ON COMPLETE MAPPINGS AND VALUE SETS OF POLYNOMIALS OVER FINITE FIELDS

by

LEYLA IŞIK

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

Sabancı University
Fall 2015

ON COMPLETE MAPPINGS AND VALUE SETS OF POLYNOMIALS OVER FINITE FIELDS

APPROVED BY

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

Assoc. Prof. Dr. Cem Güneri .....

Assoc. Prof. Dr. Selda Küçükçifçi .....

Prof. Dr. Erkay Savaş .....

Assoc. Prof. Dr. Arne Winterhof .....

DATE OF APPROVAL : September 8, 2015

ON COMPLETE MAPPINGS AND VALUE SETS OF POLYNOMIALS OVER FINITE FIELDS

Leyla Işık

Mathematics, PhD Thesis, 2015

Thesis Supervisor: Prof. Dr. Alev Topuzoğlu

Keywords: finite fields, permutation polynomials, Carlitz rank, complete mapping polynomials, value sets, minimal value set polynomials, spectrum.

Abstract

In this thesis we study several aspects of permutation polynomials over finite fields with odd characteristic. We present methods of construction of families of complete mapping polynomials; an important subclass of permutations. Our work on value sets of non-permutation polynomials focus on the structure of the spectrum of a particular class of polynomials.

Our main tool is a recent classification of permutation polynomials of $\mathbb{F}_q$, based on their Carlitz rank. After introducing the notation and terminology we use, we give basic properties of permutation polynomials, complete mappings and value sets of polynomials in Chapter 1.

We present our results on complete mappings in $\mathbb{F}_q[x]$ in Chapter 2. Our main result in Section 2.2 shows that when $q > 2n + 1$, there is no complete mapping polynomial of Carlitz rank n, whose poles are all in $\mathbb{F}_q$. We note the similarity of this result to the well-known Chowla-Zassenhaus conjecture (1968), proven by Cohen (1990), which is on the non-existence of complete mappings in $\mathbb{F}_p[x]$ of degree d, when p is a prime and is sufficiently large with respect to d. In Section 2.3 we give a sufficient condition for the construction of a family of complete mappings of Carlitz rank at most n. Moreover, for $n = 4, 5, 6$ we obtain an explicit construction of complete mappings.

Chapter 3 is on the spectrum of the class $\mathcal{F}_{q,n}$ of polynomials of the form $F(x) = f(x)+x$, where f is a permutation polynomial of Carlitz rank at most n. Upper bounds for the cardinality of value sets of non-permutation polynomials of the fixed degree d or fixed index l were obtained previously, which depend on d or l respectively. We show, for instance, that the upper bound in the case of a subclass of $\mathcal{F}_{q,n}$ is $q - 2$, i.e., is independent of n.

We end this work by giving examples of complete mappings, obtained by our methods.

SONLU CİSİMLER ÜZERİNDEKİ POLİNOMLARIN DEĞER KÜMELERİ VE TAM GÖNDERİMLER ÜZERİNE

Leyla Işık

Matematik, Doktora Tezi, 2015

Tez Danışmanı: Prof. Dr. Alev Topuzoğlu

Anahtar Kelimeler: sonlu cisimler, permütasyon polinomları, Carlitz mertebesi, tam gönderimli polinomlar, değer kümeleri, minimum değer kümesi polinomları, spektrum.

Özet

Bu tezde karakteristiği tek olan sonlu cisimler üzerindeki permütasyon polinomlarıyla ilgili bazı ilginç problemler üzerinde çalışılmıştır. Permütasyonların önemli bir alt sınıfı olan tam gönderim polinomlarını inşa etme metodları sunulmuştur. Permütasyon olmayan polinomların değer kümeleri üzerine olan çalışmamız özel bir polinom sınıfının spektrum yapısına odaklanmıştır.

Bu çalışmada kullandığımız ana araç, $\mathbb{F}_q$ üzerindeki permütasyon polinomlarının Carlitz mertebesine göre sınıflandırılmasıdır. Birinci bölümde, tanım ve terimleri verdikten sonra permütasyon polinomlarının, tam gönderimlerin ve polinomların değer kümelerinin temel özellikleri verilmiştir.

İkinci bölümde, $\mathbb{F}_q[x]$ de tam gönderimler üzerine olan sonuçlar sunulmuştur. Bu bölümdeki esas sonuçlarımızdan birisi, $q > 2n+1$ olduğu zaman tüm kutupları $\mathbb{F}_q$ da ve Carlitz mertebesi n olan tam gönderimli polinom olmadığıdır. Bu sonuç yaygın olarak bilinen ve Cohen tarafından 1990'da kanıtlanmış, Chowla-Zassenhaus varsayımına (1968) benzer özelliktedir, çünkü bu varsayım p asal sayısı d sayısına göre yeterince büyükse derecesi d olan tam gönderimli polinom olmadığını belirtmektedir. Bölüm 2.3 de Carlitz mertebesi en fazla n olan tam gönderimler ailesinin inşası için yeterli koşullar verilmiştir. Ayrıca, $n = 4, 5, 6$ için tam gönderimlerin açık inşası elde edilmiştir.

Üçüncü bölüm, Carlitz mertebesi en fazla n olan f permütasyon polinomu için $F(x) = f(x)+x$ formundaki polinomlar sınıfı $\mathcal{F}_{q,n}$'nin spektrumu üzerinedir. Permütasyon olmayan polinomların değer kümelerindeki eleman sayısı için üst sınır bulma önemli bir problemdir. Derecesi d veya indeksi l olan polinomlar için bu sınırlar d veya l'ye baglı olarak daha önce elde edilmişti. Bu çalışmada $\mathcal{F}_{q,n}$'nin bir alt sınıfı için bu üst sınırın $q-2$, yani n'den bağımsız olduğu gösterilmiştir.

Son bölümde kullandığımız yöntemlerle elde ettiğimiz tam gönderim örnekleri verilmiştir.

sevgili Anneme

ve

sevgili Babama

Acknowledgments

First of all I would like to express my sincere gratitude to my advisor Prof. Alev Topuzoğlu for her motivation, guidance and encouragement throughout this thesis. I am thankful to her continuous support during my PhD and for the opportunities she has given me to participate in international conferences. I am also very thankful to Prof. Arne Winterhof since this study was initiated by discussions we had at a conference in Barcelona in May 2014.

My special gratitude goes to my family, especially my parents, for their love and constant support throughout all the different stages of my study. Their support and love were the sustaining factors in carrying out this work successfully.

I also express deep and sincere gratitude to Michel for his useful comments on the final stage of this work, and most of all for his love and true-hearted support.

Finally, I am also very grateful to have nice friends in campus and I would like to thank them, especially İlker Arslan for all the enjoyable time we had together.

Contents

CHAPTER 1

Introduction

Throughout this thesis $\mathbb{F}_q$ will denote the finite field with $q = p^s$ elements where p is a prime, and $s \geq 1$ is a positive integer.

In this chapter, we give a survey of basic properties of permutation polynomials, and introduce the concepts of Carlitz rank, complete mapping and spectrum of a class of polynomials. In Section 1.1, we review some of the known classes of permutation polynomials over $\mathbb{F}_q$. We list the known results about Carlitz rank of a permutation polynomial in Section 1.2. After introducing the notation and some of the basic tools we will give the relation between Carlitz rank of a permutation polynomial $f \in \mathbb{F}_q[x]$, its degree, and the number of its nonzero coefficients, i.e. its weight. In Section 1.3, we will focus on some of the basic properties of value sets of polynomials and give some recent results. Finally in Section 1.4, we discuss complete mapping polynomials over finite fields.

1.1 Permutations of Finite Fields

Definition 1.1. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* if the induced function $f : \mathbb{F}_q \to \mathbb{F}_q \ : \ c \mapsto f(c)$ is a bijection.

From now on a permutation polynomial will be abbreviated as PP. PPs over finite fields have wide applications in cryptography, coding theory, combinatorics, finite geometry and computer science, and hence finding new classes of PPs is of great interest.

It is well known that each function from $\mathbb{F}_q$ to $\mathbb{F}_q$ can be represented by a polynomial. In particular, given a permutation σ of the elements of $\mathbb{F}_q$, there exists a unique polynomial $f_\sigma \in \mathbb{F}_q[x]$ with $deg(f_\sigma) < q$ such that $f_\sigma(c) = \sigma(c)$ for all $c \in \mathbb{F}_q$.

The polynomial f_σ can be found by the Lagrange interpolation formula;

$$f_\sigma(x) = \sum_{c\in\mathbb{F}_q} \sigma(c)\big(1-(x-c)^{q-1}\big). \tag{1.1}$$

On the other hand given an arbitrary polynomial $f(x) \in \mathbb{F}_q[x]$, it is in general a difficult task to determine whether $f(x)$ is a PP of $\mathbb{F}_q$. A useful criterion for a polynomial being a PP was given in 1863 by Hermite [34] for prime fields, which was then generalized in 1897 by Dickson [27] to arbitrary finite fields $\mathbb{F}_q$. We include a proof based on [37, Chapter 7].

Lemma 1.2. *For $a_0, \ldots, a_{q-1} \in \mathbb{F}_q$, the equation*

$$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{for} \quad 0 \le t \le q-2 \\ -1 & \text{for} \quad t = q-1 \end{cases}$$

holds if and only if all a_i are distinct.

