

The Pennsylvania State University

The Graduate School

Department of Mathematics

PERMUTATION POLYNOMIALS ON FINITE FIELDS  
AND COMBINATORIAL APPLICATIONS

A Thesis in

Mathematics

by

Wun-Seng Chou

©1990 Wun-Seng Chou

Submitted in Partial Fulfillment  
of the Requirements  
for the Degree of

Doctor of Philosophy

May 1990

We approve the thesis of Wun-Seng Chou

Date of Signature

Gary L. Mullen

Gary L. Mullen  
Professor of Mathematics  
Chair of Committee  
Thesis Advisor

3/19/90

W. Dale Brownawell

W. Dale Brownawell  
Professor of Mathematics

20 March 1990

Wen-Chip Winnie Li

W. C. Winnie Li  
Professor of Mathematics

March 20, 1990

Robert A. Hultquist

Robert A. Hultquist  
Professor of Statistics

March 20, 1990

Richard H. Herman

Richard H. Herman  
Professor of Mathematics  
Head of the Department of Mathematics

Mar 20, 1990

## ABSTRACT

This thesis discusses some topics in finite field theory and their applications in combinatorics. For finite field theory, set complete mappings are defined and studied, and as a combinatorial application, we consider generalized pandiagonal Latin squares defined over finite fields.

It is well known that every mapping from a finite field into itself can be expressed as a polynomial over this field. Some polynomials such as permutation polynomials and complete mappings over finite fields are not only quite interesting but very useful as well. Permutation polynomials have been studied extensively for a long time. Complete mappings are a special kind of permutation polynomials. Both of them have been applied to combinatorics, finite geometries, recreational mathematics and statistics.

In Chapter 2, set complete mappings over finite fields, which are generalizations of both permutation polynomials and complete mappings, are defined and some properties of set complete mappings are studied. In addition, some criteria for special kinds of polynomials to be set complete mappings are given and relations between set complete mappings based on different sets are discussed. Finally, in the last section, very complete mappings, which are a special kind of set complete mappings, are studied.

A pandiagonal Latin square is a Latin square with the property that each of the wrap-around right or left diagonals consists of all symbols appearing in the square. Such squares have been used in statistical or experimental design theory. In Chapter 3, generalizing the usual pandiagonal Latin square transformations, we consider the generalized pandiagonal Latin square transformations over finite fields. The group

structure of all such generalized pandiagonal Latin square transformations is determined, and generalized pandiagonal Latin squares are constructed using generalized pandiagonal Latin square transformations. As an application of very complete mappings, several methods to construct generalized pandiagonal Latin squares have been given.

Finally, some properties and criteria concerning permutation polynomials are given in Chapter 4.



## TABLE OF CONTENTS

LIST OF TABLES .....	vi
ACKNOWLEDGEMENT .....	vii
Chapter 1. PRELIMINARIES .....	1
1. Groups .....	1
2. Fields .....	3
3. Linear Algebra .....	5
4. Permutation Polynomials Over Finite Fields .....	10
Chapter 2. SET COMPLETE MAPPINGS ON FINITE FIELDS .....	17
1. Introduction .....	17
2. Definition and Existence of Set Complete Mappings .....	18
3. Mullen's Conjecture .....	32
4. Properties and Comparisons .....	39
5. Very Complete Mappings .....	49
Chapter 3. GENERALIZED PANDIAGONAL LATIN SQUARES OF ORDER $q$ .....	58
1. Introduction .....	58
2. Group Structure of PLS-Transformations on $F_q \times F_q$ .....	59
3. Generalized Pandiagonal Latin Squares Over $F_q$ .....	70
Chapter 4. MISCELLANEOUS PROPERTIES OF PERMUTATION POLYNOMIALS .....	85
1. Properties of Permutation Polynomials .....	85
2. The Polynomial $1+x+x^2+\dots+x^k$ .....	91
3. Binomial Permutations .....	99
REFERENCES .....	106

# LIST OF TABLES

## Table

1	List of complete mapping polynomials of degree $\leq 6$ .....	50
2	List of very complete mapping polynomials of degree $\leq 6$ .....	52
3	The right 1-diagonal on $F_9 \times F_9$ .....	60
4	The right 1-diagonal on $\mathbf{Z}/(9) \times \mathbf{Z}/(9)$ .....	61
5	Effects of PLS-transformations in the set of rows, columns and diagonals .....	63
6	Selected GPLS of order 9 .....	71
7	Selected GPLS $\Delta^f \circ \sigma$ .....	84

## ACKNOWLEDGEMENT

First and foremost, the author would like to express his sincere gratitude to his thesis advisor, Professor Gary L. Mullen, for giving helpful advice numerous times, sharing his experience and helping to complete this thesis. The author would also like to extend thanks to the members of his thesis committee, Professor W. Dale Brownawell, Professor Robert A. Hultquist and Professor Wen-Ching W. Li, for volunteering their time and experience.

A special word of gratitude is due the author's family, including his wife, Hay-Min, and his sons, Jimmy and Ethan. The author appreciates his sons for their cooperation and understanding. He especially wishes to express his sincere appreciation to his wife for her undying love, immeasurable support and steadfast belief in his success. The author is forever grateful to them.



## CHAPTER 1

### PRELIMINARIES

In this chapter, we are going to give a survey of known properties which we will need in subsequent chapters. Unless a method of proof is central to our later work, we will omit the proof.

In section 1, we discuss some properties of groups, especially properties about solvable groups and presentations of groups. We discuss fields and finite fields in section 2. In fact, we will concentrate on the relation between finite fields and finite extensions of the  $p$ -adic field  $\mathbb{Q}_p$ . In section 3, we study some properties of linear algebra, including circulant matrices and their determinants. In particular, we focus on the general linear group and properties of circulant matrices. In section 4, we will study permutation polynomials over finite fields.

#### 1. Groups

For definitions and basic properties of groups, subgroups, normal subgroups, permutation groups and isomorphisms of groups, the reader should consult Rotman's book [37]. Here, we just state two definitions and some properties relating these two definitions.



Definition. A normal series of a group  $G$  is a chain of subgroups  $G = G_0 \supset \dots \supset G_n = \{1\}$  in which  $G_{i+1}$  is normal in  $G_i$ , denoted  $G_{i+1} \triangleleft G_i$ , for all  $i$ . The factor groups of this normal series are the groups  $G_i/G_{i+1}$  for  $i=0, 1, \dots, n-1$ , and the length of this series is the number of strict inclusions. Moreover, a group  $G$  is solvable in case it has a normal series whose factor groups are commutative.

It is easy to see that every abelian group is solvable. For solvable groups, we have the following necessary and sufficient conditions.

Theorem 1.1.1. Let  $H \triangleleft G$ . Then  $G$  is solvable if and only if  $H$ ,  $G/H$  are solvable.

Using Theorem 1.1.1, we have the following examples.

Theorem 1.1.2.

- (1) The symmetric group  $S_n$  is solvable if and only if  $n \leq 4$ .
- (2) If  $p$  and  $q$  are primes, then any group of order  $p^2q$  is solvable. In particular, any group of order 12 is solvable.
- (3) The dihedral groups  $D_n$  are solvable.

Definition. A collection of elements  $a_1, \dots, a_m$  of a group  $G$  is called a set of generators if every element of  $G$  is expressible as a finite product of their powers. Such a group is conveniently denoted by the symbol  $\langle a_1, \dots, a_m \rangle$ . A set of relations

$g_k(a_1, \dots, a_m) = e$ , where  $e$  is the identity of  $G$  and  $k=1, \dots, s$ , satisfied by the generators of  $G$  is called a presentation of  $G$  if every relation satisfied by the generators is an algebraic consequence of these particular relations.

For our presentation, we need the following results, see [7].

Theorem 1.1.3. Let  $G$  be a group and let  $a, b \in G$  with  $e$  the identity of  $G$ .

- (1) If  $a$  and  $b$  are generators of  $G$  satisfying  $a^2 = b^m = e$  and  $aba = b^{-1}$ , then  $G$  is isomorphic to the dihedral group  $D_m$ .
- (2) If  $a$  and  $b$  are generators of  $G$  satisfying  $a^2 = b^3 = (ab)^4 = e$ , then  $G$  is isomorphic to the symmetric group  $S_4$ .

## 2. Fields

For basic properties of fields, both finite and infinite, we refer to Chapters 1 and 2 of Lidl and Niederreiter's book [22]. Here, we are going to study the relationship between finite fields and  $p$ -adic number fields (see [21]).

Let  $p$  be a prime. For any nonzero integer  $a$ , let  $\text{ord}_p a$  be the highest power of  $p$  which divides  $a$ . For any rational number  $r = \frac{a}{b}$ ,  $a, b$  nonzero integers, we define  $\text{ord}_p r = \text{ord}_p a - \text{ord}_p b$ . Using these definitions, we define a map  $| \cdot |_p$  on the set  $\mathbb{Q}$  of all rational numbers by

$$|r|_p = \begin{cases} \frac{1}{p^{\text{ord}_p r}} & \text{if } r \neq 0 \\ 0 & \text{if } r = 0. \end{cases}$$

Theorem 1.2.1.  $|\cdot|_p$  is a norm on  $\mathbb{Q}$  (i.e.,  $|\cdot|_p$  satisfies (1)  $|r_1|_p = 0$  if and only if  $r_1 = 0$ , (2)  $|r_1 r_2|_p = |r_1|_p |r_2|_p$  and (3)  $|r_1 + r_2|_p \leq |r_1|_p + |r_2|_p$  for all  $r_1, r_2 \in \mathbb{Q}$ ).

From this theorem, we can define a metric on  $\mathbb{Q}$  by  $d(a, b) = |a - b|_p$  for all  $a, b \in \mathbb{Q}$ .

Note that the norm  $|\cdot|_p$  on  $\mathbb{Q}$  is a non-Archimedean norm (a norm with the property  $|a + b|_p \leq \max\{|a|_p, |b|_p\}$  for all  $a, b$ ). Let  $|\cdot|_\infty$  denote the usual absolute value. It is not difficult to see that  $|\cdot|_\infty$  is an Archimedean norm (i.e., not a non-Archimedean norm). Furthermore, by the "trivial" norm, we mean the norm  $|\cdot|$  such that  $|0| = 0$  and  $|x| = 1$  for  $x \neq 0$ .

Now, two metrics  $d_1$  and  $d_2$  are equivalent whenever each sequence is Cauchy with respect to  $d_1$  if and only if it is Cauchy with respect to  $d_2$ , and two norms are equivalent if their induced metrics are equivalent. With this equivalence relation, we have

Theorem 1.2.2. (Ostrowski Theorem). Every nontrivial norm on  $\mathbb{Q}$  is equivalent to  $|\cdot|_p$  for some prime  $p$  or for  $p = \infty$ .

Because of this theorem, any norm we consider later is  $|\cdot|_p$ , where  $p$  is either a prime or  $p = \infty$ . Note that  $\mathbb{Q}$  is not complete with respect to any norm  $|\cdot|_p$ . Let  $\mathbb{Q}_p$  be the completion of  $\mathbb{Q}$  with respect to  $|\cdot|_p$ . We can identify  $\mathbb{Q}$  as a subset of  $\mathbb{Q}_p$ . Also, we can extend definitions of addition and multiplication on  $\mathbb{Q}$  to define operations on  $\mathbb{Q}_p$  so that  $\mathbb{Q}_p$  is a field and  $\mathbb{Q}$  is a subfield of  $\mathbb{Q}_p$ . It is not difficult to see that  $\mathbb{Q}_p$  is complete. Now, let  $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$ .  $\mathbb{Z}_p$  is called the ring of  $p$ -adic integers.

Now, we consider any finite extension of the field  $\mathbb{Q}_p$ . We have



Theorem 1.2.3. Let  $K$  be a finite extension of  $\mathbb{Q}_p$ . Then there exists a field norm on  $K$  which extends the norm  $|\cdot|_p$  on  $\mathbb{Q}_p$ .

We will use the same notation  $|\cdot|_p$  for the field norm on  $K$  which extends the norm  $|\cdot|_p$  on  $\mathbb{Q}_p$ . For any finite extension  $K$  of  $\mathbb{Q}_p$ , there is a subring of  $K$  which contains  $\mathbb{Z}_p$ .

Theorem 1.2.4. Let  $K$  be a finite extension of  $\mathbb{Q}_p$  of degree  $n$ , and let  $A = \{x \in K \mid |x|_p \leq 1\}$  and  $M = \{x \in K \mid |x|_p < 1\}$ . Then  $A$  is a ring, which is the integral closure of  $\mathbb{Z}_p$  (i.e., the set of all  $x \in K$  which satisfy an equation of the form  $x^m + a_1x^{m-1} + \dots + a_{m-1}x + a_m = 0$  with the  $a_i \in \mathbb{Z}_p$ ).  $M$  is the unique maximal ideal of  $A$ , and  $A/M$  is a finite extension of the finite prime field  $\mathbb{F}_p$  of degree at most  $n$ .

In this theorem, the field  $A/M$  is called the residue field of  $K$ . It is a field extension of  $\mathbb{F}_p$  of some finite degree  $f$ .  $A$  itself is called the "valuation ring" of  $|\cdot|_p$  in  $K$ . Moreover, Theorem 1.2.3 describes a relation between  $p$ -adic fields and finite fields. In fact, we have a more precise result.

Theorem 1.2.5. Let  $n$  be a positive integer. There is exactly one extension  $K$  (up to isomorphism) of  $\mathbb{Q}_p$  of degree  $n$  whose residue field is  $\mathbb{F}_{p^n}$ . Moreover,  $K$  can be obtained by adjoining a primitive  $p^n-1$ st root of 1 to  $\mathbb{Q}_p$ .

### 3. Linear Algebra

For basic properties of vector spaces, linear transformations and matrices, we refer to Perlis's book [33].



Let  $V$  be a vector space of dimension  $m$  over a field  $K$ . Then the set of all nonsingular linear transformations on  $V$  forms a group under functional composition. This group is called the general linear group. This group is isomorphic to the multiplicative group of all nonsingular  $m \times m$  matrices over  $K$ , denoted  $GL(m, K)$ . From Theorem 1.3.1 through Theorem 1.3.5, the reader should consult Rotman's book [37].

Theorem 1.3.1. Let  $K = F_q$  be the finite field of order  $q$ . Then  $|GL(m, F_q)| = (q^m - 1)(q^m - q) \dots (q^m - q^{m-1})$ .

Now we are going to study the solvability of  $GL(m, F_q)$ . We need some additional terminologies. Let  $K$  be a field. The special linear group  $SL(m, K)$  is the multiplicative group of all  $m \times m$  matrices over  $K$  whose determinant is 1.

Theorem 1.3.2.  $SL(m, K)$  is a normal subgroup of  $GL(m, K)$ . Moreover,  $GL(m, K)$  is a semidirect product of  $SL(m, K)$  by  $K^\times$ .

From Theorem 1.1.1 and this theorem, we see that  $GL(m, F_q)$  is solvable if and only if  $SL(m, K)$  is solvable. Also, we have  $|SL(m, F_q)| = \frac{(q^m - 1)(q^m - q) \dots (q^m - q^{m-1})}{q - 1}$  from this theorem.

Let  $Z_0$  be the center of  $SL(m, K)$ . The projective unimodular group  $PSL(m, K)$  is the group  $SL(m, K)/Z_0$ . Since  $Z_0$  is abelian,  $Z_0$  is solvable. So  $SL(m, K)$  is solvable if and only if  $PSL(m, K)$  is solvable. For  $PSL(m, K)$  we have the following two theorems.

Theorem 1.3.3. The group  $PSL(2, F_q)$  is simple if and only if  $q > 3$ .

Theorem 1.3.4. The groups  $\text{PSL}(m, K)$  are simple for all  $m \geq 3$  and all fields  $K$ .

Note that the simple groups  $\text{PSL}(m, K)$  in the above two theorems are nonabelian and not solvable. For  $m = 1$ ,  $\text{GL}(1, F_q)$  is isomorphic to  $F_q^\times$  and so is solvable. For  $m = 2$  and  $q = 2$ ,  $|\text{SL}(2, F_2)| = 6$  and so  $\text{SL}(2, F_2)$  is solvable. Now, consider  $m = 2$  and  $q = 3$ . Since  $Z_0$  is the center of  $\text{SL}(2, F_3)$ , every element of  $Z_0$  commutes with all elements of  $\text{SL}(2, F_3)$ . It is not difficult to see that every element of  $Z_0$  is of the form  $kI$ , where  $I$  is the  $3 \times 3$  identity matrix and  $k \in F_3^\times$  a constant. So  $|Z_0| = 2$ . This implies  $|\text{PSL}(2, F_3)| = \frac{(3^2-1)(3^2-3)}{2 \times 2} = 12$ . By Theorem 1.1.2 (2),  $\text{PSL}(2, F_3)$  is solvable.

Combining all results together, we have

Theorem 1.3.5.  $\text{GL}(m, F_q)$  is solvable if and only if either  $m = 1$  or  $m = 2$  and  $q = 2, 3$ .

Now, we consider a special kind of matrices, called circulant matrices. In the remaining part of this section, we consider matrices over an arbitrary field  $K$  unless we specify otherwise. For all results in this part, we refer to Davis's book [8].

Definition. A circulant matrix of order  $n$  is a square matrix of the form

$$C = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ - & - & & - \\ - & - & & - \\ c_1 & c_2 & \cdots & c_0 \end{pmatrix} = \text{circ}(c_0, c_1, \dots, c_{n-1}).$$

From the definition, the whole circulant matrix is determined by the first row (or column). So, if the first row of the circulant matrix  $C$  is  $(c_0, c_1, \dots, c_{n-1})$ , we may write it in the form  $C = (c_{ij}) = (c_{j-i})$ , subscripts mod  $n$ .

Let  $P = \text{circ}(0, 1, 0, \dots, 0)$  be an  $n \times n$  circulant matrix. Then  $P$  is the permutation matrix corresponding to the  $n$ -cycle  $\sigma = (0, 1, \dots, n-1)$ . It is easy to see that for  $0 \leq i \leq n-1$ ,  $P^i = \text{circ}(0, \dots, 0, 1, 0, \dots, 0)$  with 1 in the  $i$ th place. So  $\text{circ}(c_0, c_1, \dots, c_{n-1}) = c_0 I + c_1 P + \dots + c_{n-1} P^{n-1}$ , where  $I$  is the  $n \times n$  identity matrix. Write  $g_C(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$ . Then  $C = g_C(P)$ . The polynomial  $g_C(x)$  is called the representer of the circulant matrix  $C$ . The following theorem is easy to see.

**Theorem 1.3.6.** Let  $A$  and  $B$  be  $n \times n$  circulant matrices with representers  $f(x)$  and  $g(x)$ , respectively. Let  $a$  be any constant.

- (1)  $aA$  is a circulant matrix with representer  $af(x)$ .
- (2)  $A+B$  is a circulant matrix with representer  $f(x) + g(x)$ .
- (3)  $AB = BA$  is a circulant matrix with representer  $h(x)$  with degree of  $h(x) \leq n-1$  and  $h(x) \equiv f(x)g(x) \pmod{x^n-1}$ .

In fact, we can assume that the polynomial  $h(x)$  in this theorem can be obtained as follows: multiple out  $f(x)g(x)$ , then replace each term  $x^i$  by  $x^j$  whenever  $i = kn+j$  with  $0 \leq j \leq n-1$ .

Now suppose the field  $K$  contains a primitive  $n$ th root  $\zeta$  of unity. Let  $V_\zeta$  be the Vandermonde matrix generated by  $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ . Then we have



Theorem 1.3.7. Let  $\zeta$  be a primitive  $n$ th root of unity in the field  $K$ . If  $C$  is an  $n \times n$  circulant matrix, then  $C$  is diagonalizable. Moreover, if  $C$  has representer  $f(x)$ , then  $V_\zeta C V_\zeta^{-1} = \text{diag}(f(1), f(\zeta), \dots, f(\zeta^{n-1}))$ . Conversely, if  $D$  is an  $n \times n$  diagonal matrix, then  $C = V_\zeta^{-1} D V_\zeta$  is circulant.

Corollary 1.3.8. Let  $K$  have a primitive  $n$ th root  $\zeta$  of unity. If  $C$  is an  $n \times n$  circulant matrix with representer  $f(x)$ , then  $f(1), f(\zeta), \dots, f(\zeta^{n-1})$  are all eigenvalues of  $C$  and so  $\det C = \prod_{i=0}^{n-1} f(\zeta^i)$ .

From this corollary, we have that if we let  $g(x) = x^n - 1$ , then  $\det C = \prod_{j=0}^{n-1} f(\zeta^j) = R(g(x), f(x)) = \text{the resultant of } g(x) \text{ and } f(x)$ .

Using Corollary 1.3.8, one can prove the following two theorems.

Theorem 1.3.9. Let  $C = \text{circ}(a, \dots, a, b, \dots, b)$  be an  $n \times n$  circulant matrix with  $m$   $a$ 's and  $(n-m)$   $b$ 's, where  $a \neq b$ . Then

$$\det C = \begin{cases} (ma + (n-m)b)(a-b)^{n-1} & \text{if } \gcd(m, n) = 1 \\ 0 & \text{if } \gcd(m, n) > 1. \end{cases}$$

Theorem 1.3.10. Let  $C = \text{circ}(a_0, a_1, a_2, 0, \dots, 0)$  be an  $n \times n$  circulant matrix over the field  $K$  which has a primitive  $n$ th root of unity. Then

$$\det C = a_0^n + a_2^n - \sum_{s=0}^{\left\lfloor \frac{n}{2} \right\rfloor} (-1)^{n+s} \frac{n}{n-s} \binom{n-s}{s} (a_0 a_2)^s a_1^{n-2s}.$$



#### 4. Permutation Polynomials Over Finite Fields

In this section,  $q=p^n$  is the  $n$ th power of a prime  $p$ , and  $F_q$  is the finite field of order  $q$ . Almost all results in this section are cited from Lidl and Niederreiter's book [22].

Before we study permutation polynomials over  $F_q$ , we observe that for every function  $\varphi:F_q \rightarrow F_q$ , there is a unique polynomial  $f(x) \in F_q[x]$  such that  $\deg f \leq q-1$  and  $\varphi(a) = f(a)$  for all  $a \in F_q$ . This polynomial  $f(x)$  can be found by the Lagrange interpolation formula so that

$$f(x) = \sum_{c \in F_q} \varphi(c) \left( 1 - (x-c)^{q-1} \right).$$

Consequently, all permutations we will consider have degree  $\leq q-1$ .

Now, by a permutation polynomial (abbreviated PP) of  $F_q$  is meant a polynomial  $f(x) \in F_q[x]$  with the property that the polynomial function  $f:c \rightarrow f(c)$  from  $F_q$  into  $F_q$  is a permutation of  $F_q$ . From this definition, we immediately have the following result.

Theorem 1.4.1.

- (1) Every linear polynomial  $f(x) = ax+b \in F_q[x]$ ,  $a \neq 0$ , is a PP of  $F_q$ .
- (2) The monomial  $x^m$  is a PP of  $F_q$  if and only if  $\gcd(m, q-1) = 1$ .

For PPs of  $F_q$  we have three useful criteria. The following property is useful for proving the first criterion.

Lemma 1.4.2. Let  $a_0, a_1, \dots, a_{q-1}$  be elements of  $F_q$ . Then the following two conditions are equivalent:

- (1)  $a_0, a_1, \dots, a_{q-1}$  are distinct
- (2) 
$$\sum_{i=0}^{q-1} a_i^k = \begin{cases} 0 & \text{for } k = 0, 1, \dots, q-2 \\ -1 & \text{for } k = q-1. \end{cases}$$

The first criterion is

Theorem 1.4.3. (Hermite's Criterion).  $f(x) \in F_q[x]$  is a PP of  $F_q$  if and only if the following two conditions hold:

- (1)  $f(x)$  has exactly one root in  $F_q$ ;
- (2) for each integer  $t$  with  $1 \leq t \leq q-2$  and  $t \not\equiv 0 \pmod{p}$ , the reduction of  $f(x)^t \pmod{(x^q - x)}$  has degree  $\leq q-2$ .

In Hermite's Criterion, the reduction of  $f(x)^t \pmod{(x^q - x)}$  is a polynomial  $g(x) \in F_q[x]$  such that  $\deg g(x) \leq q-1$  and  $f(x)^t \equiv g(x) \pmod{(x^q - x)}$ . Since  $c^q = c$  for all  $c \in F_q$ , we have in fact  $f(c)^t = g(c)$ . Furthermore, the restriction  $t \not\equiv 0 \pmod{p}$  is superfluous in condition (2).

The following corollary follows easily from Hermite's Criterion.

Corollary 1.4.4. If  $d > 1$  is a divisor of  $q-1$ , then there is no PP of  $F_q$  of degree  $d$ .

For the second criterion, we need characters of  $F_q$ . Let  $G$  be a finite abelian group. A character  $\chi$  of  $G$  is a homomorphism from  $G$  into the multiplicative group of complex numbers of absolute value 1. When we consider the finite field  $F_q$ , we have two kinds of characters defined on  $F_q$ , additive characters defined on the additive group of  $F_q$

and multiplicative characters defined on the multiplicative group  $F_q^\times$ . If the additive character  $\chi_0$  of  $F_q$  satisfies  $\chi_0(c) = 1$  for all  $c \in F_q$ ,  $\chi_0$  is called the trivial character of  $F_q$ . For additive characters of  $F_q$ , we have the following important result.

**Theorem 1.4.5. (Weil's Theorem).** Let  $f(x) \in F_q[x]$  be of degree  $m \geq 1$  with  $\gcd(m, q) = 1$  and let  $\chi$  be a nontrivial additive character of  $F_q$ . Then

$$\left| \sum_{c \in F_q} \chi(f(c)) \right| \leq (m-1) q^{1/2}.$$

The multiplicative character mapping all  $c \in F_q^\times$  into 1 is called the trivial multiplicative character of  $F_q$ . If  $q$  is odd, the quadratic character  $\eta$  of  $F_q$  is defined by

$$\eta(c) = \begin{cases} 1 & \text{if } c \text{ is the square of an element of } F_q^\times \\ -1 & \text{otherwise} \end{cases}.$$

Moreover, we can extend the definition of any multiplicative character  $\psi$  by setting  $\psi(0) = 1$  if  $\psi$  is trivial and  $\psi(0) = 0$  if  $\psi$  is nontrivial.

For a quadratic character, we have the following

**Theorem 1.4.6.** Let  $f(x) = a_2x^2 + a_1x + a_0 \in F_q[x]$  with  $q$  odd and  $a_2 \neq 0$ . Let  $\eta$  be the quadratic character of  $F_q$ . Then



$$\sum_{c \in F_q} \eta(f(c)) = \begin{cases} -\eta(a_2) & \text{if } a_1^2 - 4a_0a_2 \neq 0 \\ (q-1)\eta(a_2) & \text{if } a_1^2 - 4a_0a_2 = 0. \end{cases}$$

The following corollary is a special case of this theorem, in which we consider  $f(x) = x^2 + ax$  with  $a \neq 0$ .

Corollary 1.4.7 (Lemma 14.11, [18]). Let  $\eta$  be the quadratic character of  $F_q$  and let  $a \in F_q^\times$ , where  $q$  is odd. Then

$$\sum_{c \in F_q} \eta(c) \eta(a+c) = -1.$$

Using characters, we can state our second criterion as follows.

Theorem 1.4.8. The polynomial  $f(x) \in F_q[x]$  is a PP of  $F_q$  if and only if  $\sum_{c \in F_q} \chi(f(c)) = 0$  for all nontrivial additive characters  $\chi$  of  $F_q$ .

Our third criterion is stated as follows.

Theorem 1.4.9. Let  $f(x) \in F_q[x]$ . Write

$$D(f) = \left\{ \frac{f(b) - f(a)}{a - b} \mid a \neq b \in F_q \right\}.$$

Then  $f(x)$  is a PP of  $F_q$  if and only if  $0 \notin D(f)$ .



Finally, we study two special kinds of polynomials. We have necessary and sufficient conditions for each of them to be PPs. The first is

Theorem 1.4.10. For odd  $q$ , the polynomial  $x^{(q+1)/2} + ax \in F_q[x]$  is a PP of  $F_q$  if and only if  $\eta(a^2-1) = 1$ , where  $\eta$  is the quadratic character of  $F_q$ .

The second kind is the important class of linearized polynomials which we define as follows.

Let  $k$  be a positive integer. The polynomial  $L(x) = \sum_{i=0}^{k-1} a_i x^{q^i} \in F_{q^k}[x]$  is called a linearized polynomial of  $F_{q^k}$  over  $F_q$ . For linearized polynomials, we have

Theorem 1.4.11. The linearized polynomial  $L(x) = \sum_{i=0}^{k-1} a_i x^{q^i} \in F_{q^k}[x]$  is a PP of  $F_{q^k}$  if and only if  $L(x)$  has only the root 0 in  $F_{q^k}$ .

It is easy to see that each linearized polynomial  $L(x)$  of  $F_{q^k}$  over  $F_q$  induces a linear operator on the vector space  $F_{q^k}$  over  $F_q$ . So, saying that  $L(x)$  has only the root 0 in  $F_{q^k}$  is equivalent to saying that the induced linear operator is nonsingular. Moreover, it can be seen, from the definition of linearized polynomials, that the reduction mod  $(x^{q^k} - x)$  of the composite function of two linearized polynomials is still a linearized polynomial. Hence, the set of all linearized polynomials of  $F_{q^k}$  over  $F_q$  which are PPs of  $F_{q^k}$  forms a group under the operation of composition mod  $(x^{q^k} - x)$ . In fact, this group, known as the Betti-Mathieu group, is isomorphic to  $GL(k, F_q)$ . The one-to-one correspondence was

originally pointed out by Dickson [12]. We will sketch Carlitz's proof of the homomorphism property. For this purpose, we need the following

Theorem 1.4.12. Let  $L(x) = \sum_{i=0}^{k-1} \alpha_i x^{q^i} \in F_{q^k}[x]$  be a linearized polynomial. Then  $L(x)$  is a PP of  $F_{q^k}$  if and only if  $\det A \neq 0$ , where  $A = (\alpha_{i-j}^{q^j})$ , all subscripts being computed mod  $k$ .

Theorem 1.4.13. The Betti-Mathieu group of linearized polynomials of  $F_{q^k}$  over  $F_q$  is isomorphic to  $GL(k, F_q)$ .

Proof ([5]). It is known that there exists a normal basis  $\zeta, \zeta^q, \dots, \zeta^{q^{k-1}}$  of  $F_{q^k}$  over  $F_q$  that consists of primitive elements of  $F_{q^k}$  (see [29]).

Let  $y = L(x) = \sum_{i=0}^{k-1} \alpha_i x^{q^i} \in F_{q^k}[x]$  be a linearized polynomial which is a PP of  $F_{q^k}$ .

For  $0 \leq i \leq k-1$ , write  $\alpha_i = \sum_{j=0}^{k-1} a_{ij} \zeta^{q^j}$  with each  $a_{ij} \in F_q$ . Also write  $x = \sum_{i=0}^{k-1} x_i \zeta^{q^i}$  and  $y = \sum_{i=0}^{k-1} y_i \zeta^{q^i}$ . Note that if  $x, y \in F_{q^k}$ , then all  $x_i$  and  $y_i$  are elements of  $F_q$ . In addition,

write  $x^{q^{i+j}} = \sum_{l=0}^{k-1} z_{ijl} \zeta^{q^l}$ . Then we have  $\sum_{i=0}^{k-1} y_i \zeta^{q^i} = \sum_{s,t,i,j} a_{st} x_j z_{t,j+s,i} \zeta^{q^i}$ . So

$y_i = \sum_{j=0}^{k-1} \bar{a}_{ij} x_j$ , where  $\bar{a}_{ij} = \sum_{s,t} a_{st} z_{t,j+s,i}$ .

On the other hand, we have

$$\left( \zeta^{q^{i+j}} \right) \left( \alpha_{i-j}^{q^j} \right) = \left( \left( \sum_{s=0}^{k-1} \alpha_s \zeta^{q^{i+s}} \right)^{q^j} \right)$$

and

$$\sum_{s=0}^{k-1} \alpha_s \zeta^{q^{i+s}} = \sum_{l=0}^{k-1} \bar{a}_{li} \zeta^{q^l}.$$

It follows that

$$\left( \left( \sum_{s=0}^{k-1} \alpha_s \zeta^{q^{i+s}} \right)^{q^j} \right) = (\bar{a}_{ij})^T (\zeta^{q^{i+j}}),$$

where  $(\bar{a}_{ij})^T$  denotes the transposed matrix of  $(\bar{a}_{ij})$ . Let  $H = (\zeta^{q^{i+j}})$  and  $A = (\alpha_{i-j}^{q^j})$ . Then  $HA = (\bar{a}_{ij})^T H$  and so  $HAH^{-1} = (\bar{a}_{ij})^T$ . Since  $H$  is nonsingular,  $\det A = \det (\bar{a}_{ij})$  and  $\tau(A) = (\bar{a}_{ij})^T$  is a one-to-one mapping. From Dickson's work, the correspondence  $L(x) \rightarrow A \rightarrow (\bar{a}_{ij})^T$  is a one-to-one correspondence.

