

LINEARIZED POLYNOMIALS OVER FINITE FIELDS

by

LEYLA PARLAR

Submitted to the Graduate School of Engineering and Natural Sciences

in partial fulfillment of

the requirements for the degree of

Master of Science

Sabancı University

Spring 2012

LINEARIZED POLYNOMIALS OVER FINITE FIELDS

APPROVED BY

Prof. Dr. Henning Stichtenoth
(Thesis Supervisor)

Prof. Dr. Alev Topuzođlu

Assoc. Prof. Cem Güneri

Asst. Prof. Kađan Kurşungöz

Assoc. Prof. Özgür Gürbüz

DATE OF APPROVAL: May 30, 2012

©Leyla Parlar 2012

All Rights Reserved

LINEARIZED POLYNOMIALS OVER FINITE FIELDS

Leyla Parlar

Mathematics, Master Thesis, 2012

Thesis Supervisor: Prof. Dr. Henning Stichtenoth

Keywords: Linearized polynomials, permutation polynomials, p -to-1 mappings.

Abstract

We first study the ring of q -polynomials over \mathbb{F}_q by constructing an isomorphism between this ring and the polynomial ring over \mathbb{F}_q and by presenting several important facts about the polynomials in this ring. We also give characterizations for permutation polynomials of \mathbb{F}_{p^n} derived from p -polynomials over \mathbb{F}_{p^n} , based on a paper of P. Charpin and G. Kyureghyan. Furthermore, we present several results on q -polynomials over \mathbb{F}_{q^n} with kernel of any given dimension, following a paper by S. Ling and L.J. Qu.

SONLU CİSİMLER ÜZERİNDE DOĞRUSALLAŞTIRILAN POLİNOMLAR

Leyla Parlar

Matematik, Yüksek Lisans Tezi, 2012

Tez Danışmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: Doğrusallaştırılan polinomlar, permütasyon polinomları, p 'ye 1 gönderimler.

Özet

İlk olarak, \mathbb{F}_q üzerinde q -polinomlarının oluşturduğu halka ile \mathbb{F}_q üzerindeki polinom halkası arasında bir izomorfizma kurulmuş ve bu polinomların birkaç önemli özelliği sunulmuştur. Ayrıca P. Charpin ve G. Kyureghyan'a ait bir makaleye dayanarak, \mathbb{F}_{p^n} üzerinde p -polinomları kullanılarak elde edilen \mathbb{F}_{p^n} üzerinde permütasyon polinomları için tanımlamalar verilmiştir. Son olarak S. Ling ve L.J. Qu'ya ait bir makale doğrultusunda, çekirdeği herhangi bir boyuta sahip olan \mathbb{F}_{q^n} üzerinde q -polinomları hakkında birkaç sonuca yer verilmiştir.

*To my fiancé,
İbrahim*

Acknowledgments

In the first place, I gratefully acknowledge Prof. Dr. Henning Stichtenoth for his supervision, invaluable guidance and motivation throughout the process of writing this thesis.

I would also like to express my gratitude to my parents and sisters for their endless love and support that I receive throughout my life.

Last, but certainly not least, I would like to give my sincere thanks to my fiancé, İbrahim. Without his encouragement and motivation this thesis could not have been successfully completed.

Table of Contents

Abstract	iv
Özet	v
Acknowledgments	vii
Introduction	ix
1 Linearized Polynomials over \mathbb{F}_q	1
2 Permutation Polynomials from Linearized Polynomials	12
3 Dimension of Kernels of Linearized Polynomials	21
Bibliography	28

Introduction

The class of linearized polynomials over finite fields constitutes a challenging study area. Let q be a prime power and \mathbb{F}_q the finite field of order q . Further, let \mathbb{F} be an algebraic closure of \mathbb{F}_q . We investigate linearized polynomials over finite fields, i.e., polynomials of the form

$$L(x) = \sum_{i=0}^m \alpha_i x^{q^i}, \text{ where } \alpha_i \in \mathbb{F}. \quad (*)$$

We denote the set of polynomials of type (*) by $Ore_q(\mathbb{F})$, referring to Ore [1] in which the theory of linearized polynomials over finite fields is developed. This thesis approaches the set $Ore_q(\mathbb{F})$ in terms of three main aspects, which we describe below after fixing some notations.

Any polynomial $F(x) \in \mathbb{F}_{q^n}[x]$, defines a mapping

$$F : \begin{cases} \mathbb{F}_{q^n} & \rightarrow \mathbb{F}_{q^n} \\ \alpha & \mapsto F(\alpha), \end{cases}$$

which is called the *associated mapping* of $F(x)$. During this paper, $F(x)$ denotes a polynomial and F denotes the associated mapping of the polynomial. If $F(x)$ is of the form (*), then $\text{Ker}(F)$ and $\text{Im}(F)$ denote the kernel and the image of F , respectively. For such a polynomial, we can use the phrase “kernel of $F(x)$ ” to refer $\text{Ker}(F)$. A polynomial $F(x)$ is called a *permutation polynomial* of \mathbb{F}_{q^n} if the mapping F is a permutation of \mathbb{F}_{q^n} . $Tr(x)$ is the polynomial defining the trace function from \mathbb{F}_{q^n} to \mathbb{F}_q , which is given by

$$Tr(x) = x + x^q + x^{q^2} + \dots + x^{q^{n-1}}.$$

If $q = p$ is a prime number, then $Tr(x)$ is called the absolute trace function of \mathbb{F}_{p^n} .

- In Chapter 1, we deal with the polynomials of the form (*) whose coefficients are in \mathbb{F}_q , namely, *q-polynomials over \mathbb{F}_q* . These polynomials form a ring under the operations of addition and composition. We focus on the results of the isomorphism between this ring and the polynomial ring over \mathbb{F}_q . Further, we point out several important properties of this special type of polynomials.
- In Chapter 2, we assume that q is a prime number, say p , and aim to derive permutation polynomials of \mathbb{F}_{p^n} by using the polynomials of the form (*) whose coefficients are in $\mathbb{F}_{p^n} \subseteq \mathbb{F}$.

- In Chapter 3, we give several representations and the number of linearized polynomials of type (*) whose coefficients are in \mathbb{F}_{q^n} and whose kernel is of any given dimension, which arises as a problem in Chapter 2.

Linearized Polynomials over \mathbb{F}_q

Throughout this thesis, let \mathbb{F}_q be a finite field with q elements and \mathbb{F} an algebraic closure of \mathbb{F}_q . In this section, we investigate the set of q -polynomials over \mathbb{F}_q , which forms a special class of polynomials over \mathbb{F}_q .

Definition 1.1. (i) A polynomial of the form $L(x) = \sum_{i=0}^n a_i x^{q^i}$ with coefficients in \mathbb{F}_q is called a *q -polynomial* over \mathbb{F}_q .

(ii) Denote

$$\begin{aligned} Ore_q(\mathbb{F}_q) &:= \left\{ L(x) = \sum_{i=0}^n a_i x^{q^i}, \text{ where } a_i \in \mathbb{F}_q \right\} \text{ and} \\ Ore_q(\mathbb{F}) &:= \left\{ L(x) = \sum_{i=0}^n \alpha_i x^{q^i}, \text{ where } \alpha_i \in \mathbb{F} \right\}. \end{aligned}$$

Remark 1.2. (i) Clearly, $Ore_q(\mathbb{F}_q)$ is a vector space over \mathbb{F}_q .

(ii) For any $L(x) \in Ore_q(\mathbb{F}_q)$, $\alpha, \beta \in \mathbb{F}$ and $c \in \mathbb{F}_q$,

$$L(\beta + \gamma) = L(\beta) + L(\gamma) \text{ as well as} \tag{1.1}$$

$$L(c\beta) = cL(\beta). \tag{1.2}$$

Because of this fact, one uses the term *linearized polynomials* over \mathbb{F}_q instead of q -polynomials over \mathbb{F}_q . In other words, the associated mapping $L : \mathbb{F} \rightarrow \mathbb{F}$ of $L(x)$ is a linear operator on \mathbb{F} , regarded as a vector space over \mathbb{F}_q .

Theorem 1.3. *Let $L(x) \in Ore_q(\mathbb{F}_q)$ be nonzero. Then either each root of $L(x)$ in \mathbb{F} is simple or each of them has the same multiplicity, a power of q . Further, the roots form a linear subspace of \mathbb{F} , where \mathbb{F} is considered as a vector space over \mathbb{F}_q .*

Proof. The fact that the roots form a linear subspace of \mathbb{F} follows from (1.1) and (1.2). Let $L(x) = \sum_{i=0}^n a_i x^{q^i}$, then $L'(x) = a_0$. If $a_0 \neq 0$ then all the roots of $L(x)$ are simple.

Otherwise, there exists a_k such that $a_k \neq 0$ and $a_i = 0$ for all $i < k$. Since $a_i \in \mathbb{F}_q$ implies $a_i^{q^k} = a_i$, we can write

$$L(x) = \sum_{i=k}^n a_i x^{q^i} = \sum_{i=k}^n a_i^{q^k} x^{q^i} = \left(\sum_{i=k}^n a_i x^{q^{i-k}} \right)^{q^k}.$$

Since

$$\left(\sum_{i=k}^n \alpha_i x^{q^{i-k}} \right)' = \alpha_k \neq 0,$$

$L(x)$ is the q^k th power of a linearized polynomial over \mathbb{F}_q having only simple roots, which concludes the proof. \square

There is a partial converse for Theorem 1.3, which follows from the following lemma.

Lemma 1.4. *Let $\beta_1, \beta_2, \dots, \beta_n$ be elements of \mathbb{F} . Then*

$$\begin{vmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \cdots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \cdots & \beta_2^{q^{n-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ \beta_n & \beta_n^q & \beta_n^{q^2} & \cdots & \beta_n^{q^{n-1}} \end{vmatrix} = \beta_1 \prod_{j=1}^{n-1} \prod_{c_1, \dots, c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{k=1}^j c_k \beta_k \right), \quad (1.3)$$

and so the determinant is nonzero if and only if $\beta_1, \beta_2, \dots, \beta_n$ are linearly independent over \mathbb{F}_q .

