the discriminant Δ of the equation is not a square in $\mathbf{F}_q$, i.e. if and only if $4b^2 - 4b^{q+1} + 4b^{2q} - 3u^2 = v^2$ has no solutions $u, v \in \mathbf{F}_q, u \neq 0$, which completes the proof. □

Before giving the next theorem we need the following definitions and lemma .

Definition 6.1.10 *[8] Let q be odd and let η be the real valued function on $\boldsymbol{F}_q^*$ with*

$$\eta(c) = \begin{cases} 1 & \textit{if } c \textit{ is the square of an element of } \boldsymbol{F}_q^* \\ -1 & \textit{otherwise} \end{cases}$$

Then η is a multiplicative character of $\boldsymbol{F}_q$, and it is called the quadratic character of $\mathbf{F}_q$.

Definition 6.1.11 *[8] For any finite field $\boldsymbol{F}_q$ the integer-valued function v on $\boldsymbol{F}_q$ is defined by $v(b) = -1$ for $b \in \boldsymbol{F}_q^*$ and $v(0) = q - 1$.*

Lemma 6.1.12 *[8] For odd q, let $a \in \boldsymbol{F}_q$, $\alpha, \beta \in \boldsymbol{F}_q^*$, and η be the quadratic character of $\boldsymbol{F}_q$. Then*

$$N(\alpha x_1^2 + \beta x_2^2 = a) = q + v(a)\eta(-\alpha\beta).$$

where $N(\alpha x_1^2 + \beta x_2^2 = a)$ denotes the number of solutions of the indicated equation in $\boldsymbol{F}_q^2$.

Theorem 6.1.13 *Let $q = p^m$ and $p > 3$. The polynomial $x^{q+2} + bx$ is a permutation polynomial over the field $\boldsymbol{F}_{q^2}$ if and only if $b \in \boldsymbol{F}_{q^2} \setminus \boldsymbol{F}_q$,*

$$1 - b^{q-1} + b^{2(q-1)} = 0$$

and the equation $w^2 + 3 = 0$ has no solutions in $\boldsymbol{F}_q$.

Proof. If $4b^2 - 4b^{q+1} + 4b^{2q} \neq 0$, let $a = 4b^2 - 4b^{q+1} + 4b^{2q}$, then Eq.(6.5) has always a solution $u, v \in \mathbf{F}_q, u \neq 0$, as from lemma 6.1.12,

$$N(3u^2 + v^2 = a \neq 0) = q + v(a)\eta(-3) = \begin{cases} q - 1, & \text{if } -3 \text{ is a square in } \mathbf{F}_q \\ q + 1, & \text{otherwise} \end{cases}$$

that is the number of solutions u, v in $\mathbf{F}_q$, is not less than $q - 1$, and the number of solutions for $u = 0$ is not greater than two, so the Eq.(6.5) has at least $q - 1 - 2 = q - 3$ solutions $u, v \in \mathbf{F}_q, u \neq 0$. (note that $q - 3 > 0$, since $q = p^m, p > 3$). Therefore $x^{q+2} + bx$ is not a P.P over $\mathbf{F}_q$, in this case. If $4b^2 - 4b^{q+1} + 4b^{2q} = 0$, then Eq.(6.5) becomes

$$v^2 = -3u^2,$$

therefore this equation has a solution $u, v \in \mathbf{F}_q, u \neq 0$ if and only if $-3 = a^2$ for some $a \in \mathbf{F}_q$, i.e. if and only if the quadratic equation $w^2 + 3 = 0$ has a solution a in the field $\mathbf{F}_q$.

Hence $x^{q+2} + bx$ is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$, $1 - b^{q-1} + b^{2(q-1)} = 0$ and the equation $w^2 + 3 = 0$ has no solution in $\mathbf{F}_q$.
The proof of the theorem is complete. □

Theorem 6.1.14 *Let $q = p^m$, and $p > 3$. The polynomial $x^{q+2} + bx$ is a permutation polynomial over the field $\boldsymbol{F}_{q^2}$, if and only if $p = 6k - 1$, m is odd, and b is of the form*

$$b = \alpha^{\frac{q+1}{6}(6t+1)} \quad or \quad b = \alpha^{\frac{q+1}{6}(6t+5)}, \quad t = 0, 1, \ldots, q-2, \tag{6.6}$$

where α is a primitive element of $\boldsymbol{F}_{q^2}$.

Proof. By Theorem 6.1.13 we have the equality $1 - b^{q-1} + b^{2(q-1)} = 0$. Now since

$$1 - b^{q-1} + b^{2(q-1)} = \frac{1 + b^{3(q-1)}}{1 + b^{q-1}},$$

the equation $1 - b^{q-1} + b^{2(q-1)} = 0$ has a solution, if and only if $1 + b^{3(q-1)} = 0$ which is if and only if $b^{3(q-1)} = -1$, taking the squares of both sides we get $(b^2)^{3(q-1)} = 1$, and since $b \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$, then $b^2 \neq 1$ (because if $b^2 = 1$ and since 2 divides $q - 1$ then $b \in \mathbf{F}_q^*$). Let $b^2 = c \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$, then $ord(c) \mid 3(q-1)$ but $c \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ so also $ord(c) \mid (q^2 - 1)$. So there exist nonzero integers $t, r \in \mathbf{Z}^*$ such that $3(q-1) = ord(c) \cdot t$ (note that $gcd(3, t) = 1$ as c does not belong to $\mathbf{F}_q$) and $(q-1)(q+1) = ord(c) \cdot r$, then $ord(c) = \frac{3(q-1)}{t} = \frac{(q-1)(q+1)}{r}$, thus $q + 1 = 3 \cdot \frac{r}{t}$, since $t \mid 3r$ and $gcd(3, t) = 1$ which implies that $\frac{r}{t}$ is an integer number, hence 3 divides $q + 1$.
So we proved that $1 - b^{q-1} + b^{2(q-1)} = 0$ has a solution, if and only if 3 divides $q + 1$.