Let  $G(x) = \sum_{i=0}^{k-1} \beta_i x^{q^i}$  be a PP of  $F_{q^k}$  and let  $B = (\beta_{i-j}^{q^j})$ . It is easy to see that if  $G(L(x)) \equiv \sum_{i=0}^{k-1} \gamma_i x^{q^i} \pmod{(x^{q^k} - x)}$ , then  $(\gamma_{i-j}^{q^j}) = C = AB$ . Moreover, if  $HBH^{-1} = (\bar{b}_{ij})^T$  and  $HCH^{-1} = (\bar{c}_{ij})^T$ , then  $HCH^{-1} = HAH^{-1} HBH^{-1} = (\bar{a}_{ij})^T (\bar{b}_{ij})^T$ . So  $(\bar{c}_{ij}) = (\bar{b}_{ij}) (\bar{a}_{ij})$ . This completes the proof of the theorem.



## CHAPTER 2

### SET COMPLETE MAPPINGS ON FINITE FIELDS

#### 1. Introduction

In 1942, H. B. Mann (see [23]) gave the following definition.

Let  $G$  be a group. Let  $\sigma: G \rightarrow G$  be a mapping. Define  $\tau: G \rightarrow G$  by  $\tau(g) = \sigma(g)g$  for all  $g \in G$ . The mapping  $\sigma$  is called a complete mapping of  $G$  if both  $\sigma$  and  $\tau$  are bijections.

Mann used complete mappings to construct orthogonal Latin squares. Numerous papers have since been written about complete mappings on groups and their applications (see, for example, [3], [11], [13], [31], [32]).

In 1981, Niederreiter and Robinson constructed Bol loops of order  $pq$  ( $p, q$  distinct primes) using complete mappings of the finite field  $F_p$  (see [27]). Later, they discussed complete mappings of finite fields  $F_q$  (see [28]). Some other results concerning complete mappings on finite fields have been discussed (see [14], [15]).

Another useful function is a so-called virtual path. It is defined as follows (see [1]).

A virtual path is a function  $\pi: \mathbb{Z}/(n) \rightarrow \mathbb{Z}/(n)$  such that the mappings  $x \rightarrow \pi(x)$ ,  $x \rightarrow \pi(x) - x$  and  $x \rightarrow \pi(x) + x$  are all permutations of  $\mathbb{Z}/(n)$ , where  $\mathbb{Z}/(n)$  is the quotient ring of integers  $\mathbb{Z}$  modulo the principal ideal  $(n)$  of  $\mathbb{Z}$ .

From this definition, we see that on  $\mathbb{Z}/(n)$ , each virtual path is also a complete mapping. Virtual paths of  $\mathbb{Z}/(n)$  are useful in constructing and studying so-called pandiagonal latin squares (see, for instance, [1], [2], [19], [34] and [36]).

In this chapter, we will generalize both the notions of complete mappings and virtual paths to so-called set complete mappings of a finite field  $F_q$ . In Section 2, we will give the definition of set complete mappings associated with the set  $S$  (abbreviated S-CM) and search for some S-CMs when the set  $S$  is fixed. In Section 3, we will study some properties of S-CMs. In Section 4, we will study relations between S-CMs and T-CMs (set complete mappings associated with a set  $T$ ). In the last section, we study the special case where  $S$  is taken to be the set  $\{0, \pm 1\}$ . Such S-CMs (which are the same as virtual paths if  $q = p$  a prime) are called very complete mappings and will be used in the next chapter.

## 2. Definition and Existence of Set Complete Mappings

In this section, we will first give the definition of set complete mappings of the finite field  $F_q$ . Then we give some methods to construct new set complete mappings when we already have one such mapping. And in the major part of this section, we will search for the existence of some specific kinds of set complete mappings of  $F_q$ .

**Definition.** Let  $S$  be a subset of  $F_q$ . A polynomial  $f(x) \in F_q[x]$  is called a set complete mapping, with the set  $S$ , of  $F_q$  (abbreviated S-CM) if  $f(x) + ax$  is a PP of  $F_q$  for all  $a \in S$ .

Note that a polynomial  $f(x) \in F_q[x]$  is an S-CM of  $F_q$  if and only if, for  $a \in S$ , the polynomial  $f_a(x) = f(x) + ax$  is an T-CM of  $F_q$  where  $T = \{u-a \mid u \in S\}$ . In this case,  $S$  may not contain 0 but  $T$  does.

Now, let  $f(x)$  be an S-CM of  $F_q$ . If  $0 \in S$ ,  $f(x)$  itself is a PP of  $F_q$ . If  $S = \{0, 1\}$ , then  $f(x)$  is a complete mapping. If  $S = \{0, 1, -1\}$  and  $q$  is an odd prime, then  $f(x)$  is a virtual path.

If  $S \subseteq F_q$ , we have some trivial examples of S-CMs of  $F_q$ . If  $a \notin -S = \{-b \mid b \in S\}$ ,  $ax + b$  is an S-CM of  $F_q$  for all  $b \in F_q$ .

If we have an S-CM of  $F_q$ , the following theorem provides several methods to construct new S-CMs of  $F_q$ . This theorem generalizes Theorem 2 in [28] and Lemma 1.6 in [1].

**Theorem 2.2.1.** Let  $0 \in S \subseteq F_q$ ,  $q = p^n$  with  $n \geq 1$ . Let  $f(x) \in F_q[x]$  be an S-CM of  $F_q$ .

- (1)  $af(a^{-1}x+b) + c$  is an S-CM of  $F_q$  for all  $a \neq 0, b, c \in F_q$ .
- (2) If for  $a \neq 0$ ,  $a \in S$  implies  $a^{-1} \in S$ , then any polynomial representing the inverse mapping of the mapping  $c \in F_q \rightarrow f(c)$  is an S-CM of  $F_q$ .
- (3) If  $a \in S$  implies  $-a \in S$ , then  $-f(x)$  is an S-CM of  $F_q$ .
- (4) If  $S \subseteq F_p$ , then  $(l \circ f \circ l^{-1})(x)$  is an S-CM of  $F_q$ , where  $l$  is a linearized polynomial of  $F_q$  which is also a PP of  $F_q$ .
- (5) Let  $a \in F_q$ . If  $\{a+s \mid s \in S\} = S$ , then  $f(x) + ax$  is an S-CM of  $F_q$ .

**Proof.**



- (1) Let  $a \in F_q^\times$  and  $b, c \in F_q$ . For each  $d \in S$ ,  $af(a^{-1}x+b) + c + dx = a[f(a^{-1}x+b) + d(a^{-1}x+b)] + (c-abd)$ . Since  $a^{-1}x+b$  and  $f(x)+dx$  are PPs of  $F_q$ ,  $af(a^{-1}x+b) + c + dx$  is also a PP of  $F_q$ . So  $af(a^{-1}x+b) + c$  is an S-CM of  $F_q$ .
- (2) Let  $h(x) \in F_q[x]$  be a polynomial representing the inverse mapping of  $f(x)$ . For all  $0 \neq a \in S$ ,  $h(x) + ax = h(f(y)) + af(y) = af(y) + y = a(f(y) + a^{-1}y)$ . Since  $a^{-1} \in S$ ,  $f(y) + a^{-1}y$  is a PP of  $F_q$  and so is  $h(x) + ax$ . Hence,  $h(x)$  is an S-CM of  $F_q$ .
- (3) Trivial.
- (4) Let  $l(x) = \sum_{i=0}^{n-1} b_i x^{p^i}$ ,  $q = p^n$ , be any linearized polynomial of  $F_q$  which is also a PP of  $F_q$ . Write  $y = l^{-1}(x)$ . For all  $a \in S \subseteq F_p$ ,
- $$\begin{aligned} (lofo l^{-1})(x) + ax &= (lof)(y) + al(y) = l(f(y)) + l(ay) \\ &= l(f(y) + ay) \end{aligned}$$
- Since  $f(y) + ay$  and  $l(x)$  are PPs of  $F_q$ ,  $(lofo l^{-1})(x) + ax$  is a PP of  $F_q$ . So  $(lofo l^{-1})(x)$  is an S-CM of  $F_q$ .
- (5) Since  $(a+s) \in S$  for all  $s \in S$ ,  $(f(x) + ax) + sx = f(x) + (a+s)x$  is a PP of  $F_q$ . So  $f(x) + ax$  is an S-CM. This completes the proof.

Now, we search for some nontrivial, nonlinear polynomials which are S-CMs of  $F_q$ . From Lemma 2.2.2 through Corollary 2.2.6, we consider  $q$  odd.

**Lemma 2.2.2.** Let  $f(x) = ax^{(q+1)/2} + bx \in F_q[x]$ . Then  $f(x)$  is an S-CM of  $F_q$  if and only if  $\eta(b^2 - a^2) = 1 = \eta((b+c)^2 - a^2)$  for all  $c \in S$ , where  $\eta$  is the quadratic character of  $F_q$ .

Proof. The result follows from Theorem 1.4.10.

Using this lemma, we can prove

Lemma 2.2.3. Let  $S = \{0, a_1, a_2, \dots, a_m\} \subseteq F_q$ . There are  $a, b \in F_q$ , with  $a \neq 0$ , so that the polynomial  $f(x) = ax^{(q+1)/2} + bx$  is an S-CM if and only if there are  $-u, -v \notin S$  satisfying  $u \neq v$  and  $(\eta(u), \eta(u+a_1), \dots, \eta(u+a_m)) = (\eta(v), \eta(v+a_1), \dots, \eta(v+a_m))$ .

Proof. By Lemma 2.2.2,  $f(x) = ax^{(q+1)/2} + bx \in F_q[x]$  is an S-CM of  $F_q$  if and only if  $\eta(b^2 - a^2) = 1 = \eta((b+a_i)^2 - a^2)$  for all  $1 \leq i \leq m$ . The last statement holds if and only if  $\eta(b-a) = \eta(b+a) \neq 0$  and  $\eta(b-a+a_i) = \eta(b+a+a_i) \neq 0$  for all  $1 \leq i \leq m$ .

For necessity, we take  $u = b-a$  and  $v = b+a$ . For sufficiency, we take  $a = 2^{-1}(v-u)$  and  $b = 2^{-1}(u+v)$ . This completes the proof.

Note that for  $u$  and  $v$  in Lemma 2.2.3 with  $u \neq v$ ,  $u, v$  and  $v, u$  generate two distinct S-CMs of  $F_q$  of the form  $ax^{(q+1)/2} + bx$  with  $a \neq 0$ .

Now, we can estimate the number  $N$  of S-CMs of the form  $ax^{(q+1)/2} + bx$  with  $a \neq 0$ . It is the following

Theorem 2.2.4. Let  $0 \in S \subseteq F_q$  with  $|S| = m$ . Then the number  $N$  of S-CMs of  $F_q$  of the form  $ax^{(q+1)/2} + bx$  with  $a \neq 0$  satisfies  $N \geq \frac{(q-m)(q-m-2^m)}{2^m}$ .

Proof. Write  $S = \{0, a_1, \dots, a_{m-1}\}$ . Let  $A = \{(u, u+a_1, \dots, u+a_{m-1}) \mid -u \in F_q - S\}$  and  $B = \{(x_0, x_1, \dots, x_{m-1}) \mid \text{each } x_i = \pm 1\}$ . Then  $|A| = q-m$  and  $|B| = 2^m$ .

Define a mapping  $\sigma: A \rightarrow B$  by, for each  $(u, u+a_1, \dots, u+a_{m-1}) \in A$ ,  
 $\sigma((u, u+a_1, \dots, u+a_{m-1})) = (\eta(u), \eta(u+a_1), \dots, \eta(u+a_{m-1}))$ . By Lemma 2.2.3, there are  
 $a \in F_q^\times$  and  $b \in F_q$  so that  $f(x) = ax^{(q+1)/2} + bx$  is an S-CM of  $F_q$  if and only if there are  
 $-u, -v \in F_q - S$  satisfying  $u \neq v$  and  $(\eta(u), \eta(u+a_1), \dots, \eta(u+a_{m-1})) = (\eta(v),$   
 $\eta(v+a_1), \dots, \eta(v+a_{m-1}))$ . The last statement means that  $\sigma$  is not 1-1.

Write  $B = \{B_1, \dots, B_{2^m}\}$ . For each  $1 \leq i \leq 2^m$ , let the inverse image of  $B_i$  be  
 $\sigma^{-1}(B_i) = \{(u, u+a_1, \dots, u+a_{m-1}) \in A \mid \sigma((u, u+a_1, \dots, u+a_{m-1})) = B_i\}$ . Then  $q-m = |A| =$   
 $2^m \sum_{i=1}^{2^m} |\sigma^{-1}(B_i)|$ . Note that for each  $1 \leq i \leq 2^m$ , the set  $\sigma^{-1}(B_i)$  generates exactly  $|\sigma^{-1}(B_i)| \cdot$   
 $(|\sigma^{-1}(B_i)| - 1)$  S-CMs of  $F_q$  of the form  $ax^{(q+1)/2} + bx$  with  $a \neq 0$ . So

$$\begin{aligned} N &= \sum_{i=1}^{2^m} |\sigma^{-1}(B_i)| \cdot (|\sigma^{-1}(B_i)| - 1) = \sum_{i=1}^{2^m} |\sigma^{-1}(B_i)|^2 - \sum_{i=1}^{2^m} |\sigma^{-1}(B_i)| \\ &\geq \frac{\left( \sum_{i=1}^{2^m} |\sigma^{-1}(B_i)| \right)^2}{2^m} - \sum_{i=1}^{2^m} |\sigma^{-1}(B_i)| = \frac{(q-m)^2}{2^m} - (q-m) = \frac{(q-m)(q-m-2^m)}{2^m} \end{aligned}$$

since

$$2^m \left( \sum_{i=1}^{2^m} |\sigma^{-1}(B_i)|^2 \right) - \left( \sum_{i=1}^{2^m} |\sigma^{-1}(B_i)| \right)^2 = \sum_{1 \leq i < j \leq 2^m} \left( |\sigma^{-1}(B_i)| - |\sigma^{-1}(B_j)| \right)^2 \geq 0$$

In Theorem 2.2.4, we see that the lower bound for  $N$  depends only on  $q$  and the cardinality of  $S$ .



Using Theorem 2.2.4, the following existence property is easy to prove.

Corollary 2.2.5. If  $0 \in S \subseteq F_q$  and  $q > |S| + 2^{|S|}$ , then there are at least 2 S-CMs of  $F_q$  in the form  $ax^{(q+1)/2} + bx$  with  $a \in F_q^\times$  and  $b \in F_q$ .

Proof. From Theorem 2.2.4, there is at least one S-CM of  $F_q$  in such form. Finally, it is easy, in the proof of Lemma 2.2.3, to see that if  $ax^{(q+1)/2} + bx$  is an S-CM of  $F_q$ , so is  $-ax^{(q+1)/2} + bx$ . This completes the proof.

The lower bound in Theorem 2.2.4. is the exact number when we consider the case  $S = \{0\}$ . We have

Corollary 2.2.6. The number  $N$  of all PPs of  $F_q$  in the form  $ax^{(q+1)/2} + bx$  with  $a \neq 0$  is  $N = \frac{(q-1)(q-3)}{2}$ .

Proof. Note that  $S = \{0\}$ . Write  $a = 2^{-1}(v-u)$  and  $b = 2^{-1}(v+u)$ . By Lemma 2.2.3,  $ax^{(q+1)/2} + bx$  is a PP of  $F_q$  with  $a \neq 0$  if and only if  $u, v \in F_q - S$ ,  $u \neq v$  and  $\eta(u) = \eta(v)$ . Note that we have  $\frac{(q-1)(q-3)}{2}$  such choices for  $u$  and  $v$ . So  $N = \frac{(q-1)(q-3)}{2}$ .

In Corollary 2.2.6, if we allow  $a=0$ , the number of all PPs of  $F_q$  in the form  $ax^{(q+1)/2} + bx$  is  $N = \frac{(q-1)^2}{2}$ . This number was found by G. Mullen and H. Niederreiter [26] when they investigated the group structure of the set of all PPs of  $F_q$  in such form under the operation of functional composition.

From this corollary, the lower bound for  $N$  in Theorem 2.2.4 is best possible.

The following is an example: Let  $S = \{0, \pm 1\} \subseteq F_{43}$ . We have exactly  $N = \frac{(43-3)(43-11)}{8} = 160$  S-CMs of  $F_{43}$  in the form  $ax^{22} + bx$  with  $a \neq 0$ .

Now we search for another type of S-CM of  $F_{q^k}$ , where  $k$  is a positive integer  $> 1$  and  $q$  is a prime power.

**Lemma 2.2.7.** Let  $f(x) = b_0x + b_1x^q + \dots + b_{k-1}x^{q^{k-1}} \in F_{q^k}[x]$ . Let  $A = (b_{i-j}^{p^j})$  with  $i-j \bmod k$ . Let  $0 \in S \subseteq F_q$ . Then  $f(x)$  is an S-CM of  $F_{q^k}$  if and only if every element of  $-S$  is not an eigenvalue of  $A$ .

**Proof.** From the definition,  $f(x)$  is an S-CM of  $F_{q^k}$  if and only if  $f(x) + ax$  is a PP of  $F_{q^k}$  for all  $a \in S$ . Since  $a \in F_q$  implies  $a^{q^i} = a$  for all  $0 \leq i \leq k-1$ , we have, by Theorem 1.4.12, that for all  $a \in S$ ,  $f(x) + ax$  is a PP of  $F_{q^k}$  if and only if  $\det(A + aI_k) \neq 0$  where  $I_k$  is the  $k \times k$  identity matrix. The last statement is equivalent to the fact that every element of  $-S$  is not an eigenvalue of  $A$ .

Using Lemma 2.2.7, for  $k=2$  or  $3$ , we can find the total number of linearized polynomials of  $F_{q^k}$  over  $F_q$  which are S-CMs of  $F_{q^k}$ . Before proving this in Lemma 2.2.8, we summarize the proof of Theorem 1.4.13 as follows.

Let  $f(x) = b_0x + b_1x^q + \dots + b_{k-1}x^{q^{k-1}} \in F_{q^k}[x]$ . By Lemma 2.2.7,  $f(x)$  is an S-CM of  $F_{q^k}$  if and only if every element of  $-S$  is not an eigenvalue of the matrix  $A = (b_{i-j}^{p^j})$  upon taking  $i-j \bmod k$ . Carlitz already proved (see [5]) that the Betti-Mathieu group is isomorphic to  $GL(k, F_q)$ , the group of all  $k \times k$  nonsingular matrices over  $F_q$  under the composition of mappings  $f(x) \rightarrow A \rightarrow \bar{A} = HAH^{-1}$  with  $H = (\tau^{q^{i+j}})$ , where  $\tau, \tau^q, \dots, \tau^{q^{k-1}}$  form a normal basis of  $F_{q^k}$  over  $F_q$ . Note that  $A$  and  $\bar{A}$  have the same minimal and the same characteristic polynomials since  $A$  and  $\bar{A}$  are similar. Hence  $f(x)$  is an S-CM of  $F_{q^k}$  if and only if every element of  $-S$  is not an eigenvalue of  $\bar{A}$ . Hence, the number  $N$  of

S-CMs of  $F_{q^k}$  of the form  $b_0x + b_1x^q + \dots + b_{k-1}x^{q^{k-1}} \in F_{q^k}[x]$  is equal to the number of  $\bar{A}$  in  $GL(k, F_q)$  which have no eigenvalue in  $-S$ . Since each  $\bar{A} \in GL(k, F_q)$  represents a unique non-singular linear transformation of  $F_{q^k}$  over  $F_q$ ,  $N$  equals the number of non-singular linear transformations of  $F_{q^k}$  over  $F_q$  which have no eigenvalue in  $-S$ .

Lemma 2.2.8. Let  $0 \in S \subseteq F_q$  with  $|S| = m$ .

- (1) The total number  $N_2$  of S-CMs of  $F_{q^2}$  in the form  $b_0x + b_1x^q \in F_{q^2}[x]$  is

$$N_2 = (q^2-1)(q^2-q) - \binom{m-1}{1} q (q^2-2) + \binom{m-1}{2} q (q+1).$$

- (2) The total number  $N_3$  of S-CMs of  $F_{q^3}$  in the form  $b_0x + b_1x^q + b_2x^{q^2} \in F_{q^3}[x]$  is

$$N_3 = (q^3-1)(q^3-q)(q^3-q^2) - \binom{m-1}{1} [q^3(q^3-1)(q^2-2) + q^3] +$$

$$\binom{m-1}{2} (q^2+q+1)q^3(q^2-3) - \binom{m-1}{3} (q^2+q+1)(q^2+q)q^2.$$

Proof. From the remark above, we count the number of non-singular linear transformations of  $F_{q^k}$  over  $F_q$  which have no eigenvalue in  $-S$ .

- (1)  $k=2$ . Fix  $0 \neq a \in -S$ . For each  $u \in F_{q^2}^\times$ , let  $A_u$  be the set of non-singular linear transformations of  $F_{q^2}$  over  $F_q$  which have  $u$  as an eigenvector associated with the eigenvalue  $a$ . It is easy to see that  $T(bu) = a(bu)$  for all  $b \in F_q^\times$ . So  $A_u = A_{bu}$  for all  $b \in F_q^\times$ . Moreover, if  $u_1, u_2 \in F_{q^2}^\times$  so that  $u_2 \neq bu_1$  for all  $b \in F_q$ , then there is exactly one non-singular linear transformation  $aI$  of  $F_{q^2}$  over  $F_q$  so that  $aI(u_1) = au_1$  and  $aI(u_2) = au_2$  because  $u_1, u_2$  form a basis of  $F_{q^2}$  over  $F_q$ . So, there are exactly  $\frac{q^2-1}{q-1} = q+1$  distinct sets  $A_u$ . We write  $\bar{u}$  as a representative in the set  $\{bu \mid b \in F_q^\times\}$ . Then we also have  $|A_{\bar{u}_1} \cap \dots \cap A_{\bar{u}_l}| = 1$  for arbitrary  $l \geq 2$  pairwise distinct elements  $\bar{u}_1, \dots, \bar{u}_l$ . It is easy to see that  $|A_{\bar{u}}| = q^2 - q$ . So the number of all non-singular linear transformations which have  $a$  as an eigenvalue is



$$\begin{aligned} \sum_{\text{all } \bar{u}_1, \dots, \bar{u}_l} (-1)^{l-1} |A_{\bar{u}_1} \cap \dots \cap A_{\bar{u}_l}| &= (q+1)(q^2-q) - \sum_{i=2}^{q+1} (-1)^i \binom{q+1}{i} \\ &= (q+1)(q^2-q) + 1 - \binom{q+1}{1} = q(q^2-1) - q \end{aligned}$$

by the inclusion-exclusion principle.

So we already have  $N_2 = (q^2-1)(q^2-q) = (q^2-1)(q^2-q) - \binom{1-1}{1} q(q^2-2) + \binom{1-1}{2} q(q+1)$

if  $|S| = 1$ , and  $N_2 = (q^2-1)(q^2-q) - q(q^2-2) = (q^2-1)(q^2-q) - \binom{2-1}{1} q(q^2-2) + \binom{2-1}{2} q(q+1)$

if  $|S| = 2$ .

Now we consider  $m \geq 3$ . For each  $0 \neq a \in -S$ , write  $B_a$  for the set of all non-singular linear transformations of  $F_{q^2}$  over  $F_q$  which have  $a$  as an eigenvalue. From previous work, we already have  $|B_a| = q(q^2-2)$ . Let  $a, b \in -S$  with  $a \neq b$  and  $ab \neq 0$ . Then for  $\bar{u}_1 \neq \bar{u}_2$ , there is only one  $T_{\bar{u}_1, \bar{u}_2} \in B_a \cap B_b$  so that  $T_{\bar{u}_1, \bar{u}_2}(\bar{u}_1) = a\bar{u}_1$  and  $T_{\bar{u}_1, \bar{u}_2}(\bar{u}_2) = b\bar{u}_2$ . There are exactly  $q+1$  choices for  $\bar{u}_1$  and there are exactly  $q$  choices for  $\bar{u}_2$  whenever  $\bar{u}_1$  is fixed. So  $|B_a \cap B_b| = q(q+1)$ . Since the dimension of  $F_{q^2}$  over  $F_q$  is 2, a linear transformation of  $F_{q^2}$  over  $F_q$  can have at most 2 eigenvalues. So  $B_{a_1} \cap B_{a_2} \cap \dots \cap B_{a_l} = \emptyset$  if  $l \geq 3$ . By the inclusion-exclusion principle, the number of non-singular linear transformations which have an eigenvalue in  $-S$  is  $\binom{m-1}{1} q(q^2-2) - \binom{m-1}{2} q(q+1)$ . Hence

$$N_2 = (q^2-1)(q^2-q) - \binom{m-1}{1}q(q^2-2) + \binom{m-1}{2}q(q+1).$$

(2).  $k = 3$ . Fix  $0 \neq a \in -S$ . For each  $u \in F_{q^3}^\times$ , let  $A_u$  be the set of non-singular linear transformations of  $F_{q^3}$  over  $F_q$  satisfying  $T(u) = au$ . By an argument similar to that in (1), there are exactly  $\frac{q^3-1}{q-1} = q^2+q+1$  distinct sets  $A_{\bar{u}}$ ,  $|A_{\bar{u}}| = (q^3-q)(q^3-q^2)$  and  $|A_{\bar{u}_1} \cap A_{\bar{u}_2}| = q^3-q^2$  for  $\bar{u}_1 \neq \bar{u}_2$ , where  $\bar{u}$  is a representative of the set  $\{bu \mid b \in F_q^\times\}$ . Note that there are in total  $\frac{(q^2+q+1)(q^2+q)}{2}$  such intersections  $A_{\bar{u}_1} \cap A_{\bar{u}_2}$  with  $\bar{u}_1 \neq \bar{u}_2$ . Now, let  $\bar{u}_1, \bar{u}_2$  and  $\bar{u}_3$  be pairwise distinct. If  $\bar{u}_1, \bar{u}_2$  and  $\bar{u}_3$  are linearly independent, then  $|A_{\bar{u}_1} \cap A_{\bar{u}_2} \cap A_{\bar{u}_3}| = 1$ . Note that there are exactly  $\frac{(q^2+q+1)(q^2+q)}{6} \cdot \frac{q^3-q^2}{q-1} = \frac{(q^2+q+1)(q^2+q)q^2}{6}$  such linearly independent triples. If  $\bar{u}_1, \bar{u}_2$  and  $\bar{u}_3$  are linearly dependent, then  $|A_{\bar{u}_1} \cap A_{\bar{u}_2} \cap A_{\bar{u}_3}| = q^3-q^2$ . Also, note that there are exactly  $\frac{(q^2+q+1)(q^2+q)}{6} \cdot (\frac{q^2-1}{q-1} - 2) = \frac{(q^2+q+1)(q^2+q)(q-1)}{6}$  such linearly dependent triples. Similarly,

$$|A_{\bar{u}_1} \cap \dots \cap A_{\bar{u}_l}| = \begin{cases} q^3-q^2 & \text{if } \bar{u}_1, \dots, \bar{u}_k \text{ are in the same plane} \\ 1 & \text{otherwise} \end{cases},$$

for  $4 \leq l \leq q+1$ . Note that there are exactly  $\frac{(q^2+q+1)(q^2+q)(q-1)\dots(q-l+2)}{l!}$   $l$ -tuples which are in the same plane, and there are exactly  $(q^2+q+1) - \frac{(q^2+q+1)(q^2+q)(q-1)\dots(q-l+2)}{l!}$   $l$ -tuples which are not in the same plane, for all  $4 \leq l \leq q+1$ . If  $l \geq q+2$ , then  $\bar{u}_1, \dots, \bar{u}_l$  are not in the same

plane. So, for  $l \geq q+2$ ,  $|A_{\bar{u}_1} \cap \dots \cap A_{\bar{u}_l}| = 1$  and there are exactly  $\binom{q^2+q+1}{l}$  such  $l$ -tuples.

By the inclusion-exclusion principle, the number of non-singular linear transformations which have  $a$  as an eigenvalue is

$$\begin{aligned}
 & \sum_{\bar{u}_1, \dots, \bar{u}_l} (-1)^{l-1} |A_{\bar{u}_1} \cap \dots \cap A_{\bar{u}_l}| \\
 &= (q^2+q+1)(q^3-q)(q^3-q^2) - \binom{q^2+q+1}{2} (q^3-q^2) - \sum_{l=3}^{q+1} (-1)^l \frac{(q^2+q+1)(q^2+q)(q-1) \dots (q-l+2)}{l!} (q^3-q^2) \\
 & \quad - \sum_{l=3}^{q+1} (-1)^l \left[ \binom{q^2+q+1}{l} - \frac{(q^2+q+1)(q^2+q)(q-1) \dots (q-l+2)}{l!} \right] - \sum_{l=q+2}^{q^2+q+1} (-1)^l \binom{q^2+q+1}{l} \\
 &= q^3(q^3-1)(q^2-1) - q^3(q^3-1) + q^3.
 \end{aligned}$$

If  $m = 1$ , we have  $N_3 = (q^3-1)(q^3-q)(q^3-q^2)$ . If  $m = 2$ , then we have  $N_3 = (q^3-1)(q^3-q)(q^3-q^2) - \binom{q^2+1}{1} [q^3(q^3-1)(q^2-1) - q^3(q^3-1) + q^3]$ .

Now consider  $m \geq 3$ . For each  $0 \neq a \in S$ , let  $B_a$  be the set of non-singular linear transformations which have  $a$  as an eigenvalue. Then  $|B_a| = q^3(q^3-1)(q^2-1) - q^3(q^3-1) + q^3 = q^3(q^3-1)(q^2-1) - q^3(q^3-2)$ .

Let  $a, b \in S$  with  $ab \neq 0$  and  $a \neq b$ . For  $\bar{u}_1 \neq \bar{u}_2$ , let  $C_{\bar{u}_1, \bar{u}_2}$  be the set of all non-singular linear transformations  $T$  so that  $T(\bar{u}_1) = a\bar{u}_1$  and  $T(\bar{u}_2) = b\bar{u}_2$ . Then  $|C_{\bar{u}_1, \bar{u}_2}| = q^3-q^2$  and there are exactly  $(q^2+q+1)(q^2+q)$  such sets. It is easy to see that for  $(\bar{u}_1, \bar{u}_2) \neq (\bar{u}_3, \bar{u}_4)$ ,



$$|C_{\bar{u}_1, \bar{u}_2} \cap C_{\bar{u}_3, \bar{u}_4}| = \begin{cases} 1 & \text{if either } \bar{u}_1 = \bar{u}_3 \text{ and } \bar{u}_1, \bar{u}_2, \bar{u}_4 \text{ are linearly independent} \\ & \text{or } \bar{u}_2 = \bar{u}_4 \text{ and } \bar{u}_1, \bar{u}_2, \bar{u}_3 \text{ are linearly independent} \\ 0 & \text{otherwise} \end{cases}$$

Note that there are exactly  $(q^2+q+1)(q^2+q)q^2$  such intersections  $|C_{\bar{u}_1, \bar{u}_2} \cap C_{\bar{u}_3, \bar{u}_4}| = 1$ .

Also note that if  $l \geq 3$ , then for all pairwise distinct ordered pairs  $(\bar{u}_i, \bar{v}_i)$ ,  $1 \leq i \leq l$ , we have

$$|\bigcap_{i=1}^l C_{\bar{u}_i, \bar{v}_i}| = \begin{cases} 1 & \text{if either } \bar{u}_1 = \dots = \bar{u}_l, \bar{v}_1, \dots, \bar{v}_l \text{ are on the same plane and } \bar{u}_1, \bar{v}_1, \bar{v}_2 \text{ are} \\ & \text{linearly independent, or } \bar{v}_1 = \dots = \bar{v}_l, \bar{u}_1, \dots, \bar{u}_l \text{ are on the same plane} \\ & \text{and } \bar{u}_1, \bar{u}_2, \bar{v}_1 \text{ are linearly independent} \\ 0 & \text{otherwise.} \end{cases}$$

There are exactly  $\frac{2(q^2+q+1)(q^2+q)q^2(q-1)\dots(q-l+2)}{l!}$  such intersections with  $|\bigcap_{i=1}^l C_{\bar{u}_i, \bar{v}_i}| = 1$ .