Proof. Denote by $D_n \in \mathbb{F}$ the determinant on the left-hand side. We prove that D_n is equal to the given formula by induction on n . The basis step, $n = 1$, is trivial if the empty product is taken as 1. Assume that the formula is shown for some $n > 1$. Define the polynomial

$$D(x) = \begin{vmatrix} \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} & \beta_1^{q^n} \\ \beta_2 & \beta_2^q & \cdots & \beta_2^{q^{n-1}} & \beta_2^{q^n} \\ \vdots & \vdots & & \vdots & \vdots \\ \beta_n & \beta_n^q & \cdots & \beta_n^{q^{n-1}} & \beta_n^{q^n} \\ x & x^q & \cdots & x^{q^{n-1}} & x^{q^n} \end{vmatrix}.$$

Note that

$$D(x) = D_n x^{q^n} + \sum_{i=0}^{n-1} \alpha_i x^{q^i},$$

where $\alpha_i \in \mathbb{F}$ for $0 \leq i \leq n-1$. Thus, $D(x) \in Ore_q(\mathbb{F})$. Observe that

$$D(\beta_k) = 0 \text{ for } 1 \leq k \leq n.$$

So by Theorem 1.3, we have

$$D(c_1 \beta_1 + \cdots + c_n \beta_n) = 0$$

for any $c_k \in \mathbb{F}_q$, where $1 \leq k \leq n$. First assume that $\beta_1, \beta_2, \dots, \beta_n$ are linearly independent over \mathbb{F}_q . Then there are exactly q^n distinct linear combinations of $\beta_1, \beta_2, \dots, \beta_n$ over \mathbb{F}_q . Since $\deg(D(x)) = q^n$, $D(x)$ has the factorization

$$D(x) = D_n \prod_{c_1, \dots, c_n \in \mathbb{F}_q} \left(x - \sum_{k=1}^n c_k \beta_k \right). \quad (1.4)$$

Now assume that $\beta_1, \beta_2, \dots, \beta_n$ are linearly dependent over \mathbb{F}_q . Then $D_n = 0$ by the inductive hypothesis and

$$\sum_{k=1}^n b_k \beta_k = 0$$

for some $b_1, \dots, b_n \in \mathbb{F}_q$, not all of which are 0. So

$$\sum_{k=1}^n b_k \beta_k^{q^j} = \left(\sum_{k=1}^n b_k \beta_k \right)^{q^j} = 0$$

for $j = 0, 1, \dots, n$. Then the first n row vectors in the determinant defining $D(x)$ are linearly dependent over \mathbb{F}_q , i.e., $D(x) = 0$. Thus, (1.4) is also satisfied in this case. Therefore, we can use the equation (1.4) to conclude that

$$\begin{aligned} D_{n+1} &= D(\beta_{n+1}) \\ &= D_n \prod_{c_1, \dots, c_n \in \mathbb{F}_q} \left(\beta_{n+1} - \sum_{k=1}^n c_k \beta_k \right) \\ &= \beta_1 \prod_{j=1}^n \prod_{c_1, \dots, c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{k=1}^j c_k \beta_k \right), \end{aligned}$$

that is, the formula (1.3) holds for $n + 1$. □

Theorem 1.5. *Let U be a finite dimensional linear subspace of \mathbb{F} , considered as a vector space over \mathbb{F}_q and $k \geq 0$. Then*

$$L(x) = \prod_{\beta \in U} (x - \beta)^{q^k} \in Ore_q(\mathbb{F}).$$

Proof. If $L(x) \in Ore_q(\mathbb{F})$ then $L(x)^{q^k} \in Ore_q(\mathbb{F})$, too. So it is enough to show that $L(x)$ is a q -polynomial over \mathbb{F} when $k = 0$. Let $\{\beta_1, \beta_2, \dots, \beta_n\}$ be a basis of U over \mathbb{F}_q and let D_n and $D(x)$ be defined as in the proof of Lemma 1.4. Then $D_n \neq 0$ and we have

$$\begin{aligned} L(x) &= \prod_{\beta \in U} (x - \beta) \\ &= \prod_{c_1, \dots, c_n \in \mathbb{F}_q} \left(x - \sum_{k=1}^n c_k \beta_k \right) \\ &= D_n^{-1} D(x) \end{aligned}$$

by (1.4). Thus, the fact that $D(x) \in Ore_q(\mathbb{F})$ completes the proof. □

The set of linearized polynomials is not closed under ordinary multiplication whereas it is closed under composition. Here, we use the phrase *symbolic multiplication* to refer to the composition operation in the set of linearized polynomials and denote it by

$$L_1(x) \otimes L_2(x) = L_1(L_2(x)).$$

From now on, we consider only the space $Ore_q(\mathbb{F}_q) \subseteq Ore_q(\mathbb{F})$. Observe that $Ore_q(\mathbb{F}_q)$ is closed under symbolic multiplication. Moreover, for $L_1(x) = \sum_{i=0}^n a_i x^{q^i}$, $L_2(x) = \sum_{j=0}^m b_j x^{q^j} \in Ore_q(\mathbb{F}_q)$, we have

$$\begin{aligned} L_1(x) \otimes L_2(x) &= \sum_{i=0}^n a_i \sum_{j=0}^m b_j^{q^i} x^{q^{i+j}} = \sum_{i=0}^n \sum_{j=0}^m a_i b_j x^{q^{i+j}} \\ &= \sum_{j=0}^m b_j \sum_{i=0}^n a_i^{q^j} x^{q^{i+j}} = L_2(x) \otimes L_1(x), \end{aligned}$$

that is, symbolic multiplication is commutative in $Ore_q(\mathbb{F}_q)$. So that $Ore_q(\mathbb{F}_q)$ forms a commutative ring under the operations of symbolic multiplication and ordinary addition. In addition, it can be related to $\mathbb{F}_q[x]$ under conventional arithmetic by the following concept.

Definition 1.6. The polynomials $l(x) = \sum_{i=0}^n \alpha_i x^i$ and $L(x) = \sum_{i=0}^n \alpha_i x^{q^i}$ over \mathbb{F} are called *q-associates* of each other. More specifically, $l(x)$ is the *conventional q-associate* of $L(x)$ and $L(x)$ is the *linearized q-associate* of $l(x)$.

Lemma 1.7. Let $L_1(x), L_2(x) \in Ore_q(\mathbb{F}_q)$ with conventional q-associates $l_1(x)$ and $l_2(x)$. Then $l(x) = l_1(x)l_2(x)$ and $L(x) = L_1(x) \otimes L_2(x)$ are q-associates of each other as well as $l_1(x) + l_2(x)$ and $L_1(x) + L_2(x)$ are q-associates of each other.

Proof. Let $L_1(x) = \sum_{i=0}^n a_i x^{q^i}$, $L_2(x) = \sum_{j=0}^m b_j x^{q^j}$. Then

$$L_1(x) \otimes L_2(x) = \sum_{i=0}^n a_i \left(\sum_{j=0}^m b_j x^{q^j} \right)^{q^i} = \sum_{i=0}^n \sum_{j=0}^m a_i b_j x^{q^{i+j}}.$$

On the other hand,

$$l_1(x)l_2(x) = \sum_{i=0}^n a_i x^i \sum_{j=0}^m b_j x^j = \sum_{i=0}^n \sum_{j=0}^m a_i b_j x^{i+j}.$$

The other argument that $l_1(x) + l_2(x)$ and $L_1(x) + L_2(x)$ are q-associates of each other is obvious; hence, we are done. \square

Thanks to Lemma 1.7, we get an important result that the ring of polynomials over \mathbb{F}_q and the ring of q -polynomials over \mathbb{F}_q are isomorphic to each other.

Theorem 1.8. *The mapping $\phi : (\mathbb{F}_q[x], +, \cdot) \rightarrow (Ore_q(\mathbb{F}_q), +, \otimes)$ which is given by*

$$l(x) \mapsto L(x),$$

where $l(x)$ and $L(x)$ are q -associates of each other, is a ring isomorphism.

Proof. Clearly, ϕ is bijection. Note that

$$\begin{aligned} \phi(l_1(x)l_2(x)) &= L_1(x) \otimes L_2(x) \\ &= \phi(l_1(x)) \otimes \phi(l_2(x)) \end{aligned}$$

and

$$\begin{aligned} \phi(l_1(x) + l_2(x)) &= L_1(x) + L_2(x) \\ &= \phi(l_1(x)) + \phi(l_2(x)) \end{aligned}$$

hold by Lemma 1.7. Therefore, ϕ is a ring isomorphism. \square

Being isomorphic to $\mathbb{F}_q[x]$, $Ore_q(\mathbb{F}_q)$ is a unique factorization domain with the identity element x and unit elements cx , where $c \in \mathbb{F}_q$. Also the notion of being irreducible is adapted as being *symbolically irreducible*, i.e., a q -polynomial $L(x)$ is symbolically irreducible over \mathbb{F}_q if and only if its conventional q -associate $l(x)$ is irreducible over \mathbb{F}_q .

Moreover, one says that $L(x) \in Ore_q(\mathbb{F}_q)$ is *symbolically divisible* by $L_1(x) \in Ore_q(\mathbb{F}_q)$ if $L(x) = L_1(x) \otimes L_2(x)$ for some $L_2(x) \in Ore_q(\mathbb{F}_q)$. Denote by $L_1(x) \Big|_{\otimes} L(x)$ the fact that $L_1(x)$ *symbolically divides* $L(x)$. By this notion, the following corollary is immediate from Theorem 1.8.

Corollary 1.9. *Let $L_1(x), L(x) \in Ore_q(\mathbb{F}_q)$ with conventional q -associates $l_1(x)$ and $l(x)$. Then $L_1(x) \Big|_{\otimes} L(x)$ if and only if $l_1(x) \Big| l(x)$.*

Now we indicate an important result that whereas symbolic multiplication and ordinary multiplication are different operations, symbolic division and ordinary division are equivalent in $Ore_q(\mathbb{F}_q)$.

Theorem 1.10. *Let $L_1(x), L(x) \in Ore_q(\mathbb{F}_q)$ with conventional q -associates $l_1(x)$ and $l(x)$. Then the following properties are equivalent:*

- (i) $L_1(x) \Big|_{\otimes} L(x)$,
- (ii) $L_1(x) \Big| L(x)$
- (iii) $l_1(x) \Big| l(x)$.

Proof. The equivalence of (i) and (iii) follows from Corollary 1.9. To complete the proof, first assume (i) and let $L(x) = L_1(x) \otimes L_2(x)$ for some $L_2(x) \in Ore_q(\mathbb{F}_q)$. Then

$$L(x) = L_1(x) \otimes L_2(x) = L_2(x) \otimes L_1(x) = L_2(L_1(x)),$$

which implies $L_1(x) \mid L(x)$. For the converse, assume $L_1(x) \mid L(x)$ and apply the division algorithm to write

$$l(x) = k(x)l_1(x) + r(x), \text{ where } \deg(r(x)) < \deg(l_1(x)).$$

With the linearized q -associates $K(x)$ and $R(x)$ of $k(x)$ and $r(x)$, respectively, we get

$$L(x) = K(x) \otimes L_1(x) + R(x), \text{ where } \deg(R(x)) < \deg(L_1(x)).$$

Since (i) implies (ii), we get

$$L_1(x) \mid K(x) \otimes L_1(x).$$

So $L_1(x) \mid R(x)$, which is possible only if $R \equiv 0$. Thus we conclude that $L_1(x) \mid_{\otimes} L(x)$. \square

As an analog of greatest common divisor, we consider *greatest common symbolic divisor*, gcd_{\otimes} , for two or more q -polynomials over \mathbb{F}_q , not all of which are 0. Let $L_1(x), \dots, L_k(x) \in Ore_q(\mathbb{F}_q)$ be nonzero and let

$$\begin{aligned} d(x) &:= gcd(L_1(x), \dots, L_k(x)) \text{ and} \\ D(x) &:= gcd_{\otimes}(L_1(x), \dots, L_k(x)). \end{aligned}$$

Then the roots of $d(x)$ form a linear subspace of \mathbb{F} , regarded as a vector space over \mathbb{F}_q , since the set of roots of $d(x)$ is exactly the intersection of linear subspaces formed by the roots of the given q -polynomials. Also by Theorem 1.3, we get that either each root of $d(x)$ is simple or they have the same multiplicity, a power of q . Hence, Theorem 1.5 indicates that $d(x) \in Ore_q(\mathbb{F}_q)$. Therefore, $d(x)$ symbolically divides the given q -polynomials by Theorem 1.10. Then

$$d(x) \mid D(x).$$

On the other hand,

$$D(x) \mid d(x)$$

since $D(x)$ divides the given q -polynomials in the ordinary sense again by Theorem 1.10. As a consequence, we can state the following theorem, which we have just proven.