We can present the elements b where $b^{3(q-1)} = -1$ by taking a primitive element $\alpha \in \mathbf{F}_{q^2}$. For an element b of the cyclic multiplicative group $\mathbf{F}_{q^2}^*$, $b^{3(q-1)} = -1$ so $b^{6(q-1)} = 1$ holds if and only if $b = \alpha^m$ for some $m \in \mathbf{Z}$ such that $(q^2 - 1)$ divides $6(q-1)m$, which implies that $m = \frac{(q+1)k}{6}$ for some $k \in \mathbf{Z}$. It is enough to check $k \in \mathbf{Z}$ satisfies the condition of b for k modulo 6. When $k = 1$ and $k = 5$ the condition for b satisfy. But when $k = 2$ and $k = 4$ implies that $b^{3(q-1)} = 1 \neq -1$. And $k = 3$ implies $b^{q-1} = -1$, then we get $1 - b^{q-1} + b^{2(q-1)} = 3 \neq 0$ for $p > 3$. Therefore $b = \alpha^{\frac{q+1}{6}}$ or $b = \alpha^{\frac{5(q+1)}{6}}$.

Let's analyze all of the b's in sex cases by consider the powers $6t + 1, 6t + 2, 6t + 3$, $6t + 4$, $6t + 5$ and $6t + 6$ where $t = 0, 1, \ldots, q-2$.

Case 1: Say b is of the form $b = \alpha^{\frac{q+1}{6}(6t+1)}$, then $b^{3(q-1)} = (-1)^{6t+1} = -1$. Thus this case will be included in the forms of b.
Case 2: Say b is of the form $b = \alpha^{\frac{q+1}{6}(6t+2)}$, then $b^{3(q-1)} = (-1)^{6t+2} = 1$. Thus this case will not be included in the forms of b.
Case 3: Say b is of the form $b = \alpha^{\frac{q+1}{6}(6t+3)}$, then $b^{q-1} = (-1)^{2t+1} = -1$, which implies $1 - b^{q-1} + b^{2(q-1)} = 3 \neq 0$ for $p > 3$. Thus this case will not be included in the forms of b.
Case 4: Say b is of the form $b = \alpha^{\frac{q+1}{6}(6t+4)}$, then $b^{3(q-1)} = (-1)^{6t+4} = 1$. Thus this case will not be included in the forms of b.
Case 5: Say b is of the form $b = \alpha^{\frac{q+1}{6}(6t+5)}$, then $b^{3(q-1)} = (-1)^{6t+5} = -1$. Thus this case will be included in the forms of b.
Case 6: Say b is of the form $b = \alpha^{\frac{q+1}{6}(6t+6)}$, then $b^{3(q-1)} = (-1)^{6t+6} = 1$. Thus this case will not be included in the forms of b.

Note that there is $q - 1$ elements b for each Case 1 and Case 5 , hence the number of all different elements b is equal to $(q - 1) + (q - 1) = 2(q - 1)$.

Any prime number $p > 3$ has the form $p = 6k \pm 1$. Moreover the equation $w^2 + 3 = 0$ has a solution in the field $\mathbf{F}_p$ if and only if $p = 6k + 1$ (from ch.5,[12]).
We have the following two cases for m :

- If m is odd
  - If $p = 6k + 1$, the equation $w^2 + 3 = 0$ has a solution in $\mathbf{F}_q$.
  - If $p = 6k - 1$ the equation $w^2 + 3 = 0$ has no solution in $\mathbf{F}_p$, then it has no solution for every extension $\mathbf{F}_{p^m}$, where $gcd(2, m) = 1$.
- If m is even
  Let $m = 2k$, if the equation $w^2 + c = 0, c \in \mathbf{F}_{p^k}$ has no solution in $\mathbf{F}_{p^k}$ then it is irreducible, let α be a root of $w^2 + c$ in some extension field of $\mathbf{F}_{p^k}$, then since $deg(w^2 + c) = 2$, $\mathbf{F}_{p^k}(\alpha) = \mathbf{F}_{p^{2k}}$, so $\alpha \in \mathbf{F}_{p^{2k}}$. Therefore the equation $w^2 + c = 0, c \in \mathbf{F}_{p^k}$, always has a solution in the quadratic extension $\mathbf{F}_{p^{2k}}$. Then the equation $w^2 + 3 = 0$ has a solution in $\mathbf{F}_q$.

From the discussion above and by Theorem 6.1.13, the polynomial $x^{q+2} + bx$ is a P.P over $\mathbf{F}_{q^2}$, if and only if $p = 6k-1$, m is odd, and b is of the form $b = \alpha^{\frac{q+1}{6}(6t+1)}$ or $b =$

$\alpha^{\frac{q+1}{6}(6t+5)}$, $t = 0, 1, \ldots, q-2$, where α is a primitive element of $\mathbf{F}_{q^2}$, as desired.

□

When m is odd since the numbers p^m+2 and $p^{2m}-1$ are mutually prime and $p = 6k-1$, we obtain the following result.