Moreover, if  $l \geq q+2$ ,  $\bigcap_{i=1}^l C_{\bar{u}_i, \bar{v}_i} = \emptyset$ . By the inclusion-exclusion principle, we have

$$\begin{aligned} |B_a \cap B_b| &= (q^2+q+1)(q^2+q)(q^3-q^2) - (q^2+q+1)(q^2+q)q^2 \\ &\quad + \sum_{l=3}^{q+1} (-1)^{l-1} \frac{2(q^2+q+1)(q^2+q)q^2(q-1)\dots(q-l+2)}{l!} \\ &= (q^2+q+1)q^3(q^2-3). \end{aligned}$$

So, if  $m = 3$ , then

$$N_3 = (q^3-1)(q^3-q)(q^3-q^2) - \binom{3-1}{1} [q^3(q^3-1)(q^2-2) + q^3] + \binom{3-1}{2} (q^2+q+1)q^3(q^2-3).$$

Finally, let  $m \geq 4$ . For all distinct  $a, b, c \in -S$  with  $abc \neq 0$ ,  $T \in B_a \cap B_b \cap B_c$  if and only if there are  $\bar{u}_1, \bar{u}_2$  and  $\bar{u}_3$  so that  $\bar{u}_1, \bar{u}_2, \bar{u}_3$  are linearly independent over  $F_q$  and  $T(\bar{u}_1) = a\bar{u}_1$ ,  $T(\bar{u}_2) = b\bar{u}_2$  and  $T(\bar{u}_3) = c\bar{u}_3$ . Note that there are exactly  $(q^2+q+1)(q^2+q)q^2$  choices of such ordered triples  $(\bar{u}_1, \bar{u}_2, \bar{u}_3)$ . So  $|B_a \cap B_b \cap B_c| = (q^2+q+1)(q^2+q)q^2$ . If there are distinct  $a, b, c, d \in -S$  with  $abcd \neq 0$ , it is easy to see  $B_a \cap B_b \cap B_c \cap B_d = \emptyset$ . By the inclusion-exclusion principle, we have that the number of non-singular linear transformations which have at least one eigenvalue in  $-S$  is

$$\binom{m-1}{1} [q^3(q^3-1)(q^2-2) + q^3] - \binom{m-1}{2} (q^2+q+1)q^3(q^2-3) + \binom{m-1}{3} (q^2+q+1)(q^2+q)q^2.$$

So  $N_3 = (q^3-1)(q^3-q)(q^3-q^2) - \binom{m-1}{1} [q^3(q^3-1)(q^2-2) + q^3] + \binom{m-1}{2} (q^2+q+1)q^3(q^2-3) - \binom{m-1}{3} (q^2+q+1)(q^2+q)q^2$ . This completes the proof.

It seems, from Lemma 2.2.8, that a closed form for the number  $N_k$  of  $S$ -CMs of  $F_{q^k}$  in the form  $b_0x + b_1x^q + \dots + b_{k-1}x^{q^{k-1}}$  will become more and more complicated when  $k$  becomes larger and larger. The author wonders whether or not there is a nice closed form for  $N_k$ . From Lemma 2.2.8 and its proof, it seems that  $N_k$  is a function in the variables  $q$  and  $|S|$  so that the highest exponent of  $q$  is  $k^k$  and the highest exponent of  $|S|$  is  $k$ .

Now we are ready to prove the following existence theorem.

Theorem 2.2.9. Let  $0 \in S \subseteq F_q$  and let  $k \geq 2$ . Then there is an S-CM of  $F_{q^k}$  of the form  $a_0x + a_1x^q + \dots + a_{k-1}x^{q^{k-1}}$  with  $\deg f > 1$ , except for the case  $k = 2$ ,  $q = 2$  and  $S = F_2$ .

Proof. At first, we consider  $k \geq 5$ . It is easy to see that there are distinct integers  $l, t \geq 2$  with  $l+t = k$ . It is well known that there are irreducible polynomials  $g_l(x), g_t(x) \in F_q[x]$  which have degrees  $l$  and  $t$ , respectively. Let  $g(x) = g_l(x)g_t(x)$  and let  $\bar{A}$  be the companion matrix of  $g(x)$ . Then  $\bar{A} \in GL(k, F_q)$  and  $g(x)$  is the minimal and characteristic polynomial of  $\bar{A}$ . Note that  $g(x)$  is not a power of any irreducible polynomial in  $F_q[x]$ . Let  $f(x) = a_0x + a_1x^q + \dots + a_{k-1}x^{q^{k-1}}$  be the corresponding linearized polynomial of  $\bar{A}$ , the same as in the Carlitz's proof of Theorem 1.4.13. Write

$A = (a_{i-j}^{p^j})$  taking  $i-j \bmod k$ . From Carlitz's proof,  $A$  and  $\bar{A}$  are similar.  $g(x)$  is also the minimal and characteristic polynomial of  $A$ . Since no element of  $-S$  is a root of  $g(x)$ ,  $f(x)$  is an S-CM of  $F_{q^k}$  by Lemma 2.2.7. We claim  $\deg f > 1$ . Indeed, if  $\deg f = 1$ , then  $A$  is diagonal  $(a_0, a_0^p, \dots, a_0^{p^{k-1}})$ . In this case,  $g(x)$  is a power of the minimal polynomial of  $a_0$  over  $F_q$  and we get a contradiction.

Now, for  $k = 2$  and  $3$ , we note that if a linearized polynomial  $f(x) \in F_{q^k}[x]$  is an  $F_q$ -CM of  $F_{q^k}$ , then  $f(x)$  is an S-CM of  $F_{q^k}$ . So we consider  $S = F_q$  in cases  $k = 2$  and  $3$  except for the case  $q = 2$  and  $k = 2$ .

Let  $k = 3$ . Since  $q \geq 2$ , from part (2) of Lemma 2.2.8, the number of all S-CMs of  $F_{q^3}$  in the form  $a_0x + a_1x^q + a_2x^{q^2}$  satisfies  $N_3 \geq 6q^3 > q^3 - 1$ . So there is at least one linearized polynomial  $f(x) \in F_{q^3}[x]$  which is an S-CM of  $F_{q^3}$  and  $\deg f > 1$ .

Let  $k = 2$ . From part (1) of Lemma 2.2.8, if  $q \geq 3$ ,  $N_2 \geq 2q^2 > q^2 - 1$  and so there is at least one linearized polynomial  $f(x) \in F_{q^2}[x]$  which is an S-CM of  $F_{q^2}$  and  $\deg f > 1$ . For  $q = 2$  and  $|S| = 1$ ,  $N_2 = (2^2 - 1)(2^2 - 2) = 6 > 3 = q^2 - 1$  and so there are three linearized



polynomials in  $F_4[x]$  which are S-CMs of  $F_4$  with degree  $> 1$ . For  $q = 2$  and  $|S| = 2$ ,  $N_2 = (2^2-1)(2^2-2)-2 \cdot (2^2-2) = 2$  and so all S-CMs of  $F_4$  are linear.

Finally, we consider  $k = 4$ . Since  $F_{q^4} = F_{(q^2)^2}$ ,  $q^2 \geq 4$  and  $F_{q^2} \supset F_q \supset S$ , there is at least one linearized polynomial of the form  $a_0x + a_2x^{q^2} \in F_{q^4}[x]$  which is an S-CM of  $F_{q^4}$  with degree  $> 1$  by the case  $k = 2$ . This completes the proof.

### 3. Mullen's Conjecture

Let  $p$  be a prime and  $q = p^n$  with  $n \geq 1$ . Theorem 1.2.5 says that there is a complete local field  $K$  of characteristic 0 so that if  $O_K$  is the ring of integers in  $K$ , then  $O_K/pO_K \simeq F_q$ . From the same theorem,  $O_K$  consists of all  $q$ -1st roots of unity. Let  $W$  be the set of all  $(q-1)$ st roots and 0. Then  $O_K/pO_K = \{\bar{\omega} + pO_K \mid \bar{\omega} \in W\}$ . Trivially, if  $\bar{\omega}_1, \bar{\omega}_2 \in W$ , then  $\bar{\omega}_1 + \bar{\omega}_2 = \bar{\omega}_3 + p\alpha$  for some  $\bar{\omega}_3 \in W$  and for some  $\alpha \in O_K$ . Since  $O_K/pO_K \simeq F_q$ , we embed  $F_q$  onto  $W$ . Moreover, if  $a \in F_q$ , we use  $\bar{a}$  to denote the corresponding element of  $a$  in  $W$ .

Lemma 2.3.1. Let  $S = \{0, a_1, \dots, a_{m-1}\} \subset F_q$  with  $1 < m \leq q-2$  (so  $q \geq 3$ ). Let

$f(x) \in F_q[x]$  be an S-CM of  $F_q$ . For  $1 \leq i < m$ , let the reduction of  $[f(x)]^i \bmod (x^q - x)$  be

$\sum_{l=0}^{q-1} c_{i,l} x^{q-1-l}$ . Then for each  $1 < k \leq m$  and for each  $1 \leq j < m$ , there is  $\beta_j \in O_K$  so that

$$\sum_{i=1}^{k-1} \binom{k}{i} \bar{a}_j^{k-1-i} \bar{c}_{i,k-i} = p^{r_k+1} \beta_j \text{ where } p^{r_k} \parallel k \text{ (if } (p,k) = 1, r_k = 0).$$

Proof. Let  $\bar{f}$  be the lifting of  $f$  on  $O_K$ , i.e., if  $f(x) = \delta_0 + \delta_1 x + \dots + \delta_t x^t$  then

$$\bar{f}(x) = \bar{\delta}_0 + \bar{\delta}_1 x + \dots + \bar{\delta}_t x^t. \text{ Fix } 1 < k \leq m \text{ and } 1 \leq j < m. \text{ Consider } \sum_{\bar{\omega} \in W} (\bar{f}(\bar{\omega}) + \bar{a}_j \bar{\omega})^k.$$

On one hand,

$$\begin{aligned} \sum_{\bar{\omega} \in W} (\bar{f}(\bar{\omega}) + \bar{a}_j \bar{\omega})^k &= \sum_{\bar{\omega} \in W} (\bar{b}_{\bar{\omega}} + p\alpha_{\bar{\omega}})^k \\ &= \sum_{\bar{\omega} \in W} \bar{b}_{\bar{\omega}}^k + \sum_{i=1}^k \binom{k}{i} p^i \sum_{\bar{\omega} \in W} \alpha_{\bar{\omega}}^i \bar{b}_{\bar{\omega}}^{k-i} = \sum_{\bar{\omega} \in W} \bar{b}_{\bar{\omega}}^k + \sum_{i=1}^k \binom{k}{i} p^i \alpha_i, \end{aligned}$$

where  $\bar{b}_{\bar{\omega}} \in W$  satisfies  $\bar{f}(\bar{\omega}) + \bar{a}_j \bar{\omega} = \bar{b}_{\bar{\omega}} + p\alpha_{\bar{\omega}}$ , for some  $\alpha_{\bar{\omega}} \in O_K$ , and

$$\alpha_i = \sum_{\bar{\omega} \in W} \alpha_{\bar{\omega}}^i \bar{b}_{\bar{\omega}}^{k-i} \in O_K.$$

Since  $f(x) + a_j x$  is a PP of  $F_q$ ,  $\bar{b}_{\bar{\omega}}$  ranges over all elements of  $W$  whenever  $f(\bar{\omega}) + a_j \bar{\omega}$  ranges over all elements of  $F_q$ , i.e., whenever  $\bar{\omega}$  ranges over all elements of  $W$ . Since  $2 \leq k \leq m < q-1$  and  $\bar{b}_{\bar{\omega}}$  ranges over all elements of  $W$ ,  $\sum_{\bar{\omega} \in W} \bar{b}_{\bar{\omega}}^k = 0$ . Since  $p^{r_k} \parallel k$ , it is easy to see that  $p^{r_k-i+1} \mid \binom{k}{i}$  for  $1 \leq i \leq r_k$ . So  $p^{r_k+1} \mid \binom{k}{i} p^i$  for all  $1 \leq i \leq k$ . This implies

$$\sum_{i=1}^k \binom{k}{i} p^i \alpha_i = p^{r_k+1} \beta_j$$

for some  $\beta_j' \in O_K$ . So there exists  $\beta_j' \in O_K$  so that

$$\sum_{\bar{\omega} \in W} (\bar{f}(\bar{\omega}) + \bar{a}_j \bar{\omega})^k = p^{r_{k+1}} \beta_j'.$$

On the other hand,

$$\sum_{\bar{\omega} \in W} (\bar{f}(\bar{\omega}) + \bar{a}_j \bar{\omega})^k = \sum_{i=0}^k \binom{k}{i} \bar{a}_j^{k-i} \cdot \sum_{\bar{\omega} \in W} \bar{\omega}^{k-i} [\bar{f}(\bar{\omega})]^i.$$

If  $i = 0$ ,  $\sum_{\bar{\omega} \in W} \bar{\omega}^k = 0$ . If  $i = k$ ,

$$\sum_{\bar{\omega} \in W} [\bar{f}(\bar{\omega})]^k = p^{r_{k+1}} \gamma$$

for some  $\gamma \in O_K$  since  $f(x)$  is a PP of  $F_q$ . For  $1 \leq i < k$ ,

$$[f(x)]^i \equiv \sum_{l=0}^{q-1} c_{i,l} x^{q-1-l} \pmod{(x^q - x)}$$

from the assumption. So for  $1 \leq i < k$ ,

$$\sum_{\bar{\omega} \in W} \bar{\omega}^{k-i} \cdot \sum_{l=0}^{q-1} \bar{c}_{i,l} \bar{\omega}^{q-1-l} = \sum_{l=0}^{q-1} \bar{c}_{i,l} \cdot \sum_{\bar{\omega} \in W} \bar{\omega}^{q-1-l+k-i} = (q-1) \bar{c}_{i,k-i}.$$



Hence,

$$\sum_{\bar{\omega} \in W} (\bar{f}(\bar{\omega}) + \bar{a}_j \bar{\omega})^k = p^{r_{k+1}} \gamma \sum_{i=1}^{k-1} \binom{k}{i} \bar{a}_j^{k-i} (q-1) (\bar{c}_{i,k-i} + p\gamma) = \sum_{i=1}^{k-1} \binom{k}{i} \bar{a}_j^{k-i} (q-1) c_{i,k-i} + p^{r_{k+1}} \gamma''$$

for some  $\gamma'' \in O_K$ .

Combining both results above, we have

$$\sum_{i=1}^{k-1} \binom{k}{i} \bar{a}_j^{k-i} (q-1) \bar{c}_{i,k-i} = p^{r_{k+1}} \beta_j''$$

for some  $\beta_j'' \in O_K$ . Since  $\bar{a}_j$  and  $(q-1)$  are units in  $O_K$ , we have

$$\sum_{i=1}^{k-1} \binom{k}{i} \bar{a}_j^{k-i-1} \bar{c}_{i,k-i} = p^{r_{k+1}} \beta_j$$

for some  $\beta_j \in O_K$ . This completes the proof.

Solving for  $\bar{c}_{i,k-i}$  in Lemma 2.3.1, we have the following key theorem in this section.

**Theorem 2.3.2.** Let  $0 \in S \subseteq F_q$  with  $2 \leq |S| \leq q-2$ . Let  $f(x) \in F_q[x]$  be an S-CM of  $F_q$ . For  $1 \leq i < |S|$ , let the reduction of  $[f(x)]^i \bmod (x^q - x)$  be  $\sum_{l=0}^{q-1} c_{i,l} x^{q-1-l}$ . Then for  $1 < k \leq |S|$  and  $1 \leq i < k$

$$\bar{c}_{i,k-i} = \frac{p^{r_{k+1}}}{\binom{k}{i}} \alpha_{i,k-i}$$

for some  $\alpha_{i,k-i} \in O_K$ , where  $p^{r_k} \parallel k$ .

Proof. Let  $|S| = m$  and write  $S = \{0, a_1, \dots, a_{m-1}\}$  as in Lemma 2.3.1. By Lemma 2.3.1, all  $\bar{c}_{i,k-i}$ ,  $1 \leq i < k$ , satisfy

$$\sum_{i=1}^{k-1} \binom{k}{i} \bar{a}_j^{k-i-1} \bar{c}_{i,k-i} = p^{r_{k+1}} \beta_j$$

for all  $1 \leq j < m$ . Take  $j = 1, 2, \dots, k-1$ . Then  $\bar{c}_{i,k-i}$  are common solutions of the system of  $k-1$  linear equations

$$\sum_{i=1}^{k-1} \binom{k}{i} \bar{a}_j^{k-i-1} y_i = p^{r_{k+1}} \beta_j,$$

$1 \leq j \leq k-1$ . Let  $A$  be the  $(k-1) \times (k-1)$  matrix of coefficients of all equations in this system and let  $B_i$ ,  $1 \leq i \leq k-1$ , be the  $(k-1) \times (k-1)$  matrix obtained by replacing the  $i$ th column of  $A$  with the column

$$\begin{pmatrix} p^{r_{k+1}} \beta_1 \\ \vdots \\ p^{r_{k+1}} \beta_{k-1} \end{pmatrix}$$

and fixing all other columns of  $A$ . Then, in  $O_K$ ,  $\det A = (\det V) \prod_{i=1}^{k-1} \binom{k}{i}$  where

$V = (\bar{a}_j^{k-i-1})$  is a Vandermonde matrix generated by  $\bar{a}_1, \dots, \bar{a}_{k-1}$ . Since  $\bar{a}_1, \dots, \bar{a}_{k-1} \in W$  are all non-zero and distinct,  $\det V$  is a unit in  $O_K$ . For each  $1 \leq i < k$ , it is easy to see that  $\det B_i = p^{r_k+1} \cdot \Delta_i \cdot \prod_{j \neq i} \binom{k}{j}$  for some  $\Delta_i \in O_K$ . By Cramer's rule, we have that for  $1 \leq i < k$ ,

$$\bar{c}_{i,k-i} = \frac{\det B_i}{\det A} = \frac{p^{r_k+1}}{\binom{k}{i}} \alpha_{i,k-i}$$

for some  $\alpha_{i,k-i} \in O_K$ .

Now we are in a position to prove one of our main results in this section.

**Theorem 2.3.3 (Mullen's Conjecture).** Let  $0 \in S \subseteq F_q$  with  $|S| \leq q-2$ . If  $f(x)$  is an  $S$ -CM of  $F_q$ , then the degree of the reduction of  $f(x) \bmod (x^q - x)$  is  $\leq q-1 - |S|$ .

**Proof.** If  $|S| = 1$ , it is a part of Hermite's Criterion. So we consider  $|S| \geq 2$ .

Let the reduction of  $f(x) \bmod (x^q - x)$  be  $\sum_{i=0}^{q-1} c_{1,i} x^{q-1-i}$ . Since  $0 \in S$ ,  $f(x)$  is a PP of  $F_q$  and

so  $c_{1,0} = 0$  by the same theorem above. From Theorem 2.3.2, we have that for

$1 \leq i \leq |S| - 1$ ,

$$\bar{c}_{1,i} = \frac{p^{r_{1+i}+1}}{1+i} \alpha_{1,i}$$



for some  $\alpha_{1,i} \in O_K$ , where  $p^{r_{1+i}} \parallel (1+i)$ . So  $\bar{c}_{1,i} \in pO_K$  for all  $1 \leq i \leq |S|-1$ . I.e.,  $c_{1,i} = 0$  in  $F_q$ . Hence, the degree of the reduction of  $f(x) \bmod (x^q - x)$  is  $\leq q-1 - |S|$ .

As we mentioned in the proof of Theorem 2.3.3, Mullen's Conjecture is, indeed, a part of Hermite's Criterion when  $S = \{0\}$ . If  $S = \{0,1\}$ , Niederreiter and Robinson (see [28]) proved this theorem for odd  $q$ , and Wan proved this theorem for  $q$  even in 1986 (see [40]). Basically, their techniques are the same. The method we used is a generalization of their methods.

Now, we reach a position to discuss the size of the set  $S$ . We have the following

Corollary 2.3.4. Let  $\emptyset \neq S \subseteq F_q$ . Then there is an  $S$ -CM of  $F_q$  if and only if  $S \not\subseteq F_q^\times$ .

Proof. At first, we consider  $S = F_q$  or  $S = F_q^\times$ . Let  $T \subset S$  with  $|T| = q-2$ . If  $f(x) \in F_q[x]$ , with  $\deg f \leq q-1$ , were an  $S$ -CM, then  $f(x)$  would be a  $T$ -CM. From Theorem 2.3.3,  $\deg f \leq q-1-(q-2) = 1$ . So  $f(x) = ax+b$  for some  $a \in F_q^\times$ . Since  $S \supseteq F_q^\times$ ,  $-S \supseteq F_q^\times$  and so  $a \in -S$ , where  $-S = \{-s \mid s \in S\}$ , i.e.,  $-a \in S$ . But in this case,  $f(x) + (-a)x = b$  would be a constant polynomial and also a PP of  $F_q$ . We get a contradiction.

Let  $S \not\subseteq F_q^\times$ . Then  $-S \not\subseteq F_q^\times$ . Choose  $a \in F_q^\times - (-S)$ . Then  $a+s \neq 0$  for all  $s \in S$ . Let  $f(x) = ax$ . Then  $f(x) + sx$  is a PP of  $F_q$  for all  $s \in S$  and so  $f(x)$  is an  $S$ -CM of  $F_q$ . This completes the proof.

From this corollary, we see that  $|S| \leq q-1$  if  $0 \in S$  and  $|S| \leq q-2$  if  $0 \notin S$ .

#### 4. Properties and Comparisons

In Section 2, we fixed the set  $S$  and searched for polynomials in  $F_q[x]$  which are S-CMs of  $F_q$ . In this section we consider the converse problem, i.e., given a polynomial  $f(x)$ , we consider the question of whether there is a set  $S \subseteq F_q$  so that  $f(x)$  is an S-CM of  $F_q$ .

Let  $f(x) \in F_q[x]$ . If the reduction of  $f(x) \bmod (x^q - x)$  is a linear polynomial  $ax + b$ , we have already seen in Section 2 that for any  $S \subseteq F_q$  with  $a \notin -S$ ,  $f(x)$  is an S-CM of  $F_q$ . Hence, the maximum cardinality  $|S|$  of  $S$  is  $q-1$ .

Let  $l$  be the degree of the reduction of  $f(x) \bmod (x^q - x)$ . If  $l \geq 2$  and  $l \nmid (q-1)$ , then  $f(x)$  is not a PP of  $F_q$  by Corollary 1.4.4. Hence, if  $l \geq 2$  and  $l \mid (q-1)$ , there is no  $S \subseteq F_q$  so that  $f(x)$  is an S-CM of  $F_q$ .

Now we consider linearized polynomials.

**Theorem 2.4.1.** If  $f(x)$  is a linearized polynomial of  $F_{q^k}[x]$  over  $F_q$ , there is at least one non-empty subset  $S \subseteq F_{q^k}$  so that  $f(x)$  is an S-CM of  $F_{q^k}$ . Moreover, the maximum cardinality of all such subsets is  $\geq 1 + \frac{(q-2)(q^{k-1})}{q-1}$ .

**Proof.** Write  $f(x) = a_0x + a_1x^q + \dots + a_{k-1}x^{q^{k-1}}$ . Let  $g(x) = a_1x^q + \dots + a_{k-1}x^{q^{k-1}}$  and let  $A = (b_{i-j}^q)$ , taking  $i-j \bmod k$ , where  $b_0 = y$  and  $b_i = a_i$  for  $1 \leq i \leq k-1$ . Let  $h(y) = \det A$ . Note that  $h(y)$  is a polynomial of degree  $1+q+\dots+q^{k-1}$  in the variable  $y$ . By Theorem 1.4.12, for  $a \in F_{q^k}$ ,  $g(x) + ax$  is a PP of  $F_{q^k}$  if and only if  $h(a) \neq 0$ . Let

$T = \{a \in F_{q^k} \mid h(a) \neq 0\}$ . Then  $g(x)$  is an  $T$ -CM of  $F_{q^k}$ . Since  $h(y)$  has at most

$$1+q+\dots+q^{k-1} = \frac{q^k-1}{q-1} \text{ roots in } F_{q^k}, |T| \geq q^k - \frac{q^k-1}{q-1} = 1 + \frac{(q-2)(q^{k-1})}{q-1}.$$

Let  $S = \{a-a_0 \mid a \in T\}$ . It is easy to see that  $f(x)$  is an  $S$ -CM of  $F_q$  and that  $|S| = |T|$ . This completes the proof.

We next consider polynomials of the form  $ax^{(q+1)/2} + bx$ . In this case,  $q$  is odd. First, we need the following two lemmas.

Lemma 2.4.2. Let  $\emptyset \neq S \subseteq F_q$  and let  $f(x) \in F_q[x]$ . Let  $D(f) = \{\frac{f(b)-f(a)}{b-a} \mid a, b \in F_q \text{ with } a \neq b\}$ . Then  $f(x)$  is an  $S$ -CM of  $F_q$  if and only if  $S \cap (-D(f)) = \emptyset$  where  $-D(f) = \{-a \mid a \in D(f)\}$ .

Proof. For  $a \in S$ ,  $f(x)+ax$  is not a PP of  $F_q$  if and only if there are  $x_0, y_0 \in F_q$  with  $x_0 \neq y_0$  so that  $f(x_0)+ax_0 = f(y_0)+ay_0$ . The last statement is equivalent to  $a \in -D(f)$ .

We notice that Corollary 2.3.4 is also easily proved using this lemma.

Lemma 2.4.3. Let  $q$  be odd and  $f(x) = x^{(q+1)/2}$ . Then  $|D(f)| = \frac{q+3}{2}$  and  $\pm 1 \in D(f)$ .

Proof. Write  $g_f(x,y) = \frac{f(x)-f(y)}{x-y}$ . Let  $a, b \in F_q$  with  $a \neq b$ . If either  $a = 0$  or  $b = 0$ , then  $g_f(a,b) = \pm 1 \in D(f)$ .

Now, consider  $ab \neq 0$ . Let  $c = ab^{-1}$  so that  $c \neq 1$ .



$$g_f(a,b) = \frac{f(b)-f(a)}{b-a} = a^{(q-1)/2} + a^{(q-3)/2}b + \dots + ab^{(q-3)/2} + b^{(q-1)/2} = b^{(q-1)/2} \cdot \frac{c^{(q+1)/2}-1}{c-1} = \pm \frac{c^{(q+1)/2}-1}{c-1}.$$

If  $c^{(q-1)/2} = 1$ , we have  $g_f(a,b) = \pm 1$ . Consider  $c^{(q-1)/2} = -1$ . Then

$$g_f(a,b) = \pm \frac{c^{(q+1)/2}-1}{c-1} = \pm \frac{-c-1}{c-1} = \mp \left( 1 + \frac{2}{c-1} \right).$$

Moreover, let  $c_1, c_2 \in F_q^\times$  satisfy  $c_1^{(q-1)/2} = -1 = c_2^{(q-1)/2}$ . Then  $1 + \frac{2}{c_1-1} = 1 + \frac{2}{c_2-1}$  if and only if  $c_1 = c_2$ . And  $1 + \frac{2}{c_1-1} = -1 - \frac{2}{c_2-1}$  if and only if  $-\frac{1}{c_2-1} = 1 + \frac{1}{c_1-1} = \frac{c_1}{c_1-1}$ . The last result is equivalent to  $1-c_2 = 1 - \frac{1}{c_1}$  and so equivalent to  $c_1c_2 = 1$ .

For a non-square  $c \in F_q^\times$ , there are exactly  $q-1$  ordered pairs  $(a,b)$  satisfying  $ab^{-1} = c$ . Since there are exactly  $\frac{q-1}{2}$  non-squares in  $F_q$ , there are totally  $(q-1) \cdot \frac{q-1}{2}$  such ordered pairs. From results in the last paragraph, we see that  $2(q-1)$  ordered pairs  $(a,b)$  take 2 distinct values  $\pm \left( 1 + \frac{2}{c-1} \right)$  where  $c = ab^{-1}$  or  $\frac{1}{c} = ab^{-1}$ . Also from the last paragraph,  $g_f$  assumes

$$2 \cdot \frac{(q-1) \cdot \frac{q-1}{2}}{2(q-1)} = \frac{q-1}{2}$$

distinct values of the form  $\pm \left( 1 + \frac{2}{c-1} \right)$  with  $c$  non-square. Also note  $1 + \frac{2}{c-1} \neq \pm 1$  for any

$c \in F_q^\times$  and  $c \neq 1$ . So  $|D(f)| = \frac{q-1}{2} + 2 = \frac{q+3}{2}$ .

Theorem 2.4.4. Let  $q$  be odd and let  $f(x) = ax^{(q+1)/2} + bx \in F_q[x]$  be non-zero. Then there is a non-empty subset  $S \subseteq F_q$  so that  $f(x)$  is an S-CM of  $F_q$ . Moreover, if  $a \neq 0$ , the maximum cardinality of all such  $|S|$  is  $\frac{q-3}{2}$ .

Proof. If  $a=0$ ,  $f(x)$  is linear and so the result holds. We consider  $a \neq 0$ . Let  $g(x) = ax^{(q+1)/2}$ . From Lemma 2.4.3,  $|D(g)| = \frac{q+3}{2}$ . Let  $T = F_q - (-D(g))$ . By Lemma 2.4.2,  $g(x)$  is a T-CM of  $F_q$ . It is easy to see that  $|T| = \frac{q-3}{2}$ . Let  $S = \{t-b \mid t \in T\}$ . Then  $f(x)$  is an S-CM of  $F_q$  and  $|S| = \frac{q-3}{2}$ .

In this part, we consider difference permutation polynomials. Such polynomials are a special case of planar functions and give rise to affine planes (see Dembowski [9] and Dembowski and Ostrom [10]). They are defined (on finite fields) as follows.

Definition. A polynomial  $f(x) \in F_q[x]$  is called a difference permutation polynomial if for all  $a \in F_q^\times$  the polynomial  $f_a(x) = f(x+a) - f(x)$  is a PP of  $F_q$ .

For odd  $q$ , it is easy to check that quadratic polynomials are difference permutation polynomials.

Theorem 2.4.5. If  $f(x) \in F_q[x]$  is a difference permutation polynomial, there is no subset  $S$  of  $F_q$  so that  $f(x)$  is an S-CM of  $F_q$ .

Proof. From Lemma 2.4.1, it is enough to prove  $D(f) = F_q$ . Fix  $a \in F_q^\times$ . By definition,  $g(x) = f(x+a) - f(x)$  is a PP of  $F_q$  and so is  $\frac{f(x+a)-f(x)}{(x+a)-x}$ . This implies  $D(f) \supseteq F_q$  and the proof is complete.

In the remaining part of this section, we consider a fixed non-empty subset of  $F_q$  and a fixed polynomial  $f(x) \in F_q[x]$  which is an S-CM of  $F_q$ . Using this polynomial, we will generate some new S-CMs of  $F_q$  associated with the same set  $S$  or with a new set  $T$  which satisfies some conditions.

It is known that a polynomial  $f(x)$  is a PP of  $F_q$  if and only if its normalized polynomial is a PP of  $F_q$ . (The normalized polynomial of  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ ,  $a_0 \neq 0$  is defined to be  $\bar{f}(x) = a_0^{-1} [f(x - \frac{a_1 a_0^{-1}}{n}) - f(-\frac{a_1 a_0^{-1}}{n})]$  if  $\gcd(n, q) = 1$  and  $\bar{f}(x) = a_0^{-1} [f(x) - a_n]$  if  $\gcd(n, q) > 1$ ). This property is no longer true for complete mappings (see [28]). Even so, we have

**Theorem 2.4.6.** Let  $\emptyset \neq S \subset F_q$ . Let  $f(x) = a_l x^l + a_{l-1} x^{l-1} + \dots + a_1 x + a_0 \in F_q[x]$  with  $a_l \neq 0$ , and let  $\bar{f}(x)$  be the normalized polynomial of  $f(x)$ . Moreover, let  $T = a_l^{-1} S = \{a_l^{-1} s \mid s \in S\}$ . If  $f(x)$  is an S-CM of  $F_q$ , then  $\bar{f}(x)$  is a T-CM of  $F_q$ .

**Proof.** From the definition of normalized polynomial, there is  $b \in F_q$  so that  $\bar{f}(x) = a_l^{-1} [f(x+b) - f(b)]$ . From Theorem 2.2.1,  $f(x+b) - f(b)$  is an S-CM of  $F_q$  since  $f(x)$  is an S-CM. Now, for  $a_l^{-1} s \in T$ ,  $\bar{f}(x) + a_l^{-1} s x = a_l^{-1} [f(x+b) - f(b) + s x]$  is a PP of  $F_q$ . So  $\bar{f}(x)$  is a T-CM of  $F_q$ .

Let  $\emptyset \neq S \subset F_q$ . If  $f(x)$  is an S-CM of  $F_q$ , its normalized polynomial  $\bar{f}(x)$  may not be an S-CM of  $F_q$ . For example, let's consider  $S = \{0, \pm 1\} \subset F_{13}$  and  $f(x) = 2x^7$ . By Lemma 2.2.2,  $f(x)$  is an S-CM of  $F_{13}$ . Now  $\bar{f}(x) = x^7$  by the definition.  $\eta(0-1^2) =$



$\eta(5^2) = 1$  but  $\eta((0+1)^2-1^2) = \eta(0) = 0 = \eta((0-1)^2-1^2)$  by definition of quadratic character. By Lemma 2.2.2,  $\bar{f}(x)$  is not an S-CM of  $F_q$ .