Theorem 1.11. *In the ring $(Ore_q(\mathbb{F}_q), +, \otimes)$, the greatest common divisor and the greatest common symbolically divisor are identical.*

Here, we finish analyzing the results of the correspondence between $\mathbb{F}_q[x]$ and $Ore_q(\mathbb{F}_q)$ by defining a new concept.

Definition 1.12. A finite-dimensional vector space $M \subseteq \mathbb{F}$ over \mathbb{F}_q is called a q -modulus if

$$M = \{\beta^q : \beta \in M\}.$$

On the basis of this definition, we obtain a characterization for the monic q -polynomials over \mathbb{F}_q as follows.

Theorem 1.13. *The monic polynomial $L(x)$ is a q -polynomial over \mathbb{F}_q if and only if each root of $L(x)$ is either simple or multiple with the same multiplicity, a power of q , and the roots form a q -modulus.*

Proof. Assume that $L(x) = \sum_{i=0}^n a_i x^{q^i} \in Ore_q(\mathbb{F}_q)$. By Theorem 1.3, it is enough to show that if $L(\beta) = 0$ then $L(\beta^q) = 0$. Note that

$$L(x)^q = \sum_{i=0}^n a_i^q x^{q^{i+1}} = \sum_{i=0}^n a_i x^{q^{i+1}} = L(x^q).$$

Thus, $L(\beta^q) = L(\beta)^q = 0$. For the converse, apply Theorem 1.5 to $L(x)$ to see that $L(x) \in Ore_q(\mathbb{F})$. Let M be the q -modulus formed by the roots of $L(x)$. Then, for some $k \in \mathbb{Z}^+$,

$$\begin{aligned} L(x) &= \prod_{\beta \in M} (x - \beta)^{q^k} \text{ and} \\ L(x)^q &= \prod_{\beta \in M} (x^q - \beta^q)^{q^k} = \prod_{\beta \in M} (x^q - \beta)^{q^k} = L(x^q), \end{aligned} \tag{1.5}$$

since $M = \{\beta^q : \beta \in M\}$. Let $L(x) = \sum_{i=0}^n a_i x^{q^i}$, where $a_i \in \mathbb{F}$. Then by (1.5),

$$\sum_{i=0}^n a_i^q x^{q^{i+1}} = \sum_{i=0}^n a_i x^{q^{i+1}},$$

which implies that the coefficients of $L(x)$ are in \mathbb{F}_q , i.e., $L(x) \in Ore_q(\mathbb{F}_q)$. \square

We can connect the notion of q -modulus with symbolically irreducible polynomials over \mathbb{F}_q . It is clear that if $L(x) \in Ore_q(\mathbb{F}_q)$ has degree q then it is symbolically irreducible over \mathbb{F}_q . For the ones with degree greater than q , we have the following theorem.

Theorem 1.14. *The q -polynomial $L(x)$ over \mathbb{F}_q of degree greater than q is symbolically irreducible over \mathbb{F}_q if and only if $L(x)$ has simple roots and the q -modulus M consisting of the roots of $L(x)$ contains no q -modulus except $\{0\}$ and M itself.*

Proof. Assume that $L(x)$ is symbolically irreducible over \mathbb{F}_q . Further, suppose that $L(x)$ has multiple roots. Then

$$L(x) = L_1(x)^q,$$

where $\deg(L_1) > 1$ and $L_1(x) \in Ore_q(\mathbb{F}_q)$ by Theorem 1.13. So $L(x)$ has the symbolic factorization

$$L(x) = x^q \otimes L_1(x).$$

This is a contradiction since neither of the factors is a unit. Hence, each root of $L(x)$ is simple. Now assume that $N \subseteq M$ is a q -modulus. Define

$$L_2(x) = \prod_{\beta \in N} (x - \beta),$$

which is a q -polynomial over \mathbb{F}_q by Theorem 1.13 such that $L_2(x) \mid L(x)$. Then we get $L_2(x) \mid_{\otimes} L(x)$ by Theorem 1.10. Thus $\deg(L_2(x))$ is equal to either 1 or $\deg(L(x))$, i.e., N is either $\{0\}$ or M .

For the converse, let the symbolic decomposition of $L(x)$ be

$$L(x) = L_1(x) \otimes L_2(x),$$

where $L_1(x), L_2(x) \in Ore_q(\mathbb{F}_q)$. Then $L_1(x) \mid L(x)$, which is derived from the fact that $L_1(x) \mid_{\otimes} L(x)$ by using Theorem 1.10. So the q -modulus, N , formed by the roots of $L_1(x)$ is contained in M . Then N is either $\{0\}$ or M . As a result, either $\deg(L_1)$ or $\deg(L_2)$ is equal to 1, which implies that $L(x)$ is symbolically irreducible over \mathbb{F}_q . \square

Now let $\zeta \in \mathbb{F}$ be a root of $L(x) \in Ore_q(\mathbb{F}_q)$ and let $g(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of ζ over \mathbb{F}_q . Then $g(x) \mid L(x)$. If $g(x)$ does not divide any nonzero q -polynomial over \mathbb{F}_q of lower degree, then ζ is said to be a q -primitive root over \mathbb{F}_q . Alternatively, we have the following definition.

Definition 1.15. Let $L(x) \in Ore_q(\mathbb{F}_q)$ be nonzero. A root ζ of $L(x)$ is called a q -primitive root over \mathbb{F}_q if it is not a root of any nonzero q -polynomial over \mathbb{F}_q of lower degree.

We want to determine the number of q -primitive roots over \mathbb{F}_q of a nonzero q -polynomial $L(x)$ over \mathbb{F}_q . Denote this number by N_L .

For simplicity in the future results on the number N_L , we define an analog of Euler's Φ -function for nonzero $f \in \mathbb{F}_q[x]$. Let $\Phi_q(f(x)) = \Phi_q(f)$ denote the number of polynomials in $\mathbb{F}_q[x]$ that are of smaller degree than f as well as relatively prime to f .

Lemma 1.16. *The function Φ_q defined for nonzero polynomials in $\mathbb{F}_q[x]$ has the following properties:*

- (i) $\Phi_q(f) = 1$ if $\deg(f) = 0$;
- (ii) $\Phi_q(fg) = \Phi_q(f)\Phi_q(g)$ whenever f and g are relatively prime;

(iii) if $\deg(f) = n \geq 1$, then

$$\Phi_q(f) = q^n(1 - q^{-n_1}) \cdots (1 - q^{-n_r}),$$

where the n_i are the degrees of the distinct monic irreducible polynomials appearing in the canonical factorization of f in $\mathbb{F}_q[x]$.

Proof. See [2, p.122]. □

Theorem 1.17. Let $L(x) \in Ore_q(\mathbb{F}_q)$ be nonzero with conventional q -associate $l(x)$. Then

$$N_L = \begin{cases} \Phi_q(l(x)) & \text{if } L(x) \text{ has simple roots} \\ 0 & \text{otherwise} \end{cases}. \quad (1.6)$$

Proof. First assume that $L(x)$ has multiple roots. Then by Theorem 1.13,

$$L(x) = L_1(x)^q,$$

where $L_1(x) \in Ore_q(\mathbb{F}_q)$. Thus, any root of $L(x)$ is also a root of $L_1(x)$, i.e, $N_L = 0$.

Now suppose that $L(x)$ has only simple roots. If $\deg(L(x)) = 1$ then, obviously, the only root 0 is the q -primitive root of $L(x)$ over \mathbb{F}_q . Then by Lemma 1.16,

$$N_L = 1 = \Phi_q(l(x))$$

since $\deg(l(x)) = 0$. If $\deg(L(x)) = q^n > 1$ and without loss of generality $L(x)$ is monic, let

$$L(x) = \underbrace{L_1(x) \otimes \cdots \otimes L_1(x)}_{e_1} \otimes \cdots \otimes \underbrace{L_r(x) \otimes \cdots \otimes L_r(x)}_{e_r}$$

be the symbolic factorization of $L(x)$ with distinct monic symbolically irreducible polynomials $L_i(x)$ over \mathbb{F}_q . Define for $i = 1, \dots, r$

$$R_i(x) = \underbrace{L_1(x) \otimes \cdots \otimes L_1(x)}_{e_1} \otimes \cdots \otimes \underbrace{L_i(x) \otimes \cdots \otimes L_i(x)}_{e_i-1} \otimes \cdots \otimes \underbrace{L_r(x) \otimes \cdots \otimes L_r(x)}_{e_r},$$

a q -polynomial over \mathbb{F}_q having only simple roots. Let S be the set of all roots of $L(x)$ and P be the set of q -primitive roots of $L(x)$ over \mathbb{F}_q as well as R be the union of the set of roots of $R_i(x)$, $i = 1, \dots, r$. Note that if $\zeta \in S \setminus P$ then $R_i(\zeta) = 0$ for some i , $1 \leq i \leq r$, so $S \setminus P \subseteq R$. On the other hand, any root of $R_i(x)$ is a also a root of $L(x)$ so $R \subseteq S \setminus P$. Therefore,

$$|S| = |P| + |R|. \quad (1.7)$$

Since $L(x)$ has simple roots, $|S| = \deg(L(x)) = q^n$. If $\deg(L_i(x)) = q^{n_i}$ then

$$\deg(R_i(x)) = q^{n-n_i}, \quad (1.8)$$

which is the number of roots of $R_i(x)$. If i_1, \dots, i_s are distinct subscripts, then the number of common roots of $R_{i_1}(x), \dots, R_{i_s}(x)$ is equal to the degree of the greatest

common divisor, which is the same as the degree of the greatest common symbolic divisor. Construction of $R_i(x)$ and (1.8) implies that this degree is equal to

$$q^{n-n_{i_1}-\dots-n_{i_s}}.$$

So the inclusion-exclusion principle of combinatorics yields

$$|R| = \sum_{i=1}^r q^{n-n_i} - \sum_{1 \leq i < j \leq r} q^{n-n_i-n_j} + \dots + (-1)^{r+1} q^{n-n_1-\dots-n_r}. \quad (1.9)$$

Hence by using (1.7) and (1.9), we conclude that

$$\begin{aligned} N_L &= q^n - \sum_{i=1}^r q^{n-n_i} + \sum_{1 \leq i < j \leq r} q^{n-n_i-n_j} - \dots + (-1)^r q^{n-n_1-\dots-n_r} \\ &= q^n (1 - q^{-n_1}) \dots (1 - q^{-n_r}). \end{aligned}$$

To finish the proof, note that

$$l(x) = l_1(x)^{e_1} \dots l_r(x)^{e_r}$$

is the canonical factorization of $l(x)$, where $\deg(l_i) = n_i$. Consequently, by Lemma 1.16,

$$N_L = \Phi(l(x)).$$

□

Corollary 1.18. *Every nonzero q -polynomial over \mathbb{F}_q with simple roots has at least one q -primitive root over \mathbb{F}_q .*

We use q -primitive roots to construct a special type of basis for a q -modulus over \mathbb{F}_q .