Corollary 6.1.15 *Let $q = p^m$, and $p > 3$. The polynomial $b^{-1}x^{q+2}$ is a complete permutation polynomial over the field $\mathbf{F}_{q^2}$ if and only if $p = 6k-1$, m is odd and b satisfies the condition of Theorem 6.1.14.*

Proof. The polynomial $b^{-1}x^{q+2}$ is a complete permutation polynomial over the field $\mathbf{F}_{q^2}$ if and only if $b^{-1}x^{q+2}$ and $b^{-1}x^{q+2}+x$ are permutation polynomials over the field $\mathbf{F}_{q^2}$. Since the integers p^m+2 and $p^{2m}-1$ are mutually prime, i.e, $gcd(q+2, q^2-1) = 1$, then by Theorem 2.0.42 the polynomial $b^{-1}x^{q+2}$ is a permutation polynomial over $\mathbf{F}_{q^2}$. If $p = 6k-1$, m is odd and b satisfies the condition of Theorem 6.1.14, $x^{q+2}+bx$ is a permutation polynomial over the field $\mathbf{F}_{q^2}$. Which implies by Remark 2.0.41, the polynomial $b^{-1}x^{q+2}+x$ is a permutation polynomial over $\mathbf{F}_{q^2}$. Hence for such bs, and for $p = 6k-1$, m is odd , the polynomial $b^{-1}x^{q+2}$ is a complete permutation polynomial over the field $\mathbf{F}_{q^2}$. □

6.2 The case of polynomial $x^{q^2+q+2}+bx$

Proposition 6.2.1 *The polynomial $x^{q^2+q+2}+bx$ is a permutation polynomial over the field $\mathbf{F}_{q^3}$ if and only if $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$, and the equation*

$$(x+y)^3 - 2(x+y)xy + ((x+y)^2 - xy)B_1 + (x+y)B_2 + B_3 = 0, \qquad (6.7)$$

has no solution $x, y \in \mathbf{F}_q$, $x \neq 0$, $y \neq 0$, $x \neq y$.

Proof. Since the field is $\mathbf{F}_{q^3}$, setting $n = q-1$, we get

$$1 + \frac{q^3-1}{n} = 1 + \frac{q^3-1}{q-1} = 1 + q^2 + q + 1 = q^2 + q + 2.$$

Applying Lemma 5.0.6 in this case we get that:

The polynomial $x^{q^2+q+2}+bx$ is a permutation polynomial over the field $\mathbf{F}_{q^3}$ if and only if

1. $(-b)^n \neq 1$;

2. $((b+w^i)(b+w^j)^{-1})^{q^2+q+1} \neq w^{j-i}$ holds for all i, j, such that $0 \leq i < j < n$, where w is a fixed primitive root of the nth degree of 1 in the field $\mathbf{F}_q$.

The condition $(-b)^n \neq 1$ implies that $-b$ does not belong to $\mathbf{F}_q$, thus $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$. In order to see the second condition, we set $x = w^i$ and $y = w^j$, and then the inequality in condition (2) becomes the following

$$((b+x)(b+y)^{-1})^{q^2+q+1} \neq yx^{-1}$$

which is also equivalent to

$$x(b+x)^{q^2+q+1} \neq y(b+y)^{q^2+q+1},$$

for all $x, y \in \mathbf{F}_q$, such that $x \neq 0, y \neq 0, x \neq y$. Thus $x^{q^2+q+2} + bx$ is a permutation polynomial over the field $\mathbf{F}_{q^3}$ if and only if $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$ and the equation over $\mathbf{F}_q$

$$x(b+x)^{q^2+q+1} = y(b+y)^{q^2+q+1},$$

has no solutions $x, y \in \mathbf{F}_q, x \neq 0, y \neq 0, x \neq y$. However this equation may be written as

$$x(b+x)(b+x)^q(b+x)^{q^2} - y(b+y)(b+y)^q(b+y)^{q^2} = 0,$$

and since characteristic $\mathbf{F}_{q^3}$ is p, where $q = p^m$, and $x, y \in \mathbf{F}_q$, the equation is equivalent to

$$x(b+x)(b^q+x)(b^{q^2}+x) - y(b+y)(b^q+y)(b^{q^2}+y) = 0.$$

By simple computations this equation turns into the following

$$(x-y)b^{1+q+q^2} + (x^2-y^2)(b^{1+q} + b^{1+q^2} + b^{q+q^2}) + (x^3-y^3)(b + b^q + b^{q^2}) + x^4 - y^4 = 0.$$

Now, taking

$$B_1 = b + b^q + b^{q^2}, \quad B_2 = b^{1+q} + b^{1+q^2} + b^{q+q^2}, \quad B_3 = b^{1+q+q^2},$$

and rewriting the last equation we obtain:

$$(x-y)B_3 + (x^2-y^2)B_2 + (x^3-y^3)B_1 + x^4 - y^4 = 0;$$

which gives

$$(x-y)\left((x+y)^3 - 2(x+y)xy + \left((x+y)^2 - xy\right)B_1 + (x+y)B_2 + B_3\right) = 0,$$

but $x \neq y$, so we conclude that

$$(x+y)^3 - 2(x+y)xy + \left((x+y)^2 - xy\right)B_1 + (x+y)B_2 + B_3 = 0.$$

Hence $x^{q^2+q+2} + bx$ is a permutation polynomial over the field $\mathbf{F}_{q^3}$ if and only if $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$, and the equation $(x+y)^3 - 2(x+y)xy + ((x+y)^2 - xy)B_1 + (x+y)B_2 + B_3 = 0,$ has no solution $x, y \in \mathbf{F}_q,\ x \neq 0,\ y \neq 0,\ x \neq y$, as desired. □

6.2.1 Fields of even characteristic

Theorem 6.2.2 *Let $q = 2^m$ and $m > 1$. The polynomial $x^{q^2+q+2} + bx$ is a permutation polynomial over the field $\mathbf{F}_{q^3}$ if and only if $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$, and $b + b^q + b^{q^2} = 0$. The number of such different elements b equals $q^2 - 1$.*

