ON POLYNOMIALS OVER FINITE FIELDS WITH PARTICULAR VALUE SETS

by

TUĞBA YESİN

**Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science**

**Sabancı University
January 2017**

ON POLYNOMIALS OVER FINITE FIELDS WITH PARTICULAR VALUE SETS

APPROVED BY

Prof. Dr. Alev Topuzoğlu ....
(Thesis Supervisor)

Assoc. Prof. Dr. Cem Güneri ....

Asst. Prof. Dr. Seher Tutdere ....

DATE OF APPROVAL: 6/1/2017

ON POLYNOMIALS OVER FINITE FIELDS WITH PARTICULAR VALUE SETS

Tuğba Yesin

Mathematics, Master Thesis, January 2017

Thesis Supervisor: Prof. Dr. Alev Topuzoğlu

Keywords: finite fields, value sets of polynomials, permutation polynomials, Carlitz rank

Abstract

A classical result on value sets of non-permutation polynomials over finite fields is due to Wan (1993). Denoting the cardinality of the value set of $f \in \mathbb{F}_q[x]$ by $|V_f|$, Wan's result gives the upper bound $|V_f| \leq q - \lceil \frac{q-1}{d} \rceil$, where d is the degree of f. A proof of this bound due to Turnwald, which was obtained by the use of symmetric polynomials is given in Chapter 2. A generalization of this result was obtained by Aitken that we also describe here. The work of Aitken focuses on value sets of pairs of polynomials in $\mathbb{F}_q[x]$, in particular, he studies the size of the intersection of their value sets. We present pairs of particular polynomials whose value sets do not only have the same size but are actually identical.

Clearly, a permutation polynomial f of $\mathbb{F}_q[x]$ satisfies $|V_f| = q$. In Chapter 3, we discuss permutation behaviour of pairs of polynomials in $\mathbb{F}_q[x]$.

SONLU CİSİMLER ÜZERİNDEKİ ÖZEL DEĞER KÜMELERİNE SAHİP POLİNOMLAR HAKKINDA

Tuğba Yesin

Matematik, Yüksek Lisans Tezi, Ocak 2017

Tez Danışmanı: Prof. Dr. Alev Topuzoğlu

Anahtar Kelimeler: sonlu cisimler, polinomların görüntü kümesi, permütasyon polinomu, Carlitz mertebesi,

Özet

Sonlu cisimler üzerinde permütasyon olmayan polinomların değer kümeleri hakkındaki klasik sonuçlardan birisi Wan' a aittir (1993). Derecesi $d > 0$ olan bir $f \in \mathbb{F}_q[x]$ polinomunun değer kümesinin kardinalitesini, $|V_f|$ ile gösterirsek, Wan' ın sounucu $|V_f| \leq q - \lceil \frac{q-1}{d} \rceil$, üst sınırını verir. Bu sonucun Turnwald tarafından simetrik polinomlar kullanılarak elde edilen kanıtı Bölüm 2 'de verilmiştir. Wan' ın üst sınırının Aitken tarafından elde edilen genellemesini de burada anlattık. Aitken'in çalışması $\mathbb{F}_q[x]$ içindeki polinom çiftlerinin değer kümeleri üzerine odaklanır, özel olarak, onların değer kümelerinin kesişimlerinin büyüklüğü üzerinedir. Biz bu çalışmada değer kümeleri aynı olan bazı polinom çiftlerini sunduk.

Bir permütasyon polinomu olan $f \in \mathbb{F}_q[x]$, $|V_f| = q$ eşitliğini sağlar. Bölüm 3'de, polinom çiftlerinin permütasyon olma yönündeki davranışlarını inceledik.

To my family

Acknowledgments

First of all, I would gratefully like to thank my supervisor Prof. Dr. Alev Topuzoğlu for her encouragement and motivation. Her understanding and excellent vision has helped me to find my way throughout my studies at Sabanci University.

I would also like to thank the members of my thesis committee, Assoc. Prof. Dr. Cem Güneri and Asst. Prof. Dr. Seher Tutdere, for reviewing my master thesis.

I am also grateful to my firends in Mathematics program and to Melike Efe, Kübra Serpen Ínci, Tekgül Kalayci for their invaluable friendship and encouragement.

Finally, I would like to thank my family with all my heart for all their love and encouragement that I received all through my life.

Table of Contents

Abstract **iv**

Özet **v**

Acknowledgments **vii**

1 Introduction **1**

1.1 Introductory remarks 1

1.2 Preliminaries 3

2 On Value Sets of non-permutation polynomials **7**

2.1 Wan's upper bound 7

2.2 A generalization by Aitken 12

2.3 On value sets of pairs of particular polynomials 15

3 Permutation behaviour of pairs of polynomials **25**

3.1 On differences 25

3.2 A special case 31

Bibliography **36**

CHAPTER 1

Introduction

1.1. Introductory remarks

Throughout this thesis, $\mathbb{F}_q$ denotes the finite field with q elements, where $q = p^r$, and p is a prime number. We denote the multiplicative group of $\mathbb{F}_q$ by $\mathbb{F}_q^*$.
We shall be studying value sets of polynomials over $\mathbb{F}_q$. Recall that the value set V_f of a polynomial $f \in \mathbb{F}_q[x]$ is defined as $V_f = \{f(c) : c \in \mathbb{F}_q\}$. We denote the cardinality of V_f by $|V_f|$.

Value sets of polynomials over finite fields attracted significant interest since early 1950s. A wide range of results have been obtained, particularly on the size of $|V_f|$, where f is a polynomial in $\mathbb{F}_q[x]$ of degree d. We refer the reader to Section 8.2 of [21], Section 8.3 of [18], to the papers [17], [19] and the references therein for many interesting results.

In this thesis we shall be concerned with some of the classical bounds for $|V_f|$ as well as a generalization of Wan's bound. We shall also study pairs of polynomials in relation to their value sets.

In section 1.2 we introduce basic definitions, concepts and the notation that we use.

Chapter 2 starts with Wan's bound on value sets of non-permutation polynomials. This theorem is interesting since it shows that, among the polynomials of the same degree d, there are no polynomials $f \in \mathbb{F}_q[x]$ such that $|V_f|$ lies between q and $q - \lceil \frac{q-1}{d} \rceil$, where $\lceil s \rceil$ denotes the smallest integer $\geq s$. We note that when d is small, permutations and non-permutation polynomials are for apart in terms of the size of their value sets. A proof, given later by Turnwald, uses symmetric polynomials, which we describe in detail. A result by Cusick and Müller determining polynomials that attain Wan's upper bound is also given in Chapter 2. Lower bounds for $|V_f|$ in terms of the degree d of f is known, see for example Theorem 2.1.7 below, which is due to Wan, Shiue and Chen. Wan's bound was generalized by Aitken in [1]. Aitken uses multivariable polynomials to study the size of the intersection of value sets of pairs of polynomials. An extension of this idea to images of subsets of $\mathbb{F}_q$ is also considered in [1], which we outline in Section 2.2.

Polynomials of the form $f+x$, where f is a permutation polynomial of Carlitz rank n were studied in [13]. The aim was to give conditions on q, n to ensure $f+x$ to be also a permutation of $\mathbb{F}_q$, in other words to guarantee f to be a complete mapping of $\mathbb{F}_q$. We also consider particular polynomials $f+x$ and $g+x$, which are not permutations and we show that $V_{f+x} = V_{g+x}$.

Chapter 3 deals with permutation behaviour of pairs of polynomials $f(x)$ and $g(x) = f(x) + h(x)$. We present the interesting result of Cohen, Mullen, Shiue [7] on the minimum possible degree of h when f, g are permutations of $\mathbb{F}_q$ and p is sufficiently large with respect to the $deg(f(x)) = deg(g(x)) = d \geq 3$. The proof extensively uses Dickson polynomials of the first kind. A corollary of this result is the Chowla-Zassenhaus conjecture which was first proven by Cohen in [8]. The work in [13], which was mentioned above, can be regarded as a variant of Cohen's Theorem [8]. We end this thesis by giving details of the proof of a result in [13], about V_{f+x}, where f is a permutation polynomial of Carlitz rank 2.

1.2. Preliminaries

We recall that the value set V_f of $f \in \mathbb{F}_q[x]$ is $V_f = \{f(c) : c \in \mathbb{F}_q\}$. Let $f \in \mathbb{F}_q$. For a subset $S \subset \mathbb{F}_q$, we put $f(S) = \{f(c) : c \in S\}$. Hence $V_f = f(\mathbb{F}_q)$. A polynomial $f \in \mathbb{F}_q[x]$ is a *permutation polynomial* if it induces a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$. Clearly $|V_f|$ takes its maximum value when f is a permutation polynomial, i.e., $|V_f| = q$ in this case.

The next result is well-known, see for instance [15], and shows that any self-mapping of $\mathbb{F}_q$ can be expressed as a polynomial in $\mathbb{F}_q[x]$ of degree $< q$.

Lemma 1.2.1 *For any function $\phi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, there exists a unique polynomial $f(x)$ over $\mathbb{F}_q$ of degree $\leq q-1$, such that the associated polynomial function $f : c \longmapsto f(c)$ satisfies $\phi(c) = f(c)$ for every $c \in \mathbb{F}_q$.*

Dickson polynomials play an important role in the study of finite fields. We shall also be using them in Chapter 3. Dickson polynomials may be defined over a ring.

Definition 1.2.1 *Let R be a ring. For $a \in R$ we define the Dickson polynomial $D_m(a,x)$ of the first kind of degree m over R by,*

$$D_m(a,x) = \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-j} \binom{m-j}{j} (-a)^j x^{m-2j}. \tag{1.1}$$

The Dickson polynomial $E_m(x,a)$ of the second kind of degree m is defined as

$$E_m(x,a) = \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m-j}{j} (-a)^j x^{m-2j},$$

for $a \in R$.

A Dickson polynomial of the first kind also satisfies, see [14],

$$x_1^m + x_2^m = \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-j} \binom{m-j}{j} (-x_1x_2)^j (x_1+x_2)^{m-2j},$$

and thus

$$x_1^m + x_2^m = D_m(x_1+x_2, x_1x_2),$$

where x_1, x_2 are indeterminates.

If we let $x_1 = x$, and $x_2 = \frac{a}{x}$, then we obtain the so-called functional equation,

$$D_m(x + \frac{a}{x}, a) = x^m + \frac{a^m}{x^m}. \tag{1.2}$$

The following theorems are from [14] which give conditions for $D_m(a, x)$ to be a permutation polynomial.

Theorem 1.2.2 *The monomial $D_m(x, 0) = x^m$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $gcd(m, q-1) = 1$.*

Theorem 1.2.3 *Let $a \in \mathbb{F}_q^*$. The Dickson polynomial $D_m(x, a)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $gcd(n, q^2-1) = 1$.*

When a Dickson polynomial $D_m(x, a)$ is not a permutation polynomial, it is possible to determine the value set of $D_m(x, a)$, as we state in the theorem below, which we take from [6].