Theorem 1.19. *Let M be a q -modulus of dimension $m \geq 1$ over \mathbb{F}_q . Then there exists an element $\zeta \in M$ such that $\{\zeta, \zeta^q, \zeta^{q^2}, \dots, \zeta^{q^{m-1}}\}$ is a basis of M over \mathbb{F}_q .*

Proof. Theorem 1.13 implies that $L(x) = \prod_{\beta \in M} (x - \beta)$ belongs to $Ore_q(\mathbb{F}_q)$. By the previous corollary, $L(x)$ has a q -primitive root ζ over \mathbb{F}_q . Then as a q -modulus, M contains the elements $\zeta, \zeta^q, \zeta^{q^2}, \dots, \zeta^{q^{m-1}}$. Assume that these elements are linearly dependent over \mathbb{F}_q . Then there exist elements $a_1, \dots, a_{m-1} \in \mathbb{F}_q$, not all of which are 0, such that

$$\sum_{i=0}^{m-1} a_i \zeta^{q^i} = 0,$$

which is a contradiction since $\deg(L(x)) = |M| = q^m$. Thus, these m elements form a basis of M over \mathbb{F}_q . □

A basis of $\mathbb{F}_{q^m} \subseteq \mathbb{F}$ over \mathbb{F}_q of the form $\{\zeta, \zeta^q, \dots, \zeta^{q^{m-1}}\}$ is called a *normal basis* of \mathbb{F}_{q^m} over \mathbb{F}_q . As a corollary of the next theorem, we will be able to calculate the number of different normal bases of \mathbb{F}_{q^m} over \mathbb{F}_q .

Theorem 1.20. *In \mathbb{F}_{q^m} there exist exactly $\Phi_q(x^m - 1)$ elements ζ which generates a normal basis of \mathbb{F}_{q^m} over \mathbb{F}_q .*

Proof. Since \mathbb{F}_{q^m} is a q -modulus, Theorem 1.19 guarantees the existence of normal bases of \mathbb{F}_{q^m} over \mathbb{F}_q . Here,

$$L(x) = \prod_{\beta \in \mathbb{F}_{q^m}} (x - \beta) = x^{q^m} - x.$$

By the proof of Theorem 1.19, we know that every q -primitive root of $L(x)$ over \mathbb{F}_q provides a basis of the desired type. On the other hand, if ζ is not a q -primitive root of $L(x)$ over \mathbb{F}_q than there exists a nontrivial \mathbb{F}_q -linear combination of $\zeta, \zeta^q, \zeta^{q^2}, \dots, \zeta^{q^{m-1}}$ which is equal to 0, i.e., these elements are linearly dependent over \mathbb{F}_q . Thus the elements generating a normal basis are exactly the q -primitive roots of $L(x)$ over \mathbb{F}_q . As a result, the number of such elements is equal to N_L , which is given by

$$\Phi_q(x^m - 1)$$

by Theorem 1.17. □

Corollary 1.21. *The number of different normal bases of \mathbb{F}_{q^m} over \mathbb{F}_q is given by $(1/m)\Phi_q(x^m - 1)$.*

Proof. Note that in a normal basis $\{\zeta, \zeta^q, \zeta^{q^2}, \dots, \zeta^{q^{m-1}}\}$, each element generates the same normal basis. Then the result follows from Theorem 1.20. □

Permutation Polynomials from Linearized Polynomials

During this section, let $q = p$ be a prime number and fix $\mathbb{F}_{p^n} \subseteq \mathbb{F}$. Let $Tr(x)$ be the polynomial defining the absolute trace function of \mathbb{F}_{p^n} . In this section our aim is to derive permutation polynomials of \mathbb{F}_{p^n} by using the polynomials in $Ore_p(\mathbb{F})$ with coefficient in \mathbb{F}_{p^n} . Specifically, we want to characterize the elements $\gamma \in \mathbb{F}_{p^n}$ and the polynomials $H(x) \in \mathbb{F}_{p^n}[x]$, $L(x) \in Ore_p(\mathbb{F})$ for which

$$F(x) = L(x) + \gamma Tr(H(x)) \quad (2.1)$$

is a permutation polynomial of \mathbb{F}_{p^n} , where the coefficients of $L(x)$ are in \mathbb{F}_{p^n} . Throughout the section let a linear mapping $L : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be the associated mapping of such an $L(x)$.

For the moment, consider the polynomial of the type

$$F(x) = G(x) + \gamma Tr(H(x)), \quad (2.2)$$

where $\gamma \in \mathbb{F}_{p^n}$, $G(x), H(x) \in \mathbb{F}_{p^n}[x]$. The next proposition presents a simple necessary condition on $G(x)$, for which (2.2) is a permutation of \mathbb{F}_{p^n} .

Proposition 2.1. *Let $F(x) \in \mathbb{F}_{p^n}[x]$ be a polynomial of type (2.2). Assume that $F(x)$ is a permutation of \mathbb{F}_{p^n} . Then for any $\beta \in \mathbb{F}_{p^n}$ there are at most p elements α with $G(\alpha) = \beta$.*

Proof. Assume that $G(\alpha_i) = \beta$ for distinct α_i , $i = 1, \dots, p, p+1$. Then

$$F(\alpha_i) = \beta + \gamma c_i \text{ where } c_i \in \mathbb{F}_p, 1 \leq i \leq p+1.$$

Since c_i can have at most p distinct values, by the pigeonhole principle, $F(\alpha_i) = F(\alpha_j)$ for some i and j where $1 \leq i < j \leq p+1$. Thus $F(x)$ is not a permutation polynomial of \mathbb{F}_{p^n} . \square

Consider $\text{Ker}(L)$, which is a linear subspace of \mathbb{F}_{p^n} , regarded as a vector space over \mathbb{F}_p . Let $|\text{Ker}(L)| = p^d$ where $0 \leq d \leq n$. Then the fiber of an element $\beta \in \mathbb{F}_{p^n}$ under the linear transformation L is given by

$$L^{-1}(\beta) = \{\alpha \in \mathbb{F}_{p^n} : L(\alpha) = \beta\} = \alpha_0 + \text{Ker}(L),$$

where $\alpha_0 \in \mathbb{F}_{p^n}$ is some element with $L(\alpha_0) = \beta$. Thus $|L^{-1}(\beta)| = p^d$ for all $\beta \in \text{Im}(L)$. Therefore, to construct a permutation polynomial of \mathbb{F}_{p^n} of type (2.1), L must necessarily be either bijective or p -to-1, by Proposition 2.1. The case that L is bijective can be examined separately to construct permutation polynomials of \mathbb{F}_{p^n} by using permutation polynomials of \mathbb{F}_{p^n} . So, in this paper we deal with the other case that L is a p -to-1 mapping. Note that if L is p -to-1 and $\alpha \in \text{Ker}(L)$ is nonzero then $c\alpha \in \text{Ker}(L)$ for all $c \in \mathbb{F}_p$, which implies that $\text{Ker}(L) = \alpha\mathbb{F}_p$.

Theorem 2.2. *Let $L : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be a p -to-1 linear mapping with kernel K and let $H : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$. Then the polynomial*

$$F(x) = L(x) + \gamma \text{Tr}(H(x)), \quad \gamma \in \mathbb{F}_{p^n},$$

is a permutation of \mathbb{F}_{p^n} if and only if

$$(i) \quad \gamma \notin \text{Im}(L), \text{ and}$$

$$(ii) \quad \text{Tr}(H(\alpha + \epsilon) - H(\alpha)) \neq 0 \text{ for any } \alpha \in \mathbb{F}_{p^n} \text{ and } \epsilon \in K \setminus \{0\}.$$

Proof. Assume that $\gamma \in \text{Im}(L)$, say $L(\alpha_1) = \gamma$. Let $F(\beta) = \mu$ and $\text{Tr}(H(\beta)) = c \in \mathbb{F}_p$. Then

$$\begin{aligned} \mu = F(\beta) &= L(\beta) + \gamma c \\ &= L(\beta) + L(c\alpha_1) = L(\beta + c\alpha_1), \end{aligned}$$

which yields that $\text{Im}(F) \subseteq \text{Im}(L)$. Thus F cannot be surjective since L is a p -to-1 mapping. Let $\alpha \in \mathbb{F}_{p^n}$ and $\epsilon \in K \setminus \{0\}$ be arbitrary elements. Then

$$\begin{aligned} F(\alpha + \epsilon) - F(\alpha) &= L(\alpha + \epsilon) - L(\alpha) + \gamma \text{Tr}(H(\alpha + \epsilon) - H(\alpha)) \\ &= \gamma \text{Tr}(H(\alpha + \epsilon) - H(\alpha)). \end{aligned}$$

Assume that $\text{Tr}(H(\alpha + \epsilon) - H(\alpha)) = 0$. Then $F(\alpha + \epsilon) = F(\alpha)$ while $\alpha + \epsilon \neq \alpha$. Hence, F cannot be an injective mapping. Therefore, the necessity of the conditions is proved.