Proof. To apply proposition 6.2.1, first note that, for $q = 2^m$, the identity $xy = x^2 + x(x+y)$ holds . Set $x + y = z,\ xy = u$, then equation (6.7) is equivalent to

$$uB_1 = z^3 + z^2B_1 + zB_2 + B_3, \tag{6.8}$$

with the condition $z \neq 0$ alone, because if $x, y \in \mathbf{F}_q,\ x \neq 0,\ y \neq 0$, and $x \neq y$, then $z = x + y \neq 0$ and $u \neq 0$, but form the fact that $z \in \mathbf{F}_q$ and $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$ we deduce that $u \neq 0$ (as if $u = 0$ then from (6.8) we get that

$$z^3 + z^2B_1 + zB_2 + B_3 = 0, \tag{6.9}$$

by some simple calculations we get

$$\begin{aligned} z^3 + z^2B_1 + zB_2 + B_3 &= (z+b)(z+b^q)(z+b^{q^2}) \\ &= (z+b)^{1+q+q^2} = 0 \end{aligned}$$

which implies that $z = b$, this is impossible for $z \in \mathbf{F}_q$ and $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$), therefore we have just a condition $z \neq 0$. Next, we will consider the following two cases for B_1 :

1. If $B_1 = 0$, then using the same argument as above, equation (6.8) has no solution z in $\mathbf{F}_q$ for any $u \in \mathbf{F}_q^*$. Therefore $x^{q^2+q+2} + bx$ is a permutation polynomial over $\mathbf{F}_{q^3}$ if $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$, and $B_1 = b + b^q + b^{q^2} = 0$.

2. If $B_1 \neq 0$, then equation (6.8) becomes

$$u = \frac{z^3 + z^2B_1 + zB_2 + B_3}{B_1}, \tag{6.10}$$

using the identities $x^2 + x(x+y) = xy = u$, $z = x + y$, and (6.10) follows that, $x^{q^2+q+2} + bx$ is a permutation polynomial over $\mathbf{F}_{q^3}$ if $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$ and the equation in x

$$x^2 + xz + \frac{z^3 + z^2B_1 + zB_2 + B_3}{B_1} = 0 \tag{6.11}$$

has no solution in $\mathbf{F}_q$ for any $z \in \mathbf{F}_q^*$. Considering equation (6.11) as a quadratic equation in x over $\mathbf{F}_q$, when $z \in \mathbf{F}_q^*$ is fixed, by Theorem 2.0.33 equation (6.11) has a solution in $\mathbf{F}_q$ if and only if

$$Tr_q\left(\frac{z^3 + z^2B_1 + zB_2 + B_3}{B_1z^2}\right) = 0.$$

Because

$$\begin{aligned} Tr_q\left(\frac{z^3 + z^2B_1 + zB_2 + B_3}{B_1z^2}\right) =& Tr_q\left(\frac{z}{B_1} + 1 + \frac{B_2}{B_1z} + \frac{B_3}{B_1z^2}\right) \\ =& Tr_q(1) + Tr_q\left(\frac{z}{B_1} + \frac{B_2}{B_1z} + \frac{B_2^2}{B_1^2z^2} + \frac{B_2^2 + B_1B_3}{B_1^2z^2}\right), \end{aligned}$$

and since $\frac{B_2}{B_1z}$ and $\frac{B_2^2}{B_1^2z^2}$ are conjugates in the field $\mathbf{F}_2$ they have the same trace then

$$\begin{aligned} Tr_q\left(\frac{z^3 + z^2B_1 + zB_2 + B_3}{B_1z^2}\right) =& Tr_q(1) + Tr_q\left(\frac{z^2}{B_1^2} + \frac{B_2^2 + B_1B_3}{B_1^2z^2}\right) \\ =& Tr_q(1) + Tr_q\left(v + \frac{B}{v}\right) \end{aligned}$$

where $v = \left(\frac{z}{B_1}\right)^2$, and $B = \frac{B_2^2 + B_1B_3}{B_1^4}$.

Claim: There exists $v \in \mathbf{F}_q^*$ such that $Tr_q(1) + Tr_q\left(v + \dfrac{B}{v}\right) = 0$, i.e., $Tr_q(1) = Tr_q\left(v + \dfrac{B}{v}\right)$.

Proof the claim: By using the definition of the Kloosterman sum under the canonical additive character χ and the elements 1 and B with $p = 2$ we get

$$\begin{aligned} K(\chi_1, 1, B) &= \sum_{v \in \mathbf{F}_q^*} \chi(v + Bv^{-1}) \\ &= \sum_{v \in \mathbf{F}_q^*} e^{\frac{2\pi i}{2} Tr_q(v+\frac{B}{v})} \\ &= \sum_{v \in \mathbf{F}_q^*} (-1)^{Tr_q(v+\frac{B}{v})}, \end{aligned}$$

we have the following two cases:

- If $Tr_q(1) = 0$ and $Tr_q(v + \frac{B}{v}) = 1$ for all $v \in \mathbf{F}_q$ then

  $$\begin{aligned} |K(\chi_1, 1, B)| &= |\sum_{v \in \mathbf{F}_q^*} (-1)^{Tr_q(v+\frac{B}{v})}| \\ &= q - 1, \end{aligned}$$

  but for $q \geq 8$ this contradicts with the bound that $|K(\chi_1, 1, B)| \leq 2\sqrt{q}$ (Theorem 2.0.52), because $q - 1 \geq 2\sqrt{q}$ for $q \geq 8$. hence there exist at least one $v \neq 0$ such that $Tr_q(v + \frac{B}{v}) = 0 = Tr_q(1)$.