Theorem 1.2.4 *Let $D_m(x, a)$ be a Dickson polynomial of $\mathbb{F}_q$. Suppose q is odd with $2^r|(q^2-1)$ but $2^{r+1} \nmid (q^2-1)$. Then for each $m \geq 1$ and each $a \in \mathbb{F}_q^*$ we have*

$$|V_{D_m(x,a)}| = \frac{q-1}{2gcd(m, q-1)} + \frac{q+1}{2gcd(m, q+1)} + \alpha,$$

where

$$\alpha = \begin{cases} 1 & if \;\; 2^{r-1}|d \;\, but \;\, 2^r \nmid d \;\, and \;\, a \;\, is \;\, a \;\, non\text{-}square, \\ \frac{1}{2} & if \;\; 2^t|d \;\, but \;\, 2^{t+1} \nmid d \;\, and \;\, 1 \leq t \leq r-2, \\ 0 & if \;\; otherwise. \end{cases}$$

Corollary 1.2.5 *If $gcd(m_1, q^2-1) = gcd(m_2, q^2-1)$, then $|V_{D_{m_1}(x,a)}| = |V_{D_{m_2}(x,a)}|$.*

Theorem 1.2.6 *Suppose q is even. Then for each $n \geq 1$, and each $a \in \mathbb{F}_q^*$ we have*

$$|V_{D_m(x,a)}| = \frac{q-1}{2gcd(m,q-1)} + \frac{q+1}{2gcd(m,q+1)}.$$

Polynomials over finite fields are often studied in relation to their degrees. A rather recent concept, concerning permutation polynomials of $\mathbb{F}_q$ was introduced in [2]. We first recall that the set of all permutation polynomials in $\mathbb{F}_q[x]$ of degree $< q$ forms a group under the operation of composition and subsequent reduction mod $x^q - x$. Clearly this group is isomorphic to S_q.

We also recall the following well-known result of Carlitz [4].

Theorem 1.2.7 *The group of permutation polynomials can be generated by the monomial x^{q-2} and linear polynomials $ax+b$, $a, b \in \mathbb{F}_q$, $a \neq 0$.*

Proof of this result immediately follows from the equation

$$P_3(x) = (((-x)^{q-2}+1)^{q-2}+1)^{q-2}+1 \in \mathbb{F}_q[x],$$

showing that the transposition $(0,1)$, and hence any transposition $(0,a)$, $a \in \mathbb{F}_q$ can be expressed as a composition of the monomials x^{q-2} and linear polynomials.

Consequently, as pointed out in [10], with $P_0(x) = a_0x + a_1$, any permutation polynomial $f(x)$ of $\mathbb{F}_q$ can be represented by a polynomial of the form

$$P_n(x) = P_n(a_0, a_1, \ldots, a_{n+1}; x) = (...((a_0x+a_1)^{q-2}+a_2)^{q-2}...a_n)^{q-2}+a_{n+1}, \quad (1.3)$$

$n \geq 0$, where $a_1, a_{n+1} \in \mathbb{F}_q$, $a_i \in \mathbb{F}_q^*$ for $i = 0, 2, \cdots, n$.

We note that f can have several representations of the form (1.3), i.e., the coefficients and the number n may vary. This fact motivates the following concept, introduced in [2].

Definition 1.2.2 *Let f be a permutation polynomial over $\mathbb{F}_q$. The Carlitz rank of f is the smallest integer $n > 0$ satisfying $f = P_n$ for a permutation P_n of the form (1.3).*

The Carlitz rank of f is denoted by $Crk(f)$.

Let f be a permutation polynomial over $\mathbb{F}_q$, which is represented by a polynomial in (1.3). The nth convergent $R_n(x)$, associated to f, is defined as

$$R_n(x) = \frac{\alpha_{n-1}x + \beta_{n-1}}{\alpha_n x + \beta_n},$$

where

$$\alpha_k = a_k\alpha_{k-1} + \alpha_{k-2} \text{ and } \beta_k = a_k\beta_{k-1} + \beta_{k-2}, \tag{1.4}$$

for $k \geq 2$, and $\alpha_0 = 0,\ \alpha_1 = a_0,\ \beta_0 = 1,\ \beta_1 = 0.$
Note that $R_n(x)$ is a linear polynomial when $\alpha_n = 0$.

The set of poles of f is defined as

$$O_n = \{x_i : x_i = \frac{-\beta_i}{\alpha_i}, i = 1, \cdots, n\} \subset \mathbb{F}_q \cup \{\infty\}$$

where α_i, β_i are as in (1.4).
Note that the elements of O_n are not necessarily distinct.

It can be shown, see [2], that the values of f outside O_n are determined by $R_n(x)$. That is,

$$f(c) = P_n(c) = R_n(c) \ for \ c \in \mathbb{F}_q \setminus O_n.$$

Therefore when $\alpha_n = 0$, then $f(x)$ is a linear outside the poles. We remark that the behaviour of polynomials $P_n(x)$ depend heavily on α_n being zero or not. In this thesis we only consider the case $\alpha_n \neq 0$.

The set $f(O_n)$ can also be expressed in terms of $R_n(x)$ as follows,

$$f(c) = P_n(c) = \begin{cases} \frac{\alpha_{n-1}}{\alpha_n} & \text{if } c = x_1, \\ R_n(x_{i-1}) & \text{if } c = x_i,\ 2 \leq i \leq n, \end{cases}$$

if the poles are distinct and in $\mathbb{F}_q$.

CHAPTER 2

On Value Sets of non-permutation polynomials

2.1. Wan's upper bound

Before giving the proof of the main theorem of this section, we need the following lemmas and some observations.

Lemma 2.1.1 *Let $f \in \mathbb{F}_q[x]$ be an arbitrary polynomial. If $\prod_{i=1}^{q}(x - f(c_i)) = \sum_{i=0}^{q} a_i x^{q-i}$ where $\{c_1, \ldots, c_q\} = \mathbb{F}_q$, then $deg(\prod_{i=1}^{q}(x - f(c_i))) = q - u$ where u is the least positive integer such that $a_u \neq 0$.*

Proof:

Assume

$$\begin{aligned}\prod_{i=1}^{q}(x - f(c_i)) &= \sum_{i=0}^{q} a_i x^{q-i} \\ &= a_0 x^q + a_1 x^{q-1} + \cdots + a_q x^0.\end{aligned}$$

Trivially, if u is the least positive integer such that $a_u \neq 0$, then we obtain

$$\prod_{i=1}^{q}(x - f(c_i)) = a_u x^{q-u} + a_{u+1} x^{q-u-1} + \cdots + a_q x^0.$$

Hence $deg(\prod_{i=1}^{q}(x - f(c_i))) = q - u$.

□

Lemma 2.1.2 *Let h be a non-zero polynomial over $\mathbb{F}_q$ and let $f \in \mathbb{F}_q[x]$ be such that $h \circ f \equiv 0$. Then $|V_f| \leq deg(h)$.*

Proof: Our assumption $h \circ f \equiv 0$ implies that $h(f(x)) = 0$ for all $x \in \mathbb{F}_q$. Hence we can say that roots of $h(x)$ are the values of $f(x)$, $x \in \mathbb{F}_q$. On the other hand we know that the number of distinct roots of $h(x)$ is at most $deg(h(x))$. Thus we get,

$$|V_f| \leq deg(h(x)).$$

□

A polynomial $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ is called *symmetric* if it satisfies $f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ for any permutation $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$. The *k-th elementary symmetric polynomial* S_k is defined as

$$\prod_{i=1}^{n}(t - x_i) = \sum_{k=0}^{n}(-1)^k S_k t^{n-k},$$

where t is an indeterminate over $\mathbb{F}_q[x_1, \ldots, x_n]$.

In other words, $S_0 = 1$ and

$$\begin{aligned} S_1 &= x_1 + x_2 + \cdots + x_n, \\ S_2 &= x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n, \\ &\vdots \\ S_n &= x_1x_2 \cdots x_n. \end{aligned}$$

We now recall the following well-known result, see for instance [15].

Lemma 2.1.3 ***(The fundamental theorem on symmetric polynomials)***
Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a symmetric polynomial. Then there exists a uniquely determined polynomial $h \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ such that $f(x_1, \ldots, x_n) = h(S_1, \ldots, S_n)$, where $S_1, \ldots, S_n \in \mathbb{F}_q[x_1, \ldots, x_n]$ are elementary symmetric polynomials.

Since $\prod_{c \in \mathbb{F}_q}(x - c) = x^q - x$, we get $S_k(c_1, \ldots, c_q) = 0$ for all $1 \leq k \leq q - 2$, when $\{c_1, \ldots, c_q\} = \mathbb{F}_q$.

The following theorem is proven by Wan in [24]. The proof below uses the method of the proof of Turnwald, [23]. We follow [20].

Theorem 2.1.4 *Let $f(x) \in \mathbb{F}_q[x]$, with $deg(f) = d > 0$. Suppose $f(x)$ is not a permutation polynomial of $\mathbb{F}_q$. Then*

$$|V_f| \leq q - \lceil \frac{q-1}{d} \rceil. \tag{2.1}$$

Proof: (Turnwald, 1995)

First we consider the case $d \geq q$. Then we have $\lceil \frac{q-1}{d} \rceil = 1$ and we are done. Hence we can assume that $1 \leq d \leq q-1$. Then $|V_f| \geq 2$, since $|V_f| < 2$ implies that f is a constant on $\mathbb{F}_q$ but this gives a contradiction to Lemma 1.2.1. We put $\mathbb{F}_q = \{c_1, c_2, \ldots, c_q\}$, and use Lemma 2.1.3 to write

$$\prod_{i=1}^{q}(x - f(c_i)) = \sum_{k=0}^{q}(-1)^k S_k x^{q-k}.$$

Let k be the least positive integer such that $S_k \neq 0$, if such k exists. Otherwise we put $k = \infty$. We assume first that k satisfies $0 < kd < q-1$. The polynomial $S_k(f(x_1), \ldots, f(x_q))$ has degree at most $kd < q-1$. So by Lemma 2.1.3, it is a polynomial in $S_1(x_1, \ldots, x_q), \ldots, S_{q-2}(x_1, \ldots, x_q)$. This implies that the degree of $S_k(f(x_1), \ldots, f(x_q))$ is at most $q-2$.
Hence, we have that $S_k(f(c_1), \ldots, f(c_q))$ is a polynomial in $S_1(c_1, \ldots, c_q), \ldots,$ and $S_{q-2}(c_1, \ldots, c_q)$, all of which are zero. This implies that $S_k = 0$, which contradicts our assumption that $S_k \neq 0$. Thus we obtain

$$k \geq \frac{q-1}{d}.$$

Now, consider the polynomial $h(x) = x^q - x - \prod_{i=1}^{q}(x - f(c_i))$. By Lemma 2.1.1 $deg(x^q - \prod_{i=1}^{q}(x - f(c_i))) = q - k$ and we have $deg(h) \leq q - k$.
On the other hand, we have $h(x) = 0$ if and only if $\prod_{i=1}^{q}(x - c_i) = x^q - x$, which is equivalent to f being a permutation polynomial. Hence if $f(x)$ is not a permutation polynomial then $h(x) \neq 0$. But it is easy to see that $f(c_i)$ is a root of g for all $1 \leq i \leq q$. Then from Lemma 2.1.2, we have $|V_f| \leq deg(h)$. So,

$$|V_f| \leq deg(h) \leq q - k.$$

Thus, we have $|V_f| \leq q - \lceil \frac{q-1}{d} \rceil$. □

Example 2.1.1 *Let $q = 11$ and $f(x) = ((4x)^9 + 1)^9 + x$ be the non-permutation polynomial satisfying $f(x) = P_2(4, 1, 0; x) + x$, where $P_2(x)$ is defined as in (1.3). Then the polynomial f takes the following values over $\mathbb{F}_{11}$.*

$$f(0) = 1, f(1) = 4, f(2) = 9, f(3) = 9, f(4) = 3, f(5) = 7,$$
$$f(6) = 3, f(7) = 0, f(8) = 8, f(9) = 7, f(10) = 4.$$

Thus, $V_f = \{0, 1, 3, 4, 7, 8, 9\}$, so $|V_f| = 7 \leq 11 - \lceil \frac{10}{81} \rceil$.