For the converse, assume that the assumptions (i) and (ii) hold. Let $F(\alpha) = F(\beta)$ for some $\alpha, \beta \in \mathbb{F}_{p^n}$. Suppose that $\text{Tr}(H(\alpha) - H(\beta)) = c$, where $c \in \mathbb{F}_p^*$. Then

$$0 = F(\alpha) - F(\beta) = L(\alpha - \beta) + c\gamma,$$

which contradicts with (i) by implying $L(c^{-1}(\beta - \alpha)) = \gamma$. Then we have $\text{Tr}(H(\alpha) - H(\beta)) = 0$ and

$$0 = F(\alpha) - F(\beta) = L(\alpha - \beta),$$

which provides $\alpha - \beta \in K$. On the other hand,

$$\begin{aligned} \text{Tr}(H(\alpha) - H(\beta)) &= \text{Tr}(H(\beta + (\alpha - \beta)) - H(\beta)) \\ &= 0, \end{aligned}$$

where $\beta \in \mathbb{F}_{p^n}$ and $\alpha - \beta \in K$. Thus $\alpha = \beta$ by (ii), i.e., $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ is an injection. Therefore F is a permutation of \mathbb{F}_{p^n} . \square

Given $\sigma \in \mathbb{F}_{p^n}^*$ and $c \in \mathbb{F}_p$, denote by $\mathcal{H}_\sigma(c)$ the affine hyperplane

$$\{x \in \mathbb{F}_{p^n} : Tr(\sigma x) = c\}.$$

Consider the first condition of Theorem 2.2. We are given a p -to-1 linear mapping $L : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$. Since $\omega^{p^n} = \omega$ for all $\omega \in \mathbb{F}_{p^n}$, we can represent L as

$$L : \begin{cases} \mathbb{F}_{p^n} & \rightarrow \mathbb{F}_{p^n} \\ \omega & \mapsto \sum_{i=0}^{n-1} \alpha_i \omega^{p^i}, \end{cases}$$

where $\alpha_i \in \mathbb{F}_{p^n}$. We are supposed to check whether an element $\gamma \in \mathbb{F}_{p^n}$ belongs to $\text{Im}(L)$. Since $\text{Ker}(L)$ is a 1-dimensional subspace of \mathbb{F}_{p^n} over \mathbb{F}_p , $\text{Im}(L)$ should be a hyperplane, say $\mathcal{H}_\sigma(0)$, where the defining element $\sigma \in \mathbb{F}_{p^n}^*$ satisfies the following identity:

$$\begin{aligned} Tr(\sigma L(x)) &= Tr\left(\sigma \sum_{i=0}^{n-1} \alpha_i x^{p^i}\right) \\ &= Tr\left(\alpha_0 \sigma x + \alpha_1 \sigma x^p + \cdots + \alpha_{n-1} \sigma x^{p^{n-1}}\right) \\ &= Tr\left(\alpha_0^{p^n} \sigma^{p^n} x + \alpha_1^{p^{n-1}} \sigma^{p^{n-1}} x + \cdots + \alpha_{n-1}^p \sigma^p x\right) \\ &= Tr\left(\left(\sum_{i=0}^{n-1} \alpha_i^{p^{n-i}} \sigma^{p^{n-i}}\right) x\right) \\ &= Tr(L^*(\sigma)x) \\ &= 0 \end{aligned}$$

for any $x \in \mathbb{F}_{p^n}$, where

$$L^*(x) = \alpha_0 x + \sum_{i=1}^{n-1} \alpha_{n-i}^{p^i} x^{p^i},$$

a polynomial in $\text{Ore}_p(\mathbb{F})$ with coefficient in \mathbb{F}_{p^n} . If $L^*(\sigma) \neq 0$ then $Tr(x) = 0$ for all $x \in \mathbb{F}_{p^n}$, a contradiction. Hence, $L^*(\sigma) = 0$. As a conclusion, $\gamma \in \text{Im}(L)$ if and only if $Tr(\sigma\gamma) = 0$, where σ is a nonzero root of $L^*(x)$. Let us call $L^*(x)$ as the adjoint polynomial of $L(x)$ and $L^* : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ as the adjoint mapping of L . Now we claim that $\text{Ker}(L^*) = \sigma\mathbb{F}_p$, i.e. L^* is a p -to-1 mapping.

Theorem 2.3. *Let $L(x) = \sum_{i=0}^{n-1} \alpha_i x^{p^i}$ and let $L : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be a p -to-1 linear mapping. Then L^* is a p -to-1 linear mapping, too.*

Proof. As $L^*(x) \in \text{Ore}_p(\mathbb{F})$, it is known that L^* is a linear mapping. By construction, $L^*(x)$ has a nonzero root, $\sigma \in \mathbb{F}_{p^n}^*$, where $\text{Im}(L) = \mathcal{H}_\sigma(0)$. Let $\alpha_k \neq 0$ and $\alpha_i = 0$ for all $i < k$. Then by the proof of Theorem 1.5, we know that each root of $L(x)$ has

multiplicity p^k . Since $|\text{Ker}(L)| = p$, we obtain that $\deg(L(x)) = p^{k+1}$ and so $\alpha_i = 0$ for all $i > k + 1$. Then

$$L(x) = \alpha_k x^{p^k} + \alpha_{k+1} x^{p^{k+1}} \quad \text{and} \quad L^*(x) = \alpha_{k+1}^{p^{n-1-k}} x^{p^{n-1-k}} + \alpha_k^{p^{n-k}} x^{p^{n-k}},$$

which implies that each root of $L^*(x)$ has multiplicity p^{n-1-k} again by the proof of Theorem 1.5. So, we have

$$L^*(x) = \prod_{\beta \in \text{Ker}(L^*)} (x - \beta)^{p^{n-1-k}}.$$

Since $\deg(L^*(x)) = p^{n-k}$, we have proven that $|\text{Ker}(L^*)| = p$, i.e., L^* defines a p -to-1 mapping. \square

Now let us introduce the notion of a linear structure.

Definition 2.4. Let $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ and $c \in \mathbb{F}_p$. We say that $\alpha \in \mathbb{F}_{p^n}^*$ is a c -linear structure of the function f if

$$f(x + \alpha) - f(x) = c \text{ for all } x \in \mathbb{F}_{p^n}.$$

Proposition 2.5. Let $\alpha, \beta \in \mathbb{F}_{p^n}^*$, $\alpha + \beta \neq 0$ and $a, b \in \mathbb{F}_p$. If α is an a -linear structure and β is a b -linear structure of a function $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$, then

$$\alpha + \beta \text{ is an } (a + b)\text{-linear structure of } f$$

and for any $c \in \mathbb{F}_p^*$

$$c \cdot \alpha \text{ is a } (c \cdot a)\text{-linear structure of } f.$$

In particular, if Λ^* is the set of linear structures of f , then $\Lambda = \Lambda^* \cup \{0\}$ is an \mathbb{F}_p -linear subspace, which we call the linear space of f .

Proof.

$$\begin{aligned} f(x + (\alpha + \beta)) - f(x) &= f((x + \alpha) + \beta) - f(x + \alpha) + f(x + \alpha) - f(x) \\ &= b + a. \end{aligned}$$

Thus $\alpha + \beta$ is an $(a + b)$ -linear structure of f , i.e., $\alpha + \beta \in \Lambda^*$. Now take $\beta = \alpha$. Then 2α is a $2a$ -linear structure of f . Assume that $(c - 1)\alpha$ is a $(c - 1)a$ -linear structure of f , where $c \in \mathbb{F}_p^*$. Then

$$\begin{aligned} f(x + \alpha + (c - 1)\alpha) - f(x) &= f(x + \alpha + (c - 1)\alpha) - f(x + \alpha) + f(x + \alpha) - f(x) \\ &= (c - 1)a + a \\ &= ca. \end{aligned}$$

So $c\alpha$ is a (ca) -linear structure of f , i.e., $c\alpha \in \Lambda^*$. Hence we proved that Λ is an \mathbb{F}_p -linear subspace of \mathbb{F}_{p^n} . \square

By the next theorem, we will show that existence of a linear structure yields permutations of \mathbb{F}_{p^n} of type (2.1) under certain conditions.

Theorem 2.6. *Let $L : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be a p -to-1 linear mapping and $K = \alpha\mathbb{F}_p$ the kernel of L and $\sigma\mathbb{F}_p$ the kernel of its adjoint mapping L^* . Further let $H : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be such that α is a b -linear structure of $\text{Tr}(H(x))$. Then*

$$F(x) = L(x) + \gamma\text{Tr}(H(x)), \gamma \in \mathbb{F}_{p^n},$$

is a permutation of \mathbb{F}_{p^n} if and only if

- (i) $\text{Tr}(\sigma\gamma) \neq 0$ and
- (ii) $b \neq 0$.

Moreover, if $\text{Tr}(\sigma\gamma) \neq 0$ and $b = 0$ then F is a p -to-1 mapping of \mathbb{F}_{p^n} .

Proof. Via the remark on the first condition of Theorem 2.2,

$$\text{Tr}(\sigma\gamma) \neq 0 \Leftrightarrow \gamma \notin \text{Im}(L).$$

Also by Proposition 2.5, $c\alpha$ is a cb -linear structure of $\text{Tr}(H(x))$, for any $c \in \mathbb{F}_p^*$. Then

$$\text{Tr}(H(x + c\alpha) - H(x)) = cb \text{ for all } x \in \mathbb{F}_{p^n}.$$

Thus the proof of the first part of the theorem follows from Theorem 2.2. For the other part, suppose that $\text{Tr}(\sigma\gamma) \neq 0$ and $b = 0$. Fix $\beta \in \mathbb{F}_{p^n}$ and assume that $F(\beta) = F(\theta)$ for some $\theta \in \mathbb{F}_{p^n}$. Then

$$L(\beta - \theta) = \gamma u \text{ with } u = \text{Tr}(H(\theta) - H(\beta)).$$

If $u \neq 0$ then $L(u^{-1}(\beta - \theta)) = \gamma$, which cannot be the case. Thus $u = 0$ and $\beta - \theta \in K = \alpha\mathbb{F}_p$. So $\theta = \beta + c_0\alpha$ for some $c_0 \in \mathbb{F}_p$. On the other hand,

$$\text{Tr}(H(\beta + c\alpha) - H(\beta)) = 0 \text{ for any } c \in \mathbb{F}_p$$

by Proposition 2.5 and by the assumption that $b = 0$. Hence

$$F(\beta + c\alpha) = F(\beta) \text{ for any } c \in \mathbb{F}_p.$$

Therefore, F is a p -to-1 mapping. □

Lemma 2.7. *Let $H : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be an arbitrary mapping, $\gamma, \beta \in \mathbb{F}_{p^n}, \gamma \neq 0$ and $c = \text{Tr}(\beta\gamma)$. Then γ is a c -linear structure of $f(x) = \text{Tr}(R(x))$ where*

$$R(x) = H(x^p - \gamma^{p-1}x) + \beta x.$$

Proof. Note that

$$\begin{aligned} R(x + \gamma) &= H(x^p + \gamma^p - \gamma^{p-1}x - \gamma^p) + \beta x + \beta\gamma \\ &= R(x) + \beta\gamma. \end{aligned}$$

So

$$\begin{aligned} \text{Tr}(R(x + \gamma)) - \text{Tr}(R(x)) &= \text{Tr}(R(x + \gamma) - R(x)) \\ &= \text{Tr}(\beta\gamma) \\ &= c. \end{aligned}$$

for all $x \in \mathbb{F}_{p^n}$. □

Now we can explicitly describe two classes of permutation polynomials of \mathbb{F}_{p^n} of type (2.1).

Corollary 2.8. *Let $\alpha, \beta, \gamma \in \mathbb{F}_{p^n}, \alpha \neq 0$ and $H(x) \in \mathbb{F}_{p^n}[x]$.*

(i) *Then the polynomial*

$$F(x) = x^p - \alpha^{p-1}x + \gamma \text{Tr}(H(x^p - \alpha^{p-1}x) + \beta x)$$

is a permutation polynomial of \mathbb{F}_{p^n} if and only if $\text{Tr}(\gamma\alpha^{-p}) \neq 0$ and $\text{Tr}(\alpha\beta) \neq 0$.