- If $Tr_q(1) = 1$ and $Tr_q(v + \frac{B}{v}) = 0$ for all $v \in \mathbf{F}_q$ then by the same argument in the above case

  $$\begin{aligned} |K(\chi_1, 1, B)| &= |\sum_{v \in \mathbf{F}_q^*} (-1)^{Tr_q(v+\frac{B}{v})}| \\ &= q - 1. \end{aligned}$$

  But again from Theorem 2.0.52, we have $|K(\chi_1, 1, B)| \leq 2\sqrt{q}$ this is a contradiction because $q - 1 \geq 2\sqrt{q}$ for $q \geq 8$. Hence there exists at least one $v \neq 0$ such that $Tr_q(v + \frac{B}{v}) = 1 = Tr_q(1)$.

For $q = 4$ one can directly check that there exists $v \neq 0$ such that $Tr_q(1) = Tr_q(v + \frac{B}{v}) = 0$. Therefore when $B_1 \neq 0$ the polynomial $x^{q^2+q+2} + bx$ is not a permutation polynomial over the field $\mathbf{F}_{q^3}$.

Moreover the number of distinct elements $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$, satisfying $B_1 = 0$, that is $b + b^q + b^{q^2} = 0$, is equal to

$$|\{b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q : Tr_{\mathbf{F}_{q^3}/\mathbf{F}_q}(b) = 0\}|.$$

From the fact that $|\{\alpha \in \mathbf{F}_{q^s} : Tr_{\mathbf{F}_{q^s}/\mathbf{F}_q}(\alpha) = 0\}| = q^{s-1}$, we get that

$$\begin{aligned} |\{b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q : Tr_{\mathbf{F}_{q^3}/\mathbf{F}_q}(b) = 0\}| &= |\{b \in \mathbf{F}_{q^3} : Tr_{\mathbf{F}_{q^3}/\mathbf{F}_q}(b) = 0\}| - |\{b \in \mathbf{F}_q : Tr_{\mathbf{F}_{q^3}/\mathbf{F}_q}(b) = 0\}| \\ &= q^{3-1} - |\{0\}| \\ &= q^2 - 1. \end{aligned}$$

□

Corollary 6.2.3 *Let $q = 2^m$ and $m > 1$. Then the polynomial $b^{-1}x^{q^2+q+2}$ is a complete permutation polynomial over the field $\boldsymbol{F}_{q^3}$ if and only if b satisfies the condition of Theorem 6.2.2.*

Proof. The polynomial $b^{-1}x^{q^2+q+2}$ is a complete permutation polynomial if and only if $b^{-1}x^{q^2+q+2}$ and $b^{-1}x^{q^2+q+2} + x$ are permutation polynomials over the field $\mathbf{F}_{q^3}$. Since the numbers $2^{2m} + 2^m + 2$ and $2^{3m} - 1$ are mutually prime i.e, $gcd(q^2 + q + 2, q^3 - 1) = 1$, then by Theorem 2.0.42 the polynomial $b^{-1}x^{q^2+q+2}$ is a permutation polynomial over the field $\mathbf{F}_{q^3}$. If b satisfies the condition of Theorem 6.2.2, we get $x^{q^2+q+2} + bx$ is a permutation polynomial over the field $\mathbf{F}_{q^3}$. Which implies by Remark 2.0.41 the polynomial $b^{-1}x^{q^2+q+2} + x$ is a permutation polynomial over the field $\mathbf{F}_{q^3}$, hence $b^{-1}x^{q^2+q+2}$ is a complete permutation polynomial over the field $\mathbf{F}_{q^3}$. □

6.2.2 Fields of odd characteristic

Let $q = p^m, p \geq 3$. Then we have the following proposition.

Proposition 6.2.4 *Let $q = p^m$, and $p \geq 3$. The polynomial $x^{q^2+q+2} + bx$ is a permutation polynomial over the field $\boldsymbol{F}_{q^3}$, if and only if $b \in \boldsymbol{F}_{q^3} \setminus \boldsymbol{F}_q$, and the equation*

$$(x - y)^2 (2(x + y) + B_1) + 2(x + y)^3 + 3(x + y)^2 B_1 + 4(x + y)B_2 + 4B_3 = 0, \quad (6.12)$$

has no solution $x, y \in \boldsymbol{F}_q,\ x \neq 0,\ y \neq 0,\ x \neq y$.

Proof. Let $q = p^m, p \geq 3$. Using the identity $4xy = (x+y)^2 - (x-y)^2$, equation (6.7) is equivalent to

$$(x-y)^2\,(2(x+y)+B_1) + 2(x+y)^3 + 3(x+y)^2 B_1 + 4(x+y)B_2 + 4B_3 = 0, \quad (6.13)$$

Then by Proposition 6.2.1, $x^{q^2+q+2} + bx$ is a permutation polynomial over the field $\mathbf{F}_{q^3}$, if and only if $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$, and the equation $(x-y)^2\,(2(x+y)+B_1) + 2(x+y)^3 + 3(x+y)^2 B_1 + 4(x+y)B_2 + 4B_3 = 0$, has no solution $x, y \in \mathbf{F}_q,\ x \neq 0,\ y \neq 0,\ x \neq y$, as desired. □

Proposition 6.2.5 *Let $q = p^m$, and $p \geq 3$. The polynomial $x^{q^2+q+2} + bx$ is a permutation polynomial over the field $\boldsymbol{F}_{q^3}$, if and only if $b \in \boldsymbol{F}_{q^3} \setminus \boldsymbol{F}_q$, and the equation*

$$u^2(2z + B_1) + 2z^3 + 3z^2 B_1 + 4zB_2 + 4B_3 = 0 \quad (6.14)$$

has no solution $u \in \boldsymbol{F}_q^*, z \in \boldsymbol{F}_q$.