Corollary 2.1.5 *Let $f(x) = (x+1)x^{q-1} \in \mathbb{F}_q[x]$. Then $V_f = \mathbb{F}_q \diagdown \{1\}$ i.e., $|V_f| = q-1$.*

Proof: From the proof of Theorem 2.1.4, it immediately follows that $|V_f| = q-1$. Moreover, $f(c) = c+1 \ \forall c \in \mathbb{F}_p \diagdown \{0\}$ and $f(0) = 0$.

□

Example 2.1.2 *Let $q = 13$. Consider the non-permutation polynomial $g(x) = x^{13} + x^{12}$ on $\mathbb{F}_{13}$. Then g takes the following values over $\mathbb{F}_{13}$.*

$$g(0) = 0,\ g(1) = 2,\ g(2) = 3,\ g(3) = 4,\ g(4) = 5,\ g(5) = 6,\ g(6) = 7,$$
$$g(7) = 8,\ g(8) = 9,\ g(9) = 10,\ g(11) = 12,\ g(12) = 0.$$

Hence, $V_g = \{0, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, so $|V_g| = 12$ and we obtain that $|V_g| = q - \lceil \frac{q-1}{d} \rceil = q - 1$.

The following theorem, which is given in [9], generalizes the Corolllary 2.1.5.

Theorem 2.1.6 *Let $\mathbb{F}_q$ be a finite field and K be a finite extension of $\mathbb{F}_q$. Take $f(x) = (x+1)x^{q-1}$ in $\mathbb{F}_q[x]$. Then*

$$|f(K)| = (1 - \frac{1}{q})|K|.$$

Let $f(x)$ be a polynomial of degree $d < q$ over $\mathbb{F}_q$. Because $f(x)$ cannot attain any element of $\mathbb{F}_q$ more than d times, one can give a trivial lower bound of $|V_f|$ as

$$\lfloor \frac{q-1}{d} \rfloor + 1 \leq |V_f|. \tag{2.2}$$

where $\lfloor m \rfloor$ denotes the greatest integer $\leq m$.

Let $f(x) \in \mathbb{F}_q[x]$ with $q = p^r$. Define $u_p(f)$ to be the smallest positive integer z such that $\sum_{x \in \mathbb{F}_q} f(x)^z \neq 0$, if such z exists. Otherwise, define $u_p(f) = \infty$.

The following theorem, Theorem 2.1 in [25], gives a lower bound of $|V_f|$.

Theorem 2.1.7 *If $u_p(f) < \infty$, then $u_p(f) + 1 \leq |V_f|$.*

Proof: Let N_a be the number of solutions of the equation $f(x) = a$ over $\mathbb{F}_q$. Then

$$\begin{aligned} N_a = \sum_{x\in\mathbb{F}_q}(1-(f(x)-a)^{q-1}) &= -\sum_{x\in\mathbb{F}_q}(f(x)-a)^{q-1} \\ &= -\sum_{k=1}^{q}(\sum_{x\in\mathbb{F}_q}\binom{q-1}{k}f(x)^k)(-a)^{q-1-k} \ (mod\ p). \end{aligned}$$

Since $\binom{q-1}{k} \neq 0$ $(modp)$ for $1 \leq k \leq q-1$, we conclude that the polynomial N_a (as a polynomial of a) has degree $q-1-u_p(f)$. Moreover we have $N_a = 0$ for all $a \notin V_f$. Then there are at least $q - |V_f|$ elements $a \in \mathbb{F}_q$ such that $N_a = 0$ $(mod\ p)$. Hence, $q-1-u_p(f) \geq q-|V_f|$. This proves $|V_f| \geq u_p(f)+1$.

□

From the theorem above, we have two corollaries. For the proofs, see [25].

Corollary 2.1.8 *Let $deg(f) = d$ and $u_p(f) < \infty$. Then*

$$|V_f| \geq \begin{cases} \lfloor\frac{q-1}{d}\rfloor + 2 & if\ d|q-1, \\ \lfloor\frac{q-1}{d}\rfloor + 1 & if\ d\nmid q-1. \end{cases}$$

Corollary 2.1.9 *Let $3 \leq d < p$. Suppose that $d \nmid q-1$. Then*

$$|V_f| \geq \lfloor\frac{q-1}{d}\rfloor + \frac{2(q-1)}{d^2}.$$

A polynomial $f(x)$ over $\mathbb{F}_q$ with degree d for which equality is obtained in (2.2) is called a *minimal value set polynomial.* These polynomials have been widely studied. We may refer the reader to [5], [16], [11] and [3].

The following corollary, which is taken from [12], gives the condition for a polynomial to be minimal value set polynomial.

Corollary 2.1.10 *Let $f(x)$ be a polynomial of degree d over $\mathbb{F}_q$, $q = p^r$. Assume $2 < d < p$ and*

$$|V_f| \leq \lfloor\frac{q-1}{d}\rfloor + \frac{2(q-1)}{d^2-1}.$$

Then $f(x)$ is a minimal value set polynomial, i.e.,

$$|V_f| = \lfloor\frac{q-1}{d}\rfloor + 1.$$

2.2. A generalization by Aitken

Definition 2.2.1 *Let f be a polynomial over $\mathbb{F}_q$. The value polynomial associated to f is defined by the formula*

$$\Phi_f(T) = \prod_{c \in \mathbb{F}_q} (T - f(c)).$$

Obviously, Φ_f is an element of $\mathbb{F}_q[T]$ of degree q. In addition, we can generalize this definition for any subset of $\mathbb{F}_q$. Let S be a subset of $\mathbb{F}_q$. Then *the value polynomial associated to f and S*, is defined as

$$\Phi_{f,S}(T) = \prod_{s \in S} (T - f(s)).$$

The following lemmas and theorems are from [1].

Lemma 2.2.11 *Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree d. Then $\Phi_f(T) - T^q$ has degree at most $q - \frac{q-1}{d}$, or it is the zero polynomial.*

Proof: Let $\mathbb{F}_q = \{c_1 \dots, c_q\}$. From the definition of the k-th elementary symmetric polynomial S_k, we get

$$\Phi_f(T) - T^q = \sum_{k=1}^{q} (-1)^k S_k(f(c_1), \cdots, f(c_q)) T^{q-k}.$$

From the proof of Theorem 2.1.4, we know that if $k < \frac{q-1}{d}$, then $S_k(f(c_1), \cdots, f(c)) = 0$. Thus the largest possible value of $q - k$ is $q - \frac{q-1}{d}$. □

Let σ be a permutation of $\{1, 2, \dots, q\}$, and $F \in \mathbb{F}_q[x_1, x_2, \dots, x_q]$. The polynomial $F_\sigma \in \mathbb{F}_q[x_1, x_2, \dots, x_q]$ is defined by the equation

$$F_\sigma(x_1, \dots, x_q) = F(x_{\sigma(1)}, \dots, x_{\sigma(q)}).$$

Let $b \in \mathbb{F}_q^*$, and let σ_b be the unique permutation of $\{1, 2, \dots, q\}$ satisfying $ba_i = a_{\sigma_b(i)}$.

Theorem 2.2.12 *Suppose $F \in \mathbb{F}_q[x_1, \cdots, x_q]$ is a polynomial of degree D, and G is a subgroup of $\mathbb{F}_q^*$ of order g which satisfies $F_{\sigma_b} = F$, $\forall b \in G$. If $f \in \mathbb{F}_q[x]$ is a polynomial of degree d and if $dD < g$, then*

$$F(f(c_1), f(c_2), \cdots, f(c_q)) = F(f(0), f(0), \cdots, f(0))$$

where $c_i \in \mathbb{F}_q$.

Proof: Let $h \in \mathbb{F}_q[t]$ be given as

$$h(t) = F(f(c_1 t), \ldots, f(c_q t)).$$

So, h has degree $< g$. Note that if $b \in G$, then

$$\begin{aligned} h(b) = F(f(c_1 b), \ldots, f(c_q b)) &= F(f(a_{\sigma_b(1)}), \ldots, f(a_{\sigma_b(q)})) \\ &= F_{\sigma_b}(f(a_1), \ldots, f(a_q)) \\ &= F(f(a_1), \ldots, f(a_q)) \\ &= h(1). \end{aligned}$$

Hence, $h(t) - h(1)$ has at least g zeroes, but its degree $< g$. Thus $h(t) - h(1) = 0$. In particular $h(1) = h(0)$.

□

Lemma 2.2.13 *Let $f \in \mathbb{F}_q[x]$ be a polynomial with degree d, satisfying $f(0) = 0$. Suppose that S is a subset of $\mathbb{F}_q$ with s elements, and G is a subgroup of $\mathbb{F}_q^*$ of order g that acts on S. Then $\Phi_{f,S}(T) - T^s$ has degree at most $s - g/d$ or it is the zero polynomial.*

Proof: Let $S = \{c_{i_1}, \cdots, c_{i_s}\}$. Then

$$\Phi_{f,S}(T) - T^s = \sum_{k=1}^{s} (-1)^k S_k(f(c_{i_1}), \ldots, f(c_{i_s}))T^{s-k}.$$

Put $F_k(x_1, \cdots, x_q) = S_k(x_{i_1}, \cdots, x_{i_s})$. Clearly, F_k is invariant under G. By Theorem 2.2.12, if $k < g/d$, then we have

$$S_k(f(c_{i_1}), \ldots, f(c_{i_s})) = F_k(f(c_1), \ldots, f(c_q)) = F_k(f(0), \ldots, f(0)).$$

However,

$$F_k(f(0), \ldots, f(0)) = S_k(0, \ldots, 0) = 0.$$

Hence we obtain that the term T^{s-k} of $\Phi_{f,S}(T) - T^s$ is the zero for $0 < k < g/d$. So this implies that $\Phi_{f,S}(T) - T^s$ has degree at most $s - g/d$.

□

Let $S = \{s_1, s_2, \ldots, s_r\}$ be a subset of $\mathbb{F}_q$, and let $f \in \mathbb{F}_q[x]$. We define $f[S]$ to be the set of all values $f(s)$, $s \in S$, *with multiplicities*. Note that $f[\mathbb{F}_q] = V_f$ if f is a permutation polynomial.

Theorem 2.2.14 *Let f_1, f_2 be non-constant polynomials over $\mathbb{F}_q$ with degrees at most d. Then the size of the intersection of $f_1[\mathbb{F}_q]$ and $f_2[\mathbb{F}_q]$ is either q or is at most $q - \frac{q-1}{d}$.*

Proof:

Let consider polynomials $\Phi_{f_1}(T) = \prod_{c\in\mathbb{F}_q}(T - f_1(c))$ and $\Phi_{f_2}(T) = \prod_{d\in\mathbb{F}_q}(T - f_2(d))$. Then any element of the intersection of $f_1[\mathbb{F}_q]$ and $f_2[\mathbb{F}_q]$ is the root of the polynomial $\Phi_{f_1} - \Phi_{f_2}$. By Lemma 2.2.11, $\Phi_{f_1} - \Phi_{f_2}$ has degree at most $q - \frac{q-1}{d}$ or it is the zero polynomial. So this gives that the size of intersection is either q or is at most $q - \frac{q-1}{d}$.