Proof. For any $i \in \{0, \ldots, q-1\}$, using Langrange's interpolation formula the function $\varphi_i : \mathbb{F}_q \to \mathbb{F}_q$ defined by $\varphi_i(b) = 0$ for $b \neq a_i$ and $\varphi_i(a_i) = 1$ corresponds to the polynomial

$$g_i(x) = 1 - (a_i - x)^{q-1},$$

which becomes

$$g_i(x) = 1 - \sum_{j=0}^{q-1} (-1)^j \binom{q-1}{j} a_i^{q-1-j} x^j = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j,$$

since $\binom{q-1}{j} = (-1)^j$ in $\mathbb{F}_q$ for any $j \in \{0, \ldots, q-1\}$. Then the polynomial

$$g(x) = \sum_{i=0}^{q-1} g_i(x)$$

satisfies $g(a_i) = 1$ for all $i \in \{0, \ldots, q-1\}$. If all a_i are distinct then this implies that $g(x) = 1$. Rewriting $g(x)$ we obtain

$$g(x) = \sum_{i=0}^{q-1} \left(1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j\right) = \sum_{j=0}^{q-1} \left(-\sum_{i=0}^{q-1} a_i^{q-1-j}\right) x^j, \tag{1.2}$$

and so if all a_i are distinct we obtain

$$\sum_{i=0}^{q-1} a_i^{q-1-j} = 0$$

for all $1 \leq j \leq q-1$, and hence

$$\sum_{i=0}^{q-1} a_i^t = 0$$

for all $0 \leq t \leq q-2$. If not all a_i are distinct, then $g(x) \neq 1$ and hence some non-constant term in (1.2) is nonzero, implying that for some $0 \leq t \leq q-2$

$$\sum_{i=0}^{q-1} a_i^t \neq 0,$$

which concludes the proof. □

Theorem 1.3. *(Hermite's Criterion)*
A polynomial $f(x) \in \mathbb{F}_q[x]$ is a PP of $\mathbb{F}_q$ if and only if the following two conditions are satisfied:

(i) *f has exactly one root in $\mathbb{F}_q$.*

(ii) *For each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \mod p$, the reduction of $f(x)^t \mod (x^q - x)$ has degree $\leq q-2$.*

Proof. Suppose $f(x)$ is a PP of $\mathbb{F}_q$. Then obviously f has exactly one root in $\mathbb{F}_q$. For $1 \leq t \leq q-2$, we have $\sum_{c \in \mathbb{F}_q} f(c)^t = 0$, by Lemma 1.2. Put $h(x) = f(x)^t \mod x^q - x$, say $h(x) = \sum_{i=0}^{q-1} h_i x^i$. Then again applying Lemma 1.2,

$$0 = \sum_{c \in \mathbb{F}_q} f(c)^t = \sum_{c \in \mathbb{F}_q} h(c) = \sum_{i=0}^{q-1} h_i \sum_{c \in \mathbb{F}_q} c^i = h_{q-1} \sum_{c \in \mathbb{F}_q} c^{q-1} = -h_{q-1},$$

and hence $h(x)$ has degree at most $q-2$. Conversely suppose conditions (i) and (ii) are satisfied. From (i) it follows that $\sum_{c \in \mathbb{F}_q} f(c)^{q-1} = -1$. Also as above for each $1 \leq t \leq q-2$, with $h(x) = f(x)^t \mod x^q - x$, $h(x) = \sum_{i=0}^{q-1} h_i x^i$, it follows that $\sum_{c \in \mathbb{F}_q} f(c)^t = -h_{q-1}$, which is zero by (ii). Applying Lemma 1.2 we can conclude that all values $f(c)$, $c \in \mathbb{F}_q$, are distinct, i.e. $f(x)$ is a PP. □

Remark 1.4. It immediately follows from Hermite's criterion that, $f(x)$ is not a PP if the degree of $f(x)$ divides $q-1$, which also implies that the maximal degree of a permutation polynomial modulo $x^q - x$ is $q-2$.

Let G be a finite abelian group. A *character* χ of G is a homomorphism from G into the multiplicative group U of complex numbers with absolute value 1, i.e. it is a mapping from G into U which satisfies $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$.
For any finite field $\mathbb{F}_q$, there are two classes of characters, *additive* characters which are the characters of the additive group $\mathbb{F}_q$ of q elements and *multiplicative* characters which are the characters of the multiplicative group $\mathbb{F}_q^*$ of $q-1$ elements. By using the nontrivial additive characters, another criterion for identifying PPs can be given:

Theorem 1.5. *The polynomial $f(x) \in \mathbb{F}_q[x]$ is a PP of $\mathbb{F}_q$ if and only if*

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = 0$$

for every nontrivial additive character χ of $\mathbb{F}_q$.

For a proof of the theorem see [37, Chapter 7].

Only a few good algorithms are known for testing whether a given polynomial is a PP. In general, it is not easy to find new classes of PPs. For some well known classes of polynomials, however, necessary and sufficient conditions have been determined to decide whether a polynomial in the given class is a PP.

We list some of the known classes of PPs. Obviously, every linear polynomial $ax+b \in \mathbb{F}_q[x]$, $a \neq 0$, is a PP of $\mathbb{F}_q$.

It is easy to see that a monomial x^n permutes $\mathbb{F}_q$ if and only if $gcd(n, q-1) = 1$.

A class of polynomials for which the permutation property can be seen immediately is well understood is the class of linearized polynomials, see [37, Chapter 7]. The linearized polynomial $L(x)$ defined as

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

is a PP of $\mathbb{F}_{q^k}$ if and only if $x = 0$ is the only root in $\mathbb{F}_{q^k}$ of $L(x)$.

The class of Dickson polynomials are widely studied in connection with a large variety of problems. There are two types of them. Dickson polynomials of the 1^{st} kind are defined for every $a \in \mathbb{F}_q$, by the formula

$$D_n(x,a) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-a)^j x^{n-2j}, \tag{1.3}$$

and Dickson polynomials of the 2^{nd} kind $E_n(x,a)$ with parameter $a \in \mathbb{F}_q$ are defined as

$$E_n(x,a) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-j}{j} (-a)^j x^{n-2j}. \tag{1.4}$$

Obviously, $\deg(D_n(x,a)) = n$ and $D_n(x,0)$ is just the monomial x^n, and similarly, $\deg(E_n(x,a)) = n$ and $E_n(x,0) = x^n$. Also $D_n(x,a)$ with $a \in \mathbb{F}_q^*$ is a PP of $\mathbb{F}_q$ if and only if $\gcd(n, q^2-1) = 1$, see [36, Chapter 3] for a proof. Deciding whether a Dickson polynomial of the second kind is a PP is much more complicated. It was shown by Matthews [40] that the conditions $n+1 \equiv \pm 2 \mod m$ for each of the values $m = p, (q-1)/2, (q+1)/2$ are sufficient for $E_n(x,1) \in \mathbb{F}_q[x]$ to induce a permutation of $\mathbb{F}_q$. Later, Cohen [17] proved that when q is a prime these conditions are also necessary to conclude that $E_n(x,1)$ is a PP. Further results about Dickson polynomials of the 2^{nd} kind that are PPs can be found in Coulter [19], Henderson and Matthews [33] and Henderson [32].

A large variety of further results on PPs can be found in [37, Chapter 7]. We end this section by giving some typical results on criteria that yield special classes of PPs. For a recent survey of the subject we refer to [35], see also [45, Chapter 8].

The following theorem concerns binomials.

Theorem 1.6. *[37] If q is odd, then the polynomial $x^{(q+1)/2} + ax \in \mathbb{F}_q[x]$ is a PP if and only if $a^2 - 1$ is a nonzero square.*

The following theorem describes two large classes of permutation polynomials of $\mathbb{F}_q$. Here Tr denotes, as usual, the absolute trace, defined as

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}(a) = a + a^p + \ldots + a^{p^{s-1}},$$

for $a \in \mathbb{F}_q$ and where $q = p^s$.

Theorem 1.7. *[13] If $\gamma, \beta \in \mathbb{F}_q$ and $H(x) \in \mathbb{F}_q[x]$, then*
(i) the polynomial

$$F(x) = x + \gamma \mathrm{Tr}\left(H\left(x^p - \gamma^{p-1}x\right) + \beta x\right)$$

is a PP if and only if $\mathrm{Tr}(\beta\gamma) \neq -1$, *and*
(ii) the polynomial

$$F(x) = x + \gamma \mathrm{Tr}\left(\sum_{u \in \mathbb{F}_p} H\left(x + \gamma u\right) + \beta x\right)$$

is a PP if and only if $\mathrm{Tr}(\beta\gamma) \neq -1$.

In [55] Tu et al. propose several classes of PPs of the form

$$\left(x^{p^m} - x + \delta\right)^s + L(x) \in \mathbb{F}_{p^m}[x]$$

where p is an odd prime, and $L(x)$ is a linearized polynomial with coefficients in $\mathbb{F}_p$. One of their results is the following theorem.

Theorem 1.8. *[55] For $m \in \mathbb{Z}^+$ and any $\delta \in \mathbb{F}_{3^{2m}}$, the polynomial*

$$f(x) = \left(x^{3m} - x + \delta\right)^{2\cdot 3^m - 1} + x^{3^m} + x$$

is a PP.