Proof. Set $z = x + y$ and $u = x - y$. Then the equation

$$(x-y)^2\,(2(x+y)+B_1) + 2(x+y)^3 + 3(x+y)^2 B_1 + 4(x+y)B_2 + 4B_3 = 0,$$

is equivalent to

$$u^2(2z + B_1) + 2z^3 + 3z^2 B_1 + 4zB_2 + 4B_3 = 0.$$

The conditions $x, y \in \mathbf{F}_q,\ x \neq 0,\ y \neq 0,\ x \neq y$ from Proposition 6.2.4 are equivalent to the condition $u \neq 0$ alone, because when $x \neq 0,\ y \neq 0,\ x \neq y$, then $u \neq 0$ and $u \neq z, -z$, however if $u = \pm z$ then by direct calculations we get

$$\begin{aligned} z^2(2z + B_1) + 2z^3 + 3z^2 B_1 + 4zB_2 + 4B_3 &= z^3 + z^2 B_1 + zB_2 + B_3 \\ &= (z+b)(z+b)^q (z+b)^{q^2} \\ &= (z+b)^{1+q+q^2} = 0, \end{aligned}$$

which is impossible for $z \in \mathbf{F}_q$, and $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$. □

Proposition 6.2.6 *Let $q = p^m, p \geq 3$. The polynomial $x^{q^2+q+2} + bx$ is a permutation polynomial over the field $\boldsymbol{F}_{q^3}$ if and only if*

$$b \in \boldsymbol{F}_{q^3} \setminus \boldsymbol{F}_q, \quad D \neq 0$$

and the equation

$$Y^2 = X^3 + \frac{C}{D^2}X^2 - \frac{1}{D^4} \tag{6.15}$$

has no solutions $Y, X \in \boldsymbol{F}_q^*$.

Proof. By equation(6.14) we have $u^2(2z + B_1) = -2z^3 - 3z^2B_1 - 4zB_2 - 4B_3$.

- If $2z + B_1 = 0 \implies z = \frac{-B_1}{2}$, the equation

  $$u^2(2z + B_1) = -2z^3 - 3z^2B_1 - 4zB_2 - 4B_3$$

  becomes

  $$\begin{aligned} 0 =& 2(\frac{-B_1^3}{2^3}) + 3\frac{B_1^2}{2^2}B_1 + 4(\frac{-B_1}{2}B_2) + 4B_3; \\ =& \frac{-B_1^3}{4} + 3\frac{B_1^3}{4} - 2B_1B_2 + 4B_3; \\ =& \frac{1}{2}B_1^3 - 2B_1B_2 + 4B_3; \\ =& B_1^3 - 4B_1B_2 + 8B_3. \end{aligned}$$

  So it is reduced to the condition

  $$B_1^3 - 4B_1B_2 + 8B_3 = 0 \tag{6.16}$$

  for the element b. Therefore if the element b satisfies (6.16), the polynomial $x^{q^2+q+2} + bx$ is not a permutation polynomial over $\mathbf{F}_{q^3}$, because for any $u \in \mathbf{F}_q^*$, equation(6.14) has the solution $z = \frac{-B_1}{2}$.

- If $B_1^3 - 4B_1B_2 + 8B_3 \neq 0$ and therefore $z \neq \frac{-B_1}{2}$, we have

$$\begin{aligned}
u^2 &= -\frac{2z^3 + 3z^2B_1 + 4zB_2 + 4B_3}{2z + B_1} \\
&= -\frac{4z^3 + 6z^2B_1 + 8zB_2 + 8B_3}{4z + 2B_1} \\
&= -\frac{4(z^3 + 3z^2\frac{B_1}{2} + 3z(\frac{B_1}{2})^2 - 3z(\frac{B_1}{2})^2 + (\frac{B_1}{2})^3 - (\frac{B_1}{2})^3) + 8zB_2 + 8B_3}{4(z + \frac{B_1}{2})} \\
&= -\frac{4(z + \frac{B_1}{2})^3 + 4(-3z\frac{B_1^2}{4} - \frac{B_1^3}{8}) + 8zB_2 + 8B_3}{4(z + \frac{B_1}{2})} \\
&= -(z + \frac{B_1}{2})^2 - \frac{z(8B_2 - 3B_1^2) + 8B_3 - \frac{B_1^3}{2}}{4(z + \frac{B_1}{2})} \\
&= -(z + \frac{B_1}{2})^2 - \frac{z(8B_2 - 3B_1^2) + \frac{B_1}{2}(8B_2 - 3B_1^2) - \frac{B_1}{2}(8B_2 - 3B_1^2) + 8B_3 - \frac{B_1^3}{2}}{4(z + \frac{B_1}{2})} \\
&= -(z + \frac{B_1}{2})^2 - \frac{(8B_2 - 3B_1^2)(z + \frac{B_1}{2}) - 4B_1B_2 + 3\frac{B_1^3}{2} + 8B_3 - \frac{B_1^3}{2}}{4(z + \frac{B_1}{2})} \\
&= -(z + \frac{B_1}{2})^2 - \frac{B_1^3 - 4B_1B_2 + 8B_3}{4(z + \frac{B_1}{2})} - \frac{(8B_2 - 3B_1^2)}{4}.
\end{aligned} \tag{6.17}$$

Denote

$$v = z + \frac{B_1}{2}; \qquad D = -\frac{B_1^3 - 4B_1B_2 + 8B_3}{4}; \qquad C = -\frac{(8B_2 - 3B_1^2)}{4}.$$