Part (4) of Theorem 2.2.1 can be generalized as the following

**Theorem 2.4.7.** Let  $q = p^n$  and  $\emptyset \neq S \subset F_q$ . For any  $0 \leq k < n$ , let  $S^{p^k} = \{a^{p^k} \mid a \in S\}$ . Then  $f(x) = a_l x^l + a_{l-1} x^{l-1} + \dots + a_1 x \in F_q[x]$  is an S-CM of  $F_q$  if and only if for  $0 < k < n$ ,  $f_k(x) = a_l^{p^k} x^l + a_{l-1}^{p^k} x^{l-1} + \dots + a_1^{p^k} x$  is an  $S^{p^k}$ -CM of  $F_q$ .

**Proof.** It is enough to prove that if  $f(x) = a_l x^l + \dots + a_1 x \in F_q[x]$  is an S-CM, then

$f_1(x) = a_l^p x^l + \dots + a_1^p x$  is an  $S^p$ -CM.

Let  $g(x) = x^p$ . By Theorem 1.4.1,  $g(x)$  is a PP of  $F_q$  since  $(p, q-1) = 1$ .

Since  $f(x)$  is an S-CM of  $F_q$ ,  $f(x) + ax$  is a PP of  $F_q$  for all  $a \in S$ . Now, for  $a \in S$ ,  $(g \circ f \circ g^{-1})(x) + a^p x = g(f(g^{-1}(x))) + g(a \cdot g^{-1}(x)) = g(f(g^{-1}(x)) + a g^{-1}(x))$ . Write  $g^{-1}(x) = y$ . Then we have  $(g \circ f \circ g^{-1})(x) + a^p x = g(f(y) + ay)$ . Since  $f(x) + ax$  and  $g(x)$  are PPs of  $F_q$ ,  $(g \circ f \circ g^{-1})(x) + a^p x$  is a PP of  $F_q$  for all  $a^p \in S^p$ . Now

$$\begin{aligned}
 (g \circ f \circ g^{-1})(x) &= g(f(g^{-1}(x))) \\
 &= g(a_l [g^{-1}(x)]^l + \dots + a_1 g^{-1}(x)) \\
 &= g(a_l) \cdot g([g^{-1}(x)]^l) + \dots + g(a_1) \cdot g(g^{-1}(x)) \\
 &= a_l^p [g(g^{-1}(x))]^l + \dots + a_1^p \cdot g(g^{-1}(x)) \\
 &= a_l^p x^l + \dots + a_1^p x \\
 &= f_1(x)
 \end{aligned}$$

Hence,  $f_1(x) + a^p x$  is a PP of  $F_q$  for all  $a^p \in S^p$ . So  $f_1(x)$  is an  $S^p$ -CM of  $F_q$ .

Let  $q = p^n$  and  $0 \leq k < n$ . Let  $\emptyset \neq S \subset F_q$ . Let  $f(x) = a_l x^l + \dots + a_1 x$  be an  $S$ -CM of  $F_q$ . Let  $g(x) = x^{p^k}$ . By Theorem 2.4.7,  $(g \circ f \circ g^{-1})(x) = (a_l x^{p^{n-k}} + \dots + a_1 x^{p^{n-k}})^{p^k}$  is an  $S^{p^k}$ -CM of  $F_q$ . Note that  $|S^k| = |S|$ . If we just consider  $(g \circ f)(x) = (a_l x^l + \dots + a_1 x)^{p^k}$ , this polynomial may be a T-CM of  $F_q$  associated with some other subset  $T$  of  $F_q$ . But  $|T|$  may not be equal to  $|S|$ . The following is an example.

Consider  $q = p^2$  and  $f(x) = x$ . Then  $f(x)$  is an  $(F_q - \{-1\})$ -CM of  $F_q$ . Let  $g(x) = x^p$ . Then  $(g \circ f)(x) = x^p = g(x)$ . Now  $D(g) = \left\{ \frac{g(b) - g(a)}{b - a} \mid a, b \in F_q, a \neq b \right\} = \{(b-a)^{p-1} \mid \forall a, b \in F_q, a \neq b\} = \{a^{p-1} \mid a \in F_q^\times\}$ . Then  $|D(g)| = \frac{p^2-1}{p-1} = p+1$ . Let  $T = F_q - (-D(g))$ . By Lemma 2.4.2,  $g(x)$  is a T-CM of  $F_q$ . Note that  $|T| = q^2 - p - 1 < q^2 - 1 = |F_q - \{-1\}| = |S|$ .

As noted above,  $[f(x)]^{p^k}$  may not be a T-CM of  $F_q$  with  $|T| = |S|$ . But  $[f(x)]^{p^k}$  can be a "modified" T-CM of  $F_q$ . We have

**Theorem 2.4.8.** Let  $q = p^n$  and  $\emptyset \neq S \subset F_q$ . A polynomial  $f(x) \in F_q[x]$  is an  $S$ -CM of  $F_q$  if and only if for  $0 \leq k < n$ ,  $[f(x)]^{p^k} + a^{p^k} x^{p^k}$  is a PP of  $F_q$  for all  $a \in S$ .

Proof. Let  $g(x) = x^{p^k}$ . Then  $f(x)$  is an S-CM of  $F_q$  if and only if  $f(x)+ax$  is a PP of  $F_q$  for all  $a \in S$ . Since  $g(x)$  is a PP of  $F_q$ , the last statement is equivalent to that for all  $a \in S$   $g(f(x)+ax) = (f(x)+ax)^{p^k} = [f(x)]^{p^k} + a^{p^k} x^{p^k}$  is a PP of  $F_q$ .

In this theorem, if we let  $S$  consist of all conjugates of elements in  $S$  over the prime field and let  $h(x) = [f(x)]^{p^k}$ , then we have that  $h(x)+ax^{p^k}$  is a PP of  $F_q$  for all  $a \in S$ . Furthermore, if  $g(x)=x^{p^k}$ , then  $h(x) + ag(x)$  is a PP of  $F_q$  for all  $a \in S$ . From Theorem 2.4.8,  $h(g^{-1}(x))$  is an S-CM of  $F_q$ . In general, this is the case as shown by the following theorem.

Theorem 2.4.9. Let  $f(x), g(x) \in F_q[x]$  and let  $g(x)$  be a PP of  $F_q$ . For  $a \in F_q$ ,  $f(x)+ag(x)$  is a PP of  $F_q$  if and only if  $f(g^{-1}(x)) + ax$  is a PP of  $F_q$ . Moreover, let  $\phi \neq S \subset F_q$ . Then  $f(x)+ag(x)$  is a PP of  $F_q$  for all  $a \in S$  if and only if  $f(g^{-1}(x))$  is an S-CM of  $F_q$ .

Proof. Write  $y = g(x)$ . Then  $x = g^{-1}(y)$ . So  $f(x)+ag(x)$  is a PP of  $F_q$  if and only if  $f(g^{-1}(y))+ag(g^{-1}(y)) = f(g^{-1}(y))+ay$  is a PP of  $F_q$ .

The second assertion follows immediately from the first assertion.

Now, let's look at Theorem 2.4.7 again. Fix  $0 \leq k < n$ . Let  $T = S^{p^k}$ . As we mentioned before,  $|T| = |S|$ . By Theorem 2.4.7, we can construct a T-CM of  $F_q$  using an S-CM of  $F_q$ . Also notice that such a constructed polynomial is unique. So there is a one-to-one correspondence between the set of all S-CMs and the set of all T-CMs. The following theorem tells us that there is a one-to-one correspondence between the set of all S-CMs and the set of all T-CMs if there is a linear relation between  $S$  and  $T$ . Moreover,



all polynomials we consider in the next theorem have degree  $\leq q-1$  since any polynomial and its reduction mod  $(x^q-x)$  have the same images.

**Theorem 2.4.10.** Let  $S, T$  be two non-empty subsets of  $F_q$ . Let  $\bar{C}(S)$  and  $\bar{C}(T)$  be sets of all  $S$ -CMs and all  $T$ -CMs, respectively. If there is a function  $C(x)=ax+b \in F_q[x]$  with  $a \in F_q^\times$  so that  $T = C(S) = \{C(s) \mid s \in S\}$ , then there is a one-to-one correspondence between  $\bar{C}(S)$  and  $\bar{C}(T)$  (so  $|\bar{C}(S)| = |\bar{C}(T)|$ ).

**Proof.** Define  $d: \bar{C}(S) \rightarrow \bar{C}(T)$  by  $d(f(x)) = f(ax)-bx$  for all  $f(x) \in \bar{C}(S)$ . Since  $T = C(S)$ , every element of  $T$  is of the form  $as+b$ ,  $s \in S$ .  $d(f(x)) + (as+b)x = f(ax) + s(ax) = f(y) + sy$ , where  $y = ax$ . Since  $f(x)$  is an  $S$ -CM of  $F_q$ ,  $d(f(x))$  is an  $T$ -CM of  $F_q$ . It is easy to see that  $d$  is well-defined and one-to-one.  $d$  is also onto since for  $g(x) \in \bar{C}(T)$ ,  $g(a^{-1}x)+a^{-1}bx \in \bar{C}(S)$  and  $d(g(a^{-1}x)+a^{-1}bx) = g(x)$ . So  $d$  is a one-to-one correspondence between  $\bar{C}(S)$  and  $\bar{C}(T)$ .

Let  $S, T$  be two non-empty subsets of  $F_q$ , where  $q = p^n$ . Theorem 2.4.7 says that if  $T = Sp^k$  for some  $0 \leq k < n$ , then  $|\bar{C}(S)| = |\bar{C}(T)|$ . Theorem 2.4.10 says that if there is a linear relation between  $S$  and  $T$ , then  $|\bar{C}(S)| = |\bar{C}(T)|$ . But in general,  $|S| = |T|$  does not imply  $|\bar{C}(S)| = |\bar{C}(T)|$ . The following is an example.

Consider  $F_9 = \{0, 1, 2, \beta, \beta+1, \beta+2, 2\beta, 2\beta+1, 2\beta+2\}$  where  $\beta$  satisfies  $\beta^2 = 2\beta+1$ . Let  $S = \{0, 1, 2\}$  and  $T = \{0, 1, \beta\}$ .

By Theorem 2.3.3, if  $f(x) \in F_9[x]$  is an  $S$ -CM (or a  $T$ -CM), then the degree of the reduction of  $f(x) \bmod (x^9-x)$  is  $\leq 9-1-3 = 5$ . So we just consider all polynomials of  $F_9[x]$  which have degree  $\leq 5$ . Also note that each  $S$ -CM (and  $T$ -CM) of  $F_9$  is also a complete mapping.

According to Niederreiter-Robinson's complete mapping table (see p. 50), there are exactly six kinds of complete mappings of  $F_9$ :

- (1)  $ax+b$ ,  $a, b \in F_9$ ,  $a \neq 0$ ,  $-1$
- (2)  $-ax^3+c$ ,  $a, c \in F_9$ ,  $a$  a nonsquare of  $F_9$
- (3)  $ax^3-x+c$ ,  $a, c \in F_9$ ,  $a$  a nonsquare of  $F_9$
- (4)  $(b-a)^{-1}x^3 - b(b-a)^{-1}x+c$ ,  $a, b, c \in F_9$ ,  $a \neq b$  nonsquares of  $F_9$
- (5)  $a(x+b)^5+c$ ,  $a, b, c \in F_9$ ,  $a^2 = 2$
- (6)  $a(x+b)^5 \pm x+c$ ,  $a, b, c \in F_9$ ,  $a^2 = 2$

Since  $f(x)$  is an S-CM (T-CM) of  $F_9$  if and only if  $f(x)-f(0)$  is an S-CM (T-CM) of  $F_9$ , we consider all polynomials which have constant term 0.

For (1), it is easy to see that there are six such S-CMs and six such T-CMs.

For (2), (3) and (4), let  $f(x) = tx^3$ . Then  $D(f) = \{t(u-v)^2 \mid u \neq v \in F_9\} = \{t(2\beta+1), 2t, t(\beta+2), t\}$ . For  $t$  a nonsquare,  $D(f)$  consists of all nonsquares. For (2), there are 4  $a$ 's so that  $-ax^3$  is an S-CM but there is no such T-CM. For (3), there are 4  $a$ 's so that  $ax^3-x$  is an S-CM and a T-CM (since  $\beta+2$  is a square). For (4), if  $b-a$  is square, then  $D(f)$  consists of all squares in  $F_9^\times$ . In this case,  $(b-a)^{-1}x^3-b(b-a)^{-1}x$  is an S-CM if  $(a,b) = (2\beta+2,\beta), (\beta,2\beta+2), (\beta+1,2\beta), (2\beta,\beta+1)$  and is a T-CM if  $(a,b) = (\beta+1,\beta), (\beta,2\beta+2), (2\beta+2,2\beta), (2\beta,\beta+1)$ . If  $b-a$  is nonsquare, then  $D(f)$  consists of all nonsquares in  $F_9^\times$ . In this case, there are no such  $(a,b)$  so that  $(b-a)^{-1}x^3-b(b-a)^{-1}x$  is an S-CM, and there are only two pairs  $(a,b) = (2\beta,\beta)$  and  $(\beta,2\beta)$  so that  $(b-a)^{-1}x^3-b(b-a)^{-1}x$  is a T-CM.

For (5) and (6), let  $f(x) = ax^5 = ax^{(9+1)/2}$  with  $a^2 = 2$ . From the proof of Lemma 2.4.3, we have  $D(f) = \{a, -a, a\beta, -a\beta, a(2\beta+2), -a(2\beta+2)\}$ . In fact,  $D(f) = F_9 - \{0, 1, -1\}$  for both  $a = 2\beta+1$  and  $a = \beta+2$ . So all polynomials in the forms (5) and (6) are S-CMs but not T-CMs.



Combining all of these results together, we have  $|\bar{C}(S)| = 9 \times (6+4+4+4+2 \times 9 \times 3) = 648$  and  $|\bar{C}(T)| = 9 \times (6+4+4+2) = 144$ . So  $|\bar{C}(S)| \neq |\bar{C}(T)|$ .

## 5. Very Complete Mappings

In this section, we consider  $q$  odd. Let  $S = \{0, 1, -1\} \subset F_q$ . If a polynomial  $f(x) \in F_q[x]$  is an  $S$ -CM of  $F_q$ , we call it a very complete mapping (abbreviated VCM) of  $F_q$ . From this, we see that every VCM of  $F_q$  is a complete mapping of  $F_q$  and consequently, most results in this section are similar to those of Niederreiter-Robinson's work for complete mappings of  $F_q$  (see [28]).

At first, we want to characterize VCMs which have degree  $\leq 6$ . Niederreiter and Robinson already characterized all complete mappings which have degree  $\leq 6$ . Their results are listed on the next page. In this table, complete mappings of degree 6 are considered for fields of order relatively prime to 6.

Using this table, we can characterize all VCMs of  $F_q$  which have degree  $\leq 6$ , except for polynomials of degree 6 over  $F_q$  with  $(6, q) = 3$ . We discuss case by case the entries in this table.

Since we consider odd  $q$ , the case  $q \equiv 0 \pmod{2}$  cannot happen.

Theorem 2.2.1 says that  $f(x)$  is a VCM of  $F_q$  if and only if  $f(x+b)$  is a VCM of  $F_q$  for all  $b \in F_q$ . Hence, from the table, we just need to consider polynomials of the form  $ax^k+bx$  (or  $ax^5+bx^3+cx$  in the case  $q = 13$ ). Now  $f(x)$  is a VCM of  $F_q$  if and only if both  $f(x)$  and  $f(x)-x$  are complete mappings of  $F_q$ . From this, it is easy to see that the cases  $q = 7, 13$  and  $11$  cannot happen.

For the linear polynomials, it is easy to see that  $ax$  is a VCM of  $F_q$  if and only if  $a \neq 0, \pm 1$ . Note that we consider  $q > 3$  in this section because of Corollary 2.3.4.



Table 1. List of complete mapping polynomials of degree  $\leq 6$ .

Complete Mapping Polynomials	$q$
$ax+b$ , $a, b \in F_q$ , $a \neq 0, -1$	all $q$
$-ax^3+c$ , $ax^3-x+c$ , $(b-a)^{-1}x^3-b(b-a)^{-1}x+c$ , $a, b, c \in F_q$ , $a \neq b$ nonsquares in $F_q$	$q \equiv 0 \pmod{3}$
$-(x+a)^4+3x+b$ , $(x+a)^4+3x+b$ , $a, b \in F_7$	7
$a^{-1}(x^4+bx^2+cx)+d$ , $a, b, c, d \in F_q$ , $a \neq 0$ such that $x^4+bx^2+cx$ and $x^4+bx^2+(a+c)x$ each have $x=0$ as the unique root in $F_q$	$q \equiv 0 \pmod{2}$
$5a^{-2}[(x+b)^5+a(x+b)^3+8a^2x] + c$ , $8a^{-2}[(x+b)^5+a(x+b)^3+3a^2x] + c$ $a, b, c \in F_{13}$ , $a$ not a square in $F_{13}$	13
$a(x+b)^5 + c$ , $a(x+b)^5 \pm x + c$ , $b, c \in F_9$ arbitrary, $a^2 = 2$	9
$-ax^5+c$ , $ax^5-x+c$ , $(a-b)^{-1}x^5-a(a-b)^{-1}x + c$ , $a, b, c \in F_q$ , $a \neq b$ not fourth powers in $F_q$	$q \equiv 0 \pmod{5}$
$-5(x+b)^6+x+c$ , $-2(x+b)^6-4x+c$ , $2(x+b)^6-4x+c$ , $5(x+b)^6+x+c$ $-3(x+b)^6+5x+c$ , $3(x+b)^6+5x+c$ , $5(x+b)^6-2x+c$ , $-2(x+b)^6+3x+c$ $2(x+b)^6+3x+c$ , $-5(x+b)^6-2x+c$ , $4(x+b)^6+5x+c$ , $-4(x+b)^6+5x+c$ $b, c \in F_{11}$ arbitrary	11

For degree 3, we consider the polynomial  $f(x) = tx^3$ . By similar arguments in the last example of the last section, we have  $-D(f) = \{-tr^2 \mid r \in F_q^\times\}$ . Let  $a, b \in F_q^\times$  be nonsquares with  $a \neq b$ . Let  $f_1(x) = -ax^3$ ,  $f_2(x) = ax^3$  and  $f_3(x) = (b-a)^{-1}x^3$ . From Table 1, we just need to check that  $-1 \notin -D(f_1)$ ,  $1 \notin -D(f_2)$  and  $-b(b-a)^{-1} \notin -D(f_3)$ .  $-1 \in -D(f_1)$  if and only if there is  $r \in F_q^\times$  so that  $-1 = ar^2$ . The last equality is equivalent to  $-a$  being a square in  $F_q^\times$ . This is true only when  $q \equiv 3 \pmod{4}$ . Similarly,  $1 \in -D(f_2)$  if and only if  $q \equiv 3 \pmod{4}$ . Combining together, we have that  $ax^3$ ,  $ax^3 \pm x$ , a nonsquare in  $F_q^\times$ , are VCMs of  $F_q$  when  $q \equiv 1 \pmod{4}$ . Now  $-b(b-a)^{-1} \in -D(f_3)$  if and only if there is  $r \in F_q^\times$  so that  $-b(b-a)^{-1} = -(b-a)^{-1}r^2$ . In this case,  $2b-a$  is a square in  $F_q^\times$ . So  $(b-a)^{-1}x^3 - b(b-a)^{-1}x$  is a VCM of  $F_q$  if and only if  $a \neq b$ ,  $2b-a$  are nonsquares in  $F_q^\times$ .

From Table 1, it is easy to see that  $ax^5$  and  $ax^5 \pm x$ , with  $a^2 = 2$ , are VCMs of  $F_9$ .

By an argument similar to that in the case degree 3, we have that  $-ax^5$  is a VCM of  $F_q$  if and only if  $a$  and  $2a^{-1}$  are not fourth powers,  $ax^5 - x$  is a VCM of  $F_q$  if and only if  $a$  and  $2a^{-1}$  are not fourth powers, and  $(a-b)^{-1}x^5 - a(a-b)^{-1}x$  is a VCM of  $F_q$  if and only if  $a \neq b$ ,  $2a-b$  are not fourth powers, where  $q \equiv 0 \pmod{5}$ . Notice that  $-ax^5$ ,  $-ax^5 - x$ ,  $ax^5 - x$  and  $ax^5 - 2x$  can be written in the third form if they are VCMs of  $F_q$ . We summarize our results in Table 2.

Table 2. List of very complete mapping polynomials of degree  $\leq 6$ .

Very Complete Mapping Polynomials	$q$
$ax+b$ , $a, b \in F_q$ , $a \neq 0, \pm 1$	all odd $q$
$ax^3+c$ , $ax^3 \pm x+c$ , $a, c \in F_q$ , $a$ nonsquare in $F_q$	$q \equiv 0 \pmod 3$ and $q \equiv 1 \pmod 4$
$(b-a)^{-1}x^3-b(b-a)^{-1}x+c$ , $a, b, c \in F_q$ , $a \neq b$ $a, b, 2b-a$ nonsquares in $F_q$	$q \equiv 0 \pmod 3$
$a(x+b)^5+c$ , $a(x+b)^5 \pm x+c$ , $b, c \in F_q$ arbitrary, $a^2 = 2$	9
$(a-b)^{-1}x^5-a(a-b)^{-1}x+c$ , $a, b, c \in F_q$ , $a \neq b$ , and $a, b, 2a-b$ not fourth powers in $F_q^\times$	$q \equiv 0 \pmod 5$

In Theorem 2.2.3, we estimated the total number of S-CMs in the form  $ax^{(q+1)/2}+bx$ . Now we consider the special case  $a = 1$ . We have the following theorem. The proof is similar to that of Niederreiter and Robinson (see pp. 205-206, [28]).

Theorem 2.5.1. The number  $N$  of elements  $b \in F_q$  such that  $x^{(q+1)/2} + bx$  is a VCM of  $F_q$  satisfies  $N \geq \frac{q-9q^{1/2}-24}{8}$  when  $q \not\equiv 0 \pmod 3$ . If  $F_q$  is of characteristic 3, we have

$$N = \begin{cases} \frac{q-9}{4} & \text{if } q \equiv 1 \pmod 4 \\ \frac{q-3}{4} & \text{if } q \equiv 3 \pmod 4 \end{cases}$$



Proof. For  $b \in F_q$ ,  $x^{(q+1)/2} + bx$  is a VCM of  $F_q$  if and only if  $\eta(b^2-1) = \eta((b-1)^2-1) = \eta((b+1)^2-1) = 1$ , where  $\eta$  is the quadratic character of  $F_q^\times$  (by Lemma 2.2.1). Note that  $b^2-1 = 0$  if and only if  $b = \pm 1$ ,  $(b-1)^2-1 = 0$  if and only if  $b = 0$  or  $2$ , and  $(b+1)^2-1 = 0$  is equivalent to  $b = 0$  or  $-2$ . So

$$\begin{aligned}
 N &= \frac{1}{8} \sum_{b \neq 0, \pm 1, \pm 2} \left[ 1 + \eta(b^2-1) \right] \left[ 1 + \eta((b-1)^2-1) \right] \left[ 1 + \eta((b+1)^2-1) \right] \\
 &= \frac{1}{8} \left( \sum_{b \neq 0, \pm 1, \pm 2} 1 + \sum_{b \neq 0, \pm 1, \pm 2} \eta(b(b+2)) + \sum_{b \neq 0, \pm 1, \pm 2} \eta(b(b-2)) + \sum_{b \neq 0, \pm 1, \pm 2} \eta((b-1)(b+1)) \right. \\
 &\quad + \sum_{b \neq 0, \pm 1, \pm 2} \eta(b^2(b+2)(b-2)) + \sum_{b \neq 0, \pm 1, \pm 2} \eta((b+1)b(b-1)(b-2)) + \sum_{b \neq 0, \pm 1, \pm 2} \eta((b+2)(b+1)b(b-1)) \\
 &\quad \left. + \sum_{b \neq 0, \pm 1, \pm 2} \eta(b^2(b+2)(b+1)(b-1)(b-2)) \right)
 \end{aligned}$$

If  $q = p^n$  with  $p > 3$ , then

$$\begin{aligned}
 N &= \frac{1}{8} \left\{ q-5 + \sum_{b \in F_q} \eta(b(b+2)) + \sum_{b \in F_q} \eta(b(b-2)) + \sum_{b \in F_q} \eta((b-1)(b+1)) + \sum_{b \in F_q} \eta((b+2)(b-2)b^2) \right. \\
 &\quad + \sum_{b \in F_q} \eta((b+1)b(b-1)(b-2)) + \sum_{b \in F_q} \eta((b+2)(b+1)b(b-1)) + \sum_{b \in F_q} \eta((b+2)(b+1)(b-1)(b-2)b^2) \\
 &\quad \left. - \eta(3) - \eta(-1) - \eta(8) - \eta(-1) - \eta(3) - \eta(8) - \eta(-1) - \eta(3) - \eta(3) - \eta(3) - \eta(-3) - \eta(24) - \eta(24) \right\}
 \end{aligned}$$

From Corollary 1.4.7, we have

$$\sum_{b \in F_q} \eta(b(b+2)) = -1 = \sum_{b \in F_q} \eta(b(b-2)) \text{ and } \sum_{b \in F_q} \eta((b-1)(b+1)) = -1.$$

$$\sum_{b \in F_q} \eta((b+2)(b-2)b^2) = \sum_{b \in F_q} \eta(b^2)\eta((b+2)(b-2)) = -\eta(4) - 1 = -2.$$

From Theorem 2c' in [38],

$$\left| \sum_{b \in F_q} \eta((b+1)b(b-1)(b-2)) \right| \leq 3q^{1/2} \text{ and } \left| \sum_{b \in F_q} \eta((b+2)(b+1)b(b-1)) \right| \leq 3q^{1/2}.$$

And

$$\begin{aligned} \left| \sum_{b \in F_q} \eta((b+2)(b+1)(b-1)(b-2)b^2) \right| &= \left| -\eta(4) + \sum_{b \in F_q} \eta((b+2)(b+1)(b-1)(b-2)) \right| \\ &\leq 1 + \left| \sum_{b \in F_q} \eta((b+2)(b+1)(b-1)(b-2)) \right| \leq 1 + 3q^{1/2}. \end{aligned}$$

So

$$\begin{aligned} N &= \frac{1}{8} \left\{ q - 5 - 1 - 1 - 1 - 2 - 4\eta(3) - 2\eta(-3) - 3\eta(-1) - 2\eta(2) + 2\eta(6) + \sum_{b \in F_q} \eta((b+1)b(b-1)(b-2)) \right. \\ &\quad \left. + \sum_{b \in F_q} \eta((b+2)(b+1)b(b-1)) + \sum_{b \in F_q} \eta((b+2)(b+1)(b-1)(b-2)b^2) \right\} \\ &\geq \frac{1}{8} \left\{ q - 23 - 3q^{1/2} - 3q^{1/2} - 1 - 3q^{1/2} \right\} \\ &= \frac{q - 9q^{1/2} - 24}{8}. \end{aligned}$$

Let  $p = 3$ . Then

$$\begin{aligned}
 N &= \frac{1}{8} \left\{ \sum_{b \neq 0, \pm 1} 1 + \sum_{b \neq 0, \pm 1} \eta(b(b-1)) + \sum_{b \neq 0, \pm 1} \eta(b(b+1)) + \sum_{b \neq 0, \pm 1} \eta((b-1)(b+1)) + \sum_{b \neq 0, \pm 1} \eta(b^2(b+1)(b-1)) \right. \\
 &\quad \left. + \sum_{b \neq 0, \pm 1} \eta((b+1)^2 b(b-1)) + \sum_{b \neq 0, \pm 1} \eta((b+1)b(b-1)^2) + \sum_{b \neq 0, \pm 1} \eta(b^2(b+1)^2(b-1)^2) \right\} \\
 &= \frac{1}{8} \left\{ q-3 + \sum_{b \in F_q} \eta(b(b-1)) + \sum_{b \in F_q} \eta(b(b+1)) + \sum_{b \in F_q} \eta((b-1)(b+1)) + \sum_{b \in F_q} \eta(b^2(b+1)(b-1)) \right. \\
 &\quad \left. + \sum_{b \in F_q} \eta((b+1)^2 b(b-1)) + \sum_{b \in F_q} \eta((b+1)b(b-1)^2) + q-3-\eta(-1)-\eta(-1)-\eta(-1) \right\} \\
 &= \frac{1}{8} \left\{ 2q-6-1-1-1-1-\eta(-1)-1-\eta(-1)-1-\eta(-1)-3\eta(-1) \right\} \\
 &= \frac{q-6-3\eta(-1)}{4} = \begin{cases} \frac{q-9}{4} & \text{if } q \equiv 1 \pmod{4} \\ \frac{q-3}{4} & \text{if } q \equiv 3 \pmod{4} \end{cases}
 \end{aligned}$$

Here, we used the fact that  $-1$  is a square in  $F_q$  if and only if  $q \equiv 1 \pmod{4}$ . This completes the proof.

When we consider  $q \equiv 0 \pmod{3}$  in this theorem, the formula for  $N$  is the same as Niederreiter-Robinson's formula for the number of complete mappings of  $F_q$ . This implies that every complete mapping of  $F_q$  in the form  $x^{(q+1)/2} + bx$  is also a VCM of  $F_q$ .

From Theorem 2.5.1, we have immediately the following



Corollary 2.5.2. If  $q = 27, 81$  or  $q \geq 125$ , there is a VCM of  $F_q$  in the form  $x^{(q+1)/2} + bx$ ,  $b \in F_q^\times$ .

Proof. Assume first  $q \not\equiv 0 \pmod{3}$ . From Theorem 2.5.1,  $N \geq \frac{q-9q^{1/2}-24}{8}$ .

If  $q-9q^{1/2}-24 > 0$ , there is a VCM in this form. Now,  $q-9q^{1/2}-24 > 0$  if and only if

$$(q^{1/2} - \frac{9}{2})^2 > \frac{177}{4}. \text{ Since } q > 0, \text{ the last inequality is equivalent to } q^{1/2} > \frac{9 + \sqrt{177}}{2}.$$

So  $q-9q^{1/2}-24 > 0$  if and only if  $q \geq 125$ .

For  $q \equiv 0 \pmod{3}$ , there is a VCM of  $F_{27}$  (and  $F_{81}$ ) in this form.

From computer calculations, there is a VCM of  $F_q$  in the form  $x^{(q+1)/2} + bx$  with  $b \in F_q^\times$  for  $q = 19, 23, 25, 31, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113$ , and  $121$ . From this data it is clear that the lower bound from Theorem 2.5.1 is not best possible.

Now, we are going to search for finite fields  $F_q$  which have VCMs of degree  $> 1$ .

We give the following

Theorem 2.5.3. There is a VCM  $f(x)$  of  $F_q$  so that the reduction  $f(x) \pmod{(x^q - x)}$  has degree  $> 1$  if and only if  $q = 9$  or  $q \geq 13$ .

Proof. From Theorem 2.2.3, the number  $N$  of VCMs of  $F_q$  in the form  $ax^{(q+1)/2} + bx$  with  $a \neq 0$  satisfies  $N \geq \frac{(q-3)(q-3-2^3)}{2^3} = \frac{(q-3)(q-11)}{8}$ . If  $q \geq 13$ , this number  $N$  is greater than 0.

From Theorem 2.2.9, there is a VCM of  $F_9$  in the form  $ax^3 + bx$  with  $a \neq 0$ .

From Corollary 2.3.4,  $q > 3$ . So the only remaining cases are  $q = 5, 7$  and  $11$ .

By Theorem 2.3.3, the reduction mod  $(x^5-x)$  of any VCM of  $F_5$  must be a linear polynomial.

Let  $q = 7$ . If  $f(x)$  is a VCM of  $F_7$  with  $\deg f \leq 6$ , then  $\deg f \leq 3$  by Theorem 2.3.3. From Table 2,  $f$  must be a linear polynomial.

Finally, let  $q = 11$ . By similar argument as in the case  $q = 7$ , the only remaining polynomials we have to exclude are polynomials of degree 7. But as mentioned in [2], the only VCMs of  $F_{11}$  are linear polynomials. This completes the proof.

Finally, we give one more method (in addition to methods in Theorem 2.2.1) to construct a new VCM of  $F_q$  when we already have a VCM of  $F_q$ . It is the following theorem. We will use it in Section 3 of Chapter III.

**Theorem 2.5.4.** Let  $f(x) \in F_q[x]$  be a VCM. Then the polynomial  $g(x) = -2f(x)+x$  is also a VCM of  $F_q$  where  $\underline{f}(x)$  is a polynomial representing the inverse of  $f(x)+x$ .