Polynomials of the form

$$\left(x^{2^m} + x + \delta\right)^s + x \in \mathbb{F}_{2^{2m}}[x]$$

are studied in Tu et al. in [56], and many classes of PPs of this form are obtained. Here we only mention one of their results, which says that each such polynomial with $s = 2^{m+1} - 1$ is a PP.

In the following result by Zieve [63, Theorem 1.2], the symbol μ_d denotes the set of d^{th} roots of unity in the algebraic closure of $\mathbb{F}_q$.

Theorem 1.9. *Let d, r be positive integers and $d|(q-1)$. Assume that $q = q_0^m$ satisfy $q_0 \equiv 1 \pmod d$ and $d|m$ and select $h \in \mathbb{F}_{q_0}[x]$. Then $f(x) = x^r h(x^{(q-1)/d})$ permutes $\mathbb{F}_q$ if and only if $\gcd(r, (q-1)/d) = 1$ and h has no roots in μ_d.*

Akbary et al. constructed the following classes of PPs of F_{q^2}.

Theorem 1.10. *[2] Let $q = p^m$. Then the following are PPs over F_{q^2}:*
(i) $f(x) = ax^q + bx + (x^q - x)^k$, for $a, b \in \mathbb{F}_q$ with $a \neq \pm b$ and k even,
(ii) $f(x) = ax^q + ax + (x^q - x)^k$, for $a \in \mathbb{F}_q^*$ with p, k odd and $\gcd(k, q-1) = 1$.

1.2 Carlitz Rank of a Permutation Polynomial

The set of PPs of $\mathbb{F}_q$ of degree $\leq q-2$ forms a group under the operation of composition and reduction modulo $x^q - x$. This group is isomorphic to S_q, the symmetric group on q letters.

In 1953 L. Carlitz observed that the transposition (0 1) can be represented by the polynomial

$$g(x) = (((-x)^{q-2} + 1)^{q-2} - 1)^{q-2} + 1 \tag{1.5}$$

and hence the group S_q is generated by the linear polynomials $ax + b$ for $a, b \in \mathbb{F}_q$, $a \neq 0$ and x^{q-2}, see [10]. Consequently, as pointed out in [24], any permutation f of $\mathbb{F}_q$ can be represented by a polynomial of the form

$$P_n(x) = (\ldots((a_0x + a_1)^{q-2} + a_2)^{q-2} \ldots + a_n)^{q-2} + a_{n+1},\ n \geq 0, \tag{1.6}$$

where $a_i \neq 0$, for $i = 0, 2, \ldots, n$.

We can also write (1.6) as $P_n(x) = (P_{n-1}(x))^{q-2} + a_{n+1}$ for $n \geq 1$ by defining $P_0(x) = a_0x + a_1$.

Note that n is the number of times the monomial x^{q-2} occurs in (1.6). This representation is not unique, and n is not necessarily minimal. Accordingly the Carlitz rank of f is defined in [3] to be the smallest integer $n > 0$ satisfying $f(c) = P_n(c)$ for all $c \in \mathbb{F}_q$, for a permutation P_n of the form (1.6). In other words the Carlitz rank of f is n if n is minimal such that f can be represented by a polynomial which is the composition of n "inversions", x^{q-2} , and n (or $n + 1$) linear polynomials. We denote the Carlitz rank of f by $Crk(f)$.

The representation of a permutation f as in (1.6) enables approximation of f by a rational function as described below. This property is particularly useful when $Crk(f)$ is small with respect to the field size. Suppose that f has a representation P_n as in (1.6). We follow the notation of [54] and put $P_n(x) = P_n(a_0, a_1, ..., a_{n+1}; x)$ when we wish to specify the elements $a_0, a_1, ..., a_{n+1}$ in $\mathbb{F}_q$. Since for each $c \in \mathbb{F}_q^*$, $c^{q-2} = c^{-1}$, we define T as the set $c \in \mathbb{F}_q$ for which one of the expressions

$$(\ldots((a_0c + a_1)^{q-2} + a_2)^{q-2} \ldots + a_i), \quad i = 1, \ldots, n,$$

is zero, then it makes sense to consider the function : $\Psi_n : \mathbb{F}_q \setminus T \to \mathbb{F}_q$, defined by

$$c \mapsto (\ldots((a_0c + a_1)^{-1} + a_2)^{-1} \ldots + a_n)^{-1} + a_{n+1}.$$

It follows that for each $c \in \mathbb{F}_q \setminus T$ we have $P_n(c) = \Psi_n(c)$. We may also rewrite the function Ψ_n, by its continued fraction expansion, obtaining

$$\Psi_n(c) = \frac{\alpha_{n+1}c + \beta_{n+1}}{\alpha_n c + \beta_n},$$

where $\alpha_0 = 0,\ \alpha_1 = a_0,\ \beta_0 = 1,\ \beta_1 = a_1$, and

$$\alpha_k = a_k\alpha_{k-1} + \alpha_{k-2} \quad \text{and} \quad \beta_k = a_k\beta_{k-1} + \beta_{k-2}, \tag{1.7}$$

for $k \geq 2$. We remark here that α_k and β_k cannot both be zero. We will also consider the rational function

$$R_n(x) = \frac{\alpha_{n+1}x + \beta_{n+1}}{\alpha_n x + \beta_n}, \tag{1.8}$$

which we call the *rational fraction associated to* $P_n(x)$. Then the poles of the rational functions $R_i(x)$, for $i = 1, \ldots, n$, are $-\beta_i/\alpha_i \in \mathbb{F}_q \cup \{\infty\}$, and we will denote these poles by

$$x_i = \frac{-\beta_i}{\alpha_i}, \quad i = 1, \ldots, n. \tag{1.9}$$

Note that to every rational transformation $R_n(x)$ of the form (1.8) we can naturally associate a permutation σ_n of $\mathbb{F}_q$ defined by

$$\sigma_n(c) = R_n(c) \text{ for } c \neq x_n \text{ and } \sigma_n(x_n) = \tfrac{\alpha_{n+1}}{\alpha_n} \text{ when } x_n \in \mathbb{F}_q.$$

The set $\mathbf{O}_n = \{x_i : i = 1, \ldots, n\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ is called the *set of poles of* $P_n(x)$. Obviously $P_n(c) = R_n(c)$ for $c \in \mathbb{F}_q \backslash \mathbf{O}_n$. Therefore the values of $P_n(c)$ outside the set of poles are determined by R_n. The values that $P_n(x)$ takes at the poles can also be given in terms of R_n. In the special case, where the poles are distinct elements of $\mathbb{F}_q$ we have the following.

Lemma 1.11. *[24] Suppose that the poles $x_1, x_2, \ldots, x_n$ defined above are in $\mathbb{F}_q$ and distinct. Then*

$$P_n(x_i) = \begin{cases} \sigma_n(x_{i-1}) & \text{for } 2 \leq i \leq n, \\ \sigma_n(x_n) & \text{for } i = 1, \end{cases}$$

for all $n \geq 2$. We can therefore express the permutation $c \mapsto P_n(c)$ as

$$P_n(c) = \tau(\sigma_n(c)) \tag{1.10}$$

where τ is the permutation $(\sigma_n(x_n)\sigma_n(x_{n-1})...\sigma_n(x_1)) \in S_q$.

It was proved in [3] that although a permutation can have different representations, the associated fractional transformations are unique under a certain condition.

Lemma 1.12. *Let $P_n^{'}$ and $P_m^{"}$ be two representations of a permutation of $\mathbb{F}_q$, with associated rational fractions $R_n^{'}(x)$ and $R_m^{"}(x)$, respectively. If $m+n < q-2$, then $R_n^{'}(x) = R_m^{"}(x)$.*

The Carlitz rank can be considered as a complexity measure for polynomials. An immediate question therefore is whether it is related to the usual complexity measures, namely the degree and the weight.

Let $f(x)$ be a PP in $\mathbb{F}_q[x]$. The following results show that if the degree, $deg(f) > 1$ or weight of f, $w(f)$ are small then $Crk(f)$ must be large.

Theorem 1.13. *Let $f(x)$ be a PP in $\mathbb{F}_q[x]$ with $deg(f) = d > 1$. Then*

$$Crk(f) \geq q - d - 1.$$

See [3] for the proof.

Theorem 1.14. *Let $f \in \mathbb{F}_q[x]$ be a PP, $deg(f) > 1$*

$$f(x) = \sum_{i=1}^{w(f)} a_i x^{e_i}, \quad \text{and } f(x) \neq c_1 + c_2 x^{q-2}$$

for $c_1, c_2 \in \mathbb{F}_q$, $c_2 \neq 0$. Then $Crk(f) \geq \dfrac{q}{w(f)+2} - 1$.

See [29] for the proof of this theorem. Note that both bounds above are tight for PPs of the form $f(x) = (a_0 x + a_1)^{q-2}$, with $a_0, a_1 \in \mathbb{F}_q^*$, and the bound from Theorem 1.14 depending on $w(f)$ is better when $q \leq q/(w(f)+2) + deg(f)$.

Let σ be a cycle in S_q and $l(\sigma)$ denote its length. By definition $a \in supp(\sigma)$ if $a \in \mathbb{F}_q$ is not fixed by σ.

The proof of the following theorem can be found in [3]. A permutation τ of $\mathbb{F}_q$ is called *linear* if it can be represented by a linear polynomial.