(ii) *Then the polynomial*

$$F(x) = x^p - \alpha^{p-1}x + \gamma \text{Tr}\left(\sum_{u \in \mathbb{F}_p} H(x + u\alpha) + \beta x\right)$$

is a permutation polynomial of \mathbb{F}_{p^n} if and only if $\text{Tr}(\gamma\alpha^{-p}) \neq 0$ and $\text{Tr}(\alpha\beta) \neq 0$.

Proof. Let $L(x) = x^p - \alpha^{p-1}x$. Note that $\text{Ker}(L) = \alpha\mathbb{F}_p$ and $L^*(x) = x^{p^{n-1}} - \alpha^{p-1}x$ is the adjoint polynomial of $L(x)$ with the kernel $\alpha^{-p}\mathbb{F}_p$. Then by Theorem 2.6, the condition $\text{Tr}(\gamma\alpha^{-p}) \neq 0$ is clear in both (i) and (ii). To complete the proof, observe the following and again use Theorem 2.6.

- α is a $\text{Tr}(\alpha\beta)$ -linear structure of $\text{Tr}(H(x^p - \alpha^{p-1}x) + \beta x)$ by Lemma 2.7.
- Let $g(x) = \text{Tr}\left(\sum_{u \in \mathbb{F}_p} H(x + u\alpha) + \beta x\right)$. Then

$$\begin{aligned} g(x + \alpha) &= \text{Tr}\left(\sum_{u \in \mathbb{F}_p} H(x + (u+1)\alpha) + \beta x + \beta\alpha\right) \\ &= \text{Tr}\left(\sum_{u \in \mathbb{F}_p} H(x + u\alpha) + \beta x\right) + \text{Tr}(\beta\alpha) = g(x) + \text{Tr}(\beta\alpha). \end{aligned}$$

Thus, α is a $\text{Tr}(\alpha\beta)$ -linear structure of $g(x)$.

□

Let $\beta, \gamma \in \mathbb{F}_{p^n}^*$, $L_1(x) \in \text{Ore}_p(\mathbb{F})$ with coefficients in \mathbb{F}_{p^n} . Now we want to construct polynomials of the form

$$L(x) = L_1(x) + \gamma \text{Tr}(\beta x) \quad (2.3)$$

such that $L(x)$ is both a permutation of \mathbb{F}_{p^n} and a p -polynomial over \mathbb{F} . We desire to provide a characterization for γ, β and $L_1(x)$ by focusing on the dimension of the kernel of L_1 over \mathbb{F}_p . First, recall that

$$\mathcal{H}_\beta(0) = \{x \in \mathbb{F}_{p^n} : \text{Tr}(\beta x) = 0\}.$$

Lemma 2.9. *Let $L_1 : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be a linear mapping with kernel K_1 of dimension k_1 , $0 \leq k_1 \leq n - 1$, over \mathbb{F}_p and let $\gamma, \beta \in \mathbb{F}_{p^n}^*$. Define*

$$L(x) = L_1(x) + \gamma \text{Tr}(\beta x).$$

Then the kernel K of L has dimension $k \in \{k_1 - 1, k_1, k_1 + 1\}$ over \mathbb{F}_p depending on the cases described below:

(i) $\gamma \in \text{Im}(L_1)$ then

- (a) $k = k_1 + 1$ if $K_1 \subseteq \mathcal{H}_\beta(0)$ and there exists an element g satisfying $L_1(g) = \gamma$ and $\text{Tr}(\beta g) = -1$;
- (b) otherwise $k = k_1$.

(ii) $\gamma \notin \text{Im}(L_1)$ then

- (a) $k = k_1 - 1$ if $K_1 \not\subseteq \mathcal{H}_\beta(0)$;
- (b) $k = k_1$ if $K_1 \subseteq \mathcal{H}_\beta(0)$.

Proof. To begin note that any k -dimensional subspace of \mathbb{F}_{p^n} over \mathbb{F}_p is either contained in $\mathcal{H}_\beta(0)$ or intersects it in a subspace of dimension $k - 1$ over \mathbb{F}_p .

(i) Suppose that $\gamma \in \text{Im}(L_1)$. Then $\text{Im}(L) \subseteq \text{Im}(L_1)$, which implies that

$$k_1 \leq k. \quad (2.4)$$

- (a) Assume that $g \in \mathbb{F}_{p^n}$ satisfies $L_1(g) = \gamma$ and $\text{Tr}(\beta g) = -1$. Take an element $\alpha_0 \in K$. Then

$$\begin{aligned} L_1(\alpha_0) &= -\gamma \text{Tr}(\beta \alpha_0) \\ &= L_1(g)c_0, \end{aligned}$$

where $c_0 = -\text{Tr}(\beta \alpha_0) \in \mathbb{F}_p$. So we have $L_1(\alpha_0 - c_0g) = 0$, which means that $\alpha_0 - c_0g \in K_1$ for some $c_0 \in \mathbb{F}_p$. Thus

$$K \subseteq \{\delta + cg : \delta \in K_1, c \in \mathbb{F}_p\} =: A.$$

Now take an element $\delta + cg \in A$.

$$\begin{aligned} L(\delta + cg) &= L_1(\delta) + L_1(cg) + \gamma \text{Tr}(\beta\delta) + \gamma \text{Tr}(\beta cg) \\ &= c\gamma + \gamma \text{Tr}(\beta\delta) - c\gamma \\ &= \gamma \text{Tr}(\beta\delta) \end{aligned}$$

So if $\delta \in \mathcal{H}_\beta(0)$ then $\delta + cg \in K$. Hence

$$K = \{\delta + cg : \delta \in K_1 \cap \mathcal{H}_\beta(0), c \in \mathbb{F}_p\},$$

where $g \in \mathbb{F}_{p^n}$ satisfies $L_1(g) = \gamma$ and $\text{Tr}(\beta g) = -1$. If we assume further that $K_1 \subseteq \mathcal{H}_\beta(0)$ then we get the result that

$$k = k_1 + 1.$$

- (b) We want to prove $k = k_1$ provided that either there does not exist $g \in \mathbb{F}_{p^n}$ such that $L_1(g) = \gamma$ and $\text{Tr}(\beta g) = -1$ or $K_1 \not\subseteq \mathcal{H}_\beta(0)$. By contraposition method, assume that $k \neq k_1$. Then by (2.4), we have

$$k > k_1. \tag{2.5}$$

Let $\alpha_0 \in K$. Then

$$L_1(\alpha_0) = \gamma c_0,$$

where $c_0 = -\text{Tr}(\beta\alpha_0) \in \mathbb{F}_p$. If $c_0 = 0$ then $\alpha_0 \in K_1$, which results in a contradiction by (2.5). So $c_0 \neq 0$. Set $g = c_0^{-1}\alpha_0$. Then

$$L_1(g) = \gamma \text{ and } \text{Tr}(\beta g) = -1. \tag{2.6}$$

Thus existence of an element $g \in \mathbb{F}_{p^n}$ satisfying (2.6) implies that

$$K = \{\delta + cg : \delta \in K_1 \cap \mathcal{H}_\beta(0), c \in \mathbb{F}_p\},$$

by the previous discussion. The assumption $k > k_1$ forces $K_1 \cap \mathcal{H}_\beta(0)$ to have dimension k_1 over \mathbb{F}_p , in other words,

$$K_1 \subseteq \mathcal{H}_\beta(0).$$

- (ii) Suppose that $\gamma \neq \text{Im}(L_1)$. Take $\alpha_0 \in K$. Then

$$L_1(\alpha_0) = \gamma c_0,$$

where $c_0 = -\text{Tr}(\beta\alpha_0)$. If $c_0 \neq 0$ then $L_1(c_0^{-1}\alpha_0) = \gamma$, a contradiction. Thus $\text{Tr}(\beta\alpha_0) = 0$ and consequently $L_1(\alpha_0) = 0$. Then $K \subseteq K_1 \cap \mathcal{H}_\beta(0)$. Also it is obvious that $K_1 \cap \mathcal{H}_\beta(0) \subseteq K$. Therefore

$$K = K_1 \cap \mathcal{H}_\beta(0).$$

So we have

- (a) if $K_1 \not\subseteq \mathcal{H}_\beta(0)$ then $k = k_1 - 1$;
- (b) if $K_1 \subseteq \mathcal{H}_\beta(0)$ then $k = k_1$.

□

We use this lemma in order to obtain permutation polynomials of \mathbb{F}_{p^n} in $Ore_p(\mathbb{F})$ of type (2.3).

Theorem 2.10. *Let $L_1 : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be a linear mapping and let $\gamma, \beta \in \mathbb{F}_{p^n}^*$. Then the p -polynomial*

$$L(x) = L_1(x) + \gamma \text{Tr}(\beta x)$$

over \mathbb{F} is a permutation polynomial of \mathbb{F}_{p^n} if and only if (i) or (ii) is fulfilled:

- (i) $L_1(x)$ is a permutation polynomial of \mathbb{F}_{p^n} and $\text{Tr}(\beta L_1^{-1}(\gamma)) \neq -1$, where L_1^{-1} is the inverse mapping of L_1 ;
- (ii) $L_1(x)$ defines a p -to-1 mapping on \mathbb{F}_{p^n} with kernel $\alpha \mathbb{F}_p$. Moreover, $\gamma \notin \text{Im}(L_1)$ and $\text{Tr}(\beta \alpha) \neq 0$.

Proof. Let k and k_1 be the dimensions of kernels of L and L_1 over \mathbb{F}_p , respectively. Suppose that $L(x)$ is a permutation polynomial, i.e., $k = 0$. Then according to Lemma 2.9, k_1 is equal to either 0 or 1. So we have two cases:

- (i) $k_1 = 0$. Then L_1 is a permutation of \mathbb{F}_{p^n} and $\gamma \in \text{Im}(L_1)$. By Lemma 2.9, this is only possible either if kernel of L_1 is not contained in the hyperplane $\mathcal{H}_\beta(0)$ or if $\text{Tr}(\beta L_1^{-1}(\gamma)) \neq -1$. Since $\text{Ker}(L_1) = \{0\} \subseteq \mathcal{H}_\beta(0)$, we conclude that

$$\text{Tr}(\beta L_1^{-1}(\gamma)) \neq -1.$$

- (ii) $k_1 = 1$, i.e., L_1 is a p -to-1 linear mapping. Thus we have the condition that $\gamma \notin \text{Im}(L)$ as well as $\alpha \mathbb{F}_p \not\subseteq \mathcal{H}_\beta(0)$ by Lemma 2.9, which is equivalent to the second condition of the theorem.

The converse directly results from Lemma 2.9. □

Note that the equivalence of the second case, (ii), in the above theorem can also be shown by Theorem 2.2 or Theorem 2.6 by letting $H(x) = \beta x$.

Dimension of Kernels of Linearized Polynomials

In the previous section, to construct permutation polynomials of $\mathbb{F}_{p^n} \subseteq \mathbb{F}$, we have used polynomials of the form $L(x) = \sum_{i=0}^{n-1} \alpha_i x^{p^i}$, $\alpha_i \in \mathbb{F}_{p^n}$, whose kernels are of dimension 1. Thus, we are motivated to find the explicit representations of such polynomials.