**Proof.** Write  $y = f(x)+x$ . Then  $g(y) = -2\underline{f}(y)+y = -2x+x+f(x) = f(x)-x$ ,  $g(y)+y = -2\underline{f}(y)+2y = -2x+2(x+f(x)) = 2f(x)$  and  $g(y)-y = -2\underline{f}(y) = -2x$ . Since  $f(x)$  is a VCM of  $F_q$ ,  $f(x)+x$  is a PP of  $F_q$ . So  $y$  ranges over all elements of  $F_q$  if and only if  $x$  ranges over all elements of  $F_q$  and so  $f(x)-x$ ,  $2f(x)$ ,  $-2x$  range over all elements of  $F_q$ . Hence  $g(y)$  is a VCM of  $F_q$ .

## CHAPTER 3

### GENERALIZED PANDIAGONAL LATIN SQUARES OF ORDER $q$

#### 1. Introduction

A Latin square of order  $n$  is an  $n \times n$  array with the property that each row and each column is a permutation of the numbers  $0, 1, \dots, n-1$ . By a pandiagonal Latin square (abbreviated PLS) is meant a Latin square satisfying the additional condition that each of the  $2n$  wrap-around left and right diagonals is also a permutation of  $0, 1, \dots, n-1$  (see [1]). PLSs are of importance in the construction of magic squares (see, for example, [39]) and they are also useful in the design of statistical experiments (see, for example, [20]).

It is well-known that there is a pandiagonal Latin square of order  $n$  if and only if  $n$  is not divisible by 2 or 3 (see [19]). Moreover, if  $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ ,  $p_1, \dots, p_r$  distinct primes, and if there is a pandiagonal Latin square of order  $p_i^{\alpha_i}$  for each  $i$ , then using the Kronecker product of matrices (see [16]), one can construct such a square of order  $n$ . We generalize the idea of pandiagonal Latin squares to squares over finite fields, and will call them generalized pandiagonal Latin squares.

When we consider an  $n \times n$  array, we use  $(i, j)$  to denote the position at the intersection of the  $i$ th row and the  $j$ th column. So the set  $\{(i, j) \mid 1 \leq i \leq n, 1 \leq j \leq n\}$  is the set of all positions. When we define generalized pandiagonal Latin squares, we consider, in fact, the set  $F_q \times F_q$  as the set of all positions. Then we define rows, columns



and right and left diagonals based on the additive group of  $F_q$  rather than on the additive structure of  $\mathbf{Z}/(n)$ . If  $\mathbf{Z}/(n)$  is the quotient ring of integers  $\mathbf{Z}$  modulo the principle ideal  $(n)$ , Rosser and Walker (see [36]) found the group structure of the set of all permutations of  $\mathbf{Z}/(n) \times \mathbf{Z}/(n)$ , which preserve the set of all rows, columns and diagonals. Atkin, Hay and Larson (see [1]) also determined the same group structure independently. In Section 2, we will study the group structure of all permutations on  $F_q \times F_q$  which preserve the set of all rows, columns and diagonals.

A path on an  $n \times n$  array is defined to be the set of positions in which all entries are a fixed number. When we study a pandiagonal Latin square of order  $n$ , each path corresponds to a so-called virtual path which is defined to be a function  $f: \mathbf{Z}/(n) \rightarrow \mathbf{Z}/(n)$  so that  $f(x)$ ,  $f(x)+x$  and  $f(x)-x$  are permutations on  $\mathbf{Z}/(n)$  (see [1] and [19]). Virtual paths are useful in the construction and study of pandiagonal Latin squares. Every virtual path of  $\mathbf{Z}/(p)$ ,  $p$  a prime, is actually a very complete mapping of the field  $\mathbf{Z}/(p)$ . In Section 3, we will study generalized pandiagonal Latin squares by means of VCMs of  $F_q$ .

Finally, in this chapter,  $q$  is always a power of an odd prime  $p$ .

## 2. Group Structure of PLS-Transformations on $F_q \times F_q$

In this section, we consider transformations on  $F_q \times F_q$  which generalize transformations on  $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$  which have been used to study pandiagonal Latin squares (see [1] and [36]). The methods we use in this section are similar to those used in [1].


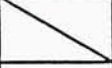
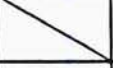
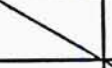
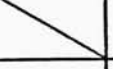
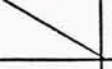
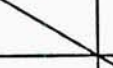
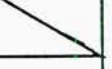
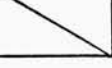
**Definition.** Let  $F_q$  be a finite field of characteristic an odd prime  $p$ . For  $a \in F_q$ , the set  $\{(a, x) \mid x \in F_q\}$  is called the  $a$ -row,  $\{(x, a) \mid x \in F_q\}$  the  $a$ -column,  $\{(x, a+x) \mid x \in$

$F_q$  the right  $a$ -diagonal, and  $\{(x, a-x) \mid x \in F_q\}$  the left  $a$ -diagonal. We always use  $T$  for the set of all rows, columns and diagonals.

We note that if  $q = p$  a prime, the additive group of  $F_p$  is cyclic but if  $q = p^n$  with  $n \geq 2$ , the additive group of  $F_q$  is not cyclic and so there is a difference between our definition and the usual one from a cyclic group. The following are examples.

Table 3. The right 1-diagonal on  $F_9 \times F_9$ .

$F_9 = \{0, 1, 2, \beta, \beta+1, \beta+2, 2\beta, 2\beta+1, 2\beta+2\}$  with  $\beta^2 = 2\beta+1$

	0	1	2	$\beta$	$\beta+1$	$\beta+2$	$2\beta$	$2\beta+1$	$2\beta+2$
0									
1									
2									
$\beta$									
$\beta+1$									
$\beta+2$									
$2\beta$									
$2\beta+1$									
$2\beta^2$									

The slanted line segments indicate the right 1-diagonal on  $F_9 \times F_9$ .

Table 4. The right 1-diagonal on  $\mathbb{Z}/(9) \times \mathbb{Z}/(9)$ .

	0	1	2	3	4	5	6	7	8
0									
1									
2									
3									
4									
5									
6									
7									
8									

The slanted line segments indicate the right 1-diagonal in the usual case of the cyclic group of integers modulo 9.

From the definition, it is easy to see that the intersection of any two different kinds of elements in  $T$  consists of exactly one ordered pair. For example,

$$\{(a,x) \mid x \in F_q\} \cap \{(x,b) \mid x \in F_q\} = \{(a,b)\}, \{(x,a+x) \mid x \in F_q\} \cap \{(x,b-x) \mid x \in F_q\} = \{(2^{-1}(b-a), 2^{-1}(b+a))\}, \text{ and so on.}$$

Definition. A mapping  $\alpha: F_q \times F_q \rightarrow F_q \times F_q$  is called a PLS-transformation if  $\alpha$  is one-to-one and if  $\alpha$  maps the set  $T$  into itself.



Since  $F_q \times F_q$  is a finite set,  $\alpha$  is one-to-one if and only if  $\alpha$  is onto. So  $\alpha$  is a one-to-one correspondence. This implies that  $\{\alpha(A) \mid A \in T\} = T$  whenever  $\alpha(A) \in T$  for all  $A \in T$ .

Now, let  $G$  be the set of all PLS-transformations on  $F_q \times F_q$ . It is easy to see that  $G$  is a group under functional composition. In  $G$ , the following PLS-transformations are important. For the remainder of the chapter we use the following notations to represent these important functions.

$$(1) \quad \text{For } (a,b) \in F_q \times F_q, \tau_{(a,b)}: (x,y) \rightarrow (x+a, y+b)$$

$$(2) \quad \nu: (x,y) \rightarrow (x, -y)$$

$$(3) \quad \sigma: (x,y) \rightarrow (x+y, -x+y)$$

$$(4) \quad \text{Let } q = p^n. \text{ For any } n\text{-tuple } (a_0, a_1, \dots, a_{n-1}) \text{ of elements in } F_q \text{ such that}$$

$$\sum_{i=0}^{n-1} a_i x^{p^i} \text{ is a PP of } F_q, \text{ define } \mu_{(a_0, \dots, a_{n-1})}: F_q \times F_q \rightarrow F_q \times F_q \text{ by } \mu_{(a_0, \dots, a_{n-1})}: \\ (x,y) \rightarrow \left( \sum_{i=0}^{n-1} a_i x^{p^i}, \sum_{i=0}^{n-1} a_i y^{p^i} \right).$$

$$(5) \quad \text{If } q = 3^n, \text{ we define } \psi: F_q \times F_q \rightarrow F_q \times F_q \text{ by } \psi: (x,y) \rightarrow (x, x-y).$$

It is easy to see that all such mappings are PLS-transformations. Moreover, we have  $|\tau_{(a,b)}| = \text{the order of } \tau_{(a,b)} = p$  for all  $(a,b) \in F_q \times F_q$  with  $(a,b) \neq (0,0)$ ,  $|\nu| = 2$  and  $|\psi| = 2$  (if  $p = 3$ ). Now  $\sigma^2(x,y) = (2y, -2x)$ ,  $\sigma^3(x,y) = (-2x+2y, -2x-2y)$  and  $\sigma^4(x,y) = (-4x, -4y)$ . So  $|\sigma| = 4$ , order of  $-4$  in  $F_p^\times$ . Finally, let  $f(x) = \sum_{i=0}^{n-1} a_i x^{p^i}$  be a PP of  $F_q$ . Let  $A_f = (a_{i,j}^j)$  taking  $i-j \bmod n$ . Let  $H = (\eta^{qi+j})$  where  $\eta, \eta^p, \dots, \eta^{p^{n-1}}$  form a normal basis of  $F_q$  over  $F_p$ . Then  $\bar{A}_f = H A_f H^{-1} \in GL(n, F_p)$ . We can see that  $f(x) \rightarrow \bar{A}_f$  is an isomorphism

of the Betti-Mathieu group BM onto  $GL(n, F_p)$ . Moreover,  $\mu_{(a_0, \dots, a_{n-1})}^i(x, y) = (f^i(x), f^i(y))$  so  $|\mu|$  = the order of  $\bar{A}_f$  in  $GL(n, F_p)$ .

It is not difficult to check that  $\nu\tau_{(a,b)} = \tau_{(a,b)}\nu$ ,  $\sigma\tau_{(a,b)} = \tau_{(a+b, -a+b)}\sigma = \tau_{\sigma(a,b)}\sigma$ ,

$$\mu_{(a_0, \dots, a_{n-1})} \tau_{(a,b)} = \tau_{\left(\sum_{i=0}^{n-1} a_i a^{p^i}, \sum_{i=0}^{n-1} a_i b^{p^i}\right)} \mu_{(a_0, \dots, a_{n-1})}, \mu_{(a_0, \dots, a_{n-1})} \nu = \nu \mu_{(a_0, \dots, a_{n-1})},$$

$$\mu_{(a_0, \dots, a_{n-1})} \sigma = \sigma \mu_{(a_0, \dots, a_{n-1})}, \psi \tau_{(a,b)} = \tau_{(a, a-b)} \psi = \tau_{\psi(a,b)} \psi, \text{ and } \psi \mu_{(a_0, \dots, a_{n-1})} = \mu_{(a_0, \dots, a_{n-1})} \psi.$$

It is perhaps easier to see the effects of these PLS-transformations in the set T of rows, columns and diagonals. We list as follows.

Table 5. Effects of PLS-transformations in the set of rows, columns and diagonals.

	rows	columns	right diagonals	left diagonals
$\tau_{(a,b)}$	rows	columns	right diagonals	left diagonals
$\nu$	rows	columns	left diagonals	right diagonals
$\sigma$	right diagonals	left diagonals	columns	rows
$\mu_{(a_0, \dots, a_{n-1})}$	rows	columns	right diagonals	left diagonals
$\psi$ (if $p = 3$ )	rows	right diagonals	columns	left diagonals

In the table the result of applying the function in a given row to the element of T labelled by a given column, lies at the intersection of that row and column. For example,  $\sigma$  maps columns onto left diagonals and left diagonals to rows.

Now, let  $K = \{\tau_{(a,b)} \mid (a,b) \in F_q \times F_q\}$  and  $H = \{\alpha \in G \mid \alpha(0,0) = (0,0)\}$ . Moreover, let  $R$  be the subgroup of  $G$  generated either by  $\nu, \sigma$  and  $\mu_{(a_0, \dots, a_{n-1})}$  if  $F_q$  has characteristic  $p > 3$  or by  $\psi, \nu, \sigma$  and  $\mu_{(a_0, \dots, a_{n-1})}$  if  $p = 3$ . Consider  $\alpha \in G$  and let  $\alpha(0,0) = (a_0, b_0)$ . Then  $(\tau_{(-a_0, -b_0)}\alpha)(0,0) = (0,0)$  and so  $h = \tau_{(-a_0, -b_0)}\alpha \in H$ . Note that  $\tau_{(-a_0, -b_0)} = \tau_{(a_0, b_0)}^{-1}$ , the inverse mapping of  $\tau_{(a_0, b_0)}$ . We have  $\alpha = \tau_{(a_0, b_0)}h$  so that  $G = KH$ . It is easy to see that  $H \cap K = \{I\}$ , where  $I$  is the identity mapping on  $F_q \times F_q$ . Hence, every element of  $G$  can be uniquely expressed as  $\alpha = \tau_{(a,b)}h$ . We have proven

Lemma 3.2.1.  $G = KH$  and  $K \cap H = \{I\}$ .

Now we study the subgroup  $H$  of  $G$ . For this purpose, we need the following lemma which shows that additive functions must be linearized polynomials.

Lemma 3.2.2. Let  $q = p^n$ . Let  $f(x) \in F_q[x]$  be of degree  $< q$ . If  $f(a+b) = f(a)+f(b)$  for all  $a, b \in F_q$ , then  $f(x)$  is a linearized polynomial of  $F_q$  over  $F_p$ .

Proof. For a fixed  $b \in F_q$ , we have  $f(x+b) = f(x)+f(b)$  and so  $f'(x+b) = f'(x)$ . This is true for all  $b \in F_q$ . We have  $f'(a+x) = f'(a)$  a constant since  $\deg f' < q$ . So  $f'(x) \in F_q[x]$  is a constant. Hence,  $f(x)$  is of the form  $f(x) = a_0 + a_1x + a_2x^{pn_2} + \dots + a_kx^{pn_k}$  where  $n_2 < \dots < n_k$  and  $pn_k < q$ . Since  $f(0) = f(0+0) = f(0) + f(0)$ , we have  $f(0) = 0$  and so  $a_0 = 0$ .

Let  $g(x) = f(x) - a_1x = a_2x^{pn_2} + \dots + a_kx^{pn_k}$ . Then  $g(a+b) = g(a)+g(b)$  for all  $a, b \in F_q$ . Since  $p$  is the characteristic of  $F_q$ , there are  $b_2, \dots, b_k \in F_q$  so that  $a_i = b_i^p$ ,  $2 \leq i \leq k$ .

Let  $h(x) = b_2x^{n_2} + \dots + b_kx^{n_k}$ . Then  $g(x) = [h(x)]^p$ . For  $a, b \in F_q$ ,  $[h(a+b)]^p = g(a+b) = g(a)+g(b) = [h(a)]^p + [h(b)]^p = [h(a)+h(b)]^p$ . So for  $a, b \in F_q$ ,  $h(a+b) = h(a)+h(b)$ .



Moreover,  $\deg h = n_k < \deg f < q$ . Thus, by induction on the degree,  $h(x)$  is a linearized polynomial of  $F_q$  over  $F_p$ . So  $n_i = p^{m_i-1}$  for  $2 < i < k$ . Hence,  $f(x) = a_1x + a_2x^{p^{m_2}} + \dots + a_kx^{p^{m_k}}$  is a linearized polynomial.

We are now ready to study the subgroup  $H$ .

Lemma 3.2.3.  $H = R$ , where  $R$  is generated by  $\nu, \sigma$  and  $\mu_{(a_0, a_1, \dots, a_{n-1})}$  (and  $\psi$  if  $p = 3$ ).

Proof. Clearly,  $R \subseteq H$ . We now prove  $H \subseteq R$ . For this purpose, let  $\alpha \in H$ . Let  $A, B \in T$ ,  $A \neq B$ , be of the same type, i.e.,  $A$  and  $B$  are two rows, two columns, two right diagonals, or two left diagonals. We claim that  $\sigma(A)$  and  $\sigma(B)$  are of the same type. Suppose not. Then  $\sigma(A) \cap \sigma(B) \neq \emptyset$  as we mentioned before. This contradicts  $\sigma$  being one-to-one on  $F_q \times F_q$  since  $A \cap B = \emptyset$ . We get our assertion.

For  $a \in F_q$ , let  $R_a$  be the  $a$ -row. By Table 5, we can multiply a suitable  $\sigma^{i_0}$  with  $0 \leq i_0 \leq 3$  so that  $\alpha_0 = \sigma^{i_0} \alpha$  maps rows onto rows. Since  $\alpha_0(0,0) = (0,0)$ , we have  $\alpha_0(R_0) = R_0$ . Since  $\alpha_0$  maps the set of all rows onto itself,  $\alpha_0(x,y) = (f(x), g_x(y))$  where  $f(x)$  and  $g_x(y)$  ( $x \in F_q$ ) are PPs of  $F_q$  and  $f(0) = 0$  and  $g_0(0) = 0$ . There are three cases:

Case 1.  $\alpha_0$  maps columns onto columns.

Multiplying suitable  $\nu^j$  with  $j = 0, 1$ , the function  $\alpha_1 = \nu^j \alpha_0$  maps rows onto rows, columns onto columns, right diagonals onto right diagonals. Also  $\alpha_1(0,0) = (0,0)$  and  $\alpha_1(R_0) = R_0$ . By similar arguments as above, there are PPs  $f_1(x)$  and  $g_1(y)$  of  $F_q$  so that  $\alpha_1(x,y) = (f_1(x), g_1(y))$ . Note that  $g_1(y)$  is independent of  $x$  since  $\alpha_1$  maps columns onto columns. Also  $f_1(0) = 0 = g_1(0)$ . Since  $\alpha_1$  maps right diagonals onto right diagonals, we have that for  $a \in F_q$ , there exists a unique  $h(a)$  such that  $(f_1(x), h(a) + f_1(x))$

$= \alpha_1(x, a+x) = (f_1(x), g_1(x+a))$ . So  $g_1(x+a) = h(a) + f_1(x)$ . Choosing  $x = -a$ , we have  $0 = g_1(0) = h(a) + f_1(-a)$  and so  $h(a) = -f_1(-a)$  for all  $a \in F_q$ . This implies  $h(0) = 0$ . So  $g_1(x) = g_1(0+x) = h(0) + f_1(x) = f_1(x)$ . Hence,  $\alpha_1(x, y) = (f_1(x), f_1(y))$ . Furthermore, for  $a \in F_q$ , there is a unique  $l(a) \in F_q$  such that  $(f_1(x), l(a) - f_1(x)) = \alpha_1(x, a-x)$ , since  $\alpha_1$  maps left diagonals onto left diagonals. So  $f_1(a-x) = l(a) - f_1(x)$ . Choosing  $x = a$ , we have  $l(a) = f_1(a)$  for all  $a \in F_q$ . This implies  $f_1(a+b) = f_1(a) + f_1(b)$  for all  $a, b \in F_q$ . By Lemma 3.2.2,  $f_1(x) = \sum_{i=0}^{n-1} a_i x^{p^i}$  is a linearized polynomial. So  $\alpha_1 = \mu_{(a_0, \dots, a_{n-1})}$ . Hence,

$$\alpha = \sigma^i \nu^j \mu_{(a_0, \dots, a_{n-1})} \in R.$$

Case 2.  $p = 3$  and  $\alpha_0$  maps columns to diagonals.

In this case, we multiply  $\alpha_0$  either by  $\psi$  if  $\alpha_0$  maps columns onto right diagonals or by  $\psi\nu$  if  $\alpha_0$  maps columns onto left diagonals. Then we have a PLS-transformation  $\alpha_1$  which maps rows onto rows and columns onto columns. From Case 1,  $\alpha_1 \in R$  and so  $\alpha_0 \in R$  and so  $\alpha \in R$ .

Case 3.  $p > 3$  and  $\alpha_0$  maps columns onto diagonals. We will show that this case cannot happen.

Without loss of generality, we assume  $\alpha_0$  maps columns onto right diagonals (since we can replace  $\alpha_0$  by  $\nu\alpha_0$  if  $\alpha_0$  maps columns onto left diagonals). For each  $a \in F_q$ , there is a unique  $g(a) \in F_q$  so that  $\alpha_0(x, a) = (f(x), g(a) + f(x))$ . Since  $\alpha_0$  maps rows onto rows,  $g(x)$  is a PP of  $F_q$ . So  $\alpha_0(x, y) = (f(x), f(x) + g(y))$ . Also,  $g(0) = 0$ . Now, there are two subcases.

(1)  $\alpha_0$  maps right diagonals onto columns. So, for each  $b \in F_q$ , there is a unique  $h(b) \in F_q$  such that  $(f(x), h(b)) = \alpha_0(x, b+x) = (f(x), f(x) + g(b+x))$ . So  $h(b) = g(b+x) + f(x)$ . Taking  $x = -b$ ,  $h(b) = f(-b)$  since  $g(0) = 0$ . This is true for all  $b \in F_q$ . So  $g(b+x) = f(-b) - f(x)$  for all  $x, b \in F_q$ . Taking  $b = 0$ , we have  $g(x) = -f(x)$ . So  $\alpha_0(x, y) =$

$(f(x), f(x) - f(y))$ . From  $g(b+x) = f(-b) - f(x)$  and  $g(x) = -f(x)$ , we have  $f(x+b) = f(x) - f(-b)$  for all  $x, b \in F_q$ . For fixed  $b \in F_q$ ,  $\alpha_o(x, b-x) = (f(x), f(x) - f(b-x)) = (f(x), f(x) - f(b+(-x))) = (f(x), f(x) - f(b) + f(x)) = (f(x), (3f(x) - f(b)) - f(x))$  for all  $x \in F_q$ . Since  $\alpha_o$  maps left diagonals onto left diagonals, we have that for fixed  $b \in F_q$ ,  $3f(x) - f(b)$  is constant for all  $x \in F_q$ . So  $3f(x)$  is constant. That is impossible since  $f(x)$  is a PP of  $F_q$  and  $3 \in F_q^\times$  for  $p > 3$ . So such  $\alpha_o$  does not exist.

(2)  $\alpha_o$  maps right diagonals onto left diagonals. Then  $\alpha_o$  maps left diagonals onto columns. For each  $a \in F_q$ , there is a unique  $l(a) \in F_q$  so that  $(f(x), l(a) - f(x)) = \alpha_o(x, a+x) = (f(x), f(x) + g(a+x))$ . So  $l(a) = g(a+x) + 2f(x)$ . Taking  $x = -a$ ,  $l(a) = 2f(-a)$ . So  $g(a+x) = 2f(-a) - 2f(x)$  for all  $a, x \in F_q$ . Since  $\alpha_o$  maps left diagonals onto columns, we have that for  $a \in F_q$ , there is a unique  $k(a) \in F_q$  so that  $(f(x), k(a)) = \alpha_o(x, a-x) = (f(x), f(x) + g(a-x))$ . So  $k(a) = f(x) + g(a-x)$  for all  $a, x \in F_q$ . This implies  $k(a) = f(a)$  for all  $a \in F_q$ . So for all  $a, x \in F_q$ ,  $f(a) - f(x) = g(a-x) = g((-x)+a) = 2f(x) - 2f(a)$ . Hence  $3(f(x) - f(a)) = 0$  for all  $a, x \in F_q$ . This is impossible since  $f(x)$  is a PP of  $F_q$  and  $3 \in F_q^\times$ . So there is no such  $\alpha_o$ .

Combining all results above, we have  $\alpha \in H$  implies  $\alpha \in R$ . Hence,  $H \subseteq R$  and so  $H = R$ . This completes the proof.

Now, we are in a position to prove our main results.



Theorem 3.2.4.  $G$  is a semidirect product of  $K$  by  $H$ . Moreover,

$$|G| = \begin{cases} 8(p^n-1)(p^n-p)\dots(p^n-p^{n-1})p^{2n} & \text{if } q = p^n \text{ with } p > 3 \\ 24(p^n-1)(p^n-p)\dots(p^n-p^{n-1})p^{2n} & \text{if } q = p^n \text{ with } p = 3. \end{cases}$$

Proof. By Lemma 3.2.1,  $G = KH$  and  $K \cap H = \{I\}$ . From the definition of semidirect product, we have to check that  $K$  is normal in  $G$ . By Lemma 3.2.3,  $H$  is generated by  $\nu$ ,  $\sigma$  and  $\mu_{(a_0, \dots, a_{n-1})}$  (and  $\psi$  if  $p = 3$ ). So we just need to check that  $\nu\tau_{(a,b)}\nu^{-1}$ ,  $\sigma\tau_{(a,b)}\sigma^{-1}$ ,  $\mu_{(a_0, \dots, a_{n-1})}^{\tau_{(a,b)}} \mu_{(a_0, \dots, a_{n-1})}^{-1}$ ,  $\psi\tau_{(a,b)}\psi^{-1} \in K$ . We have already seen that indeed this is the case, so  $G$  is a semidirect product of  $K$  by  $H$ .

Since  $G$  is a semidirect product of  $K$  by  $H$ , we have  $|G| = |K||H| = |H|q^2$ .

Now, let  $B$  be the subgroup of  $G$  generated by all  $\mu_{(a_0, \dots, a_{n-1})}$ , where  $f(x) = \sum_{i=0}^{n-1} a_i x^{p^i}$  is a PP of  $F_q$  so that from the definition of  $\mu_{(a_0, \dots, a_{n-1})}$ , it is easy to see that  $B$  is isomorphic to Betti-Mathieu group. So  $B$  is isomorphic to  $GL(n, F_p)$ . Hence,  $|B| = |GL(n, F_p)| = (p^n-1)(p^n-p)\dots(p^n-p^{n-1})$ . Moreover, we already saw that  $\mu_{(a_0, \dots, a_{n-1})}^\nu = \nu\mu_{(a_0, \dots, a_{n-1})}$ ,  $\mu_{(a_0, \dots, a_{n-1})}^\sigma = \sigma\mu_{(a_0, \dots, a_{n-1})}$  and  $\psi\mu_{(a_0, \dots, a_{n-1})} = \mu_{(a_0, \dots, a_{n-1})}\psi$  if  $p = 3$ . So  $B$  is normal in  $H$ . There are two cases:

Case 1.  $p > 3$ . In this case,  $H/B$  is generated by  $\nu B$  and  $\sigma B$ . It is easy to check that  $|\nu B| = 2$ ,  $|\sigma B| = 4$  and  $(\nu B) \cdot (\sigma B) \cdot (\nu B) = (\sigma B)^{-1}$  in  $H/B$ . From Theorem 1.1.3 (1),  $H/B$  is isomorphic to  $D_4$ , the dihedral group of order 8. So  $|H/B| = 8$ . Hence,  $|H| = 8 \cdot |B| = 8(p^n-1)\dots(p^n-p^{n-1})$ . Since  $|G| = |K||H|$ , we have  $|G| = 8(p^n-1)\dots(p^n-p^{n-1})p^{2n}$ .

Case 2.  $p = 3$ . In this case,  $H/B$  is generated by  $\nu B$ ,  $\sigma B$  and  $\psi B$ . It is easy to check that  $\sigma\psi\sigma^3\psi\sigma\psi\sigma^3 = \nu$ . So  $H/B$  is generated by  $\sigma B$  and  $\psi B$ . Now,  $(\psi B)^2 =$

$((\psi B)(\sigma B)^{-1})^3 = (\sigma B)^4 = B$ , the identity in  $H/B$ . From Theorem 1.1.3 (2),  $H/B$  is isomorphic to  $S_4$ , the symmetric group of degree 4. So  $|H/B| = 24$ . This implies  $|H| = 24|B| = 24(p^n - 1) \dots (p^n - p^{n-1})$ . Hence,  
 $|G| = |K||H| = 24(p^n - 1) \dots (p^n - p^{n-1})p^{2n}$  and this completes the proof.

From Theorem 3.2.4, every element  $\alpha \in G$  can be expressed as  $\alpha = \tau_{(a,b)}\alpha_1$  for some  $\tau_{(a,b)} \in K$  and  $\alpha_1 \in H$ . Since  $H$  is generated by  $\mu_{(a_0, \dots, a_{n-1})}$ ,  $\nu$ ,  $\sigma$  (and  $\psi$  if  $p = 3$ ), and every element of  $B$  commutes with the  $\nu$  and  $\sigma$  (and  $\psi$  if  $p = 3$ ), there is  $\mu_{(a_0, \dots, a_{n-1})} \in B$  so that  $\alpha = \tau_{(a,b)} \mu_{(a_0, \dots, a_{n-1})} \alpha_2$  for some  $\alpha_2$ , a product of  $\nu$ ,  $\sigma$  (and  $\psi$  if  $p = 3$ ).

(1)  $p > 3$ . In Case 1 of the proof of Theorem 3.2.4, we have  $\nu\sigma\nu = \sigma^3 \mu_{(b_0, \dots, b_{n-1})}$  for some  $\mu_{(b_0, \dots, b_{n-1})} \in B$ . We can write  $\alpha_2 = \nu^i \sigma^j$  with  $i = 0, 1$  and  $j = 0, 1, 2, 3$  when we choose  $\mu_{(a_0, \dots, a_{n-1})}$  suitably. So  $G = \{\tau_{(a,b)} \mu_{(a_0, \dots, a_{n-1})} \nu^i \sigma^j \mid a, b \in F_q, f(x) = \sum_{l=0}^{n-1} a_l x^{p^l} \text{ is a PP of } F_q, i = 0, 1 \text{ and } j = 0, 1, 2, 3\}$ .

(2)  $p = 3$ . From Case 2 in the proof of Theorem 3.2.4, we can write  $\alpha_2$  as  $\psi^{i_1} \sigma^{j_1} \dots \psi^{i_r} \sigma^{j_r}$  where  $r \geq 1$ ,  $i_1 = 0, 1$ ,  $i_2 = \dots = i_r = 1$ ,  $j_r = 0, 1, 2, 3$  and  $j_l = 1, 2, 3$  for  $1 \leq l < r$ . So  $G = \{\tau_{(a,b)} \mu_{(a_0, \dots, a_{n-1})} \psi^{i_1} \sigma^{j_1} \dots \psi^{i_r} \sigma^{j_r} \mid a, b \in F_q, f(x) = \sum_{l=0}^{n-1} a_l x^{p^l} \text{ is a PP of } F_q, r \geq 1, i_1 = 0, 1, i_2 = \dots = i_r = 1, j_r = 0, 1, 2, 3 \text{ and } j_l = 1, 2, 3 \text{ for } 1 \leq l < r\}$ .

Finally, we have the following

**Theorem 3.2.5.** The group  $G$  is solvable if and only if either  $q = p$  is a prime or  $q = 9$ .

**Proof.** From Theorem 3.2.4,  $G$  is a semidirect product of  $H$  by  $K$ . So  $G/H$  is isomorphic to  $K$ . From Theorem 1.1.1,  $G$  is solvable if and only if both  $K$  and  $H$  are

solvable. From the same theorem,  $H$  is solvable if and only if both  $B$  and  $H/B$  are solvable.

Now, from the definition of  $K$ , it is easy to see that  $K$  is isomorphic to the elementary  $p$ -group  $\mathbf{Z}/(p) \times \dots \times \mathbf{Z}/(p)$  with  $2n$  copies of  $\mathbf{Z}/(p)$  if  $q = p^n$ . So  $K$  is solvable.

We already see that  $B$  is isomorphic to  $GL(n, F_p)$  if  $q = p^n$ . From Theorem 1.3.5,  $GL(n, F_p)$  is solvable if and only if either  $n = 1$  or  $n = 2$  and  $p = 2, 3$ . So  $B$  is solvable if and only if either  $F_q = F_9$  or  $F_q = F_p$ .

If  $p > 3$ ,  $H/B$  is isomorphic to  $D_4$  (from Case 1 in the proof of Theorem 3.2.4) and so is solvable. In this case,  $H$  is solvable if and only if  $q = p$  is a prime. If  $p = 3$ ,  $H/B$  is isomorphic to  $S_4$  (from Case 2 in the proof of Theorem 3.2.4) and so is solvable. In this case,  $H$  is solvable if and only if either  $F_q = F_9$  or  $F_q = F_3$ .

Combining all results above together, we see that  $G$  is solvable if and only if either  $q = p$  is a prime or  $q = 9$ . This completes the proof.

### 3. Generalized Pandiagonal Latin Squares Over $F_q$

In this section, we will study so-called generalized pandiagonal Latin squares over finite fields. They are a generalization of pandiagonal Latin squares of order  $p$ , a prime number. We study some properties of generalized pandiagonal Latin squares. We then give two methods to construct such squares and then compare these two methods. All notations we used in the previous section are still kept fixed in this section.