Theorem 1.15. *Suppose a permutation f has a representation $P_m(x)$ satisfying*

$$P_m(c) = \tau_1 \dots \tau_s \sigma_m(c),$$

where $\tau_1, \dots, \tau_s$ are disjoint cycles of length $l(\tau_j) = l_j \geq 2$, $1 \leq j \leq s$.

(i) If σ_m is not linear and $\sigma_m(x_m) \in \mathrm{supp}(\tau_j)$ for some $1 \leq j \leq s$, then there exists a permutation $\bar{P}_n(x)$ with $n = s + \sum_{j=1}^{s} l_j - 1$ such that $f(c) = \bar{P}_n(c)$ for all $c \in \mathbb{F}_q$.

(ii) If σ_m is not linear and $\sigma_m(x_m) \notin \mathrm{supp}(\sigma_j)$ for any $1 \leq j \leq s$, then there exists a permutation $\bar{P}_n(x)$ with $n = s + \sum_{j=1}^{s} l_j + 1$ such that $f(c) = \bar{P}_n(c)$ for all $c \in \mathbb{F}_q$.

(iii) If σ_m is linear then there exists a permutation $\bar{P}_n(x)$ with $n = s + \sum_{j=1}^{s} l_j$ such that $f(c) = \bar{P}_n(c)$ for all $c \in \mathbb{F}_q$.

In all three cases, $Crk(P) = n$ if $n < (q-1)/2$.

We denote the number of permutations of $\mathbb{F}_q$ of Carlitz rank n by $B(n)$. Obviously $B(0) = q(q-1)$, $B(1) = q^2(q-1)$ and $B(2) = q^2(q-1)^2$. When $n \geq 3$, two different representations P_n and $P_n^{'}$ may induce the same permutation f, although the coefficients are different. However $n < (q-1)/2$ implies that the permutation f has a unique decomposition $P = \tau_1 \ldots \tau_s \sigma$, where $\tau_1 \ldots \tau_s$ are disjoint cycles. Hence one can obtain the value of $B(n)$ by counting such decompositions. Let t, k, s be integers with $t, k \geq 1$, $s \geq 0$. Consider the set $s(t,k,s)$ of permutations $\pi \in S_k$ with decomposition $\pi = \sigma_1 ... \sigma_s$ into disjoint cycles $\sigma_1 ... \sigma_s$ such that $l(\sigma_i) \geq t$ for $i = 1, 2, \ldots, s$. The integers $S(t,k,s) = |s(t,k,s)|$ are called the associated Stirling numbers of the first kind.

Theorem 1.16. *The number $B(n)$ of permutations of $\mathbb{F}_q$ with Carlitz rank n is given by*

$$\begin{aligned} B(n) &= (q^2-q) \sum_{s=1}^{\lfloor \frac{n+1}{3} \rfloor} \binom{q}{n+1-s} S(2, n+1-s, s)(n+1-s) \\ &\quad + (q^2-q) \sum_{s=1}^{\lfloor \frac{n-1}{3} \rfloor} \binom{q}{n-1-s} S(2, n-1-s, s)(q-(n-1-s)) \\ &\quad + (q^2-q) \sum_{s=1}^{\lfloor \frac{n}{3} \rfloor} \binom{q}{n-s} S(2, n-s, s) \end{aligned}$$

for all $2 \leq n < (q-1)/2$.

See [3] for the proof of this theorem.

We close this subsection by an example illustrating an application in cryptography which involves permutation polynomials of Carlitz rank 1 and 2, see Çeşmelioğlu et

al. [25]. In symmetric cryptography, one is interested in finding permutations which are easy to implement, provide a good resistance to differential and Matsui's linear attacks, and have large polynomial degree and large weight, see [9], [39], [51].

The difference map of a given polynomial $f \in \mathbb{F}_q[x]$, and $a \in \mathbb{F}_q^*$ is defined as

$$D_{f,a}(x) = f(x+a) - f(a).$$

The function f is called *perfect nonlinear* (PN) if $D_{f,a}$ is a permutation for all $a \in \mathbb{F}_q^*$, and f is *almost perfect nonlinear* (APN) if $D_{f,a}$ is 2-to-1 for all $a \in \mathbb{F}_q^*$. The *differential uniformity* δ_f of f is defined by

$$\delta_f = \max\{\delta_{f,a}(b) \ : \ b \in \mathbb{F}_q, a \in \mathbb{F}_q^*\},$$

where $\delta_{f,a}(b) = |\{x \in \mathbb{F}_q \ : \ D_{f,a} = b\}|$. One of the essential properties of a PP to be used in cryptography is to have low differential uniformity, see [6, 7, 9]. We note that a PP can not be a PN, so APN permutations have the lowest differential uniformity possible. It is well known that the differential uniformity of a function is invariant under the so-called EA-equivalence. It is expected therefore that when $q = p^s$, $p \equiv 5 \mod 6$, and s is odd, permutations of Carlitz rank 1, being EA equivalent to the inversion x^{q-2}, are APN. It is quite unexpected however that a new class of permutations with differential uniformity 4, when $p \equiv 5 \mod 6$, and s is odd, can be obtained from permutation polynomials of Carlitz rank 2.

Theorem 1.17. *[25] Let f be a permutation of $\mathbb{F}_q$, where $q = p^s$, $s \geq 1$ is odd, $p \equiv 5 \ mod \ 6$.*

(i) If $Crk(f) = 1$, then f is APN.

(ii) If $Crk(f) = 2$, then $\delta_f = 4$.

Suppose a permutation $f(x) \in \mathbb{F}_q[x]$ has Carlitz rank n, $n > 2$, with a representation

$$f(x) = P_n(a_0, \ldots, a_n; x),$$

where $a_i \neq 0$, for $i = 0, 2, \ldots, n$. As we have seen above, if the element α_n, defined in (1.7), is nonzero, then the associated rational function $R_n(x)$ is nonlinear. The permutations f and σ_n therefore differ at most at n elements of $\mathbb{F}_q$. But then the

values of $D_{f,a}$ and $D_{\sigma_n,a}$ differ at most at $2n$ elements. Since the permutation σ_n is APN, it follows that $\delta_{f,a}(b) \leq 2n+2$. In particular $\delta_{f,a}(b) \leq 8$ if $n = 3$ and $a_2a_3+1 \neq 0$.

The theorem above adds to known results on differential uniformity in characteristic 2, where the inversion is the classical example of an APN permutation (when the extension degree is odd).

Remark 1.18. As mentioned above, for polynomials to be interesting from the point of view of cryptographical applications, one often requires the polynomial to be (i) easy to implement; (ii) provide good resistance to differential and linear attacks; (iii) have large degree; (iv) have large weight (i.e. have many nonzero coefficients). Due to the first requirement, in most cases, only sparse polynomials have been considered, although these polynomials have of course the disadvantage of having low weight. The approach using Carlitz rank has the advantage of providing a method of obtaining PP which have large degree, have large weight, and moreover are still easy to implement due to the representation (1.6), therefore providing rare, if not the first examples of such permutations. Chapter 4 contains many examples of such PP, with additional interesting properties.

Another suprising application of the concept of Carlitz rank, concerning distribution properties of infinite sequences of real numbers is given in [52], see also [54].

In this thesis we use this concept not only to construct an important subclass of PPs, the so-called complete mapping polynomials, but also to provide very first examples of families of non-permutation polynomials with interesting value sets. The value sets we obtain are of significantly different nature than those, previously known.

1.3 Value Sets of Polynomials

The image of a function described by a polynomial $f(x)$ is called the *value set of* $f(x)$.

Value sets of polynomials over finite fields are widely studied, in particular in relation to the degree of the polynomials, and have received a lot of attention recently. In this section we highlight some of the main results concerning value sets to motivate our results. We use the following notation.

Definition 1.19. Let $f(x) \in \mathbb{F}_q[x]$, *the value set of* f is the set $V_f = \{f(a) : a \in \mathbb{F}_q\}$. The cardinality of the value set V_f is denoted by $|V_f|$.

Of course every subset of $\mathbb{F}_q$ occurs as the value set of some polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $< q-1$ by Lagrange's interpolation formula (1.1). There are few types of polynomials of which the value sets are known explicitly.

For monomials $x^d \in \mathbb{F}_q[x]$ the size of the value set is easily determined, and depends only on $(d, q-1)$, the greatest common divisor of d and $q-1$.

Theorem 1.20. *[58] If $f(x) = x^d \in \mathbb{F}_q[x]$, then $|V_f| = 1 + (q-1)/(d, q-1)$.*

Proof. Put $\delta = (d, q-1)$ and let β be a primitive δ-th root of unity in $\mathbb{F}_q$. If $a \in V_f$, $a \neq 0$, say $a = b^d$ with $b \in \mathbb{F}_q^*$, then for each $0 \leq i \leq \delta - 1$,

$$f(b\beta^i) = b^d(\beta^i)^d = a(\beta^\delta)^{ki} = a$$

where $k = d/\delta$. Hence the pre-image of each nonzero $a \in V_f$ has size δ. It follows that $|V_f| = 1 + (q-1)/\delta$. □

As a corollary we again obtain the classification of monomial PP's, i.e. x^d is a PP over $\mathbb{F}_q$ if and only if $(d, q-1) = 1$.

For the Dickson polynomials of the 1st kind the following results are known. The results depend on the parity of q. As usual the 2-adic valuation of an integer a is denoted by $v_2(a)$.