In terms of v, D and C, equation(6.17) becomes

$$u^2 = -v^2 + \frac{D}{v} + C.$$

Dividing both sides of equation $u^2 = -v^2 + \frac{D}{v} + C$ by D^4v^2 we get

$$\frac{u^2}{D^4v^2} = \frac{-1}{D^4} + \frac{D}{v^3D^4} + \frac{C}{v^2D^4}.$$

Now, setting $Y = \frac{u}{vD^2}$ and $X = \frac{1}{vD}$ we have

$$Y^2 = X^3 + \frac{C}{D^2}X^2 - \frac{1}{D^4}.$$

Thus the problem of existence a solution of equation (6.14) is reduced to the existence of solutions of the the equation $Y^2 = X^3 + \frac{C}{D^2}X^2 - \frac{1}{D^4}$, for $Y, X \in \mathbf{F}_q^*$. Hence by Proposition 6.2.5 the polynomial $x^{q^2+q+2} + bx$ is a permutation polynomial over the field $\mathbf{F}_{q^3}$ if and only if $b \in \mathbf{F}_{q^3} \setminus \mathbf{F}_q$, and the equation $Y^2 = X^3 + \frac{C}{D^2}X^2 - \frac{1}{D^4},\ D \neq 0$ has no solutions $Y, X \in \mathbf{F}_q^*$. □

Theorem 6.2.7 *Let $q = p^m$, and $p \geq 3$. The polynomial $x^{q^2+q+2} + bx$ is a permutation polynomial over the field $\boldsymbol{F}_{q^3}$ if and only if $q = 3$ or $q = 7$ and $b = \alpha^k$, where $k = 2, 4, 5, 17,$ and their cyclotomic cosets C_r of positive integers modulo 26, where α is a primitive element of $\boldsymbol{F}_{3^3}$ (or respectively $b = \alpha^k$, where $k = 30, 38, 39, 45, 87, 95, 96, 144,$ and their cyclotomic cosets C_r of positive integers modulo 342, where α is a primitive element of $\boldsymbol{F}_{7^3}$).*

Proof. Consider the plane curve C over $\mathbf{F}_q$ defined by

$$C = \{(X, Y) : X^3 + \frac{C}{D^2}X^2 - \frac{1}{D^4} - Y^2 = 0\}$$

This plane curve is absolutely irreducible because the polynomial

$$f(X, Y) = X^3 + \frac{C}{D^2}X^2 - \frac{1}{D^4} - Y^2 = g(X) + h(Y),$$

where $g(X) = X^3 + \frac{C}{D^2}X^2 - \frac{1}{D^4}$ and $h(Y) = -Y^2$, note that $gcd(deg\ g(X), deg\ h(Y)) = gcd(3, 2) = 1$, then by Corollary in 2.0.46 the polynomial $f(X, Y)$ is irreducible over $\mathbf{F}_q$ and so it is irreducible over any extension of $\mathbf{F}_q$, which implies that C is absolutely irreducible. By Hasse-Weil bound Theorem 2.0.53, the number N of $\mathbf{F}_q$-rational points of the plane curve satisfies $N \geq q + 1 - 2\sqrt{q}$. The number of points with $Y = 0$, or $X = 0$ does not exceed 5, then when $q + 1 - 2\sqrt{q} > 5$, i.e, $N > 5$, there exist a solution $Y, X \in \mathbf{F}_q^*$ of the equation (6.15). For $q \geq 11$ we have $q + 1 - 2\sqrt{q} > 5$, therefore by Proposition 6.2.6 the polynomial of the type $x^{q^2+q+2} + bx$ is not permutation polynomials over $\mathbf{F}_{q^3}$ in the case $q \geq 11$.

Now we will consider the cases $q = 3, 5, 7, 9$,

- For $q = 5,\ q = 9$.

  claim: The permutation polynomial over $\mathbf{F}_{q^3}$ of the type $x^{q^2+q+2} + bx$ does not exist for $q = 5$ and $q = 9$.

  Proof the claim: We will prove that there exists a solution $Y \neq 0,\ X \neq 0$ for equation(6.15).

  - If $C \neq 0$

    We know that for $q = 9, \mathbf{F}_9 \cong \mathbf{F}_3(\alpha) = \{0, 1, 2, \alpha, 2\alpha, 1+\alpha, 1+2\alpha, 2+2\alpha, 2+\alpha\}$, where α is a root of the irreducible polynomial x^2+1 over $\mathbf{F}_3$, that is $-1 = \alpha^2$. And for $q = 5$, $-1 = 2^2$, so -1 is a quadratic residue in both $\mathbf{F}_5$ and $\mathbf{F}_{3^2}$. Now, setting $X = -C/D^2$, equation(6.15) becomes:

    $$Y^2 = \frac{-C^3}{D^6} + \frac{C}{D^2}\frac{C^2}{D^4} - \frac{1}{D^4} = \frac{-1}{D^4} = \frac{b^2}{D^4}$$

    where $b^2 = -1$, for some $b \in \mathbf{F}_5$ respectively $b \in \mathbf{F}_{3^2}$ (since -1 is a quadratic residue in the fields $\mathbf{F}_5$ and $\mathbf{F}_{3^2}$), which implies that $Y = \pm\frac{b}{D^2} \in \mathbf{F}_q^*$.

    Thus, since there is a solution $X = -C/D^2, Y = \pm\frac{b}{D^2} \in \mathbf{F}_q^*$ for equation(6.15), there is no permutation polynomial in this case.

  - If $C = 0$.

    Set $X = (\frac{2}{D^4})^{\frac{1}{3}}$ this is an element in $\mathbf{F}_q^*$ for $q = 5$ and $q = 9$, because the mapping $w \longmapsto w^3$ is bijection in the fields $\mathbf{F}_5$ and $\mathbf{F}_{3^2}$, which implies that for the element $\frac{2}{D^4} \in \mathbf{F}_q^*$, there exist $b \in \mathbf{F}_q^*$ such that $b^3 = \frac{2}{D^4}$. Hence equation(6.15) becomes $Y^2 = \frac{2}{D^4} - \frac{1}{D^4} = \frac{1}{D^4}$, thus $Y = \pm\frac{1}{D^2}$.