□

Corollary 2.2.15 *Let $f(x)$ be a polynomial over a finite field $\mathbb{F}_q$ with positive degree d. If $f(x)$ is not a permutation polynomial of $\mathbb{F}_q$, then*

$$|V_f| \leq q - \lceil \frac{q-1}{d} \rceil,$$

where $\lceil s \rceil$ denotes the smallest integer $\geq s$.

Proof: Take $f_1(x) = f(x)$ and $f_2(x) = x$ in Theorem 2.2.14. □

Theorem 2.2.16 *Let $f_1, f_2 \in \mathbb{F}_q[x]$ be non-constant polynomials of degree d such that $f_1(0) = f_2(0)$. Suppose that G is a subgroup of $\mathbb{F}_q^*$ with g elements, and S_1 and S_2 are subsets of $\mathbb{F}_q$, both with size s and invariant under multiplication by elements of G. Then the size of the intersection of $f_1[S_1]$ and $f_2[S_2]$ is either s or is at most $s - g/d$.*

Proof: W.L.O.G, we can assume that $f_1(0) = f_2(0) = 0$. Let consider the polynomial $\Phi_{f_1,S_1} - \Phi_{f_2,S_2}$. Then any element of the intersection of $f_1[S_1]$ and $f_2[S_2]$ is the root of $\Phi_{f_1,S_1} - \Phi_{f_2,S_2}$. By Lemma 2.2.13, it has degree at most $s - g/d$ or it is the zero polynomial. Thus the size of intersection is either s or is at most $s - g/d$.

□

Example 2.2.3 *Let $q = 11$, $f_1 = 3x^7 + 4x^3$ and $f_2 = 2x^7 + x$. Take the trivial subgroup of $\mathbb{F}_q^*$, $G = \{1\}$. Assume $S_1 = \{2, 3, 5, 6\}$ and $S_2 = \{1, 7, 9, 10\}$. Then we have the following values,*

$$f_1(2) = 9,\ f_1(3) = 3,\ f_1(5) = 3,\ f_1(6) = 8,$$
$$f_2(1) = 3,\ f_2(7) = 8,\ f_2(9) = 6,\ f_2(10) = 8.$$

Thus the size of intersection of $f_1[S_1]$ and $f_1[S_2]$ is $2 < 4 - 1/7$.

2.3. On value sets of pairs of particular polynomials

As we described in the previous section, Aitken studies the size of the intersection of value sets of pairs of polynomials. In this section, we focus on polynomials $F(x) = f(x) + x$ and $G(x) = g(x) + x$, where f, g are permutation polynomials of a given Carlitz rank. The behaviour of this type of polynomials have been studied in [13], in connection with complete mappings. More details of this work can be found in Chapter 3.

Since $F(x) = f(x) + x$, where $f(x)$ is a permutation polynomial in the form (1.3), we define the poles of F as the roots of the denominators of

$$R_i(x) + x = \frac{\alpha_{i-1}x + \beta_{i-1}}{\alpha_i x + \beta_i} = \frac{\alpha_i x^2 + \alpha_{i-1}x + \beta_i x + \beta_{i-1}}{\alpha_i x + \beta_i}, \quad 1 \le i \le n.$$

In other words, "the poles of $F(x)$" are the same as on the poles of $f(x)$. We note that $F(x) = R_n(x) + x$ for $x \notin O_n$.
We give conditions on f, g so that V_{f+x} and V_{g+x} are actually identical. We first study monic permutation polynomials f, g with Carlitz rank 3.

Theorem 2.3.17 *Let q be odd, $b \in F_q^*$ with $b^2 + 1 \neq 0$, and $f_+(x) = ((x^{q-2} + b)^{q-2} + b)^{q-2}$ and $f_-(x) = ((x^{q-2} - b)^{q-2} - b)^{q-2}$ be permutation polynomials over $\mathbb{F}_q^*[x]$ of Carlitz rank 3. Put $F_+(x) = f_+(x) + x$ and $F_-(x) = f_-(x) + x$, we have $V_{F_+} = V_{F_-}$.*

Proof: First of all, we find the set of poles of $F_+(x)$ and $F_-(x)$, which we denote by O_3^+, O_3^-, respectively.

$$O_3^+ = \{0, \ \frac{-1}{b}, \ \frac{-b}{b^2+1}\}, \qquad O_3^- = \{0, \ \frac{1}{b}, \ \frac{b}{b^2+1}\}.$$

We can obtain $F_+(O_3^+)$ and $F_-(O_3^-)$ as follows.

$$F_+(0) = \frac{b}{b^2+1}, \quad F_+(\frac{-1}{b}) = 0, \quad F_+(\frac{-b}{b^2+1}) = \frac{-b}{b^2+1},$$

$$F_-(0) = \frac{-b}{b^2+1}, \quad F_-(\frac{1}{b}) = 0, \quad F_-(\frac{b}{b^2+1}) = \frac{b}{b^2+1}.$$

Therefore $F_+(O_3^+) = F_-(O_3^-)$. Moreover, using the definition of the 3rd convergents R_3^+ and R_3^- associated to f_+ and f_-, we get

$$F_+(x) = R_3^+(x) + x = \frac{bx+1}{(b^2+1)x+b} + x$$

for $x \in \mathbb{F}_q \diagdown O_3^+$, and

$$F_-(y) = R_3^-(y) + y = \frac{-by+1}{(b^2+1)y-b} + y$$

for $y \in \mathbb{F}_q \diagdown O_3^-$

We put $V_+ = \{u \in \mathbb{F}_q \ : \ u = F_+(x) \text{ for some } x \in \mathbb{F}_q \diagdown O_3^+\}$ and
$V_- = \{u \in \mathbb{F}_q \ : \ u = F_-(y) \text{ for some } y \in \mathbb{F}_q \diagdown O_3^-\}$. We now prove that $V_+ = V_-$.

Let $u \in V_+$, that is

$$\frac{(b^2+1)x^2 + 2bx + 1}{(b^2+1)x+b} = u$$

So, we have

$$(b^2+1)x^2 + (2b - (u(b^2+1)))x + 1 - bu = 0$$

In order that this equation has a solution, we need $\Delta = u^2(b^2+1)^2 - 4$ to be a square. Suppose $\Delta = \gamma^2 \geq 0$. Then we have the solutions,

$$x_1 = \frac{-2b + u(b^2+1) - \gamma}{2(b^2+1)}, \quad x_2 = \frac{-2b + u(b^2+1) + \gamma}{2(b^2+1)}.$$

Now, take $y_1 = u - x_2$ and $y_2 = u - x_1$, then one can easily check that y_1 and y_2 are the solutions of $F_-(y) = u$.
Thus we get $u \in V_-$. Hence we get $V_+ \subset V_-$. One can similarly show that $V \subset V_+$.

□

It is proved in [13] that when $b^2 + 1 \neq 0$, then V_{F^+} and V_{F^-} satisfy

$$|V_{F^+}| \leq min\{3 + \lfloor \frac{q+1}{2} \rfloor, q\} \ \text{ and } \ |V_{F^-}| \leq min\{3 + \lfloor \frac{q+1}{2} \rfloor, q\}.$$

Example 2.3.4 *Let $q = 11$ and $b = 2$ in Theorem 2.3.17. Then consider the polynomials,*

$$F_+(x) = ((x^9 + 2)^9 + 2)^9 + x, \quad F_-(x) = ((x^9 - 2)^9 - 2)^9 + x.$$

Note that $b^2 + 1 = 5 \neq -1$. The poles are $O_2^+ = \{0, 5, 4\}$ and $O_2^- = \{0, 6, 7\}$. Now we compute the value sets of these polynomials,

$$\begin{aligned} F_+(0) &= 7, & F_-(0) &= 4, \\ F_+(1) &= 3, & F_-(1) &= 8, \\ F_+(2) &= 7, & F_-(2) &= 3, \\ F_+(3) &= 6, & F_-(3) &= 6, \\ F_+(4) &= 4, & F_-(4) &= 3, \\ F_+(5) &= 0, & F_-(5) &= 7, \\ F_+(6) &= 4, & F_-(6) &= 0, \\ F_+(7) &= 8, & F_-(7) &= 7, \\ F_+(8) &= 5, & F_-(8) &= 5, \\ F_+(9) &= 8, & F_-(9) &= 4, \\ F_+(10) &= 4, & F_-(10) &= 8. \end{aligned}$$

Hence $F^+(O_2^+) = \{0, 4, 7\} = F^-(O_2^-)$, $V_+ = V_- = \{3, 5, 6, 8\}$ Therefore $V_{F_+} = V_{F_-} = \{0, 3, 4, 5, 6, 7, 8\}$, and $|V_{F^+}| = |V_{F^-}| = 7 \leq min\{3 + 6, 11\}$.

The theorem below is a generalization of the Theorem 2.3.17 to polynomials $F_+(x) = f_+(x) + x$ and $F_-(x) = f_-(x) + x$, where f_+ and f_- are permutation polynomials with representations,

$$f_+(x) = P_n(1, b, \ldots, 0; x) \text{ and } f_-(x) = P_n(1, -b, -b, \ldots, 0; x). \tag{2.3}$$

for $n \geq 2$.

We first calculate the values α_i, β_i in (1.4), $i = 1, \ldots, 6$ for the polynomials $f_+(x)$.

Since

$$\alpha_0 = 0, \ \beta_0 = 1,$$
$$\alpha_1 = 1, \ \beta_1 = 0$$

and

$$\alpha_i = b\alpha_{i-1} + \alpha_{i-2},\ \beta_i = b\beta_{i-1} + \beta_{i-2},$$

we have ,

$$\begin{aligned}\alpha_2 = b,\ \beta_2 = 1,\\ \alpha_3 = b^2 + 1,\ \beta_3 = b,\\ \alpha_4 = b^3 + 2b,\ \beta_4 = b^2 + 1,\\ \alpha_5 = b^4 + 3b^2 + 1,\ \beta_5 = b^3 + 2b,\\ \alpha_6 = b^5 + 4b^3 + 3b,\ \beta_6 = b^4 + 3b^2 + 1.\end{aligned}$$

Similarly, $\bar{\alpha_i}, \bar{\beta_i}$, $i = 1, \ldots, 6$ for the polynomial $f_{-}(x)$ are

$$\begin{aligned}\bar{\alpha_0} = 0,\ \bar{\beta_0} = 1,\\ \bar{\alpha_1} = 1,\ \bar{\beta_1} = 0,\\ \bar{\alpha_2} = -b,\ \bar{\beta_2} = 1,\\ \bar{\alpha_3} = b^2 + 1,\ \bar{\beta_3} = -b,\\ \bar{\alpha_4} = -b^3 - 2b,\ \bar{\beta_4} = b^2 + 1,\\ \bar{\alpha_5} = b^4 + 3b^2 + 1,\ \bar{\beta_5} = -b^3 - 2b,\\ \bar{\alpha_6} = -b^5 - 4b^3 - 3b,\ \bar{\beta_6} = b^4 + 3b^2 + 1.\end{aligned}$$

These calculations motivate the following lemma.