Theorem 1.21. *[14] If $f(x) = D_d(x, a) \in \mathbb{F}_q[x]$, q odd, $d \geq 1$, $a \in \mathbb{F}_q^*$, and $v_2(q^2-1) = r$, then*

$$|V_f| = \frac{q-1}{2(d, q-1)} + \frac{q+1}{2(d, q+1)} + \alpha,$$

where $\alpha = 1$ if $v_2(d) = r-1$ and a is a non-square in $\mathbb{F}_q$; $\alpha = 1/2$ if $1 \leq v_2(d) \leq r-2$; $\alpha = 0$ otherwise.

The result is simpler when q is even.

Theorem 1.22. *[14] If $f(x) = D_d(x, a) \in \mathbb{F}_q[x]$ and q is even, $d \geq 1$, $a \in \mathbb{F}_q^*$, then*

$$|V_f| = \frac{q-1}{2(d, q-1)} + \frac{q+1}{2(d, q+1)}.$$

If one does not consider specific polynomials but a class of polynomials (for instance all polynomials of degree d) then one might be interested in all possible sizes of the value set of polynomials in that class. Similarly it is natural to ask how the sizes of value sets are distributed, or how polynomials are distributed in terms of value sets. This motivates the following definition.

Definition 1.23. For a class of polynomials $\mathcal{C}$ the set $v(\mathcal{C}) = \{|V_f| \ : \ f \in \mathcal{C}\}$ is called the *spectrum* of $\mathcal{C}$.

As there are too many spectrum results for classes of polynomials to cover all of them in this brief overview, we refer to [53, 8.2], [45, 8.3.3] for more details and references.

As mentioned earlier, most previous results on spectrum concerns the class $\mathcal{C}_d$ of polynomials of degree d. We will briefly review these results here in order to motivate our study. We firstly state the trivial upper and lower bounds for $|V_f|$, $f \in \mathcal{C}_d$. Since for any $a \in \mathbb{F}_q$, $f(x) = a$ has at most d solutions one has,

$$\left\lceil \frac{q-1}{d} \right\rceil \leq |V_f| \leq q \tag{1.11}$$

Clearly $f(x) \in \mathbb{F}_q[x]$ is a PP if and only if $|V_f| = q$. Equality for the lower bound is reached for the so-called *minimal value set polynomials* which will be discussed in Section 1.3.2.

When $d \leq 4$ the complete spectrum $\mathcal{C}_d$ is known, see e.g. [45].

Theorem 1.24. *If $f(x) \in \mathbb{F}_q[x]$ has degree 2 then $|V_f| \in \{q/2, (q+1)/2, q\}$.*

Theorem 1.25. *If $f(x) \in \mathbb{F}_q[x]$ has degree 3 then*

$$|V_f| \in \{q/3, (q+2)/3, (2q-1)/3, 2q/3, (2q+1)/3, q\}.$$

We note that our results stated in Theorems 3.1, 3.2 and Corollary 3.5, for instance, are of similar nature.

Theorem 1.26. *[41] If $f(x) \in \mathbb{F}_q[x]$ has degree 4 and q is an odd prime then $|V_f|$ is either $(q+3)/4$, $(q+1)/2$, $(3q+4+i)/8$ with $\pm i \in \{1, 3, 5\}$, or $5q/8 + O(\sqrt{q})$.*

1.3.1 Large value sets

Obviously the spectrum $v(\mathcal{C})$ of a class of polynomials $\mathcal{C}$ is a subset of the interval $[1, \ldots, q]$ and the spectrum of the class of PPs is $\{q\}$. In the class $\mathcal{C}_d$, one would be interested to know how large $|V_f|$ can be when $f \in \mathcal{C}_d$ is not a PP. The following very nice result was proved by Wan in 1992.

Theorem 1.27. *[59] If $f(x) \in \mathbb{F}_q[x]$ is not a PP and f has degree d then*

$$|V_f| \leq q - \left\lceil \frac{q-1}{d} \right\rceil .$$

We remark that in [46] this result has recently been extended to polynomials in several variables. It was shown by Cusick and Müller in [22] that the upper bound from Theorem 1.27 is achieved by the polynomial

$$f(x) = (x+1)x^{s-1} \in \mathbb{F}_q[x],$$

where $q = s^t$ for some positive integer t. This result shows that there is a gap in the spectrum of the class of $\mathcal{C}_d$ for a fixed degree d. Similar gaps occur further down the spectrum. The results proven in 1997 by Guralnick and Wan [31, Theorem1.1] imply the following.

Theorem 1.28. *[31] If $f(x) \in \mathbb{F}_q[x]$ is not a PP, f has degree $d > 6$, and $|V_f| \neq (1-1/d)q$, then*

$$|V_f| \leq (1-2/d)q + O_d(\sqrt{q}).$$

In the same paper, the authors also prove a bound which does not depend on the degree d, but which only holds for polynomials of degree d in $\mathbb{F}_q[x]$ with $(q,d) = 1$.

Theorem 1.29. *[31] If $f(x) \in \mathbb{F}_q[x]$ is not a PP, f has degree d, with $(q,d) = 1$, then $|V_f| \leq (5/6)q + O_d(\sqrt{q})$.*

The proof of these results use techniques from number theory and group theory and rely on the classification of finite simply groups.

An interesting question is whether one can obtain results similar to Theorem 1.27 when one considers other classes of polynomials. This question was first tackled recently by Mullen, Wan, Wang in [47], where they obtain an upper bound in terms of the *index* for the value set for polynomials, which are not PP. This concept was first introduced by Akbary et al. in [1] based on the earlier notion of [50].

For any nonconstant monic polynomial $g(x) \in \mathbb{F}_q[x]$ of degree $< q-1$ with $g(0) = 0$, let r be the vanishing order of $g(x)$ at zero and let $f_1(x) := g(x)/x^r$. Then let l be the least divisor of $q-1$ with the property that there exists a polynomial f(x) of degree $\frac{l.\deg(f_1)}{q-1}$ such that $f_1(x) = f(x^{(q-1)/l})$. So $g(x)$ can be written uniquely as

$$x^r f(x^{(q-1)/l}).$$

We call l the index of g.

Mullen et al. proved the following theorem.

Theorem 1.30. *[47] If $f(x) \in \mathbb{F}_q[x]$ is not a PP, then*

$$|V_f| \leq q - \frac{q-1}{\ell}.$$

This improves Wan's result, Theorem 1.27 above, when the index ℓ of a polynomial is strictly smaller than the degree d, which always happens if $\ell \leq \sqrt{q} - 1$.

Our results in Chapter 3 illustrate that considering other classes; the spectrum may have a significantly different structure. We study the class of polynomials of the form $F(x) = f(x) + x$, where $f(x)$ is a PP of Carlitz rank at most n. We show for instance that, for a subclass of such polynomials the upper bound for $|V_F|$, when F is not a PP is $q - 2$, i.e., independent of n, see Remark 3.14.

1.3.2 Minimal value set polynomials

On the other side of the interval (1.11), as mentioned before, if f has degree d, then $|V_f| \geq \lceil q/d \rceil$. Polynomials achieving this bound are called *minimal value set polynomials*.

There are many results on minimal value set polynomials. The following theorem concerns polynomials over prime fields and gives a nice characterisation of minimal value set polynomials.

Theorem 1.31. *[11] If $f(x) \in \mathbb{F}_p[x]$ has degree $d < p$ and $|V_f| = \lceil p/d \rceil \geq 3$ then d divides $p - 1$ and $f(x) = a(x + b)^d + c$ for some $a, b, c \in \mathbb{F}_p$.*

For minimal value set polynomials over a field of prime power order q a similar result is obtained.

Theorem 1.32. *[42] If $f(x) \in \mathbb{F}_q[x]$ is monic and has degree $d \leq \sqrt{q}$, where $(d, q) = 1$, and $|V_f| = \lceil q/d \rceil$ then d divides $q - 1$ and $f(x) = (x + b)^d + c$ for some $b, c \in \mathbb{F}_q$.*

In fact, in [42] all minimal value set polynomials over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ are determined. In [8] minimal value set polynomials whose values form a subfield are characterised.

We note that the problem to determine all minimal value set polynomials over $\mathbb{F}_{p^s}$ where $s > 2$ is still open.

For polynomials which have value sets of size less than twice the size of the value set of a minimal value set polynomial of the same degree the following theorem was obtained in [14], [28].

Theorem 1.33. *[14, 28] If $f(x) \in \mathbb{F}_q[x]$ is monic and has degree $d > 15$, where $d^4 < q$, and $|V_f| < 2q/d$ then $f(x)$ has one of the following forms:*

(i) $(x+b)^d + c$, *where* d *divides* $q-1$;

(ii) $((x+a)^{d/2} + b)^2 + c$, *where* d *divides* $q^2 - 1$;

(iii) $((x+a)^2 + b)^{d/2} + c$, *where* d *divides* $q^2 - 1$,

for some $a, b, c \in \mathbb{F}_q$.

Finally we also mention a result from [4] which holds for polynomials with only two different values at nonzero elements of $\mathbb{F}_p$.

Theorem 1.34. *[4] If $f(x) \in \mathbb{F}_p[x]$ has degree $d < \frac{3}{4}(p-1)$, p prime, and $f(x)$ only takes two values on $\mathbb{F}_p^*$ then $f(x)$ is a polynomial in $x^{(p-1)/k}$ for some $k \in \{2, 3\}$.*

1.3.3 Lower bounds

It follows from Lemma 1.2 that if $f(x) \in \mathbb{F}_q[x]$ is a PP then $\sum_{a \in \mathbb{F}_q} (f(a))^t = 0$ for all $0 \leq t \leq q-2$. If this is not the case, then we have the following nice result on the value set of f.