**Definition.** A generalized pandiagonal Latin square (abbreviated GPLS) of order  $q$  is a function  $\Delta: F_q \times F_q \rightarrow F_q$  such that  $\Delta(A) = F_q$  for all  $A \in T$ .



We note that if  $q$  is a prime, this definition reduces to that of the usual definition of a pandiagonal Latin square defined in Section 1. We give an example in the following table.

Table 6. Selected GPLS of order 9.

$F_9 = \{0, 1, 2, \beta, \beta+1, \beta+2, 2\beta, 2\beta+1, 2\beta+2\}$  with  $\beta^2 = 2\beta+1$ .

	0	1	2	$\beta$	$\beta+1$	$\beta+2$	$2\beta$	$2\beta+1$	$2\beta+2$
0	0	$\beta$	$2\beta$	2	$2\beta+1$	$\beta+1$	1	$2\beta+2$	$\beta+2$
1	2	$\beta+2$	$2\beta+2$	1	$2\beta$	$\beta$	0	$2\beta+1$	$\beta+1$
2	1	$\beta+1$	$2\beta+1$	0	$2\beta+2$	$\beta+2$	2	$2\beta$	$\beta$
$\beta$	$2\beta$	0	$\beta$	$2\beta+2$	$\beta+1$	1	$2\beta+1$	$\beta+2$	2
$\beta+1$	$2\beta+2$	2	$\beta+2$	$2\beta+1$	$\beta$	0	$2\beta$	$\beta+1$	1
$\beta+2$	$2\beta+1$	1	$\beta+1$	$2\beta$	$\beta+2$	2	$2\beta+2$	$\beta$	0
$2\beta$	$\beta$	$2\beta$	0	$\beta+2$	1	$2\beta+1$	$\beta+1$	2	$2\beta+2$
$2\beta+1$	$\beta+2$	$2\beta+2$	2	$\beta+1$	0	$2\beta$	$\beta$	1	$2\beta+1$
$\times$ $2\beta^2$	$\beta+1$	$2\beta+1$	1	$\beta$	2	$2\beta+2$	$\beta+2$	0	$2\beta$

We note that each of the rows, columns, left and right diagonals as defined in the previous section is a permutation of  $F_9$ .

Let  $\Delta$  be a GPLS of order  $q$ . From the definition, it is easy to see that  $\Delta \circ \alpha$  is a GPLS of order  $q$  for all PLS-transformations  $\alpha \in G$ . Moreover, if  $f(x) \in F_q[x]$  is a PP of  $F_q$ , then  $f \circ \Delta$  is a GPLS of order  $q$ . Now, let  $c \in F_q$  and consider the inverse image  $\Delta^{-1}(c) = \{(a,b) \in F_q \times F_q \mid \Delta(a,b) = c\}$ . We have the following

**Theorem 3.3.1.** For each  $c \in F_q$ , there is a polynomial  $f_c(x) \in F_q[x]$  so that  $\Delta^{-1}(c) = \{(a, f_c(a)) \mid a \in F_q\}$ . Moreover, for each  $c \in F_q$ , the polynomial  $f_c(x)$  is a VCM of  $F_q$ .

**Proof.** Fix  $c \in F_q$ . For each  $a \in F_q$ ,  $R_a = \{(a, b) \mid b \in F_q\}$  is the  $a$ -row. By the definition of a GPLS,  $\Delta(R_a) = F_q$ . So there is a unique  $f_c(a) \in F_q$  so that  $(a, f_c(a)) \in R_a \cap \Delta^{-1}(c)$ . Hence,  $f_c(x)$  is a function on  $F_q$  and so  $f_c(x) \in F_q[x]$ .

Suppose  $a, b \in F_q$  with  $f_c(a) = f_c(b) = d$ . Then  $(a, d)$  and  $(b, d)$  are in the column  $C_d = \{(e, d) \mid e \in F_q\}$  and  $\Delta(a, d) = c = \Delta(b, d)$ . Since  $\Delta(C_d) = F_q$ ,  $(a, d) = (b, d)$  and so  $a = b$ . This implies  $f_c(x)$  one-to-one. So  $f_c(x)$  is a PP of  $F_q$ .

For each  $b \in F_q$ , let  $D_b = \{(a, b+a) \mid a \in F_q\}$  be the right  $b$ -diagonal. Since  $\Delta(D_b) = F_q$ , there is a unique  $x_b \in F_q$  so that  $(x_b, b+x_b) \in \Delta^{-1}(c)$ . So  $(x_b, b+x_b) = (x_b, f_c(x_b))$ . Hence,  $b+x_b = f_c(x_b)$  and thus,  $b = f_c(x_b) - x_b$ . Since  $b$  ranges over all  $F_q$ , the polynomial  $f_c(x) - x$  maps  $F_q$  onto itself. So  $f_c(x) - x$  is a PP of  $F_q$ .

By a similar argument,  $f_c(x) + x$  is also a PP of  $F_q$ .

Combining all results together,  $f_c(x)$  is a VCM of  $F_q$ .

Let  $\Delta$  be a GPLS of order  $q$ . For each  $a \in F_q$ , let  $R_a(x) = \Delta(a, x)$ ,  $C_a(x) = \Delta(x, a)$ ,  $D_a(x) = \Delta(x, a+x)$  and  $L_a(x) = \Delta(x, a-x)$ . So  $R_a(x)$  is defined by the image of the  $a$ -row,  $C_a(x)$  by the image of the  $a$ -column,  $D_a(x)$  by the image of the right  $a$ -diagonal and  $L_a(x)$  by the image of the left  $a$ -diagonal. Since  $\Delta(A) = F_q$  for all  $A \in T$ , all of  $R_a(x)$ ,  $C_a(x)$ ,  $D_a(x)$  and  $L_a(x)$  are PPs of  $F_q$ . For each  $b \in F_q$ , let  $f_b(x)$  be the VCM of  $F_q$  defined as in Theorem 3.3.1. Then we have the following relations.

Theorem 3.3.2. For  $a, b \in F_q$ ,  $f_b(a) = R_a^{-1}(b)$ ,  $f_b^{-1}(a) = C_a^{-1}(b)$ ,  $(f_b-1)^{-1}(a) = D_a^{-1}(b)$ , and  $(f_b+1)^{-1}(a) = L_a^{-1}(b)$ , where  $(f_b-1)(x) = f_b(x)-x$  and  $(f_b+1)(x) = f_b(x)+x$ .

Proof. Let  $a, b \in F_q$ .

$$b = \Delta(a, f_b(a)) = R_a(f_b(a)) \text{ and so } f_b(a) = R_a^{-1}(b).$$

$$b = \Delta(f_b^{-1}(a), a) = C_a(f_b^{-1}(a)) \text{ and so } f_b^{-1}(a) = C_a^{-1}(b).$$

$$\begin{aligned} \text{Write } c = (f_b-1)^{-1}(a). \text{ Then } D_a((f_b-1)^{-1}(a)) &= \Delta((f_b-1)^{-1}(a), a+(f_b-1)^{-1}(a)) = \\ \Delta(c, (f_b-1)(c)+c) &= \Delta(c, f_b(c)) = b. \text{ So } D_a^{-1}(b) = (f_b-1)^{-1}(a). \end{aligned}$$

Similarly, we have  $L_a^{-1}(b) = (f_b+1)^{-1}(a)$ . This completes the proof.

From Theorem 3.3.1, if  $\Delta$  is a GPLS of order  $q$ , there are  $q$  VCMs of  $F_q$ , say  $f_a(x)$  for all  $a \in F_q$ , such that  $\Delta(x, f_a(x)) = a$ . Since  $\Delta(C) = F_q$  for all columns  $C$ , we have that  $f_a(x_0) \neq f_b(x_0)$  for all  $x_0 \in F_q$  whenever  $a, b \in F_q$  with  $a \neq b$ .

Definition. Two polynomials  $f(x), g(x) \in F_q[x]$  are compatible if  $f(a) \neq g(a)$  for all  $a \in F_q$ . Polynomials  $f_1(x), \dots, f_m(x) \in F_q[x]$  are compatible if they are compatible pairwise.

From this definition, if  $f_1(x), \dots, f_m(x) \in F_q[x]$  are compatible polynomials, then for any  $a \in F_q$ ,  $|\{f_i(a) \mid 1 \leq i \leq m\}| = m$ . In particular, if  $m = q$ ,  $\{f_i(a) \mid 1 \leq i \leq q\} = F_q$  for all  $a \in F_q$ .

The remark immediately before the definition says that if there is a GPLS of order  $q$ , then we have a set of  $q$  compatible VCMs of  $F_q$ . The converse is also true. It is

Theorem 3.3.3. If  $\{f_a(x) \in F_q[x] \mid a \in F_q\}$  is a set of  $q$  compatible VCMs of  $F_q$ , the mapping  $\Delta: F_q \times F_q \rightarrow F_q$  defined by  $\Delta(b, f_a(b)) = a$  for all  $a, b \in F_q$  is a GPLS of order  $q$ .



Proof. Since  $\{f_a(x) \mid a \in F_q\}$  is a set of  $q$  compatible VCMs of  $F_q$ ,  $F_q \times F_q = \{(b, f_a(b)) \mid a, b \in F_q\}$  by the remark above. So the mapping  $\Delta: F_q \times F_q \rightarrow F_q$  defined by  $\Delta(b, f_a(b)) = a$  for all  $a, b \in F_q$  is a well-defined function. For proving  $\Delta$  a GPLS of order  $q$ , we have to show  $\Delta(A) = F_q$  for all  $A \in T$ .

Since  $\{f_a(x) \mid a \in F_q\}$  is a set of  $q$  compatible VCMs of  $F_q$ ,  $\Delta(\{(a, y) \mid y \in F_q\}) = \Delta(\{(a, f_b(a)) \mid b \in F_q\}) = F_q$ .

Fix  $b \in F_q$ . For any  $a \in F_q$ , there is  $x_a \in F_q$  so that  $b = f_a(x_a)$  and so  $x_a = f_a^{-1}(b)$ . If there are  $a_1, a_2 \in F_q$  so that  $f_{a_1}^{-1}(b) = x_{a_1} = x_{a_2} = f_{a_2}^{-1}(b) = x_0$ , then  $f_{a_1}(x_0) = b = f_{a_2}(x_0)$ . Since  $\{f_a(x) \mid a \in F_q\}$  is a set of  $q$  compatible VCMs of  $F_q$ ,  $a_1 = a_2$ . So  $\Delta(\{(x, b) \mid x \in F_q\}) = \Delta(\{(f_a^{-1}(b), b) \mid a \in F_q\}) = \Delta(\{(f_a^{-1}(b), f_a(f_a^{-1}(b))) \mid a \in F_q\})$ . So  $\Delta(\{(x, b) \mid x \in F_q\}) = F_q$ .

Let  $a \in F_q$ . For any  $b \in F_q$ , there is a unique  $c_b \in F_q$  satisfying  $f_{c_b}(b) = a+b$  because we already have  $\{f_c^{-1}(a+b) \mid c \in F_q\} = F_q$  in the last paragraph. Such  $c_b, b \in F_q$ , are all distinct since  $c_{b_1} = c_{b_2}$  implies  $f_{c_{b_1}}(b_1) - b_1 = a = f_{c_{b_2}}(b_2) - b_2 = f_{c_{b_1}}(b_2) - b_2$  and so  $b_1 = b_2$  since  $f_{c_{b_1}}(x)$  is a VCM of  $F_q$ . So,  $\Delta(\{(b, a+b) \mid b \in F_q\}) = \Delta(\{(b, f_{c_b}(b)) \mid b \in F_q\}) = \{c_b \mid b \in F_q\} = F_q$ .

Similarly,  $\Delta(\{(b, a-b) \mid b \in F_q\}) = F_q$ . This completes the proof.

From this theorem, if we can find a set of  $q$  compatible VCMs of  $F_q$ , we can construct a GPLS of order  $q$ . Furthermore, if there is a VCM of  $F_q$ , we can use the following lemma to find at least one set of  $q$  compatible VCMs of  $F_q$ .

Lemma 3.3.4. Let  $f(x)$  be a VCM of  $F_q$ . Then both  $S_f = \{f(x)+a \mid a \in F_q\}$  and  $S^f = \{f(x+a) \mid a \in F_q\}$  are sets of  $q$  compatible VCMs of  $F_q$ .

Proof. It is easy to see.

Let  $f(x)$  be a VCM of  $F_q$ . For each  $a \in F_q$ , let  $f_a(x) = f(x)+a$  and  $g_a(x) = f(a+x)$ . Now, let  $\Delta_f$  be the GPLS defined as in Theorem 3.3.3 using the set  $S_f$ , and let  $\Delta^f$  be the GPLS defined as in Theorem 3.3.3 using  $S^f$ . The example at the beginning of this section is a  $\Delta^f$  with  $f(x) = (2\beta+1)x^5+2x$ .

Corollary 3.3.5. There is a GPLS of order  $q$  if and only if  $q > 3$ .

Proof. From Corollary 2.3.4, there is a VCM of  $F_q$  if and only if  $q > 3$ . When  $q > 3$ , we take a VCM  $f(x)$  of  $F_q$  to construct a GPLS of order  $q$ .

In the following part, we will study  $\Delta_f$  and  $\Delta^f$ . At first, we need the following

Lemma 3.3.6. Let  $f(x) = ax+b$  and  $g(x) = cx+d$  be polynomials over  $F_q$ . Then  $f(x)$  and  $g(x)$  are compatible if and only if  $a = c$  and  $b \neq d$ .

Proof. It is easy to see that the sufficient part is true.

Since  $f(x)$  and  $g(x)$  are compatible,  $b = f(0) \neq g(0) = d$ . Suppose, by the way of contradiction, that  $a \neq c$ . Then the equation  $(a-c)x = d-b$  has a solution, say  $u$ . So  $au+b = cu+d$ , i.e.,  $f(u) = g(u)$ . We have a contradiction. So the necessity is also true and this completes the proof.

Using this lemma, we can characterize all GPLSs  $\Delta$  of order  $q$  so that  $\Delta^{-1}(c)$  defines (by Theorem 3.3.1) a linear polynomial for all  $c \in F_q$ .

**Theorem 3.3.7.** If  $\Delta$  is a GPLS of order  $q$  so that for each  $c \in F_q$ , the polynomial  $f_c(x)$  defined by  $\Delta^{-1}(c)$  (i.e.,  $\Delta(\{(a, f_c(a)) \mid a \in F_q\}) = \{c\}$ ) is linear, then there are a VCM  $f(x)$  and a PP  $g(x)$  of  $F_q$  such that  $\Delta = g \circ \Delta_f$ .

**Proof.** For  $c \in F_q$ , we can write  $f_c(x) = a_c x + b_c$  since  $f_c(x)$  is linear. We already saw that all  $f_c(x)$  are compatible. From Lemma 3.3.6, all  $a_c$  are the same, say  $a_c = a$  for all  $c \in F_q$ , and if  $c_1 \neq c_2 \in F_q$ ,  $b_{c_1} \neq b_{c_2}$ . So we can rewrite  $f_c(x) = ax + b_c$  for all  $c \in F_q$ . And  $\{b_c \mid c \in F_q\} = F_q$ . Let  $f(x) = ax$  and define  $g: F_q \rightarrow F_q$  by  $g(b_c) = c$  for all  $c \in F_q$ . Then, for all  $c \in F_q$  and for all  $u \in F_q$ ,  $c = \Delta(u, f_c(u)) = \Delta(u, au + b_c) = g(\Delta_f(u, f(u) + b_c))$ . So  $\Delta = g \circ \Delta_f$ .

Let  $\Delta_1, \Delta_2$  be GPLS of order  $q$ . Sometimes it happens that there is a PP  $g(x)$  of  $F_q$  such that  $\Delta_2 = g \circ \Delta_1$  (for instance, Theorem 3.3.7). In this case, the set of all VCMs defined by  $\Delta_1^{-1}(c)$ ,  $c \in F_q$ , and the set of VCMs defined by  $\Delta_2^{-1}(c)$ ,  $c \in F_q$ , are the same. Conversely, if  $C$  is a set of  $q$  compatible VCMs, we can construct a GPLS  $\Delta$  of order  $q$  by Theorem 3.3.3. If there is another GPLS  $\bar{\Delta}$  of order  $q$  constructed in some other way so that the previous set  $C$  is still the set of all VCMs of  $F_q$  defined by  $\bar{\Delta}^{-1}(c)$ ,  $c \in F_q$ , in Theorem 3.3.1, then there is a PP  $h(x)$  of  $F_q$  such that  $\bar{\Delta} = h \circ \Delta$ .

**Definition.** Two GPLS  $\Delta_1$  and  $\Delta_2$  of order  $q$  are equivalent if there is a PP  $g(x)$  of  $F_q$  such that  $\Delta_2 = g \circ \Delta_1$ . If  $\Delta_1$  and  $\Delta_2$  are equivalent, we denote  $\Delta_1 \sim \Delta_2$ .



It is easy to see that the relation  $\sim$  in the set of all GPLSs of order  $q$  is an equivalence relation. So there is one-to-one correspondence between equivalence classes and sets of  $q$  compatible VCMs of  $F_q$ . From Corollary 3.3.5 and Theorems 3.3.3 and 3.3.7, there is at least one equivalence class of GPLSs of order  $q$  whose corresponding set consists of  $q$  compatible linear VCMs of  $F_q$ . We already know (in Section 5 of Chapter II) that  $ax+b$  is a VCM of  $F_q$  if and only if  $a \neq 0, \pm 1$ . By Lemma 3.3.6 and Theorem 3.3.7, there are precisely  $q-3$  non-equivalent classes of GPLSs so that each of their corresponding sets consists of  $q$  compatible linear VCMs of  $F_q$ .

Moreover, in each equivalence class of GPLSs of order  $q$ , we take the GPLS  $\Delta$  with  $\Delta(0,a) = a$ ,  $a \in F_q$ , as a representative element of this equivalence class. In the corresponding set of  $q$  compatible VCMs of  $F_q$ , the VCM  $f_a(x)$  defined by  $\Delta^{-1}(a)$  satisfies  $f_a(0) = a$ .

For studying Theorem 3.3.8 below, we need the following definition. This definition is a restriction of the definition of mutual orthogonality of Latin squares (see Definition 9.81, p. 513, [22]).

**Definition.** Let  $\Delta_1, \Delta_2$  be GPLSs of order  $q$ .  $\Delta_1$  and  $\Delta_2$  are mutually orthogonal if all ordered pairs  $(\Delta_1(a,b), \Delta_2(a,b))$  are distinct.

It is easy to see that if  $\Delta_1$  and  $\Delta_2$  are in the same equivalence class, then  $\Delta_1$  and  $\Delta_2$  cannot be mutually orthogonal. Also, note that if  $\Delta_1$  and  $\Delta_2$  are the representatives of non-equivalent classes  $Y_1$  and  $Y_2$ , respectively, and if  $\Delta_1$  and  $\Delta_2$  are mutually orthogonal, then for arbitrary  $\bar{\Delta}_1 \in Y_1$  and  $\bar{\Delta}_2 \in Y_2$ ,  $\bar{\Delta}_1$  and  $\bar{\Delta}_2$  are mutually orthogonal.

Theorem 3.3.8. For  $a \in F_q$  with  $a \neq 0, \pm 1$ , let  $f_a(x) = ax$ . Then the  $q-3$  GPLSs  $\Delta_{f_a}$  of order  $q$  are mutually orthogonal.

Proof. Suppose, for the sake of contradiction, that  $\Delta_{f_a}$  and  $\Delta_{f_b}$  are not mutually orthogonal, where  $a \neq b$ . There are ordered pairs  $(x_1, y_1) \neq (x_2, y_2)$  of  $F_q \times F_q$  such that  $(\Delta_{f_a}(x_1, y_1), \Delta_{f_b}(x_1, y_1)) = (\Delta_{f_a}(x_2, y_2), \Delta_{f_b}(x_2, y_2))$ . Then  $\Delta_{f_a}(x_1, y_1) = \Delta_{f_a}(x_2, y_2)$  and  $\Delta_{f_b}(x_1, y_1) = \Delta_{f_b}(x_2, y_2)$ . Let  $\Delta_{f_a}(x_1, y_1) = c$  and  $\Delta_{f_b}(x_1, y_1) = d$ . From the definition of  $\Delta_f$ , we have  $f_a(x_1) + c = y_1 = f_b(x_1) + d$  and  $f_a(x_2) + c = y_2 = f_b(x_2) + d$ , i.e.,  $ax_1 + c = bx_1 + d$  and  $ax_2 + c = bx_2 + d$ . These imply  $(a-b)x_1 = (a-b)x_2$ . Since  $a-b \neq 0$ ,  $x_1 = x_2$ . This implies  $y_1 = y_2$  since  $\Delta(R) = F_q$  for any row  $R \in T$ . So  $(x_1, y_1) = (x_2, y_2)$ . We get a contradiction.

It is well known that the maximum possible number of pairwise orthogonal Latin squares of order  $n$  is  $\leq n-1$ . Gergely proved in [17] that the maximum possible number of pairwise orthogonal doubly diagonalized Latin squares of order  $n$  is  $\leq n-3$ , where a doubly diagonalized Latin square is a Latin square such that all elements of its symbol set occur exactly once both on its main diagonal and on its off diagonal. Theorem 3.3.8 says that there is a set which consists of  $q-3$  mutually orthogonal GPLSs of order  $q$ . Using methods similar to those Gergely used, we will show that the number  $q-3$  is the maximum possible one. It is

Theorem 3.3.9. The maximum number of mutually orthogonal GPLSs of order  $q$  is  $q-3$ .

Proof. From Theorem 3.3.8, it is enough to prove that if  $\Delta_1, \dots, \Delta_n$  are mutually orthogonal GPLSs of order  $q$ , then  $n \leq q-3$ . Moreover, we can assume, without loss of



generality,  $\Delta_i(0,a) = a$  for all  $a \in F_q$  and  $1 \leq i \leq n$ , since if  $1 \leq i \neq j \leq n$  and if  $\bar{\Delta}_i$  and  $\bar{\Delta}_j$  are equivalent to  $\Delta_i$  and  $\Delta_j$ , respectively, then  $\Delta_i$  and  $\Delta_j$  are orthogonal.

Fix  $a \in F_q^\times$ . At first, we claim that all  $\Delta_i(a,a)$  are distinct. Indeed, if there are  $1 \leq i, j \leq n$  so that  $\Delta_i(a,a) = \Delta_j(a,a) = c$ , then  $(\Delta_i(0,c), \Delta_j(0,c)) = (c,c) = (\Delta_i(a,a), \Delta_j(a,a))$ . This implies either  $a = c = 0$  or  $i = j$ , since  $\Delta_i$  and  $\Delta_j$  are orthogonal when  $i \neq j$ . Thus, the cardinality of the set  $M = \{\Delta_i(a,a) \mid 1 \leq i \leq n\}$  is  $n$ .

Since  $(a,a)$  is in the  $a$ -column,  $\Delta_i(a,a) \neq a$  for all  $1 \leq i \leq n$ . So  $a \notin M$ . Since  $(a,a) = (a,0+a)$  is the right 0-diagonal,  $\Delta_i(a,a) \neq 0 = \Delta_i(0,0)$  and so  $0 \notin M$ . Since  $(a,a) = (a,2a-a)$  is in the left  $2a$ -diagonal,  $\Delta_i(a,a) \neq 2a = \Delta_i(0,2a)$  for all  $i$ , and thus,  $2a \notin M$ . Combining all together,  $M \subseteq F_q - \{0, a, 2a\}$ . Hence,  $n = |M| \leq q-3$ .

In Theorem 3.3.8, we just considered  $\Delta_f$  because of the following theorem.

**Theorem 3.3.10.** Let  $f(x), g(x)$  be VCMs of  $F_q$  with  $f(0) = 0 = g(0)$  and  $\deg f, \deg g < q$ . Then  $\Delta_f, \Delta^g$  are equivalent if and only if  $g(x) = f(x)$  is a linearized polynomial.

**Proof.** Let  $\Delta_f$  and  $\Delta^g$  be equivalent. Since  $\Delta^g(0, g(0)) = 0 = \Delta_f(0, f(0))$ , we have  $(a, g(a)) = (a, f(a))$  for all  $a \in F_q$ . So  $g(x) = f(x)$ . Since  $\Delta_f$  and  $\Delta^g$  are equivalent, there is a PP  $h(x)$  of  $F_q$  so that  $\Delta^g(x_0, y_0) = h(\Delta_f(x_0, y_0))$  for all  $x_0, y_0 \in F_q$ . For any fixed  $b \in F_q$ ,  $\Delta^g(a, f(b+a)) = \Delta^g(a, g(b+a)) = b = h(\Delta_f(a, f(b+a)))$  for all  $a \in F_q$ . Write  $c_b = \Delta_f(a, f(b+a))$  for all  $a \in F_q$ . By the definition of  $\Delta_f$ ,  $c_b = \Delta_f(a, f(a) + c_b)$  for all  $a \in F_q$ . This implies  $f(b+x) = f(x) + c_b$ . Take  $x = 0$ , we have  $c_b = f(b)$ . So  $f(b+a) = f(a) + f(b)$  for all  $a, b \in F_q$ . By Lemma 3.2.2,  $f(x)$  is a linearized polynomial.

Conversely, we assume that  $f(x) = g(x)$  is a linearized polynomial. Then, for each  $b \in F_q$ ,  $g(b+x) = f(b+x) = f(x) + f(b)$ . Let  $h(x)$  be a polynomial in  $F_q[x]$  representing



the inverse mapping of  $f$ . Then  $h(x)$  is a PP of  $F_q$ . For all  $a, b \in F_q$ ,  $h(\Delta_f(a, g(b+a))) = h(\Delta_f(a, f(a)+f(b))) = h(f(b)) = b = \Delta^g(a, g(b+a))$ . So  $\Delta_f$  and  $\Delta^g$  are equivalent. This completes the proof.

In the last theorem, we gave a necessary and sufficient condition for  $\Delta_f \sim \Delta^g$ . We will give a necessary and sufficient condition for either  $\Delta_f \sim \Delta_g$  or  $\Delta^f \sim \Delta^g$  in the next theorem.

**Theorem 3.3.11.** Let  $f(x), g(x)$  be VCMs of  $F_q$  with  $f(0) = 0 = g(0)$  and  $\deg f < q$  and  $\deg g < q$ . Then  $\Delta_f \sim \Delta_g$  if and only if  $f(x) = g(x)$ , and  $\Delta^f \sim \Delta^g$  if and only if  $f(x) = g(x)$ .

**Proof.**  $\Delta_f \sim \Delta_g$  if and only if there is a PP  $h(x)$  of  $F_q$  so that  $\Delta_f(a, b) = h(\Delta_g(a, b))$  for all  $a, b \in F_q$ . Now  $\Delta_f(0, 0) = \Delta_f(0, f(0)+0) = 0 = \Delta_g(0, g(0)+0)$  and  $h(0) = 0$ . For all  $a \in F_q$ ,  $\Delta_f \sim \Delta_g$  implies  $h(\Delta_g(a, f(a))) = \Delta_f(a, f(a)) = 0$  and so  $\Delta_g(a, f(a)) = 0 = \Delta_f(a, f(a))$  for all  $a \in F_q$ . Since  $\Delta_g(a, g(a)) = 0$ , for all  $a \in F_q$  and  $\Delta_g(R) = F_q$  for any row  $R$  in  $T$ , we have  $f(a) = g(a)$  for all  $a \in F_q$  whenever  $\Delta_f$  and  $\Delta_g$  are equivalent. So if  $\Delta_f \sim \Delta_g$ , then  $f(x) = g(x)$ . Conversely,  $g(x) = f(x)$  implies  $\Delta_f = \Delta_g$ .

By similar arguments,  $\Delta^f \sim \Delta^g$  if and only if  $f(x) = g(x)$ . This completes the proof.

Now, we try to express  $\Delta^g$  in another way. This is based on the following theorem.

**Theorem 3.3.12.** Let  $f(x) \in F_q[x]$  be a VCM and  $\deg f < q$ . Then the function  ${}^f\Delta: F_q \times F_q \rightarrow F_q$  defined by  ${}^f\Delta(a, b) = -a + f(b)$  for all  $a, b \in F_q$  is a GPLS of order  $q$ . Furthermore, for  $b \in F_q$ ,  $f_b(x) \in F_q[x]$ , with  $\deg f_b < q$ , is a VCM and satisfies

$\{(a, f_b(a)) \mid a \in F_q\} = {}^f\Delta^{-1}(b)$  if and only if  $f_b(x) = f^{-1}(b+x)$  where  $f^{-1}(x)$  is the polynomial of degree  $< q$  representing the inverse mapping of  $f(x)$ .

Proof. Let  $a \in F_q$  be arbitrary. Since  $f(x)$  is a VCM of  $F_q$ , each of the polynomials  ${}^f\Delta(a, x) = -a + f(x)$ ,  ${}^f\Delta(x, a) = -x + f(a)$ ,  ${}^f\Delta(x, a+x) = -x + f(a+x) = [-(a+x) + f(a+x)] + a$  and  ${}^f\Delta(x, a-x) = -x + f(a-x) = [(a-x) + f(a-x)] - a$  is a PP of  $F_q$ . So  ${}^f\Delta$  is a GPLS of order  $q$ .

Fix  $b \in F_q$ .  $f_b(x)$  is a VCM satisfying  $\{(a, f_b(a)) \mid a \in F_q\} = {}^f\Delta^{-1}(b)$  if and only if  $b = {}^f\Delta(a, f_b(a)) = -a + f(f_b(a))$  for all  $a \in F_q$ . The last statement is equivalent to  $f_b(x) = f^{-1}(b+x)$ . This completes the proof.

From this theorem, we see that  $\Delta^g(a, b) = -a + g^{-1}(b)$  for all  $a, b \in F_q$ .

We already mentioned at the beginning of this section that if  $\Delta$  is a GPLS of order  $q$  and if  $\alpha$  is a PLS-transformation, then  $\Delta \circ \alpha$  is still a GPLS of order  $q$ . We will see later that if  $f(x)$  is a VCM of  $F_q$ , then  $\Delta_f \alpha$  is equivalent to  $\Delta_g$  for some VCM  $g(x)$ . At first, we need two Lemmas.

Lemma 3.3.13. Let  $f(x)$  be a VCM of  $F_q$  and let  $\alpha \in G$  be a PLS-transformation. Let  $L = \{(a, f(a)) \mid a \in F_q\}$ . Then

- (1) if  $(x_1, y_1), (x_2, y_2) \in \alpha(L)$  and  $x_1 = x_2$ , then  $y_1 = y_2$ ,
- (2) if we rewrite  $\alpha(L) = \{(a, g(a)) \mid a \in F_q\}$ , then  $g(x)$  is a VCM of  $F_q$ .

Proof. From Theorem 3.2.4,  $G$  is generated by  $\tau_{(a,b)}$ ,  $\nu$ ,  $\sigma$ ,  $\mu_{(a_0, \dots, a_{n-1})}$  and  $\psi$  (if  $p = 3$ ). So it is enough to check all such mappings with  $\alpha$ .

$\tau_{(a,b)}(L) = \{(x_0 + a, f(x_0) + b) \mid x_0 \in F_q\} = \{(x_0, f(x_0 - a) + b) \mid x_0 \in F_q\}$ . By Theorem 2.2.1, we see that (1) and (2) hold and  $g(x) = f(x-a) + b$ .

$\nu(L) = \{(a, -f(a)) \mid a \in F_q\}$ . By the same theorem, (1) and (2) hold and  $g(x) = -f(x)$ .

$\sigma(L) = \{(a+f(a), -a+f(a)) \mid a \in F_q\} = \{(a, -2\underline{f}(a)+a) \mid a \in F_q\}$  where  $\underline{f}(x)$  is the polynomial representing the inverse of  $f(x)+x$ . By Theorem 2.5.4, (1) and (2) hold and  $g(x) = -2\underline{f}(x)+x$ .

For  $\mu_{(a_0, \dots, a_{n-1})} \in G$ , let  $h(x) = a_0x + a_1x^p + \dots + a_{n-1}x^{p^{n-1}}$ . Then  $h(x)$  is a PP of  $F_q$ .

Let  $h^{-1}(x)$  be the inverse mapping of  $h(x)$ . Then

$$\begin{aligned} \mu_{(a_0, \dots, a_{n-1})}(L) &= \left\{ \left( \sum_{i=0}^{n-1} a_i x^{p^i}, \sum_{i=0}^{n-1} a_i (f(a))^{p^i} \right) \mid a \in F_q \right\} = \{(h(a), (h \circ f)(a)) \mid a \in F_q\} \\ &= \{(a, (h \circ f \circ h^{-1})(a)) \mid a \in F_q\}. \end{aligned}$$

By Theorem 2.2.1, (1) and (2) hold and  $g(x) = (h \circ f \circ h^{-1})(x)$ .

For  $p = 3$ ,  $\psi(L) = \{(a, a-f(a)) \mid a \in F_q\}$ . By the same theorem again, (1) and (2) hold and  $g(x) = -f(x)+x$ . This completes the proof.