Let q be a prime power and let

$$L(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i}, \alpha_i \in \mathbb{F}_{q^n}. \quad (3.1)$$

We achieve our aim by giving several explicit representations and the number of the polynomials of the form (3.1) such that kernel of L is of any given dimension.

In this section, we have the following notations. For $m, n \in \mathbb{Z}^+$, the space of $m \times n$ matrices over \mathbb{F}_q is denoted by $\mathbb{F}_q^{m \times n}$. For any matrix A over \mathbb{F}_q , $\text{Rank}_{\mathbb{F}_q}(A)$ denotes the rank of A . For a set of vectors $\{v_1, \dots, v_r\}$ of the same length over \mathbb{F}_q , $\text{Span}(v_1, \dots, v_r)$ denotes the vector space spanned by $\{v_1, \dots, v_r\}$ over \mathbb{F}_q , and $\text{Rank}_{\mathbb{F}_q}\{v_1, \dots, v_r\}$ is the dimension of $\text{Span}(v_1, \dots, v_r)$ over \mathbb{F}_q . $\text{Tr}(x)$ is the trace function from \mathbb{F}_{q^n} to \mathbb{F}_q .

Lemma 3.1. *Let $m, n, k \in \mathbb{Z}^+$, $k \leq \min\{m, n\}$ and*

$$S_k(m, n) = \{A \in \mathbb{F}_q^{m \times n} : \text{Rank}_{\mathbb{F}_q}(A) = k\}.$$

Then

$$|S_k(m, n)| = \frac{\prod_{i=0}^{k-1} (q^m - q^i)(q^n - q^i)}{\prod_{i=0}^{k-1} (q^k - q^i)}.$$

Proof. Let $A = [\alpha_1, \alpha_2, \dots, \alpha_n] \in S_k(m, n)$ where $\alpha_i \in \mathbb{F}_q^m$ and let

$$V = \text{Span}(\alpha_1, \alpha_2, \dots, \alpha_n).$$

Then $\dim_{\mathbb{F}_q}(V) = k$. Note that there are

$$\prod_{i=0}^{k-1} (q^m - q^i)$$

ways of ordering k elements in \mathbb{F}_q^m that are linearly independent over \mathbb{F}_q while

$$\prod_{i=0}^{k-1} (q^k - q^i)$$

gives the number of distinct ordered bases of a subspace of \mathbb{F}_q^m with dimension k . Thus, there are

$$\frac{\prod_{i=0}^{k-1} (q^m - q^i)}{\prod_{i=0}^{k-1} (q^k - q^i)}$$

different subspaces with dimension k in \mathbb{F}_q^m . Once a k -dimensional subspace V is fixed, we have to choose n vectors with rank k from V to construct A . Let $\{\beta_1, \beta_2, \dots, \beta_k\}$ be a basis of V over \mathbb{F}_q . Then we have

$$A = [\beta_1, \beta_2, \dots, \beta_k]B,$$

where $B \in \mathbb{F}_q^{k \times n}$ is unique with rank k . There are

$$\prod_{i=0}^{k-1} (q^n - q^i)$$

different choices for the matrix B . To conclude,

$$|S_k(m, n)| = \frac{\prod_{i=0}^{k-1} (q^m - q^i)(q^n - q^i)}{\prod_{i=0}^{k-1} (q^k - q^i)}.$$

□

Lemma 3.2. *Let $L(x)$ be of the form (3.1) such that $L(x) \in \mathbb{F}_q$ for all $x \in \mathbb{F}_{q^n}$. Then there is a unique element $\theta \in \mathbb{F}_{q^n}$ such that $L(x) = \text{Tr}(\theta x)$.*

Proof. Note that the set of linear transformations from \mathbb{F}_{q^n} to \mathbb{F}_q has cardinality q^n . On the other hand, the set $\{\text{Tr}(\theta x), \theta \in \mathbb{F}_{q^n}\}$ contains q^n distinct linearized polynomials over \mathbb{F}_{q^n} such that $\text{Tr}(\theta x) \in \mathbb{F}_q$ for all $x \in \mathbb{F}_{q^n}$. Thus, the result is clear. □

Now can present the first results satisfying our main goal in this section.

Theorem 3.3. *Let $\{\beta_1, \beta_2, \dots, \beta_n\}$ be any given basis of \mathbb{F}_{q^n} over \mathbb{F}_q and let $L(x)$ be of the form (3.1). Then there exists a unique vector $(\theta_1, \theta_2, \dots, \theta_n) \in \mathbb{F}_{q^n}^n$ such that*

$$L(x) = \text{Tr}(\theta_1 x)\beta_1 + \dots + \text{Tr}(\theta_n x)\beta_n = \sum_{i=0}^{n-1} \left(\sum_{j=1}^n \beta_j \theta_j^{q^i} \right) x^{q^i}. \quad (3.2)$$

Moreover, let k be an integer such that $0 \leq k \leq n$, then $\dim_{\mathbb{F}_q}(\text{Ker}(L)) = k$ if and only if $\text{Rank}_{\mathbb{F}_q}\{\theta_1, \theta_2, \dots, \theta_n\} = n - k$. In particular, $k = n$ if and only if $L(x) \equiv 0$. If $k < n$, then there are exactly

$$\frac{\prod_{i=0}^{n-k-1} (q^n - q^i)^2}{\prod_{i=0}^{n-k-1} (q^{n-k} - q^i)}$$

different $L(x)$ of the form (3.1) with coefficients in \mathbb{F}_{q^n} and with $\dim_{\mathbb{F}_q}(\text{Ker}(L)) = k$.

Proof. The equation (3.2) follows from the Lemma 3.2. Let $W = \text{Span}(\theta_1, \dots, \theta_n)$ and define the orthogonal complement

$$W^\top = \{\alpha \in \mathbb{F}_{q^n} : \text{Tr}(\theta\alpha) = 0 \text{ for every } \theta \in W\}.$$

Since $\text{Tr} : \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q$ is a non-degenerate bilinear form, we have

$$n = \dim W^\top + \dim W.$$

We also have

$$\text{Ker}(L) = \{\alpha \in \mathbb{F}_{q^n} : \text{Tr}(\theta_i\alpha) = 0, 1 \leq i \leq n\} = W^\top.$$

Thus,

$$\dim_{\mathbb{F}_q} \text{Ker}(L) = \dim_{\mathbb{F}_q} W^\top = n - \dim_{\mathbb{F}_q} W = n - \text{Rank}_{\mathbb{F}_q} \{\theta_1, \theta_2, \dots, \theta_n\}.$$

Via this equality, we get the result that the number of $L(x)$ of the form (3.2) with $\dim_{\mathbb{F}_q}(\text{Ker}(L)) = k < n$ is the number of vector sets $\{\theta_1, \theta_2, \dots, \theta_n\}$ in \mathbb{F}_{q^n} with rank $n - k$, which is $|S_{n-k}(n, n)|$. Also it is obvious that $\dim_{\mathbb{F}_q}(\text{Ker}(L)) = n$ if and only if $L(x) \equiv 0$. \square

Theorem 3.4. *Let $\{\theta_1, \theta_2, \dots, \theta_n\}$ be any given basis of \mathbb{F}_{q^n} over \mathbb{F}_q , and let*

$$L(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i} \in \text{Ore}_q(\mathbb{F}), \text{ where } \alpha_i \in \mathbb{F}_{q^n}.$$

(i) *Then there exists a unique vector $(\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{F}_{q^n}^n$ such that*

$$L(x) = \text{Tr}(\theta_1 x)\beta_1 + \dots + \text{Tr}(\theta_n x)\beta_n = \sum_{i=0}^{n-1} \left(\sum_{j=1}^n \beta_j \theta_j^{q^i} \right) x^{q^i}. \quad (3.3)$$

(ii) *Let $D = [d_{i,j}]_{n \times n}$ be a square matrix of size n over \mathbb{F}_{q^n} , where $d_{i,j} = \theta_j^{q^{i-1}}$, $1 \leq i, j \leq n$. Then D is invertible and*

$$(\beta_1, \beta_2, \dots, \beta_n)^T = D^{-1}(\alpha_0, \alpha_2, \dots, \alpha_{n-1})^T,$$

where T denotes the transpose.

(iii) *Let k be an integer such that $0 \leq k \leq n$. Then $\dim_{\mathbb{F}_q}(\text{Ker}(L)) = k$ if and only if $\text{Rank}_{\mathbb{F}_q} \{\beta_1, \beta_2, \dots, \beta_n\} = n - k$.*

Proof. (i) We will construct a one to one correspondence between the vectors in $\mathbb{F}_{q^n}^n$ and the polynomials in $\text{Ore}_q(\mathbb{F})$ of degree $n - 1$ with coefficients in \mathbb{F}_{q^n} . Define

$$\Phi : \mathbb{F}_{q^n}^n \rightarrow \text{Ore}_q(\mathbb{F}) \text{ as}$$

$$\Phi : \beta = (\beta_1, \beta_2, \dots, \beta_n) \mapsto L_\beta(x) = \text{Tr}(\theta_1 x)\beta_1 + \text{Tr}(\theta_2 x)\beta_2 + \dots + \text{Tr}(\theta_n x)\beta_n.$$

Then $L_\beta(x) \in \mathbb{F}_{q^n}[x]$. For an element $\beta \in \text{Ker}(\Phi)$, we have

$$L_\beta(x) \equiv 0. \quad (3.4)$$

Since $\text{Tr}(\theta_i x)$, $1 \leq i \leq n$, runs through all the elements in \mathbb{F}_q as x runs over \mathbb{F}_{q^n} , (3.4) is possible only if $\beta = 0$. Thus, Φ is an injective mapping between two sets of the same cardinality, q^{n^2} . Therefore, Φ is a bijection, that is, for $L(x)$, there exists a unique vector $(\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{F}_{q^n}$ satisfying (3.3).

(ii) The equation (3.3) implies that

$$\alpha_i = \sum_{j=1}^n \beta_j \theta_j^{q^i}, \quad 0 \leq i \leq n-1,$$

which is equivalent to

$$\begin{aligned} (\alpha_0, \alpha_1, \dots, \alpha_{n-1})^T &= \begin{pmatrix} \theta_1 & \theta_2 & \dots & \theta_n \\ \theta_1^q & \theta_2^q & \dots & \theta_n^q \\ \vdots & \vdots & & \vdots \\ \theta_1^{q^{n-1}} & \theta_2^{q^{n-1}} & \dots & \theta_n^{q^{n-1}} \end{pmatrix} (\beta_1, \beta_2, \dots, \beta_n)^T \\ &= D(\beta_1, \beta_2, \dots, \beta_n)^T. \end{aligned}$$

The fact that D is invertible stems from Lemma 1.4 since $\{\theta_1, \theta_2, \dots, \theta_n\}$ is a basis of \mathbb{F}_{q^n} over \mathbb{F}_q . Thus, we obtain the result.