Lemma 2.3.18 *Let α_i, β_i and $\bar{\alpha_i}, \bar{\beta_i}$ are as defined in (1.4), corresponding to the polynomials f_+ and f_- in (2.3), respectively. Then $\beta_i = \alpha_{i-1}$ and $\bar{\beta_i} = \bar{\alpha}_{i-1}$ for $i \in \{1, 2, 3, \ldots, n\}$.*

Proof:

It is sufficient to show that $\beta_i = \alpha_{i-1}$. We use induction on i.
Note that for $i = 1$, we get $\beta_1 = \alpha_0 = 0$.
Now assume that $\beta_t = \alpha_{t-1}$ for $t \leq i - 1$. By definition, $\beta_i = b\beta_{i-1} + \beta_{i-2}$. Then we have,

$$\beta_i = b\alpha_{i-2} + \alpha_{i-3} = \alpha_{i-1}.$$

□

Now, it is clear that
$\bar{\alpha}_i = -\alpha_i$ and $\bar{\beta}_i = \beta_i$, if i is even and
$\bar{\alpha}_i = \alpha_i$ and $\bar{\beta}_i = -\beta_i$, If i is odd.

Now, let $R_n^+(x)$ be the nth convergent of $f_+(x)$ and $R_n^-(x)$ be the nth convergent of $f_-(x)$. Suppose that $\alpha_n \neq 0$. Then we get

$$R_n^+(x) = \frac{\alpha_{n-1}x + \beta_{n-1}}{\alpha_n x + \beta_n},$$

and

$$R_n^-(x) = \frac{\alpha_{n-1}x - \beta_{n-1}}{-\alpha_n x + \beta_n}.$$

By straightforward calculations, we get

$$R_n^-(x) = -R_n^+(-x).$$

for $x \in \mathbb{F}_q \diagdown \{\frac{\beta_n}{\alpha_n}\}$.
We also note that R_n^+ is 1-1 on $\mathbb{F}_q \diagdown \{-\frac{\beta_n}{\alpha_n}\}$ and R_n^- is 1-1 on $\mathbb{F}_q \diagdown \{\frac{\beta_n}{\alpha_n}\}$. Moreover, we have

$$\begin{aligned} R_n^-(R_n^+(x)) &= \frac{\alpha_{n-1}(\frac{\alpha_{n-1}x+\beta_{n-1}}{\alpha_n x+\beta_n}) - \beta_{n-1}}{-\alpha_n(\frac{\alpha_{n-1}x+\beta_{n-1}}{\alpha_n x+\beta_n}) + \beta_n} \\ &= \frac{(\alpha_{n-1}^2 - \alpha_n\beta_{n-1})x + \alpha_{n-1}\beta_{n-1} - \beta_n\beta_{n-1}}{(-\alpha_n\alpha_{n-1} + \alpha_n\beta_n)x + \beta_n^2 - \alpha_n\beta_{n-1}}. \end{aligned}$$

By using Lemma 2.3.18, we have

$$R_n^-(R_n^+(x)) = x \quad \forall x \in \mathbb{F}_q \diagdown \{\frac{\beta_n}{\alpha_n}, \frac{-(\beta_n^2 + \alpha_n\beta_{n-1})}{2\beta_n\alpha_n}\} \tag{2.4}$$

We use the notation,
$O_n^+ = \{-x_1 = 0, -x_2, -x_3, \ldots, -x_n\}$ to denote the set of poles of f_+ (or F_+) and
$O_n^- = \{x_1 = 0, x_2, x_3, \ldots, x_n\}$ for the set of poles of f_- (or F_-).

We again put,
$V_+ = \{u \in \mathbb{F}_q : u = F_+(x) \text{ for some } x \in \mathbb{F}_q \diagdown O_n^+\}$,
$V_- = \{u \in \mathbb{F}_q : u = F_-(y) \text{ for some } y \in \mathbb{F}_q \diagdown O_n^-\}$.

We now give the main theorem.

Theorem 2.3.19 *Let $\mathbb{F}_q$ be of odd characteristic. Let $f_+(x) = P_n(1, b, b, \ldots, 0; x)$ and $f_-(x) = P_n(1, -b, -b, \ldots, 0; x)$ be permutations of $\mathbb{F}_q$ with representations as in (2.3), for some $b \in \mathbb{F}_q^*$ such that $|O_n^+| = |O_n^-| = n$ and $O_n^+ \subset \mathbb{F}_q$. Then $V_{f_+(x)+x} = V_{f_-(x)+x}$.*

Proof:
Since $f_+(x) = R_n^+(x)$ for $x \in \mathbb{F}_q \diagdown O_n^+$ and $f_-(y) = R_n^-(y)$ for $y \in \mathbb{F}_q \diagdown O_n^-$, we have;

$$F_+(x) = R_n^+(x) + x = \frac{\alpha_n x^2 + (\alpha_{n-1} + \beta_n)x + \beta_{n-1}}{\alpha_n x + \beta_n} \quad \text{for } x \in \mathbb{F}_q \diagdown O_n^+,$$

$$F_-(x) = R_n^-(y) + y = \frac{\alpha_n y^2 - (\alpha_{n-1} + \beta_n)y + \beta_{n-1}}{\alpha_n y - \beta_n} \quad \text{for } y \in \mathbb{F}_q \diagdown O_n^-.$$

We first prove that $V_+ = V_-$.

Let $u \in V_+$, i.e., $F_+(x) = u$. Then we have

$$\alpha_n x^2 + (\alpha_{n-1} + \beta_n - \alpha_n u)x - \beta_{n-1} - u\beta_n = 0. \tag{2.5}$$

We put $\Delta = (\alpha_{n-1} + \beta_n - \alpha_n u)^2 - 4\alpha_n(\beta_{n-1} - u\beta_n)$.
Assuming that Δ is a square in $\mathbb{F}_q$, we have the solutions of the equation (2.5) as

$$x_1 = \frac{-(\alpha_{n-1} + \beta_n - \alpha_n u) - \gamma}{2\alpha_n}, \qquad x_2 = \frac{-(\alpha_{n-1} + \beta - \alpha u) + \gamma}{2\alpha_n},$$

where $\gamma^2 = \Delta \geq 0$.

Let $y_1 = u - x_2$ and $y_2 = u - x_1$. Then one can check that y_1 and y_2 are solutions of $F_-(y) = u$. Hence, $u \in V_-$. Similarly one can prove that $V_- \subset V_+$, and hence we obtain $V_+ = V_-$.

Now we check if 0 is in V_+ or V_-.

Let $x \in \mathbb{F}_q \diagdown O_n^+$, and hence $F_+(x) = R_n^+(x) + x$. Suppose

$$R_n^+(x) + x = \frac{\alpha_n x^2 + (\alpha_{n-1} + \beta_n)x + \beta_{n-1}}{\alpha_n x + \beta_n} = 0.$$

We put $\Delta = (\alpha_{n-1}+\beta_n)^2 - 4\alpha_n\beta_{n-1}$. We wish to solve $\alpha_n x^2 + (\alpha_{n-1}+\beta_n)x + \beta_{n-1} = 0$. We note that putting $R_n^-(y) + y = 0$, we obtain the same Δ.

Now if $\Delta = \theta^2$ for some $\theta \in \mathbb{F}_q$, then

$$x_1 = \frac{-(\alpha_{n-1} + \beta_n) - \theta}{2\alpha_n}, \quad x_2 = \frac{-(\alpha_{n-1} + \beta_n) + \theta}{2\alpha_n}$$

are the solutions of $R_n^+(x) + x = 0$. Then $y_1 = -x_1$ and $y_2 = -x_2$ are the solutions of $R_n^-(y) + y = 0$.

If, on the other hand, $\Delta \neq \theta^2$ for any $\theta \in \mathbb{F}_q$, then we cannot find $x \in \mathbb{F}_q \diagdown O_n^+$ such that $F_+(x) = 0$. Also we cannot have $y \in \mathbb{F}_q \diagdown O_n^-$ such that $F_-(y) = 0$. Therefore $0 \in V_+$ if and only if $0 \in V_-$, as already shown above, and that $0 \in V_+ = V_-$ only when $(\alpha_{n-1} + \beta_n)^2 - 4\alpha_n\beta_{n-1}$ is a square in $\mathbb{F}_q$.

Now we turn our attention to the values F_+ and F_- take on O_n^+ and O_n^-, respectively.

Recall that $O_n^+ = \{0, -x_2, -x_3, \ldots, -x_n\}$ and $O_n^- = \{0, x_2, x_3, \ldots, x_n\}$ are the sets of poles of f_+, f_-, respectively. We claim that $F_+(0) = -F_-(0)$ and $F_+(-x_i) = -F_-(x_i)$ for $i \in \{2, 3, \ldots, n\}$.

Clearly,

$$F_+(-x_i) = \begin{cases} \frac{\alpha_{n-1}}{\alpha_n} - x_i & \text{if } i = 1 \\ R_n^+(-x_{i-1}) - x_i & \text{if } 2 \leq i \leq n \end{cases}$$

and

$$F_{-}(x_i) = \begin{cases} -\frac{\alpha_{n-1}}{\alpha_n} + x_i & \text{if } i = 1 \\ R_n^{-}(x_{i-1}) + x_i & \text{if } 2 \leq i \leq n. \end{cases}$$

Firstly, consider $i = 1$, that is $x_1 = 0$. Then we have,

$$F_{+}(0) = \frac{\alpha_{n-1}}{\alpha_n}.$$

$$F_{-}(0) = -\frac{\alpha_{n-1}}{\alpha_n}.$$

Hence $F_{+}(0) = -F_{-}(0)$. Now consider $x_i \in O_n^{+}$ with $2 \leq \ i \leq n$. We have

$$F_{+}(-x_i) = R_n^{+}(-x_{i-1}) - x_i = \frac{-\alpha_{n-1}x_{i-1} + \beta_{n-1}}{-\alpha_n x_{i-1} + \beta_n} - x_i,$$

and

$$F_{-}(x_i) = R_n^{-}(x_{i-1}) + x_i = \frac{\alpha_{n-1}x_{i-1} - \beta_{n-1}}{-\alpha_n x_{i-1} + \beta_n} + x_i.$$

Thus, we get $F_{+}(-x_i) = -F_{-}(x_i)$ for $2 \leq i \leq n$, proving our claim.

We observe that $x_{i-1} = \frac{1}{x_i} - b$ for $i \geq 2$. We also note that

$$F_{+}(-x_1) = F_{+}(0) = \frac{\alpha_{n-1}}{\alpha_n} = \frac{\beta_n}{\alpha_n},$$

and

$$F_{+}(-x_n) = R_n^{+}(-x_{n-1}) - x_n = R_n^{+}(-\frac{\beta_{n-1}}{\alpha_{n-1}}) - \frac{\beta_n}{\alpha_n} = 0 - \frac{\beta_n}{\alpha_n}.$$

Hence $F_{+}(-x_1) = -F_{+}(-x_n)$.

In fact, such a relation holds for all $i \geq 1$, namely $F_{+}(-x_i) = -F_{+}(-x_{n+1-i})$ for $i \geq 1$.

In order to prove that $F_+(-x_i) = -F_+(-x_{n+1-i})$ for $i \geq 2$, we need to show that the relation $F_+(-x_i) = x_{n+1-i} - x_i$ for $i \geq 2$.