In Lemma 3.3.13, the polynomial  $g(x)$  is unique when we consider  $\deg g < q$ . We denote this polynomial  $g(x) = (\alpha f)(x)$ .

**Lemma 3.3.14.** Let  $f(x)$  be a VCM of  $F_q$  and let  $a \in F_q$ . Then for all  $\alpha \in G$ ,  $\alpha f_a(x) = \alpha f(x) + b_a$  for some  $b_a \in F_q$ , where  $f_a(x) = f(x) + a$ . Furthermore, if  $a_1 \neq a_2$ , then  $b_{a_1} \neq b_{a_2}$ .

**Proof.** As in Lemma 3.3.13, it is enough to consider  $\tau_{(a,b)}$ ,  $\nu$ ,  $\sigma$ ,  $\mu_{(a_0, \dots, a_{n-1})}$  and  $\psi$  (if  $p = 3$ ). As we showed in Lemma 3.3.13, it is easy to see that this lemma is true for  $\alpha = \tau_{(a,b)}$ ,  $\nu$  and  $\psi$  (if  $p = 3$ ).



From the proof of Lemma 3.3.13 again, if  $y = x+f(x)$ , then  $\sigma f_a(y) = -x+f(x)+a = \sigma f(y)+a$  and so this lemma holds.

Also,  $\mu_{(a_0, \dots, a_{n-1})} f_a(x) = (h \circ f_a \circ h^{-1})(x) = h(f(h^{-1}(x))+a) = h(f(h^{-1}(x)))+h(a) = \mu_{(a_0, \dots, a_{n-1})} f(x)+h(a)$  and so the lemma holds. This completes the proof.

Now we can prove our claim using Lemmas 3.3.13 and 3.3.14.

Theorem 3.3.15. Let  $f(x)$  be a VCM and  $\alpha \in G$ . Then  $\Delta_f \alpha \sim \Delta_{\alpha^{-1}f}$ .

Proof. By Lemma 3.3.14,  $\alpha^{-1}f_a(x) = \alpha^{-1}f(x)+b_a$  and  $b_a$  ranges over  $F_q$  when  $a$  does. Define the polynomial  $g(x) \in F_q[x]$  by  $g(a) = b_a$  for all  $a \in F_q$ . Then  $g(x)$  is a PP of  $F_q$ . Note that

$$F_q \times F_q = \{(u, f(u)+a) \mid u, a \in F_q\} = \{(u, \alpha^{-1}f(u)+b_a) \mid u, a \in F_q\}.$$

Now, for all  $(u, \alpha^{-1}f(u)+b_a) \in F_q \times F_q$ ,  $\Delta_{\alpha^{-1}f}(u, \alpha^{-1}f(u)+b_a) = b_a = g(a) = g(\Delta_f(u, f(u)+a)) = g(\Delta_f(\alpha(u, \alpha^{-1}f(u)+b_a))) = (g \circ \Delta_f \alpha)(u, \alpha^{-1}f(u)+b_a)$ . So  $\Delta_{\alpha^{-1}f} = g \circ \Delta_f \alpha$ .

We note that, in Theorem 3.3.15, the polynomial  $g(x)$  may be taken as follows:  $g(x) = x$  if  $\alpha = \tau_{(a,b)}$  or  $\sigma$ ;  $g(x) = -x$  if  $\alpha = \nu$  or  $\psi$  (if  $p = 3$ ); and  $g(x) = \sum_{i=0}^{n-1} a_i x^{p^i}$  if  $\alpha = \mu_{(a_0, \dots, a_{n-1})}$ . In any case,  $g(x)$  is a linearized polynomial of  $F_q$  over  $F_p$ .

Also note that Theorem 3.3.15 is no longer true if we consider  $\Delta^f$ . The following is a counterexample.

Example. Let  $F_9 = \{0, 1, 2, \beta, \beta+1, \beta+2, 2\beta, 2\beta+1, 2\beta+2\}$  with  $\beta^2 = 2\beta+1$ . Let  $f(x) = (2\beta+1)x^5+2x$ . By Lemma 2.2.2, we see that  $f(x)$  is a VCM of  $F_q$ . The following table is the GPLS  $\Delta^f \sigma$ .

Table 7. Selected GPLS  $\Delta^f \circ \sigma$ .

	0	1	2	$\beta$	$\beta+1$	$\beta+2$	$2\beta$	$2\beta+1$	$2\beta+2$
0	0	$\beta+2$	$2\beta+1$	$2\beta+2$	$\beta$	2	$\beta+1$	1	$2\beta$
1	$2\beta+2$	1	$\beta$	0	$2\beta$	$\beta+1$	$2\beta+1$	$\beta+2$	2
2	$\beta+1$	$2\beta$	2	$\beta+2$	1	$2\beta+1$	0	$2\beta+2$	$\beta$
$\beta$	$2\beta+1$	$\beta+1$	0	$\beta$	$2\beta+2$	1	2	$2\beta$	$\beta+2$
$\beta+1$	1	$2\beta+2$	$\beta+2$	2	$\beta+1$	$2\beta$	$\beta$	0	$2\beta+1$
$\beta+2$	$\beta$	2	$2\beta$	$2\beta+1$	0	$\beta+2$	$2\beta+2$	$\beta+1$	1
$2\beta$	$\beta+2$	0	$2\beta+2$	1	$2\beta+1$	$\beta$	$2\beta$	2	$\beta+1$
$2\beta+1$	$2\beta$	$\beta$	1	$\beta+1$	2	$2\beta+2$	$\beta+2$	$2\beta+1$	0
$2\beta+2$	2	$2\beta+1$	$\beta+1$	$2\beta$	$\beta+2$	0	1	$\beta$	$2\beta+2$

Let  $g_a(x)$ ,  $a \in F_9$  be the corresponding 9 compatible VCMs of this GPLS  $\Delta^f \circ \sigma$ . So for all  $b \in F_9$ ,  $\Delta^f \circ \sigma(b, g_a(b)) = a$ . It is not difficult to see that  $g_0(x) = (\beta+2)x^5 + x$ . Suppose, by the way of contradiction, that there is  $c \in F_9$  so that  $g_1(x) = g_0(x+c)$ . In this case,  $2\beta+1 = g_1(0) = g_0(c)$  and so  $c = \beta+1$ . Now,  $1 = g_1(1) = g_0(\beta+2) = \beta+1$  and we get a contradiction. So  $\Delta^f \circ \sigma$  is not equivalent to  $\Delta^g$  for any VCM  $g(x)$  of  $F_9$ . By a similar argument,  $\Delta^f \circ \sigma$  is not equivalent to  $\Delta_g$  for all VCM  $g(x)$  of  $F_9$ .

## CHAPTER 4

### MISCELLANEOUS PROPERTIES OF PERMUTATION POLYNOMIALS

#### 1. Properties of Permutation Polynomials

As indicated in Chapter I, Section 4, permutation polynomials have been studied extensively. An excellent reference is Lidl and Niederreiter's book [22]. In this section, we will give some additional properties of permutation polynomials.

Throughout this section, any polynomial  $f(x) \in F_q[x]$  we consider satisfies  $f(0) = 0$ . For  $f(x) \in F_q[x]$ , write  $f(x) = a_1x^{n_1} + \dots + a_tx^{n_t}$  where  $1 \leq n_1 < \dots < n_t \leq q-1$  and  $a_1 \dots a_t \neq 0$ . Let  $d = \gcd(q-1, n_1-1, \dots, n_t-1)$ . Let  $U = \langle \zeta^{(q-1)/d} \rangle$  be the subgroup of  $F_q^\times$  generated by  $\zeta^{(q-1)/d}$  where  $\zeta$  is a primitive element of  $F_q$ . If  $e = \frac{q-1}{d}$ , then the quotient group is  $F^\times/U = \{\zeta^0U, \zeta^1U, \dots, \zeta^{e-1}U\}$ .

**Definition.** The numbers  $d$  and  $e$  are called the rank and index of  $f(x)$ , respectively.



Now, for any  $a \in F_q^\times$ , there are  $0 \leq i \leq e-1$  and  $0 \leq j \leq d-1$  such that  $a = \zeta^{i+je}$ . So  
 $f(a) = a_1 a^{n_1} + \dots + a_t a^{n_t} = a(a_1 a^{n_1-1} + \dots + a_t a^{n_t-1}) = a(a_1 \zeta^{i(n_1-1)} + \dots + a_t \zeta^{i(n_t-1)})$ . If we write  
 $\alpha_i = a_1 \zeta^{i(n_1-1)} + \dots + a_t \zeta^{i(n_t-1)}$  for each  $0 \leq i \leq e-1$ , then  $f(a) = a\alpha_i$  whenever  $a \in \zeta^i U$ .

Lemma 4.1.1.  $f(x)$  is a PP of  $F_q$  if and only if the mapping defined by  $\sigma(\zeta^i U) = (\alpha_i \zeta^i)U$  is a permutation on  $F_q^\times/U$ .

Proof. We already saw that  $f(a) = a\alpha_i$  whenever  $a \in \zeta^i U$ . So, if  $\alpha_i \neq 0$ ,  $f(\zeta^i U) = (\alpha_i \zeta^i)U \in F_q^\times/U$ .

$f(x)$  is a PP of  $F_q$  if and only if  $f(F_q) = F_q$ . Since  $f(0) = 0$ ,  $f(F_q) = F_q$  if and only if  $f(F_q^\times) = F_q^\times$ . The last equality is equivalent to that all  $\alpha_0, \dots, \alpha_{e-1}$  are non-zero and  $(\alpha_i \zeta^i)U \neq (\alpha_j \zeta^j)U$  for  $0 \leq i \neq j \leq e-1$ , and so equivalent to that  $\sigma$  is a permutation on  $F_q^\times/U$ . This completes the proof.

Let  $\psi_e$  be a multiplicative character of  $F_q$  of order  $e$ .

Lemma 4.1.2. Let  $\beta_1, \dots, \beta_e \in F_q^\times$ . Then the mapping defined by  $\sigma(\zeta^i U) = (\beta_i \zeta^i)U$  is a permutation on  $F_q^\times/U$  if and only if  $\psi_e(\beta_i \beta_j^{-1}) \neq \psi_e(\zeta^{j-i})$  whenever  $1 \leq i \neq j \leq e$ .

Proof. Since  $\beta_1, \dots, \beta_e \in F_q^\times$ ,  $\sigma: F_q^\times/U \rightarrow F_q^\times/U$ . For  $0 \leq i, j \leq e-1$ ,  $\sigma(\zeta^i U) = \sigma(\zeta^j U)$  if and only if  $\beta_i \zeta^i U = \beta_j \zeta^j U$  and so  $\beta_i \zeta^i \beta_j^{-1} \zeta^{-j} \in U$ . Hence, it is equivalent to  
 $1 = \psi_e(\beta_i \beta_j^{-1} \zeta^{i-j}) = \psi_e(\beta_i \beta_j^{-1}) [\psi_e(\zeta^{j-i})]^{-1}$ .

Combining Lemmas 4.1.1 and 4.1.2 together, we have immediately

Theorem 4.1.3. Let  $f(x) \in F_q[x]$  have rank  $d$  and index  $e$ . Let  $\zeta$  be a primitive element of  $F_q$ . Moreover, let  $\alpha_i = \zeta^{-i} f(\zeta^i)$  for  $0 \leq i \leq e-1$ . Then  $f(x)$  is a PP of  $F_q$  if and only if  $\alpha_i \neq 0$  for all  $0 \leq i \leq e-1$ , and  $\psi_e(\alpha_i \alpha_j^{-1}) \neq \psi_e(\zeta^{j-i})$  for  $0 \leq i \neq j \leq e-1$ , where  $\psi_e$  is a multiplicative character of  $F_q$  of order  $e$ .

Note that Niederreiter and Robinson [28] got a similar result for special polynomials of the form  $ax^{(q+n-1)/n} + bx$  with  $q \equiv 1 \pmod n$ .

Lemma 4.1.4. Let  $f(x) \in F_q[x]$  be of index  $e$ . Let  $\zeta$  be a primitive element of  $F_q$  and let  $\alpha_i = \zeta^{-i} f(\zeta^i)$  for  $0 \leq i \leq e-1$ . If  $f(x)$  is a PP of  $F_q$ , then  $\psi_e(\prod_{i=0}^{e-1} \alpha_i) = 1$ , where  $\psi_e$  is a multiplicative character of  $F_q$  of order  $e$ .

Proof. Let  $U_d = \{\zeta^{ei} \mid 0 \leq i < d = \frac{q-1}{e}\}$ . By Lemma 4.2.1, if  $f(x)$  is a PP of  $F_q$ ,  $\{(\alpha_i \zeta^i) U_d \mid 0 \leq i \leq e-1\} = F_q^\times / U_d$ . So  $(\prod_{i=0}^{e-1} \alpha_i) (\prod_{i=0}^{e-1} \zeta^i) = \prod_{i=0}^{e-1} (\alpha_i \zeta^i)$  is either in  $U_d$  whenever  $e$  is odd or in  $\zeta^{e/2} U_d$  whenever  $e$  is even. If  $e$  is odd,  $\prod_{i=0}^{e-1} \zeta^i \in U_d$ . If  $e$  is even,  $\prod_{i=0}^{e-1} \zeta^i \in \zeta^{e/2} U_d$ . In any case, we have  $\prod_{i=0}^{e-1} \alpha_i \in U_d$ . So  $\psi_e(\prod_{i=0}^{e-1} \alpha_i) = 1$ .

Note that the converse of Lemma 4.1.4 is not true. For example, let's consider  $q = 13$  and  $f(x) = 6x^9 + 10x^5 + 11x$ . Note that 2 is a primitive element of  $F_{13}$ . Also note that the index of  $f(x)$  is 3 since  $d = \gcd(12, 0, 4, 8) = 4$ . Now  $\alpha_0 = 1$ ,  $\alpha_1 = 4$  and  $\alpha_2 = 2$ . So  $\psi_3(1 \cdot 4 \cdot 2) = 1$ . But  $(\alpha_0 2^0) U_4 = U_4 = (\alpha_1 \cdot 2) U_4$ . By Lemma 4.1.1,  $f(x)$  is not a PP of  $F_{13}$ .

When we consider  $f(x)$  to be of rank  $d$  and of index  $e$ , we may write as  $f(x) = \sum_{i=0}^{e-1} a_i x^{id+1}$ . Now, let  $C_f = \text{circ}(a_0, a_1, \dots, a_{e-1})$ .

**Lemma 4.1.5.** Let  $f(x) \in F_q[x]$  be of index  $e$ . Let  $P(x)$  be the characteristic polynomial of  $C_f$ . Then  $P(x) = \prod_{i=0}^{e-1} (x - \alpha_i)$  where  $\alpha_i = \zeta^{-i} f(\zeta^i)$  for  $0 \leq i \leq e-1$ . Moreover,  $C_f$  is similar to the diagonal matrix  $\text{diag}(\alpha_0, \alpha_1, \dots, \alpha_{e-1})$  and so  $\det C_f = \alpha_0 \alpha_1 \dots \alpha_{e-1}$ .

**Proof.** Let  $f(x)$  be of rank  $d$  and write  $f(x) = \sum_{i=0}^{e-1} a_i x^{id+1}$ . Then  $C_f = \text{circ}(a_0, a_1, \dots, a_{e-1})$ . Let  $g(x)$  be the representer of  $C_f$ . Then  $g(x) = \sum_{i=0}^{e-1} a_i x^i$ . Since  $\zeta$  is a primitive element of  $F_q$ ,  $b = \zeta^d$  is a primitive  $e$ th root of unity. By Theorem 1.3.7,  $C_f$  is similar to  $\text{diag}(g(1), g(b), \dots, g(b^{e-1}))$ . By Corollary 1.3.8,  $\det C_f = \prod_{i=0}^{e-1} g(b^i)$  and  $P(x) = \prod_{i=0}^{e-1} (x - g(b^i))$ . If we can prove  $g(b^i) = \zeta^{-i} f(\zeta^i) = \alpha_i$ , we are done.

Now,  $g(b^i) = \sum_{j=0}^{e-1} a_j b^{ij} = \sum_{j=0}^{e-1} a_j (\zeta^i)^{dj} = \zeta^{-i} \sum_{j=0}^{e-1} a_j (\zeta^i)^{dj+1} = \zeta^{-i} f(\zeta^i) = \alpha_i$ . This completes the proof.

Combining Lemmas 4.1.4 and 4.1.5 together, we have immediately the following

**Theorem 4.1.6.** If  $f(x) \in F_q[x]$  is a PP of  $F_q$  and is of index  $e$ , then  $\psi_e(\det C_f) = 1$ , where  $\psi_e$  is a multiplicative character of order  $e$ .



If  $f(x) \in F_q[x]$  with degree  $\leq q-1$  and  $f(0) = 0$ , we may write  $f(x) = a_1x + a_2x^2 + \dots + a_{q-1}x^{q-1}$ . Hence, we may consider each polynomial of degree  $\leq q-1$  as a polynomial of rank 1. Since we discuss properties of PPs in this section, we consider all polynomials with degree  $\leq q-2$  by Theorem 2.3.3. Moreover, we consider the circulant matrix  $M_f$  with the first row-vector  $(0, a_1, \dots, a_{q-2})$  instead of the circulant matrix  $C_f$  with the first row-vector  $(a_1, a_2, \dots, a_{q-2}, 0)$ . With this modification we have

**Theorem 4.1.7.** Let  $f(x) = a_1x + \dots + a_{q-2}x^{q-2} \in F_q[x]$ . Then  $f(x)$  is a PP of  $F_q$  if and only if the characteristic polynomial  $P_f(x)$  of  $M_f$  is  $P_f(x) = x^{q-1} - 1$ .

**Proof.** Since  $f(0) = 0$ ,  $f(x)$  is a PP of  $F_q$  if and only if  $\{f(a) \mid a \in F_q^\times\} = F_q^\times$ . Since  $f(x) = a_1x + \dots + a_{q-2}x^{q-2}$  and every element of  $F_q^\times$  is a  $q-1$ st root of unity, we have  $P_f(x) = \prod_{a \in F_q^\times} (x - f(a))$  by Corollary 1.3.8. So  $\{f(a) \mid a \in F_q^\times\} = F_q^\times$  is equivalent to  $P_f(x) = x^{q-1} - 1$ . This completes the proof.

We note that Raussnitz [35] obtained the result that if  $f(x) = \sum_{i=0}^{q-2} a_i x^i$  and  $M_f$  is the circulant matrix with the first row-vector  $(a_0, a_1, \dots, a_{q-2})$ , then  $f(x)$  permutes  $F_q$  if and only if the characteristic polynomial of  $M_f$  is  $(x^q - x)/(x - f(0))$ . Theorem 4.1.7 is a special case of Raussnitz's result.

For  $f(x) = a_1x + \dots + a_{q-2}x^{q-2} \in F_q[x]$ , let  $L_f(x) = \sum_{i=1}^{q-2} a_i x^{qi-1}$  be the associated linearized polynomial of  $F_{q^{q-1}}$  over  $F_q$ . For these two polynomials  $f(x)$  and  $L_f(x)$ , we have the following relation.

Theorem 4.1.8. If  $f(x)$  is a PP of  $F_q$ , then  $L_f(x)$  is a PP of  $F_{q^{q-1}}$ .

Proof. Since  $f(x)$  is a PP of  $F_q$ ,  $P_f(x) = x^{q-1} - 1$  by Theorem 4.1.7. In particular,  $\det M_f = -1 \neq 0$ .

On the other hand, let  $A = (a_{i-j+1}^{q-1})$  with  $i-j \bmod (q-1)$ . Since each  $a_i \in F_q$ ,  $a_i^q = a_i$  for all  $1 \leq i \leq q-1$  (note  $a_{q-1} = 0$ ). So  $A$  is the circulant matrix with the first row-vector  $(a_1, 0, a_{q-2}, \dots, a_2)$ . Since  $M_f$  is the circulant matrix with the first row-vector  $(0, a_1, a_2, \dots, a_{q-2})$ , it is easy to see that  $\det A = (-1)^{(q-2)^2} \det M_f = 1 \neq 0$ . From Theorem 1.4.12,  $L_f(x)$  is a PP of  $F_{q^{q-1}}$ .

Note that the converse of Theorem 4.1.8 is not true. For example,  $f(x) = x^2$  is not a PP of  $F_3$ , but  $L_f(x) = x^3$  is a PP of  $F_{3^2}$ .

Using Theorem 4.1.7, we also have

Theorem 4.1.9. Let  $q$  be odd. If  $f(x), g(x) \in F_q[x]$ , with  $f(0) = 0 = g(0)$ , are PPs of  $F_q$ , then  $f(x)g(x)$  is not a PP of  $F_q$ .

Proof. Since  $f(x)$  and  $g(x)$  are PPs of  $F_q$ ,  $P_f(x) = x^{q-1} - 1 = P_g(x)$  by Theorem 4.1.7. So  $\det M_f = -1 = \det M_g$ . Hence,  $\det (M_f M_g) = (\det M_f)(\det M_g) = 1$ .

Now write  $f(x) = a_0 + a_1x + \dots + a_{q-2}x^{q-2}$  and  $g(x) = b_0 + b_1x + \dots + b_{q-2}x^{q-2}$  with  $a_0 = 0 = b_0$ . Also, we can write  $f(x)g(x) \equiv \sum_{i=1}^{q-1} c_i x^i \bmod (x^q - x)$ . Then  $c_i = \sum_{j=1}^{q-2} a_j b_{i-j}$  with  $i-j \bmod (q-1)$ . If  $c_{q-1} \neq 0$ ,  $f(x)g(x)$  is not a PP of  $F_q$ . So we consider  $c_{q-1} = 0$ . Then  $M_{f,g}$  is the circulant matrix with the first row-vector  $(0, c_1, \dots, c_{q-2}) = (c_{q-1}, c_1, \dots, c_{q-2})$ . From the

formula  $c_i = \sum_{j=1}^{q-2} a_j b_{i-j}$ , each  $c_i$  is the inner product of the first row-vector of  $M_f$  and each column-vector of  $M_g$ . Since  $M_f M_g$  is still a circulant matrix,  $M_{f \cdot g} = M_f M_g$ . So  $\det M_{f \cdot g} = \det (M_f M_g) = 1$  and hence,  $P_{f \cdot g}(x) \neq x^{q-1} - 1$ . Thus,  $f(x)g(x)$  is not a PP of  $F_q$  by Theorem 4.1.7.

Note that Theorem 4.1.9 is no longer true when  $q$  is even. For example, both  $f(x) = x$  and  $g(x) = x^2 = f(x)f(x)$  are PPs of  $F_q$  when  $q$  is even.

## 2. The Polynomial $1+x+x^2+\dots+x^k$

The polynomial  $1+x+\dots+x^k$  plays a very important role in the study of finite geometries. We first recall some basic properties of finite geometries which can be found in Lidl and Niederreiter's book (see Section 3, Chapter 9, [22]).

A finite projective plane is defined as a set of elements, called points, together with sets of points called lines, as well as a relation  $I$ , called incidence, between points and lines subject to the following conditions: (1) every pair of distinct lines is incident with a unique point; (2) every pair of distinct points is incident with a unique line; (3) there exist four points such that no three of them are incident with a single line. Let  $K$  be any field. Let  $P = \{(x,y,1) \mid x,y \in K\} \cup \{(1,0,0)\} \cup \{(x,1,0) \mid x \in K\}$  and let  $L$  be the collection of sets  $L$  which are either  $L = \{(1,0,0)\} \cup \{(x,1,0) \mid x \in K\}$  or  $L = \{(x,y,1) \mid \text{there are } a,b,c \in K \text{ with } (a,b) \neq (0,0) \text{ such that } ax+by+c = 0\}$ . Every element of  $P$  is called a point and every element of  $L$  is called a line. Moreover, we define a relation  $I$  so that a point  $P \in P$  is incident with a line  $L \in L$  if and only if  $P \in L$ . It is known that  $(P,L,I)$  forms a projective plane. This projective plane is usually denoted by  $PG(2,K)$ .



Now, let  $q = 2^n$ ,  $n$  a positive integer. An oval in  $PG(2, F_q)$  is defined to be a set of  $q+2$  points of  $PG(2, F_q)$  no three of which are collinear (i.e., on the same line). For any  $f(x) \in F_q[x]$ , let  $A(f) = \{(f(c), c, 1) \mid c \in F_q\} \cup \{(1, 0, 0), (0, 1, 0)\}$ . Then we have the following

**Theorem A.** The set  $A(x^{k+1})$  with  $0 \leq k \leq q-2$  is an oval in  $PG(2, F_q)$ ,  $q$  even and  $q > 2$ , if and only if the following conditions hold;

- (1)  $\gcd(k+1, q-1) = 1$ ;
- (2)  $\gcd(k, q-1) = 1$ ;
- (3)  $[(x+1)^{k+1}+1]/x$  is a PP of  $F_q$ .

In fact, if we consider  $(x+1)^{k+1}$  instead of  $x^{k+1}$ , this theorem is still true. In this case, condition (3) becomes

$$(3') \quad (x^{k+1}+1)/(x+1) = 1+x+\dots+x^k \text{ is a PP of } F_q.$$

Since  $[(x+1)^{k+1}+1]/x$  is a PP of  $F_q$  if and only if  $(x^{k+1}+1)/(x+1)$  is a PP of  $F_q$ , we may restate this theorem as follows.

**Theorem B.** The set  $A(x^{k+1})$  with  $0 \leq k \leq q-2$  is an oval in  $PG(2, F_q)$ ,  $q$  even and  $q > 2$ , if and only if the following conditions hold:

- (i)  $\gcd(k+1, q-1) = 1$ ;
- (ii)  $\gcd(k, q-1) = 1$ ;
- (iii)  $1+x+\dots+x^k$  is a PP of  $F_q$ .

In this section, we will prove first that conditions (i) and (ii) in this theorem are superfluous. Later, we will study some properties of this polynomial  $1+x+\dots+x^k$ .

Lemma 4.2.1. Let  $q = p^n$ ,  $p$  a prime. If  $f(x) = 1+x+\dots+x^k$  is a PP of  $F_q$ , then there is a nonnegative integer  $m$  such that  $k \equiv mp(p-1)+1 \pmod{p(q-1)}$ ,  $mp(p-1)+1 \leq q-2$ , and

$$\gcd(mp(p-1)+1, q-1) = 1 = \begin{cases} \gcd\left(\frac{mp(p-1)}{2} + 1, \frac{q-1}{2}\right) & \text{if } q \text{ is odd} \\ \gcd(m+1, q-1) & \text{if } q \text{ is even.} \end{cases}$$

Proof. Write  $k = l(q-1)+r$ , where  $0 \leq r < q-1$ . Let  $g(x) = 1+(l+1)x+\dots+(l+1)x^r+lx^{r+1}+\dots+lx^{q-1}$ . Then  $f(x) \equiv g(x) \pmod{(x^q-x)}$ . Since  $f(x) = 1+x+\dots+x^k$  is a PP of  $F_q$ ,  $1 \leq \deg g \leq q-2$  from Theorem 2.3.3. So  $l \equiv 0 \pmod{p}$ . Hence,  $k \equiv r \pmod{p(q-1)}$ ,  $1 \leq r \leq q-2$  and  $g(x) = 1+x+\dots+x^r$ .

Since  $f(x) \equiv g(x) \pmod{(x^q-x)}$ ,  $f(x)$  is a PP of  $F_q$  if and only if  $g(x)$  is a PP of  $F_q$ . Also,  $g(x)$  is a PP of  $F_q$  if and only if  $g_0(x) = x+\dots+x^r$  is a PP of  $F_q$ .

Let  $M_{g_0}$  be the circulant matrix of order  $(q-1) \times (q-1)$  with the first row-vector  $(0, 1, \dots, 1, 0, \dots, 0)$ . Moreover, let  $C$  be the circulant matrix of order  $(q-1) \times (q-1)$  with first  $r$ -terms row-vector  $(1, \dots, 1, 0, \dots, 0)$ . From Theorem 1.3.9,

$$\det C = \begin{cases} r & \text{if } \gcd(r, q-1) = 1 \\ 0 & \text{if } \gcd(r, q-1) > 1 \end{cases}.$$

So,  $\det M_{g_0} = (-1)^{q-2} \det C = -r$ . Since  $g_0(x)$  is a PP of  $F_q$ ,  $\det M_{g_0} = -1$  in  $F_q$ , by Theorem 4.1.7. So,  $r \equiv 1 \pmod{p}$  and  $\gcd(r, q-1) = 1$ .

If  $q = p$ , then  $r = 1$  and so  $k \equiv 1 \pmod{p(p-1)}$ . Let  $q = p^n$  with  $n > 1$ . Since  $F_p$  is a subfield of  $F_q$  and  $g_0(x)$  is a PP of  $F_q$ ,  $g_0(x)$  is also a PP of  $F_p$ . So  $r \equiv 1 \pmod{p(p-1)}$ .

There is a nonnegative integer  $m$  such that  $r = mp(p-1)+1$ . Hence,  $k \equiv mp(p-1)+1 \pmod{p(q-1)}$ .

Finally, we write  $g(x) = 1+x+\dots+x^{mp(p-1)+1}$ . For  $1 \neq a \in F_q$ ,

$$g(a) = \frac{a^{mp(p-1)+2} - 1}{a - 1} = \frac{(a^2)^{mp(p-1)/2+1} - 1}{a - 1}.$$

Now, it is easy to see  $g(-1) = 0$ . Since  $g(x)$  is a PP of  $F_q$ ,  $g(a) \neq 0$  for all  $a \neq -1$ . So  $(a^2)^{mp(p-1)/2+1} - 1 \neq 0$  for all  $a \neq \pm 1$ . This implies that either  $\gcd(\frac{mp(p-1)}{2} + 1, \frac{q-1}{2}) = 1$  when  $q$  is odd, or  $\gcd(m+1, q-1) = 1$  when  $q$  is even.

Matthews [24] has proved that if  $q = p$  or  $q = p^2$  is odd, then  $f(x) = 1+x+\dots+x^k$  is a PP of  $F_q$  if and only if  $k \equiv 1 \pmod{p(q-1)}$ . Using Hermite's Criterion, one can easily get Matthew's result from Lemma 4.2.1.

Now we can modify Theorem B as follows.

**Theorem 4.2.2.** The set  $A(x^{k+1})$  with  $1 \leq k \leq q-2$  is an oval in  $PG(2, F_q)$ ,  $q$  even and  $q > 2$  if and only if  $1+x+\dots+x^k$  is a PP of  $F_q$ .

**Proof.** From the theorem before Lemma 4.2.1, we just need to show that if  $1+x+\dots+x^k$  is a PP of  $F_q$ , then  $\gcd(k, q-1) = 1 = \gcd(k+1, q-1)$ . But the last statement follows from Lemma 4.2.1 immediately. This completes the proof.



Now, we study some properties of the polynomial  $1+x+\dots+x^k$ . From now on, we always consider  $k = mp(p-1)+1 < q-1$ ,  $\gcd(mp(p-1)+1, q-1) = 1$  and either  $\gcd(\frac{mp(p-1)}{2}+1, \frac{q-1}{2}) = 1$  if  $q$  is odd or  $\gcd(m+1, q-1) = 1$  if  $q$  is even because of Lemma 4.2.1.

**Theorem 4.2.3.** Let  $q = 2^n$  with  $n \geq 2$ . Let  $f(x) = 1+x+\dots+x^k \in F_q[x]$  with  $k \leq q-3$ . Then  $f(x)$  is a PP of  $F_q$  if and only if  $g(x) = 1+x+\dots+x^{q-2-k}$  is a PP of  $F_q$ .

**Proof.**  $g(x) = 1+x+\dots+x^{q-2-k}$  is a PP of  $F_q$  if and only if  $h(x) = x+\dots+x^{q-2-k}$  is a PP of  $F_q$ .

For  $a \in F_q$  and  $a \neq 0, 1$ ,

$$\begin{aligned} h(a^{-1}) &= a^{-1} + a^{-2} + \dots + (a^{-1})^{q-2-k} = a^{-1} \frac{(a^{-1})^{q-2-k+1} + 1}{a^{-1} + 1} = \frac{(a^{-1})^{q-1} (a^{-1})^{-k-1} + 1}{a + 1} \\ &= \frac{a^{k+1} + 1}{a + 1} = 1 + a + \dots + a^k = f(a). \end{aligned}$$

Moreover,  $h(0) = 0$  and  $h(1) = \begin{cases} 0 & \text{if } k \text{ is even} \\ 1 & \text{if } k \text{ is odd} \end{cases}$ . Also,  $f(0) = 1$  and

$f(1) = \begin{cases} 1 & \text{if } k \text{ is even} \\ 0 & \text{if } k \text{ is odd} \end{cases}$ . So if  $k$  is odd,  $h(0) = f(1)$  and  $h(1) = f(0)$ .