(iii) From (3.3), we know that $L(x)$ runs over all the linear combinations of $\beta_1, \beta_2, \dots, \beta_n$ over \mathbb{F}_q as x runs over \mathbb{F}_{q^n} . Therefore, $\dim_{\mathbb{F}_q}(\text{Ker}(L)) = k$ implies that

$$n - k = \dim_{\mathbb{F}_q} \text{Im}(L) = \text{Rank}_{\mathbb{F}_q} \{\beta_1, \beta_2, \dots, \beta_n\}.$$

□

Note that the conditions in both of Theorem 3.3 and Theorem 3.4 are necessary and sufficient. Thus, any polynomial of the form (3.1) whose kernel is of any given dimension can be represented uniquely in the forms (3.2) and (3.3). Also observe that these representations involve $2n$ elements in \mathbb{F}_{q^n} . Now we give another representation which uses $2n - 2k$ elements.

Theorem 3.5. *Let $L(x)$ be of the form (3.1) and let k be an integer such that $0 \leq k \leq n$. Then $\dim_{\mathbb{F}_q}(\text{Ker}(L)) = k$ if and only if there exist two vector sets over \mathbb{F}_{q^n} with rank $n - k$ over \mathbb{F}_q , $\{\omega_1, \omega_2, \dots, \omega_{n-k}\}$ and $\{\gamma_1, \gamma_2, \dots, \gamma_{n-k}\}$, such that*

$$L(x) = \sum_{i=1}^{n-k} \text{Tr}(\gamma_i x) \omega_i = \sum_{i=0}^{n-1} \left(\sum_{j=1}^{n-k} \omega_j \gamma_j^{q^i} \right) x^{q^i}. \quad (3.5)$$

Proof. Fix a basis $\{\theta_1, \theta_2, \dots, \theta_n\}$ of \mathbb{F}_q^n over \mathbb{F}_q . Assume that $\dim_{\mathbb{F}_q}(\text{Ker}(L)) = k$. Then by Theorem 3.4, there exists a unique vector $(\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{F}_q^n$ with rank $n - k$ over \mathbb{F}_q satisfying

$$L(x) = \sum_{j=1}^n \text{Tr}(\theta_j x) \beta_j.$$

Let

$$\beta_j = \sum_{i=1}^{n-k} c_{i,j} \omega_i, c_{i,j} \in \mathbb{F}_q, 1 \leq j \leq n,$$

where $\omega_1, \omega_2, \dots, \omega_{n-k}$ form a basis for $\text{Span}(\beta_1, \beta_2, \dots, \beta_n)$ and denote $C = [c_{i,j}]_{(n-k) \times n}$. Then

$$\text{Rank}_{\mathbb{F}_q}(C) = n - k$$

and

$$L(x) = \sum_{j=1}^n \text{Tr}(\theta_j x) \sum_{i=1}^{n-k} c_{i,j} \omega_i = \sum_{i=1}^{n-k} \omega_i \sum_{j=1}^n \text{Tr}(c_{i,j} \theta_j x) = \sum_{i=1}^{n-k} \omega_i \text{Tr} \left(\left(\sum_{j=1}^n c_{i,j} \theta_j \right) x \right). \quad (3.6)$$

Set

$$\gamma_i = \sum_{j=1}^n c_{i,j} \theta_j, 1 \leq i \leq n - k.$$

Thus, (3.5) is satisfied by the remark that

$$\text{Rank}_{\mathbb{F}_q} \{\gamma_1, \gamma_2, \dots, \gamma_{n-k}\} = \text{Rank}_{\mathbb{F}_q}(C) = n - k.$$

For the converse, assume that the conditions of the theorem hold. Let $\gamma_i, 1 \leq i \leq n - k$, have the linear representation in terms of the basis elements as follows

$$\gamma_i = \sum_{j=1}^n c_{i,j} \theta_j, c_{i,j} \in \mathbb{F}_q$$

and denote $C = [c_{i,j}]_{(n-k) \times n}$. Then

$$\text{Rank}_{\mathbb{F}_q}(C) = n - k$$

and by the assumption (3.5) and by the equality (3.6), we get

$$L(x) = \sum_{j=1}^n \text{Tr}(\theta_j x) \sum_{i=1}^{n-k} c_{i,j} \omega_i.$$

Set

$$\beta_j = \sum_{i=1}^{n-k} c_{i,j} \omega_i, 1 \leq j \leq n.$$

Thus, since

$$\text{Rank}_{\mathbb{F}_q} \{\beta_1, \beta_2, \dots, \beta_n\} = \text{Rank}_{\mathbb{F}_q}(C) = n - k,$$

$\dim_{\mathbb{F}_q}(\text{Ker}(L)) = k$ by Theorem 3.4. □

Observe that the representations given by Theorem 3.3 and Theorem 3.4 are unique while the one given by Theorem 3.5 is not unique. Call the matrix C in the previous proof as the corresponding matrix of the representation (3.5). Among the representations of $L(x)$ of the form (3.5), one of them provides a unique representation in terms of the corresponding matrix.

Theorem 3.6. *Let $\{\theta_1, \theta_2, \dots, \theta_n\}$ be any given basis of \mathbb{F}_{q^n} over \mathbb{F}_q and let k be an integer such that $0 \leq k \leq n$. Then all the polynomials of the form (3.1) with kernel of dimension k are uniquely given by*

$$L(x) = \sum_{i=1}^{n-k} \text{Tr}(\gamma_i x) \omega_i = \sum_{i=0}^{n-1} \left(\sum_{j=1}^{n-k} \omega_j \gamma_j^{q^i} \right) x^{q^i}, \quad (3.7)$$

where ω_i, γ_i satisfy the following conditions:

- (i) $\{\omega_1, \omega_2, \dots, \omega_{n-k}\}$ is some vector set over \mathbb{F}_{q^n} with rank $n - k$ over \mathbb{F}_q ,
- (ii) $\gamma_i = \sum_{j=1}^n c_{i,j} \theta_j$, $c_{i,j} \in \mathbb{F}_q$, $1 \leq i \leq n - k$, $1 \leq j \leq n$, where $C = [c_{i,j}]_{(n-k) \times n}$ is in reduced row echelon form of rank $n - k$.

Proof. Let $L(x)$ of the form (3.1) with $\dim_{\mathbb{F}_q}(\text{Ker}(L)) = k$. Then there exists a unique vector $(\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{F}_{q^n}^n$ with $\text{Rank}_{\mathbb{F}_q}\{\beta_1, \beta_2, \dots, \beta_n\} = n - k$ such that $L(x) = \sum_{i=1}^n \text{Tr}(\theta_i x) \beta_i$ by Theorem 3.4. Moreover, $L(x)$ can be represented as

$$L(x) = \sum_{i=1}^{n-k} \text{Tr}(\gamma_i x) \omega_i, \quad (3.8)$$

where ω_i and γ_i are as in the proof of Theorem 3.5 with the corresponding matrix $C \in \mathbb{F}_q^{(n-k) \times n}$. Then C is of rank $n - k$. First, we show the existence of the representation (3.7). Let C' be the unique reduced row echelon form of C . Then there exists a unique invertible matrix P such that $C = PC'$. Let

$$\begin{aligned} (\omega'_1, \omega'_2, \dots, \omega'_{n-k}) &= (\omega_1, \omega_2, \dots, \omega_{n-k})P \\ (\gamma'_1, \gamma'_2, \dots, \gamma'_{n-k})^T &= C'(\theta_1, \theta_2, \dots, \theta_n)^T. \end{aligned}$$

Since $\{\omega_1, \omega_2, \dots, \omega_{n-k}\}$ is a basis of $\text{Span}(\beta_1, \beta_2, \dots, \beta_n)$ over \mathbb{F}_q with the corresponding matrix C , we have

$$\begin{aligned} (\beta_1, \beta_2, \dots, \beta_n) &= (\omega_1, \omega_2, \dots, \omega_{n-k})C \\ &= (\omega_1, \omega_2, \dots, \omega_{n-k})PC' = (\omega'_1, \omega'_2, \dots, \omega'_{n-k})C'. \end{aligned}$$

Thus, by Theorem 3.5 and its proof, $L(x)$ can be represented as

$$L(x) = \sum_{i=1}^{n-k} \text{Tr}(\gamma'_i x) \omega'_i,$$

with the corresponding matrix C' , where ω'_i and γ'_i satisfy (i) and (ii). Therefore, to get the uniqueness of the representation (3.7), it suffices to show the uniqueness of C' . Let

$$\sum_{i=1}^{n-k} \text{Tr}(\gamma_i x) \omega_i = L(x) = \sum_{i=1}^{n-k} \text{Tr}(\bar{\gamma}_i x) \bar{\omega}_i$$

be two representations of $L(x)$ of the form (3.8) with the corresponding matrices C and \bar{C} , respectively. Then $\{\omega_1, \omega_2, \dots, \omega_{n-k}\}$ and $\{\bar{\omega}_1, \bar{\omega}_2, \dots, \bar{\omega}_{n-k}\}$ are bases over \mathbb{F}_q of the same vector space, $\text{Span}(\beta_1, \beta_2, \dots, \beta_n)$, again by Theorem 3.5 and its proof. It follows that there exists an invertible matrix P such that

$$(\bar{\omega}_1, \bar{\omega}_2, \dots, \bar{\omega}_{n-k}) = (\omega_1, \omega_2, \dots, \omega_{n-k})P.$$

Thus, we have

$$\begin{aligned} (\omega_1, \omega_2, \dots, \omega_{n-k})C &= (\beta_1, \beta_2, \dots, \beta_n) \\ &= (\bar{\omega}_1, \bar{\omega}_2, \dots, \bar{\omega}_{n-k})\bar{C} = (\omega_1, \omega_2, \dots, \omega_{n-k})P\bar{C}. \end{aligned}$$

Therefore,

$$C = P\bar{C},$$


that is, C and \bar{C} have the same reduced row echelon form. □

Bibliography

- [1] O. Ore, On a special class of polynomials, *Trans. Amer. Math. Soc.* **35** (1933) 559-584.
- [2] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia Math. Appl., vol. 20, *Cambridge University Press, Cambridge* (1997).
- [3] P. Charpin, G. Kyureghyan, When does $G(x) + \gamma \text{Tr}(H(x))$ permute \mathbb{F}_{p^n} ?, *Finite Fields Appl.* **15** (2009) 615-632.
- [4] S. Ling, L.J. Qu, A note on linearized polynomials and the dimension of their kernels, *Finite Fields Appl.* **18** (2012) 56-62.
- [5] P. Yuan, X. Zeng, A note on linear permutation polynomials, *Finite Fields Appl.* **17** (5) (2011) 488-491.
- [6] K. Zhou, A remark on linear permutation polynomials, *Finite Fields Appl.* **14** (2008) 532-536.

LINEARIZED POLYNOMIALS OVER FINITE FIELDS

APPROVED BY

Prof. Dr. Henning Stichtenoth 
(Thesis Supervisor)

Prof. Dr. Alev Topuzođlu 

Assoc. Prof. Cem Güneri 

Asst. Prof. Kađan Kurşungöz 

Assoc. Prof. Özgür Gürbüz 

DATE OF APPROVAL: May 30, 2012