We use induction on i. Firstly consider $i = 2$. Then

$$F_+(-x_2) = R_n^+(-x_1) - x_2 = R_n^+(0) - x_2 = \frac{\beta_{n-1}}{\beta_n} - x_2 = \frac{\beta_{n-1}}{\alpha_{n-1}} - x_2 = x_{n-1} - x_2.$$

Now assume that $F_+(-x_i) = x_{n+1-i} - x_i$, i.e., $R_n^+(-x_{i-1}) = x_{n+1-i}$ for some i, $2 \leq i \leq n-1$. We wish to show that $R_n^+(-x_i) = x_{n-i}$.
Since $x_{n-i} = \frac{1}{x_{n-i+1}} - b$, we have

$$\begin{aligned} x_{n-i} = \frac{1}{R_n^+(-x_{i-1})} - b &= \frac{-\alpha_{i-1}x_{i-1} + \beta_n}{-\alpha_{n-1}x_{i-1} + \beta_{n-1}} - b \\ &= \frac{(-\alpha_n + \alpha_{n-1}b)x_{i-1} + \beta_n - \beta_{n-1}b}{-\alpha_{n-1}x_{i-1} + \beta_{n-1}} \\ &= \frac{-\alpha_{n-2}x_{i-1} + \beta_{n-2}}{-\alpha_{n-1}x_{i-1} + \beta_{n-1}}. \end{aligned}$$

Using $x_{i-1} = \frac{1}{x_i} - b$, we get

$$\begin{aligned} &= \frac{\frac{-\alpha_{n-2}}{x_i} + b\alpha_{n-2} + \beta_{n-2}}{\frac{-\alpha_{n-1}}{x_i} + b\alpha_{n-1} + \beta_{n-1}} \\ &= \frac{\beta_n x_i - \alpha_{n-2}}{\alpha_n x_i - \alpha_{n-1}} \\ &= \frac{\alpha_{n-1}x_i - \beta_{n-1}}{\alpha_n x_i - \beta_n} \\ &= R_n^+(-x_i). \end{aligned}$$

We therefore have

$$R_n^+(-x_i) = x_{n-i}.$$

We use (2.4) to obtain $-x_i = R_n^-(x_{n-i})$. Adding x_{n+1-i} to both sides, we get

$$R_n^-(x_{n-i}) + x_{n+1-i} = x_{n+1-i} - x_i,$$

which yields $F_-(x_{n+1-i}) = x_{n+1-i} - x_i$. We finally get

$$F_+(-x_i) = F_-(x_{n+1-i}) = -F_+(-x_{n+1-i}).$$

In other words, $F_+(O_n^+) = F_-(O_n^-)$, which completes the proof.

□

Remark 2.3.1 *If n is odd, then $F_+(-x_{\frac{n+1}{2}}) = -F(-x_{\frac{n+1}{2}})$. Thus, $F_+(-x_{\frac{n+1}{2}}) = 0$.*

We emphasize that the result of Aitken is on the size of the intersection of value sets of pairs of polynomials. For polynomials of the form $f + x$ and $g + x$, where f, g are permutations of Carlitz rank 2 and 3, we have partial results on the intersection of the size of their value sets. We plan to obtain more results in this direction.

CHAPTER 3

Permutation behaviour of pairs of polynomials

In this chapter we focus on permutation behaviour of pairs of polynomials of the form $f(x)$ and $g(x) = f(x)+h(x)$ where $f, g \in \mathbb{F}_p[x]$ are monic polynomials of the same degree d. Section 3.1 describes a result of Cohen, Mullen and Shiue [7] , on the lower bound of the degree of $h(x)$, given in terms of d. In section 3.2, we outline a recent result of [13], on permutation behaviour of $g(x) = f(x) + x$, where f is a permutation polynomial of Carlitz rank n.

3.1. On differences

In this section we describe a result of Cohen, Mullen and Shiue, which shows that the degree of the difference $h(x)$ of two permutation polynomials $f(x)$ and $g(x) = f(x) + h(x) \in \mathbb{F}_p[x]$ of the same degree $d \geq 3$ satisfies $deg(h(x)) \geq \frac{3d}{5}$ when $p > (d^2 - 3d + 4)^2$.

We recall that a polynomial $f(x) \in \mathbb{F}_p[x]$ of degree d is called *normalized* if the coefficient of x^{d-1} is the zero.

The following lemmas are taken from [8].

Lemma 3.1.1 *Let f be a monic, normalized polynomial of $\mathbb{F}_p[x]$ with $deg(f) = d$, and $p > d \geq 2$. Suppose that f decomposes as $f = f_2(f_1)$ over $\mathbb{F}_p$. If $d_1 = deg(f_1)$, $d_2 = deg(f_2)$ and $d = d_1 d_2$, then f_1 and f_2 can be regarded as monic, normalized polynomials over $\mathbb{F}_p$. Moreover if the coefficient of x^{d_1-r} in f_1 is α, then the coefficient of x^{d-r} in f is $d_2\alpha$.*

Proof: Suppose, $\beta \neq 0$ is the leading coefficient of f_1. We substitute $f_1(x)$ and $f_2(x)$ by $\beta^{-1} f_1(x)$ and $f_2(\beta x)$, respectively. Then we get that a monic polynomial $f_1(x)$. Hence f_2 is a monic since f is a monic. Denote the coefficient of x^{d_2-1} in f_2 by γ.

Then we replace $f_1(x)$ by $f_1(x) + d_2^{-1}\gamma$ and $f_2(x)$ by $f_2(x - d_2^{-1}\gamma)$. Thus we obtain that f_2 is normalized. This being so, the final claim of the lemma comes from a basic calculation. Therefore, f_1 must be a normalized polynomial.

□

Lemma 3.1.2 *Suppose that f is a monic, normalized permutation polynomial of $\mathbb{F}_p$ of odd degree $d \geq 3$ and $p > (d^2 - 3d + 4)^2$. Then $f = f_2(f_1)$ where f_1, f_2 are monic normalized polynomials of degrees d_1, d_2, respectively with $d = d_1 d_2$ and polynomial f_1 can be expressed as,*

$$f_1(x) = D_{m_1}(a, x^{m_2}) + \alpha \tag{3.1}$$

for some integers m_1, m_2 with $m_1 m_2 = d_1 \geq 3$, $\alpha \in \mathbb{F}_q$, $a \neq 0$.
Moreover if $m_1 = 1$ in (2.1), i.e., $f_1(x) = x^{d_1} + \alpha$, we can assume that $\alpha \neq 0$ unless $f(x) = x^d$.

We now state and prove the main theorem of this section.

Theorem 3.1.3 *[7] Suppose f and g are monic permutation polynomials of odd degree $d \geq 3$ over a finite field $\mathbb{F}_p$, where $p > (d^2 - 3d + 4)^2$. Let $h = f - g$ and t be the degree of h. Assume $t \geq 1$. Then $t \geq \frac{3d}{5}$.*
Moreover, if $d \geq 5$ and $t \leq d - 3$, then $gcd(t, d) > 1$.

Proof: First of all we consider the case $t = d - 1$. Our assumption $d \leq 3$, i.e., $d \leq \frac{5}{2}$ implies that $d - 1 \geq \frac{3d}{5}$. Then we have $t \geq \frac{3d}{5}$. So, we can assume $t < d - 1$.
We normalize f and g so that they are both monic. Now assume that $f(x) = f_0(l(x))$ and $g(x) = g_0(l(x))$ for some normalized permutation polynomial $l(x)$. Also we can choose $l(x)$ such that its degree e is maximal and we write $deg(f_0) = deg(g_0) = d_0$, where $d = ed_0$.
If $e = d$, then $d_0 = 1$ i.e., $f_0(x) = x + a$ and $g_0(x) = x + b$ for some constants a, b. But in this case, $deg(f - g) = deg(a - b) = 0 = t$, a contradiction to our assumption $t \geq 1$. So, we get $e < d$.
Let $h(x) = h_0(l(x))$ where $deg(h_0) = t_0$ and $t = et_0$. Suppose $e > 1$. Then $gcd(t, d) > 1$. Moreover, $t < \frac{3d}{5}$ if and only if $t_0 < \frac{3d_0}{5}$. We may replace f and g by f_0 and g_0. For the rest of this proof we may assume $e = 1$. In other words, we can assume f and g are monic, normalized polynomials.

Next, we consider the case $t = d - 2$, then d cannot be 3 otherwise $t \ngeq \frac{3n}{5}$. Also in this case, if $d \geq 5$, then $t \geq \frac{3d}{5}$ with equality only if $d = 5, t = 3$ as in the Example 3.1.5. Thus we may also assume $t \leq d - 3$ with $d \geq 5$.

From Lemma 3.1.2, we have that $f = f_2(f_1)$ and $g = g_2(g_1)$ are normalized and

$$f_1(x) = D_{m_1}(a, x^{m_2}) + \alpha,\ a \neq 0,\ \alpha \in \mathbb{F}_p,\ m = m_1m_2 \geq 3, \tag{3.2}$$

$$g_1(x) = D_{k_1}(b, x^{k_2}) + \beta,\ b \neq 0,\ \beta \in \mathbb{F}_p,\ k = k_1k_2 \geq 3. \tag{3.3}$$

Moreover in (3.2) if $m_1 = 1$, then $\alpha \neq 0$ unless $f(x) = x^d$ and a similar statement holds for $g(x)$.

Recall the definition of Dickson polynomial in (1.1),

$$D_m(a, x) = \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-j} \binom{m-j}{j} (-a)^j x^{m-2j}.$$

Now, we prove the theorem considering the following three cases:

Case 1: $m_1 = 1$, $k_1 = 1$.

Then we have $f_1(x) = x^m + \alpha$ and $g_1(x) = x^k + \beta$ with $\alpha\beta \neq 0$. Since $e = 1$, we have $(m, k) = 1$. From Lemma 3.1.1, $t = max\{d - m, d - k\}$. Since $k|n$ and $m|n$, $gcd(t, d) = k > 1$ or $gcd(t, d) = m > 1$. Also $k|d$ and $m|d$ and $gcd(k, m) = 1$ implies $km|n$. Then we have $3m \leq km \leq d$. So, $m < \frac{d}{3}$. Assume $t = d - m$, then

$$t > n - \frac{d}{3} = \frac{2d}{3} > \frac{3d}{5}.$$

Case 2: $m_1 > 1$ and $k_1 = 1$.

Then we have $f_1(x) = D_{m_1}(a, x^{m_2}) + \alpha$ and $g_1(x) = x^k + \beta$. Since $e = 1$, $gcd(k, m_2) = 1$. By Lemma 3.1.1, we have $t = max\{d - 2m_2, d - k\}$ where $m_2 > 1$ since $t \neq d - 2$. So, for each possible value of t, $gcd(t, d) > 1$.

Now there are 2 cases:

If $k < 2m_2$, then $t = d - k$. Since $k|d$, $m_2|d$ and $gcd(k, m_2) = 1$, $km_2|d$. So, we get $\frac{k}{d} < \frac{1}{m_2}$. Hence,

$$\frac{t}{d} = 1 - \frac{k}{d} > 1 - \frac{1}{m_2} > 1 - \frac{1}{3} = \frac{2}{3} > \frac{3}{5}.$$

If $k \geq 2m_2$, then $t = d - 2m_2$. We can assume $m_1 \geq 5$, otherwise $f_1(x)$ is not a permutation polynomial. We also have $\frac{m_2}{n} < \frac{1}{m_1}$ since $m_1m_2 = m|d$. Thus,

$$\frac{t}{d} = 1 - \frac{2m_2}{d} > 1 - \frac{2}{m_1} > 1 - \frac{2}{5} = \frac{3}{5}.$$

Case 3: $m_1 > 1$ and $k_1 > 1$.