From Lemma 4.2.1, if  $f(x)$  (or  $h(x)$ ) is a PP of  $F_q$ , then  $k$  is odd. Hence,  $f(x)$  is a PP of  $F_q$  if and only if  $h(x)$  is a PP of  $F_q$ . This completes the proof.

Combining Theorems 4.2.2 and 4.2.3, we have

Theorem 4.2.4. Let  $1 \leq k \leq q-3$ , where  $q > 2$  is even. The set  $A(x^{k+1})$  is an oval in  $PG(2, F_q)$  if and only if the set  $A(x^{q-k-1})$  is an oval in  $PG(2, F_q)$ .

Note that when  $q$  is odd, Theorem 4.2.3 is no longer true. For example,  $f(x) = 1+x$  is a PP of  $F_q$ . But  $g(x) = 1+x+\dots+x^{q-3}$  is not a PP of  $F_q$ , by Lemma 4.2.1, because  $q-3 \not\equiv 1 \pmod p$  for any odd prime  $p$ . In fact, we will see that if  $f(x) = 1+x+\dots+x^k$  is a PP of  $F_q$  and  $q$  is odd, then  $k < \frac{q-1}{2}$ . To prove this, we need the following

Lemma 4.2.5. Let  $C$  be an  $n \times n$  circulant matrix with the first row-vector  $(0, 1, \dots, 1, 0, \dots, 0)$ . If  $\frac{n}{l+1} \leq m < \frac{n}{l}$ , then the coefficient  $b_{l+1}$  of  $x^{n-(l+1)}$  in the  $m$ -terms characteristic polynomial of  $C$  is  $b_{l+1} = (-1)^l \frac{n}{l+1} \binom{l+m(l+1)-n}{l}$ .

Proof. Write  $a_0 = 0 = a_{m+1} = \dots = a_{n-1}$  and  $a_1 = 1 = \dots = a_m$ . Then  $b_{l+1} = \sum_{\tau} \text{sign}(\tau) a_{\tau(i_1)-i_1} \dots a_{\tau(i_{l+1})-i_{l+1}}$ . If  $a_{\tau(i)-i} = 1$  and  $\tau(i)-i \equiv j \pmod n$  with  $0 \leq j < n$ , then  $1 \leq j \leq m$ . So, if  $a_{\tau(i_1)-i_1} \dots a_{\tau(i_{l+1})-i_{l+1}} = 1$  appears in the expansion of  $b_{l+1}$ , then  $\tau$  is a cycle of length  $l+1$  because  $\frac{n}{l+1} \leq m < \frac{n}{l}$ . Then, we can write  $b_{l+1} = (-1)^l \sum_{\substack{0 \leq i_1 < i_2 < \dots < i_{l+1} \leq n-1 \\ 0 < i_{j+1}-i_j \leq m \text{ for } 1 \leq j \leq l \\ 0 \leq i_1 \leq m-1, 0 < i_1-i_{l+1}+n \leq m}} a_{i_1} \dots a_{i_{l+1}}$ .

Let  $a_{i_1} \dots a_{i_{l+1}}$  be a term in the expansion of  $b_{l+1}$ . And let  $t_j = i_{j+1} - i_j$  for  $1 \leq j \leq l$  and let  $t_{l+1} = i_1 - i_{l+1} + n$ . Then  $0 \leq i_1 \leq m-1$ ,  $\sum_{i=1}^{l+1} t_i = n$  and  $1 \leq t_i \leq m$  for  $1 \leq i \leq l+1$ . Since  $i_{l+1} \leq n-1$  and  $lm \leq n$ , we have  $m \geq t_{l+1} \geq \max \{i_1+1, n-lm\}$ . Fix  $0 \leq i_1 \leq m-1$  and max

$\{i_1+1, n-lm\} \leq t_{l+1} \leq m$ . Then  $\sum_{i=1}^l t_i = n-t_{l+1}$  with  $1 \leq t_i \leq m$  for all  $1 \leq i \leq l$ . The number of ordered  $l$ -tuples  $(t_1, \dots, t_l)$  satisfying  $\sum_{i=1}^l t_i = n-t_{l+1}$  and  $1 \leq t_i \leq m$  for  $1 \leq i \leq l$  is the coefficient of the term  $x^{n-t_{l+1}}$  in the expansion of  $(x+x^2+\dots+x^m)^l$  and thus is the coefficient of the term  $x^{n-t_{l+1}-l}$  in the expansion of  $(1+x+\dots+x^{m-1})^l$ . Since the coefficient of the term  $x^{n-t_{l+1}-l}$  equals the coefficient of the term  $x^{ml-n+t_{l+1}}$  in the expansion of  $(1+x+\dots+x^{m-1})^l$ , and  $0 \leq ml-n+t_{l+1} \leq m-1$ , we have  $s = \binom{l-1+ml-n+t_{l+1}}{l-1}$ . (Note that if  $0 \leq c \leq a$ , the coefficient of the term  $x^c$  in the expansion of  $(1+x+\dots+x^a)^b$  is  $\binom{b-1+c}{b-1}$ ).

Now, there are two cases.

Case 1.  $0 \leq i_1 \leq n-lm-1$ . The number of ordered  $(l+1)$ -tuples  $(t_1, \dots, t_l, t_{l+1})$  satisfying  $\sum_{i=1}^{l+1} t_i = n$ ,  $n-lm \leq t_{l+1} \leq m$ , and  $1 \leq t_i \leq m$  for  $1 \leq i \leq l$  is

$$\sum_{t_{l+1}=n-lm}^m \binom{l-1+ml-n+t_{l+1}}{l-1} = \sum_{i=0}^{m(l+1)-n} \binom{l-1+i}{i} = \binom{l+m(l+1)-n}{m(l+1)-n}.$$

So the number of nonzero terms  $a_{i_1} \dots a_{i_l} a_{i_{l+1}}$  with  $0 \leq i_1 \leq n-lm-1$  is  $(n-lm) \binom{l+m(l+1)-n}{m(l+1)-n}$ .

Case 2.  $n-lm \leq i_1 \leq m-1$ . The number of ordered  $(l+1)$ -tuples  $(t_1, \dots, t_l, t_{l+1})$  satisfying  $\sum_{i=1}^{l+1} t_i = n$ ,  $i_1+1 \leq t_{l+1} \leq m$  and  $1 \leq t_i \leq m$  for  $1 \leq i \leq l$  is

$$\sum_{t_{l+1}=i_1+1}^m \binom{l-1+ml-n+t_{l+1}}{l-1} = \sum_{i=0}^{m(l+1)-n} \binom{l-1+i}{i} - \sum_{i=0}^{ml-n+i_1} \binom{l-1+i}{i} = \binom{l+m(l+1)-n}{m(l+1)-n} - \binom{l+ml-n+i_1}{ml-n+i_1}.$$

So the number of nonzero terms  $a_{i_1} \dots a_{i_l} a_{i_{l+1}}$  with  $n-lm \leq i_1 \leq m-1$  is



$$\begin{aligned}
& \sum_{i_1=n-lm}^{m-1} \left[ \binom{l+m(l+1)-n}{m(l+1)-n} - \binom{l+m(l+1)-n+i_1}{m(l+1)-n+i_1} \right] = \binom{l+m(l+1)-n}{m(l+1)-n} - \sum_{i_1=n-lm}^{m-1} \binom{l+m(l+1)-n+i_1}{m(l+1)-n+i_1} \\
& = \binom{l+m(l+1)-n}{m(l+1)-n} - \sum_{i=0}^{m(l+1)-n-1} \binom{l+i}{i} = \binom{l+m(l+1)-n}{m(l+1)-n} - \binom{l+m(l+1)-n}{m(l+1)-n-1}
\end{aligned}$$

Combining Cases 1 and 2 together, we have

$$\begin{aligned}
b_{l+1} &= (-1)^l \left\{ (n-lm) \binom{l+m(l+1)-n}{m(l+1)-n} + \binom{l+m(l+1)-n}{m(l+1)-n} - \binom{l+m(l+1)-n}{m(l+1)-n-1} \right\} \\
&= (-1)^l \left\{ m \binom{l+m(l+1)-n}{l} - \binom{l+m(l+1)-n}{l+1} \right\} = (-1)^l \frac{n}{l+1} \binom{l+m(l+1)-n}{l}.
\end{aligned}$$

This completes the proof.

From the proof of Lemma 4.2.5, it is easy to see that if  $\frac{n}{l+1} \leq m < \frac{n}{l}$  for some positive integer  $l$ , then the coefficient of the term  $x^{n-i}$ ,  $1 \leq i \leq l$ , in the characteristic polynomial of an  $n \times n$  circulant matrix  $C$  with the first row-vector  $(0, 1, \dots, 1, 0, \dots, 0)$  is 0.   
 m-terms

**Theorem 4.2.6.** Let  $f(x) = x + \dots + x^{mp(p-1)+1} \in F_q[x]$  and let  $\frac{q-1}{l+1} \leq mp(p-1) + 1 < \frac{q-1}{l}$  for some positive integer  $l$ . If  $f(x)$  is a PP of  $F_q$ , then  $\binom{l+(l+1)(mp(p-1)+1)-(q-1)}{l} \equiv 0 \pmod{p}$ . In particular, if  $q$  is odd and  $f(x) = x + \dots + x^{mp(p-1)+1}$ ,  $1 \leq mp(p-1)+1 < q-1$ , is a PP of  $F_q$ , then  $1 \leq mp(p-1)+1 \leq \frac{q-1}{2}$ .

**Proof.** Consider the associated matrix  $M_f$  and its characteristic polynomial  $P_f$ .

By Lemma 4.2.5, the coefficient of the term  $x^{q-1-(l+1)}$  of  $P_f$  is

$(-1)^l \frac{q-1}{l+1} \binom{l+(mp(p-1)+1)(l+1)-(q-1)}{l}$ . If  $f(x) = x + \dots + x^{mp(p-1)+1}$  is a PP of  $F_q$ , then, from Theorem 4.1.7, it is 0. So  $\binom{l+(mp(p-1)+1)(l+1)-(q-1)}{l} \equiv 0 \pmod{p}$ .

Now, let  $q$  be odd and  $1 \leq mp(p-1)+1 < q-1$ . If  $mp(p-1)+1 \geq \frac{q-1}{2}$ , then the coefficient of the term  $x^{q-3}$  of  $P_f$  is  $\binom{1+(1+1)(mp(p-1)+1)-(q-1)}{1} = 2mp(p-1)-q+4 \equiv 4 \not\equiv 0 \pmod{p}$  and so  $f(x)$  is not a PP of  $F_q$ .

### 3. Binomial Permutations

One of the major problems in finite field theory is to characterize when a polynomial permutes a given field. Dickson characterized all polynomials which have degree  $\leq 5$ , and some polynomials of degree 6 (see [22]). In general, it seems very difficult to characterize a polynomial to be a PP, even if the polynomial has a simple form like a binomial  $f(x) = ax^k + bx^j$ . Lots of work have been done on binomials (see [4], [6], [25], [28]). In this section, we study some properties of binomials which are PPs on finite fields. First, we generalize a result obtained by Niederreiter and Robinson ([28]).

**Theorem 4.3.1.** Let  $q = p^n$  be odd. Let  $1 \leq m \leq \frac{q-1}{2}$ . Then the polynomial  $f(x) = ax^{(q-1)/2+m} + bx^m \in F_q[x]$  with  $ab \neq 0$  is a PP over  $F_q$  if and only if  $\gcd(m, \frac{q-1}{2}) = 1$  and either  $\eta(b^2 - a^2) = 1$  when  $m$  is odd or  $\eta(b^2 - a^2) = -1$  when  $m$  is even, where  $\eta$  is the quadratic character of  $F_q$ .

Proof. From Hermite's Criterion, if  $f(x)$  is a PP of  $F_q$ ,  $f(x)$  has only one root in  $F_q$ . Since  $c^{(q-1)/2} = \pm 1$  for all  $c \in F_q^\times$ , the necessary and sufficient condition that  $f(x) = ax^{(q-1)/2+m} + bx^m = ax^m(x^{(q-1)/2} + a^{-1}b)$  have only one root on  $F_q$  is that  $a^{-1}b \neq \pm 1$ . It is equivalent to  $\eta(b^2 - a^2) \neq 0$ . From now on, we assume  $a^{-1}b \neq \pm 1$ .

Let  $g$  be a primitive element of  $F_q$  and let  $\gcd(m, \frac{q-1}{2}) = d$ . If  $d > 1$ , we have  $f(g^{2((q-1)/2d+1)}) = f(g^2)$  and so  $f(x)$  is not a PP of  $F_q$ . Hence,  $\gcd(m, \frac{q-1}{2}) = 1$  is a necessary condition for  $f(x)$  to be a PP of  $F_q$ . Now, for  $u \in F_q$ ,

$$f(u) = \begin{cases} 0 & \text{if } u = 0 \\ u^m(a+b) & \text{if } u \text{ is a square} \\ u^m(b-a) & \text{if } u \text{ is a nonsquare.} \end{cases}$$

We have the following two cases.

Case 1.  $m$  is odd. Then for  $u \in F_q^\times$ ,  $u^m$  is a square of  $F_q$  if and only if  $u$  is a square of  $F_q$ . Moreover,  $\gcd(m, \frac{q-1}{2}) = 1$  implies  $\gcd(m, q-1) = 1$  and so  $u^m \neq v^m$  whenever  $u \neq v$ . So  $f(x)$  is a PP of  $F_q$  if and only if  $\gcd(m, \frac{q-1}{2}) = 1$  and exactly one of  $f(u)$  and  $f(v)$  is a square of  $F_q$  whenever  $\eta(u) \neq \eta(v)$ . The last statement is equivalent to



that  $\gcd(m, \frac{q-1}{2}) = 1$  and  $\eta(b+a) = \eta(b-a)$ . So  $f(x) = ax^{(q-1)/2+m} + bx$  is a PP of  $F_q$  if and only if  $\gcd(m, \frac{q-1}{2}) = 1$  and  $\eta(b^2 - a^2) = 1$ .

Case 2.  $m$  is even. Then  $\gcd(m, \frac{q-1}{2}) = 1$  implies that  $q \equiv 3 \pmod{4}$  and that  $\gcd(m, q-1) = 2$ . Hence,  $u^m \neq v^m$  whenever  $u \neq v \in F_q$  and both of them are either squares or non-squares. So  $f(x)$  is a PP of  $F_q$  if and only if  $\gcd(m, \frac{q-1}{2}) = 1$  and  $\eta(f(u)) \neq \eta(f(v))$  whenever  $\eta(u) \neq \eta(v)$  in  $F_q^\times$ . From the expression for  $f(u)$ , the last statement is equivalent to that  $\gcd(m, \frac{q-1}{2}) = 1$  and  $\eta(b+a) \neq \eta(b-a)$  because  $\eta(u^m) = 1 = \eta(v^m)$  for all  $u, v \in F_q^\times$ . Hence, the necessary and sufficient condition for  $f(x) = ax^{(q-1)/2+m} + bx^m$  to be a PP of  $F_q$  is that  $\gcd(m, \frac{q-1}{2}) = 1$  and  $\eta(b^2 - a^2) = -1$ . This completes our proof.

Now, we consider the general case:  $f(x) = ax^k + bx^l \in F_q[x]$ ,  $1 \leq l < k \leq q-2$ . We need the following

Lemma 4.3.2. Let  $K$  be a field and let  $a, b \in K$ . Let  $0 < k < n$  be an integer. Let  $C$  be the  $n \times n$  circulant matrix with the first row-vector  $(b, 0, \dots, 0, a, 0, \dots, 0)$ . If  $d = \gcd(k, n)$ , then  $\det C = (b^{n/d} - (a)^{n/d})^d$ .

$\uparrow$   
 the  $k+1$ st position

Proof. Let  $(\text{sign } \sigma) a_{1, \sigma(1)} \dots a_{n, \sigma(n)}$  be a non-zero term in the expansion of  $\det C$ . Then for  $1 \leq i \leq n$ ,  $a_{i, \sigma(i)} = a$  or  $b$ . If  $a_{i, \sigma(i)} = b$ , then  $\sigma(i) = i$ . So  $\text{sign } \sigma$  is determined by those  $i$  with  $a_{i, \sigma(i)} = a$ .

Suppose that  $a_{i_0, \sigma(i_0)} = a$ . Then  $\sigma(i_0) \equiv i_0 + k \pmod n$ . This implies  $a_{\sigma(i_0), \sigma^2(i_0)} = a$  and so  $\sigma^2(i_0) = \sigma(\sigma(i_0)) \equiv i_0 + 2k \pmod n$ . Continuing this process, we finally get  $\sigma^{n/d}(i_0) = i_0$ . So we get a cycle  $(i_0, \sigma(i_0), \dots, \sigma^{n/d-1}(i_0))$  of length  $\frac{n}{d}$ . Note that any two such cycles  $(i_0, \sigma(i_0), \dots, \sigma^{n/d-1}(i_0))$  and  $(i_1, \sigma(i_1), \dots, \sigma^{n/d-1}(i_1))$  are not disjoint if and only if  $i_1 \equiv i_0 \pmod d$ . So  $\sigma$  can be expressed as a product of disjoint cycles which all have length  $\frac{n}{d}$ . When  $\sigma$  is a product of  $l$  disjoint such cycles,

$$(\text{sign } \sigma) a_{1, \sigma(1)} \dots a_{n, \sigma(n)} = (-1)^{l(n/d-1)} a^{nl/d} b^{n-nl/d} = (-1)^l (-a)^{nl/d} b^{n(d-l)/d}.$$

Finally, for each  $1 \leq l \leq d$ , there are exactly  $\binom{d}{l}$  permutations  $\sigma$  such that

$$(\text{sign } \sigma) a_{1, \sigma(1)} \dots a_{n, \sigma(n)} = (-1)^l (-a)^{nl/d} b^{n(d-l)/d}$$

because we can choose  $1 \leq i_0 \leq d$ , where  $i_0$  is as in the last paragraph the first element in each cycle of  $\sigma$ . So

$$\det C = \sum_{l=0}^d \binom{d}{l} (-1)^l (-a)^{nl/d} b^{n(d-l)/d} = (b^{n/d} - (-a)^{n/d})^d.$$

This completes the proof.

This lemma is a generalization of Ore's result (see [30]). Using this lemma, we have the following necessary condition.

Theorem 4.3.3. Let  $f(x) = ax^k + bx^l \in F_q[x]$  with  $1 \leq l < k \leq q-2$ . Let  $d = \gcd(k-1, l-1, q-1)$  and let  $m = \gcd(\frac{k-l}{d}, \frac{q-1}{d})$ . If  $f(x)$  is a PP of  $F_q$ , then

$$\Psi_{(q-1)/d} \left( (-1)^{((q-1)/d-1)(l-1)/d} (b^{(q-1)/md} - (-a)^{(q-1)/md})^m \right) = 1,$$

where  $\Psi_{(q-1)/d}$  is any character of  $F_q$  of order  $\frac{q-1}{d}$ .

Proof. Let  $C$  be the  $\frac{q-1}{d} \times \frac{q-1}{d}$  circulant matrix with the first row-vector  $(0, \dots, 0, b, 0, \dots, 0, a, 0, \dots, 0)$ . Let  $A$  be the  $\frac{q-1}{d} \times \frac{q-1}{d}$  circulant matrix with the first row-vector  $(0, \dots, 0, b, 0, \dots, 0, a, 0, \dots, 0)$ . Then we have

$\begin{array}{cc} \uparrow & \uparrow \\ (l-1)/d \text{ th place} & (k-1)/d \text{ th place} \end{array}$

$\begin{array}{c} \uparrow \\ (k-l)/d \text{ th place} \end{array}$

$$\det C = (-1)^{((q-1)/d-1)(l-1)/d} \det A = (-1)^{((q-1)/d-1)(l-1)/d} (b^{(q-1)/md} - (-a)^{(q-1)/md})^m$$

by Lemma 4.3.2. If  $f(x)$  is a PP of  $F_q$ , then

$$\Psi_{(q-1)/d} \left( (-1)^{((q-1)/d-1)(l-1)/d} (b^{(q-1)/md} - (-a)^{(q-1)/md})^m \right) = 1$$

by Theorem 4.1.6.

In this theorem, if  $l = 1$  and  $d = k-1$ , then  $m = 1$  and

$$\Psi_{(q-1)/d} \left( (-1)^{((q-1)/d-1) \cdot 0} (b^{(q-1)/d} - (-a)^{(q-1)/d}) \right) = 1$$

implies  $b^{(q-1)/d} - (-a)^{(q-1)/d} = c^{(q-1)/d}$  for some  $c \in F_q$ .



Theorem 4.3.3 is a necessary condition for a binomial to be a PP of  $F_q$ . Now, we give a sufficient condition.

**Theorem 4.3.4.** Let  $f(x) = bx^{k+1} + ax \in F_q[x]$  with  $k \mid (q-1)$ . Write  $q-1 = km$ . Let  $g(x) = ((b+a)x-a)^m - b^m$ . If  $a \neq -b$  and  $g(x) \mid (x^k-1)$ , then  $f(x)$  is a PP of  $F_q$ .

**Proof.** If  $b = 0$ , then  $f(x) = ax$  is a PP of  $F_q$  for  $a \in F_q^\times$  and thus the theorem holds. So, we consider  $b \neq 0$ . Moreover,  $f(x) = bx^{k+1} + ax$  is a PP of  $F_q$  if and only if  $x^{k+1} + b^{-1}ax$  is a PP of  $F_q$ . Hence, it is enough to prove this theorem in the case  $b = 1$ .

Since  $a \neq -1$ ,  $g(x)$  had degree  $m$ . Moreover,  $g(x) \mid (x^k-1)$  implies that  $g(x)$  has  $m$  distinct roots in  $F_q$ . Let  $\zeta$  be a primitive element of  $F_q$ . Then each root of  $g(x)$  is of the form  $\zeta^{jm}$  for some  $0 \leq j < k$ . Say  $\zeta^{j_1 m}, \dots, \zeta^{j_m m}$  are all distinct roots of  $g(x)$ . So, for each  $1 \leq i \leq m$ ,  $(1+a)\zeta^{j_i m} - a$  is a root of  $x^m - 1$ . We can write  $(1+a)\zeta^{j_i m} - a = \zeta^{t_i k}$  for some  $0 \leq t_i \leq m-1$ . Since all  $\zeta^{j_i m}$  are distinct,  $\zeta^{t_i k}$  are all distinct. So,  $\zeta^{t_1 k}, \dots, \zeta^{t_m k}$  are all distinct roots of  $x^m - 1$ .

Write  $1 + a = \zeta^{s+s_0 m}$ . Then  $\zeta^{t_i k} + a = (1+a)\zeta^{j_i m} = \zeta^{s+(s_0+j_i)m}$  for  $1 \leq i \leq m$ . For  $u \in F_q^\times$ , write  $u = \zeta^{t_u + l_u m}$  with  $0 \leq t_u \leq m-1$  and  $0 \leq l_u \leq k-1$ . Then we have  $f(u) = u(u^k + a) = \zeta^{t_u + l_u m} (\zeta^{t_u k} + a) = \zeta^{t_u + s + (s_0 + j_u + l_u)m}$  for some  $0 \leq j_u \leq k-1$ . So if  $u_1$  and  $u_2$  are in the same coset of  $F_q^\times / \langle \zeta^m \rangle$ , then  $t_{u_1} = t_{u_2}$  and so  $j_{u_1} = j_{u_2}$ . But  $l_{u_1} \neq l_{u_2}$  whenever  $u_1 \neq u_2$ . So  $f(u_1) \neq f(u_2)$  if  $u_1 \neq u_2$  are in the same coset of  $F_q^\times / \langle \zeta^m \rangle$ . If  $u_1$  and  $u_2$  are in different cosets of  $F_q^\times / \langle \zeta^m \rangle$ , then  $t_{u_1} \neq t_{u_2}$  and so  $f(u_1) \neq f(u_2)$ . Moreover  $f(0) = 0$ . So  $f(x) = x^{k+1} + ax$  is a PP of  $F_q$ .

Note that  $g(x) \mid (x^k-1)$  implies  $m \leq k$  and so  $k \geq \sqrt{q-1}$ . For  $q = p$ , we have

Theorem 4.2.5. Let  $p$  be an odd prime,  $k \leq \sqrt{p-1}$  and  $k \nmid (p-1)$ . Then  $f(x) = ax^{k+1}+bx \in F_p[x]$  is a PP of  $F_p$  if and only if either  $a = 0$  and  $b \neq 0$  or  $b = 0$ ,  $a \neq 0$  and  $\gcd(k+1, p-1) = 1$ .

Proof. Write  $p-1 = kl$  and write  $p-1 = m(k+1)+r$  with  $0 \leq r \leq k$ . If  $s$  and  $t$  are nonnegative integers such that  $s+t = m+r$  and  $s(k+1)+t = i(p-1)$  for some positive integer  $i$ , then  $(i-1)(p-1) = (s-m)k$  and so  $s = m+(i-1)l$ . This implies  $0 \leq t = r-(i-1)l$ . Since  $k \leq \sqrt{p-1}$ ,  $l \geq \sqrt{p-1}$  and  $r \leq \sqrt{p-1}$ . So  $i = 1$  or  $2$ . If  $i = 2$ , then  $t = 0$  and so  $r = l = k$ . but in this case,  $p-1 = m(k+1)+r = (m+1)k+m$  implies  $k \mid m$ . This is impossible because either  $m > 0$  implies  $m(k+1)+r > p-1$  or  $m = 0$  implies  $p-1 = r = k \leq \sqrt{p-1}$ . So  $i = 1$  and thus  $s = m$  and  $t = r$ .

Now, we consider  $(ax^{k+1}+bx)^{m+r}$ . From above, we see that the coefficient of the term  $x^{p-1}$  in the reduction of  $(ax^{k+1}+bx)^{m+r} \bmod (x^p-x)$  is  $\binom{m+r}{m} a^m b^r$ . Since  $m+r < p$ ,  $\binom{m+r}{m} a^m b^r = 0$  implies either  $a = 0$  or  $b = 0$ .

If  $f(x) = ax^{k+1}+bx$  is a PP of  $F_q$ ,  $\binom{m+r}{m} a^m b^r = 0$ , by Hermite's Criterion, and so either  $a = 0$  or  $b = 0$ . In this case, we have either that  $a = 0$  implies  $b \neq 0$  or that  $b = 0$  implies  $a \neq 0$  and  $\gcd(k+1, p-1) = 1$ . This proves the necessary part.

Finally, it is not difficult to see the sufficient part holds as well.

## REFERENCES

1. A.O.L. Atkin, L. Hay and R. G. Larson, "Enumeration and construction of pandiagonal Latin squares of prime order," *Comp. and Math. with Appls.*, Vol. 9, No. 2 (1983), 267-292.
2. A. Bruen and R. Dixon, "The n-queens problem," *Discrete Math.* 12 (1975), 393-395.
3. R. H. Bruck, "Finite nets, I: numerical invariants," *Canad. J. Math.* 3 (1951), 94-107.
4. L. Carlitz, "Some theorems on permutation polynomials," *Bull. Amer. Math. Soc.* 68 (1962), 120-122.
5. L. Carlitz, "A note on the Betti-Mathieu group," *Portugal. Math.* 22 (1963), 121-125.
6. L. Carlitz, "Permutations in finite fields," *Acta Sci. Math. Szeged* 24 (1963), 196-203.
7. H.S.M. Coxeter and W.O.J. Moser, Generators and Relations for Discrete Groups, Springer-Verlag, New York, 4th ed., 1979.
8. P.J. Davis, Circulant Matrices, Wiley, New York, 1979.
9. P. Dembowski, Finite Geometries, Springer, Berlin, 1968.
10. P. Dembowski and T. Ostrom, "Planes of order  $n$  with collineation groups of order  $n^2$ ," *Math. Zeit.* 103 (1968), 239-258.
11. J. Dénes and A. D. Keedwell, Latin Squares and Their Applications, Academic Press, New York, 1974.
12. L. E. Dickson, Linear Groups with an Exposition of the Galois Field Theory, Teubner Leipzig, 1901; Dover, New York, 1958.
13. A. L. Dulmage, D. M. Johnson and N. S. Mendelsohn, "Orthomorphisms of groups and orthogonal Latin squares, I," *Canad. J. Math.* 13 (1961), 356-372.
14. A. B. Evans, "Generating orthomorphisms of  $GF(q)^+$ ," *Discrete Math.* 63 (1987), 21-26.



15. A. B. Evans, "Orthomorphisms of  $Z_p$ ," *Discrete Math.* 64 (1987), 147-156.
16. W. T. Federer and A. Hedayat, "On the nonexistence of Knut Vik designs for all even orders," *Ann. Statistics* 3 (1975) 445-457.
17. E. Gergely, "A remark on doubly diagonalized orthogonal latin squares," *Discrete Math.* 10 (1974), 185-188.
18. M. Hall, Jr., Combinatorial Theory, Blaisdell Publ. Co., Waltham, Mass., 1st ed., 1967.
19. A. Hedayat, "A complete solution to the existence and nonexistence of Knut Vik designs and orthogonal Knut Vik designs," *J. Comb. Thoery (A)* 22 (1977), 331-337.
20. O. Kempthorne, Design and Analysis of Experiments, Wiley, New York, 1952.
21. N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer-Verlag, New York-Berlin-Heidelberg-Tokyo, 2nd ed., 1984.
22. R. Lidl and H. Niederreiter, Finite Fields, *Encyclo. Math. and Appls.*, Vol. 20, Addison-Wesley, Reading, Mass., 1983 (now distributed by Cambridge Univ. Press).
23. H. B. Mann, "The construction of orthogonal Latin squares," *Ann. Math. Statist.* 13 (1942), 418-423.
24. R. W. Matthews, Permutation Polynomials in One and Several Variables, Ph.D. Thesis, Univ. of Tasmania, Hobart, 1982.
25. R. A. Mollin and C. Small, "On permutation polynomials over finite fields," *Internat. J. Math and Math. Sci.* 10 (1987), 535-543.
26. G. L. Mullen and H. Niederreiter, "The structure of a group of permutation polynomials," *J. Austral. Math. Soc. (Series A)* 38 (1985), 164-170.
27. H. Niederreiter and K. H. Robinson, "Bol loops of order pq," *Math. Proc. Camb. Phil. Soc.* 89 (1981), 241-256.
28. H. Niederreiter and K. H. Robinson, "Complete mappings of finite fields," *J. Austral. Math. Soc. (Series A)* 33 (1982), 197-212.
29. O. Ore, "Contributions to the theory of finite fields," *Trans. Amer. Math. Soc.* 36 (1934), 243-274.
30. O. Ore, "Some studies on cyclic determinants," *Duke Math. J.* (1951), 343-354.
31. L. J. Paige, "Neofields," *Duke Math. J.* 16 (1949), 39-60.

32. L. J. Paige, "Complete mappings of finite groups," *Pacific J. Math.* 1 (1951), 111-116.
33. S. Perlis, Theory of Matrices, Addison-Wesley Press Inc., 1952.
34. G. Pólya, "Über die "doppelt-periodischen" Lösungen des n-Damenproblem," *Mathematische Unterhaltungen und Spiele* (Edited by W. Ahrens), Teubner, Leipzig, 2nd ed. (1918), 364-374.
35. G. Raussnitz, *Math. Naturw. Ber. Ungarn* 1 (1882/83), 266-278.
36. B. Rosser and R. J. Walker, "Magic squares," *Published Paper and Supplement, Section 6, 729-753*, Cornell Univ. Library (typed manuscript).
37. J. J. Rotman, The Theory of Groups, an Introduction, Allyn and Bacon Inc., Boston, 2nd ed., 1973.
38. W. M. Schmidt, Equations over Finite Fields, *Lecture Notes in Math.*, Vol. 536, Springer-Verlag, Berlin-Heidelberg-New York, 1976.
39. E. Stern, "Number of magic squares belonging to certain classes," *Am. Math. Monthly* 46 (1939), 555-581.
40. D. Wan, "On a problem of Niederreiter and Robinson about finite fields," *J. Austral. Math. Soc. (Series A)* 41 (1986), 336-338.

## VITA

Name: Wun-Seng Chou

Date of Birth: September 9, 1950

Degrees: Bachelor of Science, Mathematics  
Fu-Jen Catholic University, Taiwan, R.O.C., 1974

Master of Arts, Mathematics  
Fu-Jen Catholic University, Taiwan, R.O.C., 1976

Doctor of Philosophy, Mathematics  
The Pennsylvania State University, Pennsylvania, U.S.A.

- Publications:
1. Permutation Polynomials on Finite Fields and Combinatorial Applications, Ph.D. Thesis, The Pennsylvania State University (supervised by Gary L. Mullen).
  2. Formulas for counting chains in multisets, submitted.
  3. Binomial permutations of finite fields, Bull. Austral. Math. Soc., 38 (1988), 325-327.
  4. (With J. Gomez-Calderon and G. L. Mullen), Value sets of Dickson polynomials over finite fields, J. Number Theory, 30 (1988), 3, 34-344.

Memberships: American Mathematical Society since 1984  
Mathematical Association of America since 1989