    Thus, since there is a solution $X = (\frac{2}{D^4})^{\frac{1}{3}}, Y = \pm\frac{1}{D^2} \in \mathbf{F}_q^*$ for equation(6.15), also there is no permutation polynomial in this case.

  Therefore, there is no permutation polynomial over $\mathbf{F}_{q^3}$ of the type $x^{q^2+q+2} + bx$ for $q = 5$ and $q = 9$.

- For $q = 3$

  Let α be a primitive element of $\mathbf{F}_{3^3}$ given by $f(x) = x^3 + 2x^2 + 1$. The polynomial $x^{14} + bx$ is a permutation polynomial over $\mathbf{F}_{3^3}$ for the elements $b = \alpha^k$, where k runs through the following cyclotomic cosets C_r of positive integer modulo 26:

  $$C_2 = \{2, 6, 18\}, \quad C_4 = \{4, 12, 10\},$$

  $$C_5 = \{5, 15, 19\}, \quad C_{17} = \{17, 23, 25\}. \tag{6.18}$$

- For $q = 7$.

  Let α be a primitive element of $\mathbf{F}_{7^3}$ given by $f(x) = x^3 + x^2 + x + 2$. The polynomial $x^{58} + bx$ is a permutation polynomial over $\mathbf{F}_{7^3}$ for the elements $b =$

α^k, where k runs through the following cyclotomic cosets C_r of positive integers modulo 342:

$$C_{30} = \{30, 210, 102\}, \quad C_{38} = \{38, 266, 152\}, \quad C_{39} = \{39, 273, 201\},$$

$$C_{45} = \{45, 315, 153\}, \quad C_{37} = \{87, 267, 159\}, \quad C_{95} = \{95, 323, 209\},$$

$$C_{96} = \{96, 330, 258\}, \quad C_{144} = \{144, 324, 216\}. \qquad (6.19)$$

□

Corollary 6.2.8 *Let $q = p^m$ and $p \geq 3$. Then the polynomial $b^{-1}x^{q^2+q+2}$ is not a complete permutation polynomial over the field $\boldsymbol{F}_{q^3}$ for any $b \in \boldsymbol{F}^*_{q^3}$.*

Proof. Since the $gcd(14, 3^3 - 1) \neq 1$, and $gcd(58, 7^3 - 1) \neq 1$, by Theorem 2.0.42 the polynomial x^{14} (respectively x^{58}) is not a permutation polynomial over the field $\mathbf{F}_{3^3}$ (respectively over the field $\mathbf{F}_{7^3}$). □

REFERENCES

[1] G. Angermüller, *A Generalization of Ehrenfeucht's Irreducibility Criterion,* Mathematisches Institute der Universitat Erlangen-Nürnberg, West Germany, June 1, 1985.

[2] E. Bombieri, *On exponential sums in finite fields,* Amer. J. Math. 88(1966), 71-105.

[3] L.A. Bassalygo, V.A. Zinoviev, *On one class of permutation polynomials over finite fields of characteristic two ,* Mosc. Math. J. 15 (2015), no. 4, 703-713.

[4] L.A. Bassalygo, V.A. Zinoviev, *Permutation and complete permutation polynomials,* Finite Fields Appl. 33 (2015), 198-211.

[5] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves Over a Finite Field, Princeton University Press, USA, 2008.

[6] G. Kyureghyan, *Constructing permutations of finite fields via linear translators,* J. Combinatorial Theory, Series A 118 (2011), 1052-1061.

[7] S. Lang,Algebra, Third edition, Springer, USA, 2002.

[8] R. Lidl, H. Niederreiter, Finite Fields Encyclopedia of Mathematics and Its Applications, volume 20, Addison-Wesley Publishing Company, London, 1983.

[9] H. Niederreiter, K.H. Robinson, *Complete mapping of finite fields,* J. Aust. Math. Soc. A 33 (1982) 197-212.

[10] X. Qin, S. Hong, *Constructing permutation polynomials over finite fields ,* Bull. Aust. Math. Soc. 89 (2014), 420-430.

[11] X. Qin, G. Qian, S. Hong, *New results on permutation polynomials over finite fields,* Int. J. Number Theory, 11 (2015),no. 2, 437-449.

[12] I.M. Vinogradov, Basics of Number Theory, edition VIII, Nauka, Moscow, 1972.

[13] G. Wu, N. Li, T. Helleseth, Y. Zhang, *Some classes of monomial complete permutation polynomials over finite fields of characteristic two,* Finite Fields Appl. 28 (2014) 148-165.

VITA

PERSONAL INFORMATION

Surname, Name:	M.M.DabboorAsad, Maha
Nationality:	Palestinian (PS)
Date and Place of Birth:	August 4, 1986, Saudi Arabia
email:	maha_alattar@hotmail.com

EDUCATION

Degree	Institution	Year of Graduation
B.S.	Atılım, Mathematics	2017
under graduate	Islamic University of Gaza, Mathematics	2007
High School	19 High School	2003

WORK EXPERIENCE

Year	Place	Enrollment
2009-present	UNRWA Schools , Mathematics	teacher
2007-2008	Islamic University of Gaza, Mathematics Department	Assistant

FOREIGN LANGUAGES

English (fluent), Turkish (Basics)

AWARDS and SCHOLARSHIPS

- Graduation seminar in IUG, Islamic University Award for extensive researches, Weierstrass approximation theorem, 2007.

CONFERENCE PRESENTATIONS

- *On permutation polynomials over finite fields*, Seminar Studies Course, Jan 17, 2017, Atılım, Ankara.