In this case we have $f_1(x) = D_{m_1}(a, x^{m_2}) + \alpha$, $g_1(x) = D_{k_1}(b, x^{k_2}) + \beta$. Since $e = 1$,

$(m_2, k_2) = 1$. Lemma 3.1.1 implies that $t = max\{d - 2m_2, d - 2k_2\}$.

Now there are four cases:
If $m_2 \neq 0$ and $k_2 \neq 0$, then $t = d - 2m_2$ or $t = d - 2k_2$. W.L.O.G, we can assume $t = d - 2m_2$. Then we have,

$$\frac{t}{d} = 1 - \frac{2m_2}{d} > 1 - \frac{2}{m_1} > \frac{3}{5}.$$

If $m_2 = 1, k_2 \neq 1$ or $m_2 \neq 1, k_2 = 1$, then for each case $t = d - 2$, and we get a contradiction to our assumption.

If $m_2 = k_2 = 1$ and $a \neq b$ then by using the definition of Dickson polynomial, we can observe that there is no cancellation, i.e., we have non-zero term with degree $d - 2$. Hence we will obtain $t = d - 2$. So, again we have a contradiction.

If $m_2 = k_2 = 1$ and $a = b$, then we will have $gcd(k, m) = 1$. In case $gcd(k, m) > 1$, we get $f_1 = f_0(D_r(a, x))$ and $g_1 = g_0(D_r(a, x))$ with $r = gcd(k, m)$. Since f_1 is as in (3.2), this gives a contradiction to maximality of m. By a similar argument k is maximal. We also have,

$$h = f - g = f_2(D_m(a, x) + \alpha) - g_2(D_k(a, x) + \beta).$$

Applying the identity

$$D_k(a, x + \frac{a}{x}) = x^k + \frac{a^k}{x^k}.$$

see the formula (1.2), we deduce that

$$\begin{aligned}
h(x + \frac{a}{x}) &= f_2(D_m(a, x + \frac{a}{x}) + \alpha) - g_2(D_k(a, x + \frac{a}{x}) + \beta) \\
&= f_2(x^m + \frac{a^m}{x^m} + \alpha) - g_2(x^k + \frac{a^k}{x^k} + \beta) \\
&= f_2(x^m + \alpha x^0 + a^m x^{-m}) - g_2(x^k + \beta x^0 + a^k x^k) \\
&= ((\frac{d}{m}\alpha)x^{d-m} + \cdots + (\frac{d}{m}a^m + A)x^{d-2m} + \cdots) \\
&- (\frac{d}{k}\beta x^{d-k} + \cdots + (\frac{d}{m}a^k + B)x^{d-2k} + \cdots),
\end{aligned}$$

where

$$f_2(x) = x^N + Ax^{N-2} + \cdots$$
$$g_2(x) = x^N + Bx^{N-2} + \cdots$$

with $N = \frac{d}{m}$.

We note that $d - m$ and $d - k$ are even while $d - 2m$ and $d - 2k$ are odd so that no cancellation occurs among the displayed terms. Moreover by the maximality of m, if $\alpha = 0$ the coefficient of x^{d-2m} is non-zero and similarly that of x^{d-2k} is non-zero if $\beta = 0$.
Also k and m both divide d with $k \geq 5$, $m \geq 5$. Depending on α or β being zero, we have:

$$t = \begin{cases} max\{d-2m, d-2k\} & \text{if } \alpha = \beta = 0, \\ max\{d-m, d-2k\} & \text{if } \alpha \neq 0, \\ max\{d-m, d-k\} & \text{if } \alpha\beta \neq 0 \end{cases}$$

We also note that if $\alpha = 0$, $\beta \neq 0$, then we have $t = max\{d-2m, d-k\}$, and the proof is the same case as $\alpha \neq 0, \beta = 0$. Clearly in each case $gcd(t, d) = k$ or $gcd(t, d) = m$ so that $gcd(t, n) > 1$.

Now, we have three cases concerning t;

Case 3.1: Assume $m < k$. Then $t = d - 2m$. Since $d \geq 5$, we obtain

$$\frac{t}{d} = 1 - \frac{2m}{d} \geq \frac{3}{5}.$$

Similar argument can be used for $k < m$.

Case 3.2: We have two subcases:
First of all, assume $m < 2k$. On the other hand $d \geq 5m$ since $d \geq km$ and $k \geq 5$. So in this case, we get

$$\frac{t}{d} = 1 - \frac{m}{d} \geq \frac{4}{5} > \frac{3}{5}.$$

Secondly, assume $m > 2k$. Since $d \geq km \geq$ and $m \geq 5$, we have $d \geq 5k$. Then in this case, we get

$$\frac{t}{d} = 1 - \frac{2k}{d} \geq \frac{3}{5}.$$

Case 3.3: Assume $m < k$. Then $t = d - m$. So, we get

$$\frac{t}{d} = 1 - \frac{m}{d} \geq \frac{3}{5}.$$

The case $k < m$ follows similarly. □

The following example shows that $deg(h(x))$ may attain the lower bound.

Example 3.1.5 *Assume $p \equiv 2 \mod 5$. Let*

$$g(x) = D_5(a, x^m) = x^{5m} - 5ax^{3m} + 5a^2x^m \quad \textit{and} \quad f(x) = x^{5m}$$

where $D_5(a, x) = x^5 - 5ax^3 + 5a^2x$ is the Dickson polynomial of degree 5 with $gcd(m, p - 1) = 1$.

Now $f(x)$ is a permutation polynomial, see Theorem 1.2.2, since $gcd(m, p - 1) = 1$. Also $g(x)$ is a permutation polynomial Theorem 1.2.3 since $p \equiv 2\ mod 5$, i.e., $gcd(5, p^2 - 1) = 1$. Thus both f and g are permutations of $\mathbb{F}_p$. Consider the difference

$$h(x) = f(x) - g(x) = +5ax^{3m} - 5a^2x^m$$

So, $deg(h(x)) = t = 3m$. Note that $5m = d$. Thus we get $t = 3d/5$.

The theorem that we have just proved yields a proof of the well-known Chowla-Zassenhaus conjecture as a special case. The first proof of the conjecture was given by Cohen in (1990), see [8]. We state it below.

Theorem 3.1.4 *Let p be a prime satisfying $p > (d^2 - 3d + 4)^2$ and $f(x) \in \mathbb{F}_p[x]$ be a permutation polynomial of degree $d \geq 2$. Then, there is no integer c with $1 \leq c < p$ such that $f(x) + cx$ is also a permutation polynomial of $\mathbb{F}_p$.*

Proof: Let c be an arbitrary constant with $1 \leq c < p$ and take $g(x) = f(x) + cx$. Assume $g(x)$ is a permutation polynomial. Then $h(x) = f(x) - g(x) = cx$ so that $deg(h) = t = 1 < 5d/3$ with $d \geq 2$. Hence we get a contradiction to Theorem 3.1.3.

□

3.2. A special case

As mentioned in the previous section, Chowla- Zassenhaus conjecture (the Theorem of Cohen [8]) states that if p is sufficiently large, when compared with the degree d of polynomials $f(x)$ and $g(x)+x$, then $f+x$ is not a permutation of $\mathbb{F}_p$ while f is. We recall that a permutation polynomial f is called a *complete mapping* if $f+x$ is also a permutation polynomial. This work of Işık, Topuzoğlu, Winterhof [13], takes a different viewpoint and studies the similar problem of existence of complete maps when f is a polynomial in $\mathbb{F}_q[x]$ of Carlitz rank n.

Theorem 3.2.5 *[13] Let $f(x) \in \mathbb{F}_q[x]$ be of Carlitz rank n, with a representation $f(x) = P_n(a_0, 0, a_2 \ldots, 0; x)$. Suppose $\alpha_n \neq 0$ where α_n is as in (1.4). If $q > 2n-1$, then $f+x$ is not a complete mapping.*

When $q > 2n+1$ and hence $f+x$ is not a permutation of $\mathbb{F}_q$, the value set V_{f+x} is also studied in [13], see Theorem 3. When f is of Carlitz rank 2, the values of $|V_{f+x}|$ were also given in [13], Proposition 5. We use the notation of [13], and put

$$a_0 = c_0, \ a_1 = 0, \ a_2 = c_1 \text{ and } a_3 = 0$$

and give the details of the proof of Proposition 5, in [13].

We shall be concerned with the permutation polynomial $f(x) = ((c_0x)^{q-2}+c_1)^{q-2} \in \mathbb{F}_q[x]$ for odd q with $c_0, c_1 \neq 0$ and $c_0 \neq -1$. Let $F(x) = f(x)+x = ((c_0x)^{q-2}+c_1)^{q-2}+x$. Then by definition of poles, $O_2 = \{0, -\frac{1}{c_0c_1}\}$. We can also use the 2nd convergent $R_2(x)$.

$$F(x) = R_2(x) + x = \frac{x(c_0c_1x + (c_0+1))}{c_0c_1x+1} \quad \text{for} \quad x \in \mathbb{F}_q \diagdown O_2.$$

Moreover, we know the set $F(O_2)$,

$$F(0) = \frac{1}{c_1}, \quad F(-\frac{1}{c_0c_1}) = -\frac{1}{c_0c_1}.$$

We note that $F(x) = 0$ for $x = \frac{-(1+c_0)}{c_0c_1}$. Since $c_0 \neq -1$, this is the only element c in $\mathbb{F}_q$ with $F(c) = 0$.

We observe that $F(x) = F(y)$ if and only if $y = -\frac{c_0c_1x+(c_0+1)}{(c_0c_1)^2x+c_0c_1}$. Since assuming $F(x) = F(y)$, that is

$$\frac{x(c_0c_1x + (c_0+1))}{c_0c_1x+1} = \frac{y(c_0c_1y + (c_0+1))}{c_0c_1y+1},$$

one gets $y = -\frac{c_0c_1x+(c_0+1)}{(c_0c_1)^2x+c_0c_1}$.

On the other hand assuming $y = -\frac{c_0c_1x+(c_0+1)}{(c_0c_1)^2x+c_0c_1}$. Then,

$$\begin{aligned} F(y) &= F(-\frac{c_0c_1x+(c_0+1)}{(c_0c_1)^2x+c_0c_1}) \\ &= \frac{x(c_0c_1x+c_0+1)}{c_0c_1x+1} \\ &= F(x). \end{aligned}$$

Note that in this case F is not 1-1 on $\mathbb{F}_q \diagdown O_2$. Thus if we consider the case $x = y$, i.e.,

$$x = -\frac{c_0c_1x+(c_0+1)}{(c_0c_1)^2x+c_0c_1}. \tag{3.4}$$

then we obtain x_1 and x_2 such that $F(x_1) = F(x_2)$.
If we assume (3.4), then we have

$$(c_0c_1)^2x^2 + 2c_0c_1x + c_0 + 1 = 0. \tag{3.5}$$

To solve the equation (3.5), we need $\Delta = 4(c_0c_1)^2(-c_0) \geq 0$ to be a square. But this holds only if $-c_0$ is a square.
Moreover, if $-c_0 = \lambda^2$ with $\lambda \in \mathbb{F}_q$, then we get

$$x_1 = \frac{-1+\lambda}{c_0c_1}, \quad x_2 = \frac{-1-\lambda}{c_0c_1}.$$

Finally, in case $-c_0 = \lambda^2$, we have $F(x_1) = F(x_2)$ with $x_1 \neq x_2$.