Theorem 1.35. *[58] If $f \in \mathbb{F}_q[x]$ and $\mu_q(f)$ is the smallest positive integer i so that*

$$\sum_{a \in \mathbb{F}_q} (f(a))^i \neq 0$$

then $|V_f| \geq \mu_q(f) + 1$.

Obviously if $\mu_q(f) = q-1$, then f is a PP.

In order to state another interesting lower bound we need to introduce some notation. If $f(x) \in \mathbb{F}_q[x]$ has degree $d < q-1$, then we may consider the matrix $A_f = (a_{ij})$, where $a_{ij} = b_{ij}^{q-1}$ and b_{ij} is defined as the coefficient of x^j in $f(x)^i \bmod (x^q - x)$, i.e.

$$f(x)^i = \sum_{j=0}^{q-1} b_{ij} x^j \mod (x^q - x).$$

If the j-th column of A_f consists entirely of 0's or entirely of 1's then define $l_j := 0$, otherwise arrange the entries in a circle and define l_j to be the maximum number of consecutive zeros appearing in this circular arrangement. Then put

$$L_f = \max\{l_1, \ldots, l_{q-1}\}.$$

With this notation the following was proved in [26].

Theorem 1.36. *If $f(x) \in \mathbb{F}_q[x]$, then $|V_f| \geq L_f + 2$.*

A similar results uses the matrix $B = (b_{ij})$.

Theorem 1.37. *(Remark 8.3.25, [45]) If $f(x) \in \mathbb{F}_q[x]$, then $|V_f| = rank\ (B_f) + 1$.*

Note that Hermite's criterion essentially says that a polynomial f is a PP if and only if the first $q-2$ elements of the last column of A_f are zero. In other words f is a PP if and only if $L_f = q - 2$.

1.4 Complete Mapping Polynomials

Definition 1.38. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a *complete mapping polynomial* (or just a *complete mapping*) if both $f(x)$ and $f(x) + x$ are permutations of $\mathbb{F}_q$.

These polynomials were introduced by Mann in 1942 [38], where it was shown that complete mapping polynomials are pertinent for the construction of mutually orthogonal latin squares. Complete mapping polynomials also have applications in other areas of combinatorics and in non-associative algebras (see [44] for references). Recently further applications were discovered in certain aspects of cryptography related to bent functions.([60], [48]).

A detailed study of complete mapping polynomials over finite filelds was carried out by Niederreiter and Robinson (1982, [49]), where many basic properties of such maps were obtained. We include the proofs of the following two results from [49].

Theorem 1.39. *[49] A complete mapping polynomial of $\mathbb{F}_q$, with q odd and $q > 3$, has reduced degree $\leq q - 3$.*

Proof. Let $f(x)$ be a complete mapping polynomial of $\mathbb{F}_q$. By Hermite's criterion, both $f(x)$ and $f(x)^2$ have reduced degree $\leq q-2$ since $f(x)$ is a PP. Similarly also $(f(x)+x)^2$

has reduced degree $\leq q-2$ since by definition of a complete mapping polynomial also $f(x)+x$ is a PP. Now

$$(f(x)+x)^2 = f(x)^2 + 2xf(x) + x^2$$

which has reduced degree $\leq q-2$ only if $2xf(x)$ has reduced degree $\leq q-2$. Since q is odd, the result follows. □

Theorem 1.40. *[49] If $f(x)$ is a complete mapping polynomial of $\mathbb{F}_q$, then so are the following polynomials:*

(i) $f(x+a)+b$ for all $a, b \in \mathbb{F}_q$;

(ii) $af(a^{-1}x)$, for every $a \in \mathbb{F}_q^*$;

(iii) the inverse mapping $f^{-1}(x)$.

Proof. (i) Since $f(x)$ and $f(x)+x$ are both permutation polynomials over $\mathbb{F}_q$, both $f(x+a)$ and $f(x+a)+x+a$ are PP over $\mathbb{F}_q$ and hence also both $f(x+a)+b$ and $f(x+a)+b+x$ are PP over $\mathbb{F}_q$.
(ii) Let $h(x) = af(a^{-1}x)$ and $g(x) = f(x)+x$. Then

$$h(x)+x = af(a^{-1}x) + aa^{-1}x = ag(a^{-1}x).$$

Therefore both $h(x)$ and $h(x)+x$ are PP, since they are both compositions of permutation polynomials.
(iii) We know that $f^{-1}(x)$ is a PP since $f(x)$ is a PP. Now

$$f^{-1}(x)+x = f^{-1}(x) + f(f^{-1}(x))$$

which is a composition of permutation polynomials since $f(x)$ is a complete mapping polynomial. It follows that $f^{-1}(x)$ is a complete mapping polynomial. □

In [49] a necessary and sufficient condition is given for a binomial in $\mathbb{F}_q[x]$ of the form

$$ax^{(q+d-1)/d} + bx,$$

to be a complete mapping polynomial over $\mathbb{F}_q$, when $q \equiv 1 \mod d$, $d \geq 2$, and the case $d = 2$ is examined more closely. One of their results is the following.

Theorem 1.41. *[49, Corollary 1] Complete mapping polynomials of $\mathbb{F}_q$ of the form $x^{(q+1)/2} + bx$ exist exactly for all odd $q \geq 13$ and for $q = 7$.*

A basic question for applications is that of the existence of complete mappings polynomials of reduced degree > 1, which was also answered in [49].

Theorem 1.42. *For any finite field $\mathbb{F}_q$ with $q > 5$ there exist complete mapping polynomials of $\mathbb{F}_q$ of reduced degree > 1.*

The next theorem states the well-known conjecture of Chowla and Zassenhaus (1968), which was proved by Cohen [18] in 1990.

Theorem 1.43. *[15], [18] If $d \geq 2$ and $p > (d^2 - 3d + 4)^2$, then there is no complete mapping polynomial of degree d over $\mathbb{F}_p$.*

There are also non-existence results over finite fields which are not of prime order. For instance, Niederreiter and Robinson [49] proved the following.

Theorem 1.44. *[49] If $q \geq (d^2 - 4d + 6)^2$, $d \geq 2$ and $a \neq 0$, then $ax^d + bx$ is not a complete mapping polynomial over $\mathbb{F}_q$.*

In [44] Mullen and Niederreiter proved that a Dickson polynomial can be a complete mapping only in some special cases, as a result of the following theorem.

Theorem 1.45. *Let $k > 2$ be an integer and let $a, b, c \in \mathbb{F}_q$ with $abc \neq 0$. Then $bD_k(x, a) + cx$ can be a permutation polynomial of $\mathbb{F}_q$ only in one of the following cases:*

(i) $k = 3$, $c = 3ab$, and $q \equiv 2 \mod 3$;

(ii) $k > 3$ and the characteristic of $\mathbb{F}_q$ divides k;

(iii) $k > 4$, the characteristic of $\mathbb{F}_q$ does not divide k, and $q < (9k^2 - 27k + 22)^2$.

Charpin and Kyureghyan [12] constructed a class of monomial complete mappings.

Theorem 1.46. *[12] If k is odd and $a \in \beta\mathbb{F}_{2^k}$, where $\beta \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, then $a^{-1}x^{2^k+2}$ is a complete mapping polynomial of $\mathbb{F}_{2^{2k}}$.*

Recently Tu, Zeng and Hu (2014) gave three classes of exponents d for which a complete mapping polynomial of the form ax^d over $\mathbb{F}_{2^s}$ exists.

Theorem 1.47. *[57] If one of the following conditions is satisfied then there exists a complete mapping polynomial over $\mathbb{F}_{2^s}$ of the form ax^d.*

(i) $d = 2^{2k} + 2^k + 2$, $s = 3k$, $(k, 3) = 1$;

(ii) $d = 2^{k+1} + 3$, $s = 2k$, k *odd;*

(iii) $d = 2^{k-2}(2^k + 3)$, $s = 2k$, k *odd.*

Wu et al. presented (2014) three other classes of complete mapping polynomials over $\mathbb{F}_{2^s}$.

Theorem 1.48. *[61] If one of the following conditions is satisfied then there exists a complete mapping polynomial over $\mathbb{F}_{2^s}$, of the form ax^d.*

(i) $s = 4k$, *and* $d = \frac{2^{4k}-1}{2^k-1} + 1$, *where* $(k, 4) = 1$,

(ii) $s = 6k$, *and* $d = \frac{2^{6k}-1}{2^k-1} + 1$, *where* $(k, 6) = 1$,

(iii) $s = 10k$, *and* $d = \frac{2^{10k}-1}{2^k-1} + 1$, *where* $(k, 10) = 1$,

(iv) $s = 3k$, *and* $d = \frac{2^{3k}-1}{2^k-1} + 1$, *where* $(k, 9) = 1$.

In 2015, Guangkui and Cao presented the following three classes of complete mapping polynomials over finite fields of odd characteristic.