Next, we determine when $F(0) = \frac{1}{c_1}$ and $F(\frac{-1}{c_0c_1}) = \frac{-1}{c_0c_1}$ have pre-images in $\mathbb{F}_q \diagdown O_2$.

Lemma 3.2.6 *Let $F(x) = ((c_0x)^{q-2} + c_1)^{q-2} + x$. Then*
(a) If $1 + 4c_0$ is a square, then $F(0) = F(c)$ for some $c \in \mathbb{F}_q^*$.
(b) If $c_0(c_0 + 4)$ is a square, then $F(\frac{-1}{c_0c_1}) = F(c)$ for some $c \in \mathbb{F}_q \diagdown O_2$.

Proof:

(a) If

$$F(0) = \frac{1}{c_1} = \frac{x(c_0c_1x + (c_0+1))}{c_0c_1x+1} = F(x),$$

then we have $c_0c_1^2x^2 + c_1x - 1 = 0$ and to solve this equation, we need

$$c_1^2(1 + 4c_0) \geq 0 \text{ to be a square,}$$

which implies that $1 + 4c_0$ is a square.

(b) If

$$F(\frac{-1}{c_0c_1}) = \frac{-1}{c_0c_1} = \frac{x(c_0c_1x + (c_0 + 1))}{c_0c_1x + 1} = F(x),$$

then we obtain the equation $(c_0c_1)^2x^2 + (c_0c_1)(c_0 + 2)x + 1 = 0$ and again to solve it, we need

$$(c_0c_1)^2c_0(c_0 + 4) \geq 0 \text{ to be a square.}$$

Hence, $c_0(c_0 + 4)$ must be a square.

□

With the observation above we have the following result.

Theorem 3.2.7 *Let q be an odd prime power and $f(x) = ((c_0x)^{q-2} + c_1)^{q-2}$ be a permutation polynomial over $\mathbb{F}_q$, with $c_0, c_1 \neq 0$ and $c_0 \neq -1$. If $F(x) = f(x) + x$, then $|V_F|$ depends on $-c_0$, $(1 + 4c_0)$, and $c_0(4 + c_0)$, as follows.*

(i) If $-c_0$ is a square and $(1 + 4c_0)$, $c_0(4 + c_0)$ are non-squares, then $|V_F| = \frac{q+5}{2}$.

(ii) If $-c_0$ is a square and one of $(1 + 4c_0)$ and $c_0(4 + c_0)$ is a non-square, then $|V_F| = \frac{q+3}{2}$.

(iii) If $-c_0$, $(1 + 4c_0)$ and $c_0(4 + c_0)$ are all non-squares, then $|V_F| = \frac{q+3}{2}$.

(iv) If $-c_0$, $(1 + 4c_0)$, $c_0(4 + c_0)$ are all squares, then $|V_F| = \frac{q+1}{2}$.

(v) If $-c_0$ is a non-square, one of $(1 + 4c_0)$ and $c_0(4 + c_0)$ is a non-square, then $|V_F| = \frac{q+1}{2}$.

(vi) If $-c_0$ is a non-square, $(1+4c_0)$ and $c_0(4+c_0)$ are both squares, then $|V_F| = \frac{q-1}{2}$.

Proof:

(i) If $-c_0$ is a square, $(1+4c_0)$ and $c_0(4+c_0)$ are non-squares, then this gives the maximum value for $|V_F|$ since there exist distinct elements x_1, x_2 such that $F(x_1) = F(x_2)$ and we have $x_0 = \frac{-(1+c_0)}{c_0c_1}$ with $F(x_0) = 0$ and $F(\mathbb{F}_q \diagdown O_2) \cap F(O_2) = \emptyset$. Thus we obtain,

$$|V_F| = 2+2+1+\frac{q-2-2-1}{2} = \frac{q+5}{2}.$$

(ii) If $-c_0$ is a square, one of $(1+4c_0)$ and $c_0(4+c_0)$ is a non-square, then

$$|V_F| = 2+1+1+\frac{q-2-1-2}{2} = \frac{q+3}{2}.$$

(iii) If $-c_0$ is a non-square, $(1+4c_0)$ and $c_0(4+c_0)$ are non-squares, then

$$|V_F| = 1+2+\frac{q-2-1}{2} = \frac{q+3}{2}.$$

(iv) If $-c_0$ is a square, $(1+4c_0)$ and $c_0(4+c_0)$ are squares, then

$$|V_F| = 2+1+\frac{q-2-1-2}{2} = \frac{q+1}{2}.$$

(v) If $-c_0$ is a non-square, one of $(1+4c_0)$ and $c_0(4+c_0)$ is a non-square, then

$$|V_F| = 1+1+\frac{q-2-1}{2} = \frac{q+1}{2}.$$

(vi) If $-c_0$ is a non-square, $(1+4c_0)$ and $c_0(4+c_0)$ are squares, then there do not exist distinct elements x_1, x_2 such that $F(x_1) = F(x_2)$. However there exists $x_0 = \frac{-(1+c_0)}{c_0c_1}$ such that $F(x_0) = 0$ and for each pole $x_1, x_2 \in O_2$ we have x, y such that $F(x_1) = F(x)$, $F(x_2) = F(y)$. Therefore,

$$|V_F| = 1 + \frac{q-2-1}{2} = \frac{q-1}{2}.$$

□

Example 3.2.6 *Let $q = 7$ and $F(x) = ((c_0x)^5 + c_1)^5 + x$. In $\mathbb{F}_7$, the elements $0, 1, 2, 4$ are squares and $3, 5, 6$ are non-squares. Hence we can obtain some examples for some of the cases in Theorem 3.2.7.*

If we take $c_0 = 5$, then $-c_0 = 2$ is a square. Also we have $1 + 4c_0 = 0$ is a square, $c_0(4 + c_0) = 3$ is a non-square. So, we are in Case (iii).

Now take any $c_1 \in \mathbb{F}_7$, say $c_1 = 4$. Then the values of F over $\mathbb{F}_7$ are follows:

$$F(0) = 2,\ F(1) = 1,\ F(2) = 6,\ F(3) = 6,\ F(4) = 2,\ F(5) = 4,\ F(6) = 0$$

Hence, we obtain $V_F = \{0, 1, 2, 4, 6\}$, i.e.,

$$|V_F| = 5 = \frac{q+3}{2}.$$

If we take $c_0 = 2$, then $-c_0 = 5$ is not a square. Also we have $1 + 4c_0 = 2$ is a square, $c_0(4 + c_0) = 5$ is not a square. So we are in Case (vi).

Now take any $c_1 \in \mathbb{F}_7$, say $c_1 = 6$. Then the polynomial F takes the following values over $\mathbb{F}_7$:

$$F(0) = 6,\ F(1) = 6,\ F(2) = 3,\ F(3) = 6,\ F(4) = 4,\ F(5) = 0,\ F(6) = 1$$

Thus, we obtain $V_F = \{0, 1, 3, 6\}$ i.e.,

$$|V_F| = 4 = \frac{q+1}{2}.$$

Bibliography

[1] W. Aitken, *On Value Sets of Polynomials over a Finite Field*, Finite Fields and Their Appl. 4, pp. 441-449, (1998).

[2] E. Aksoy, A. Cesmelioğlu, W. Meidl , A. Topuzoğlu, *On the Carlitz rank of permutation polynomials.* Finite Fields Appl. 15, 428-440, (2009).

[3] H. Borges, R. Conceicao, *On the characterization of minimal value set polynomials*, J. Number Theory, 133, 2021-2035, (2013).

[4] L. Carlitz, *Permutations in a finite field*, Proc. American Math. Society, 4, 538, (1953).

[5] L.Carlitz, D. J. Lewis, W.H.Mills and E.G. Straus, *Polynomials over finite fields with minimal value set.* Mathematika, 8, 121-130, (1961).

[6] W.S. Chou , J. Gomez-Calderon , G.L. Mullen, *Value Sets of Dickson Polynomials over Finite Fields*, J. Number Theory, 30, 334-344, (1988).

[7] S. D. Cohen, G. L. Mullen, Peter J.S. Shiue, *The Difference Between Permutation Polynomials over Finite Fields*, Proc. Amer. Math. Soc. 123, 2011-2015, (1991).

[8] S. D. Cohen , *Proof of a Conjecture of Chowla Zassenhaus on Permutation Polynomials*, Canad. Math. Bull. Vol 33 (2), 230-234, (1990).

[9] T.W. Cusick, P. Muller, *Wan's bound for value sets of polynomials*, Finite Fields and Their Appl., (1996).

[10] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, *On the cycle structure of permutation polynomials*, Finite Fields Appl. 14. 593-614, (2008).

[11] J. Gomez-Calderon, D.J. Madden, *Polynomials with small value sets over finite fields*, J.Number Theory, 28 (2), 167-188, (1988).

[12] J.Gomez-Calderon, *A note on polynomials with minimal value sets over finite fields*, Mathematika, 35, 144-148, (1988).

[13] L. Işık, A. Topuzoğlu, A. Winterhof, *Complete mappings and Carlitz rank* , Designs, Codes and Cryptography, (2016).

[14] R. Lidl, G. L. Mullen, G. Turnwald, *Dickson Polynomials*, Longman Scientific and Technical, (1993).

[15] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, (1997).

[16] W.H. Mills, *Polynomials with minimal value sets.* Pacific J. of Math., 14, 225-241, (1964).

[17] G.L. Mullen, Permutation polynomials over finite fields, in *Proc. of the Intl. Conf. on Finite Fields, Coding Theory and Advances in Communications and Computing*, Lecture notes in Pure and Appl. Math., Vol. 141, pp. 131-151, Dekker, New York, (1993).

[18] G. L. Mullen, D. Panario, *Handbook of Finite Fields*, CRC Press, (2013).

[19] G.L. Mullen, D. Wan, Q. Wang, *Index bound for value sets of polynomials over finite fields*, in Applied Algebra and Number Theory, Larcher Pillichshemmer, Winterhof, Xing (Ed), Cambridge University Press, (2014).

[20] C. J. Shallue, *Permutation Polynomials of Finite Fields*, arXiv:1211.6044v [math.NT] 23 Nov 2012.

[21] I. Shparlinski, *Finite Fields: Theory and Computation*, Kluwer, May 31, (1999).

[22] A. Topuzoğlu, *Carlitz rank of permutations of finite fields*: A survey, Journal of Symbolic Computation 64, 182-193, (2014).

[23] G. Turnwald, *A new criterion for permutation polynomials*, Finite Fields Appl., 1, 64-82, (1995)

[24] D. Wan, A p-adic lifting lemma and its applications to permutation polynomials, in *Proc. of the Intl. Conf. on Finite Fields, Coding Theory and Advances in Communications and Computing*, Lecture notes in Pure and Appl. Math., Vol. 141, pp. 209-216, Dekker, New York, (1993).

[25] D. Wan, P.J. Shiue, C.S. Chen., *Value sets of polynomials over finite fields*, Proceedings of the American Math. Soc., Volume 119, Number 3, (1993).