Theorem 1.49. *[30] If one of the following conditions is satisfied then there exists a complete mapping polynomial over $\mathbb{F}_{2^s}$, of the form ax^d.*

(i) $d = 3^k + 2$, $p = 3$, $s = 2k$, k *odd;*

(ii) $d = 2 \cdot 3^k + 3$, $p = 3$, $s = 2k$, k *odd;*

(iii) $d = t(p^k - 1) + 1$, $s = 2k$, $(t - 1, p^k + 1) = 1$, $2t$ *divides* $p^k + 1$.

We refer to [62] for more results about complete mapping polynomials. A recursive construction of complete mappings over finite fields is provided in [48]. Moreover, in the same paper it is shown that the existence of complete mappings of algebraic degree $r(t-1)$ over $\mathbb{F}_{2^{rt}}$ gives the possibility to construct bent-negabent Boolean functions over $\mathbb{F}_{2^{2rt}}$ of degree $t(r-1)+1$ (see [48]).

In [50] Niederreiter and Winterhof study orthomorphisms of finite fields, which are closely related to complete mappings. In fact f is an orthomorphism if and only if $-f$ is a complete mapping. They prove the existence of several classes of cyclotomic orthomorphisms and also introduce the concept of R-orthomorphisms.

CHAPTER 2

Constructions of Complete Mapping Polynomials

In this chapter, we construct families of complete mapping polynomials over finite fields by using the concept of Carlitz rank. First we introduce some notation which we use throughout this work.

2.1 Notation and Terminology

Let $f(x)$ be a PP over $\mathbb{F}_q$, where q is an odd prime power. Suppose that f has a representation P_n for $n \geq 1$, as in the equation (1.6), i.e.,

$$f(x) = P_n(a_0, a_1, ..., a_{n+1}; x)$$

where $a_i \neq 0$, for $i = 0, 2, \ldots, n$, and

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

Since we are interested in complete mapping polynomials, the value of a_{n+1} is irrelevant. Also, by using the substitution $x \mapsto x - a_0^{-1}a_1$, we see that the size of the value set of $f(x) + x$ does not depend on a_1. Therefore w.l.o.g. we may restrict ourselves to the cases $a_1 = a_{n+1} = 0$. We relabel the coefficients $c_0 = a_0$, $c_i = a_{i+1}$ for $i = 1, .., n-1$, and for simplicity we use the shortened notation

$$f(x) = P_n(c_0, ..., c_{n-1}; x).$$

As before we obtain its associated rational fraction

$$R_n(x) = \frac{\alpha_{n-1}x + \beta_{n-1}}{\alpha_n x + \beta_n}, \tag{2.1}$$

where

$$\alpha_k = c_{k-1}\alpha_{k-1} + \alpha_{k-2} \quad \text{and} \quad \beta_k = c_{k-1}\beta_{k-1} + \beta_{k-2}, \tag{2.2}$$

for $k \geq 2$ and $\alpha_0 = 0,\ \alpha_1 = c_0,\ \beta_0 = 1,\ \beta_1 = 0$. Note that α_1, α_2 can not be zero and $\beta_2 = 1$.

Recall that the set of *poles* $\mathbf{O}_n$ is defined by

$$\mathbf{O_n} = \{x_i : x_i = \frac{-\beta_i}{\alpha_i},\ i = 1, \ldots, n\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}. \tag{2.3}$$

where the elements of $\mathbf{O_n}$ are not necessarily distinct. We note that any three consecutive elements x_{i-1}, x_i, x_{i+1} are distinct, see [23]. Also $f(c) = P_n(c) = R_n(c)$ for $c \in \mathbb{F}_q \backslash \mathbf{O}_n$.

Now we define the following sets

$$\begin{aligned} \mathcal{P}_{q,n} &= \Big\{ f(x) \in \mathbb{F}_q[x] \ :\ f(x) = P_n(c_0, c_1, ..., c_{n-1}; x) \mid c_0, \ldots, c_{n-1} \in \mathbb{F}_q \Big\} \\ \mathcal{F}_{q,n} &= \big\{ F(x) = f(x) + x \ :\ f(x) \in \mathcal{P}_{q,n} \big\}. \end{aligned}$$

Clearly characterizing the complete mappings in $\mathcal{P}_{q,n}$ is the same as characterizing permutations in the set $\mathcal{F}_{q,n}$.

We consider the following three subclasses of $\mathcal{P}_{q,n}$ defined by the properties of the poles as follows. We have $\mathcal{P}_{q,n} = \mathcal{P}^{(1)}_{q,n} \cup \mathcal{P}^{(2)}_{q,n} \cup \mathcal{P}^{(3)}_{q,n}$ where

$$\begin{aligned} \mathcal{P}^{(1)}_{q,n} &= \{f \in \mathcal{P}_{q,n} \mid \alpha_i \neq 0 \text{ for } i = 3, ..., n\}, \\ \mathcal{P}^{(2)}_{q,n} &= \{f \in \mathcal{P}_{q,n} \mid \alpha_n = 0 \text{ and } \alpha_i \neq 0 \text{ for } i = 3, ..., n-1\}, \\ \mathcal{P}^{(3)}_{q,n} &= \{f \in \mathcal{P}_{q,n} \mid \alpha_i = 0 \ \text{ for some } i \in \{3, ..., n-1\}\}. \end{aligned}$$

Note that $\mathcal{P}^{(2)}_{q,1}$ and $\mathcal{P}^{(2)}_{q,2}$ are empty. Moreover we have $\mathcal{P}_{q,1} = \mathcal{P}^{(1)}_{q,1}$ and $\mathcal{P}_{q,2} = \mathcal{P}^{(1)}_{q,2}$. Similarly we partition $\mathcal{F}_{q,n}$ as $\mathcal{F}_{q,n} = \mathcal{F}^{(1)}_{q,n} \cup \mathcal{F}^{(2)}_{q,n} \cup \mathcal{F}^{(3)}_{q,n}$ where

$$\mathcal{F}^{(i)}_{q,n} = \big\{ F(x) = f(x) + x,\ f(x) \in \mathcal{P}^{(i)}_{q,n} \big\} \ \text{ for } i = 1, 2, 3.$$

Now define the rational function of degree 2, associated to $F(x)$ as

$$\mathcal{R}_n(x) = R_n(x) + x = \frac{\alpha_n x^2 + (\alpha_{n-1} + \beta_n)x + \beta_{n-1}}{\alpha_n x + \beta_n}. \tag{2.4}$$

Then we have the following formulas for $c \in \mathbb{F}_q \setminus \mathbf{O}_n$.

1. If $f(x) \in \mathcal{P}_{q,n}^{(1)}$ then for $c \in \mathbb{F}_q \setminus \mathbf{O}_n$

$$f(c) = R_n(c) = \frac{\alpha_{n-1}c + \beta_{n-1}}{\alpha_n c + \beta_n}, \tag{2.5}$$

which implies

$$F(c) = R_n(c) + c = \mathcal{R}_n(c) = \frac{\alpha_n c^2 + (\alpha_{n-1} + \beta_n)c + \beta_{n-1}}{\alpha_n c + \beta_n}. \tag{2.6}$$

2. If $f(x) \in \mathcal{P}_{q,n}^{(2)}$, $n > 2$ then for $c \in \mathbb{F}_q \setminus \mathbf{O}_n$

$$f(c) = R_n(c) = \frac{\alpha_{n-1}c + \beta_{n-1}}{\beta_n}, \tag{2.7}$$

which implies

$$F(c) = R_n(c) + c = \mathcal{R}_n(c) = \frac{(\alpha_{n-1} + \beta_n)c + \beta_{n-1}}{\beta_n}. \tag{2.8}$$

3. If $f(x) \in \mathcal{P}_{q,n}^{(1)} \cup \mathcal{P}_{q,n}^{(2)}$ and $|\mathbf{O}_n| = n$, then for $x_i \in \mathbf{O}_n \setminus \{x_1\}$

$$f(x_i) = R_n(x_{i-1}) = \mathcal{R}_n(x_{i-1}) - x_{i-1}, \tag{2.9}$$

which implies

$$F(x_i) = R_n(x_{i-1}) + x_i = \mathcal{R}_n(x_{i-1}) - x_{i-1} + x_i. \tag{2.10}$$

In this work, we only study $\mathcal{P}_{q,n}^{(1)}$ and $\mathcal{P}_{q,n}^{(2)}$ and

$$v(\mathcal{F}_{q,n}^{(i)}) = \left\{ |V_F| \ : \ F \in \mathcal{F}_{q,n}^{(i)} \right\} \quad \text{for } i = 1, 2.$$

2.2 The class $\mathcal{P}_{q,n}^{(1)}$

Our aim in this section is to find complete mapping polynomials in the set $\mathcal{P}_{q,n}^{(1)}$. This, of course, means that we look for permutations in $\mathcal{F}_{q,n}^{(1)}$. Therefore we focus on the polynomials $F \in \mathcal{F}_{q,n}^{(1)}$, for $n \geq 3$, i.e., $F(x) = f(x) + x$, where $f \in \mathcal{P}_{q,n}^{(1)}$ and has a representation

$$f(x) = P_n(c_0, ..., c_{n-1}; x). \tag{2.11}$$

Hence the set $\mathbf{O}_n$ of poles of f satisfies $\mathbf{O}_n \subseteq \mathbb{F}_q$.

In order to obtain the permutations $F \in \mathcal{F}_{q,n}^{(1)}$ we study $v(\mathcal{F}_{q,n}^{(1)})$ and determine when the maximum possible value q in $v(\mathcal{F}_{q,n}^{(1)})$ is attained. The main result of this section shows that when n is small with respect to the field size q, there is no complete mapping polynomial in $\mathcal{P}_{q,n}^{(1)}$ (Theorem 2.19).

We remind the reader that the first pole x_1 is always 0, since $\beta_1 = 0$ when f is as in (2.11). The following lemma shows that the image of the first pole is determined by α_{n-1} and α_n.

Lemma 2.1. $F(x_1) = F(0) = \dfrac{\alpha_{n-1}}{\alpha_n}$.

Proof. Since $F(x) = \Big(\cdots \big((c_0 x)^{q-2} + c_1\big)^{q-2} \cdots + c_{n-1} \Big)^{q-2} + x$, for $x_1 = 0$ we have

$$F(x_1) = \Big(\cdots \big((c_1)^{-1} + c_2\big)^{-1} \cdots + c_{n-1} \Big)^{-1}.$$

We proceed by induction on n. For $n = 1$, and $n = 2$, the statement trivially holds since $\alpha_0 = 0$ and $\frac{1}{c_1} = \frac{\alpha_1}{\alpha_2}$. Now suppose that the statement holds for all $k < n$. Then

$$F(0) = \frac{1}{c_{n-1} + F_1(0)}$$

where $F_1(x) \in \mathcal{F}_{q,n-1}^{(1)}$, i.e., $F_1(x) = f_1(x) + x$, with $f_1(x) = P_{n-1}(c_0, c_1, \ldots, c_{n-2}; x)$, and hence by the induction hypothesis (use $k = n-1$),

$$F_1(x_1) = F_1(0) = \frac{\alpha_{n-2}}{\alpha_{n-1}}.$$

Therefore

$$F(0) = \frac{1}{c_{n-1} + F_1(0)} = \frac{1}{c_{n-1} + \frac{\alpha_{n-2}}{\alpha_{n-1}}},$$

and since $c_{n-1} + \dfrac{\alpha_{n-2}}{\alpha_{n-1}} = \dfrac{\alpha_n}{\alpha_{n-1}}$, we have the assertion. □

Now consider the function $\varphi : \mathbb{F}_q \setminus \{x_n\} \to \mathbb{F}_q$ defined by

$$\varphi(c) = -\frac{\alpha_n \beta_n c + \beta_n^2 - (\alpha_n \beta_{n-1} - \alpha_{n-1}\beta_n)}{\alpha_n^2 c + \alpha_n \beta_n}. \tag{2.12}$$

The relevance of the function φ will become apparent in the following lemmas.

Lemma 2.2. *For $c, y \in \mathbb{F}_q \setminus \mathbf{O}_n$, $c \neq y$, we have*

$$F(c) = F(y) \iff y = \varphi(c).$$

Proof. If $F(c) = F(y)$ for $c, y \in \mathbb{F}_q \setminus \mathbf{O}_n$, $c \neq y$ then from (2.6) we obtain

$$\begin{aligned} & \frac{\alpha_n c^2 + (\beta_n + \alpha_{n-1})c + \beta_{n-1}}{\alpha_n c + \beta_n} = \frac{\alpha_n y^2 + (\beta_n + \alpha_{n-1})y + \beta_{n-1}}{\alpha_n y + \beta_n} \\ \iff \quad & \big(c - y\big)\big(\alpha_n^2 cy + \alpha_n\beta_n(c + y) + \beta_n^2 - (\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n\big) = 0 \\ \iff \quad & y(\alpha_n^2 c + \alpha_n\beta_n) + \alpha_n\beta_n c + \beta_n^2 - (\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n) = 0 \\ \iff \quad & y = -\frac{\alpha_n\beta_n c + \beta_n^2 - (\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n)}{\alpha_n^2 c + \alpha_n\beta_n}, \end{aligned}$$

which by (2.12) is $\varphi(c)$. □

Lemma 2.3. *The map φ is injective.*

Proof. For $c, y \in \mathbb{F}_q \setminus \{x_n\}$, $\varphi(c) = \varphi(y)$ implies

$$-\frac{\alpha_n\beta_n c + \beta_n^2 - (\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n)}{\alpha_n^2 c + \alpha_n\beta_n} = -\frac{\alpha_n\beta_n y + \beta_n^2 - (\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n)}{\alpha_n^2 y + \alpha_n\beta_n}.$$

Hence

$$(c - y)(\alpha_n^2\beta_n^2 - (\alpha_n^2\beta_n^2 - d_0\alpha_n^2)) = 0,$$

where $d_0 = \alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n$, which is nonzero since $x_{n-1} \neq x_n$. This implies $c = y$. □

Lemma 2.4. *The equation $\varphi(c) = c$ has exactly two solutions*

$$\{x', x''\} = \Big\{\frac{-\beta_n \mp \sqrt{\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n}}{\alpha_n}\Big\}$$

with $\{x', x''\} \in \mathbb{F}_{q^2} \setminus \mathbf{O}_n$.

Proof. If $\varphi(c) = c$ then

$$\begin{aligned} & -\frac{\alpha_n\beta_n c + \beta_n^2 - (\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n)}{\alpha_n^2 c + \alpha_n\beta_n} = c \\ \Rightarrow \quad & \alpha_n^2 c^2 + \alpha_n\beta_n c = -\alpha_n\beta_n c - \beta_n^2 + \alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n \\ \Rightarrow \quad & (\alpha_n c + \beta_n)^2 = \alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n \\ \Rightarrow \quad & c = \frac{-\beta_n \pm \sqrt{\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n}}{\alpha_n}. \end{aligned}$$

This completes the proof. □

Lemma 2.5.

$$\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n = \begin{cases} -c_0 & \text{if } n \text{ is even,} \\ c_0 & \text{if } n \text{ is odd.} \end{cases}$$

Proof. We prove the lemma by induction. Clearly for $n = 1$ we have $\alpha_1\beta_0 - \alpha_0\beta_1 = c_0$. Assume that the statement holds for $k = n - 1$. Suppose that n is even. By the induction hypothesis $\alpha_{n-1}\beta_{n-2} - \alpha_{n-2}\beta_{n-1} = c_0$. Hence

$$\begin{aligned}\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n &= (c_{n-1}\alpha_{n-1} + \alpha_{n-2})\beta_{n-1} - \alpha_{n-1}(c_{n-1}\beta_{n-1} + \beta_{n-2}) \\ &= \alpha_{n-2}\beta_{n-1} - \alpha_{n-1}\beta_{n-2} \\ &= -c_0.\end{aligned}$$

The same argument works when n is odd. □

Note that the elements x', x'' belong to $\mathbb{F}_q$ if c_0 (respectively $-c_0$) is a square in $\mathbb{F}_q$ when n is odd (respectively n is even).

Lemma 2.6. *The equation $\varphi(c) = x_n$, has no solution c in $\mathbb{F}_q \setminus \mathbf{O}_n$.*

Proof. Suppose that $\varphi(c) = x_n$ for some $c \in \mathbb{F}_q \setminus \mathbf{O}_n$. Then

$$\begin{aligned}&\Rightarrow \quad -\frac{\alpha_n\beta_n c + \beta_n^2 \pm c_0}{\alpha_n^2 c + \alpha_n\beta_n} = -\frac{\beta_n}{\alpha_n} \\ &\Rightarrow \quad \alpha_n^2\beta_n c + \alpha_n\beta_n^2 \pm \alpha_n c_0 = \beta_n\alpha_n^2 c + \alpha_n\beta_n^2 \\ &\Rightarrow \quad \pm\alpha_n c_0 = 0.\end{aligned}$$

This is a contradiction since $c_0 \neq 0$ and $\alpha_n \neq 0$ ($\alpha_n = 0$ implies $x_n = \infty$). □

Lemma 2.7. *If $(-1)^{n-1}c_0$ is a square in $\mathbb{F}_q$, then $F(x') \neq F(x'')$ where $\{x', x''\}$ is defined as in Lemma 2.4.*

Proof. If $F(x') - F(x'') = 0$ then with $d_0 = (-1)^{n-1}c_0$,

$$\begin{aligned}&\frac{\alpha_n(x')^2 + (\beta_n + \alpha_{n-1})(x') + \beta_{n-1}}{\alpha_n(x') + \beta_n} - \frac{\alpha_n(x'')^2 + (\beta_n + \alpha_{n-1})(x'') + \beta_{n-1}}{\alpha_n(x'') + \beta_n} = 0 \\ \Rightarrow \quad &\frac{\alpha_n\left(\frac{-\beta_n+\sqrt{d_0}}{\alpha_n}\right)^2 + (\beta_n + \alpha_{n-1})\left(\frac{-\beta_n+\sqrt{d_0}}{\alpha_n}\right) + \beta_{n-1}}{\alpha_n\left(\frac{-\beta_n+\sqrt{d_0}}{\alpha_n}\right) + \beta_n} \\ &- \frac{\alpha_n\left(\frac{-\beta_n-\sqrt{d_0}}{\alpha_n}\right)^2 + (\beta_n + \alpha_{n-1})\left(\frac{-\beta_n-\sqrt{d_0}}{\alpha_n}\right) + \beta_{n-1}}{\alpha_n\left(\frac{-\beta_n-\sqrt{d_0}}{\alpha_n}\right) + \beta_n} = 0\end{aligned}$$

and hence

$$\begin{aligned}
&\frac{\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n + (\alpha_{n-1} - \beta_n)\sqrt{d_0} + d_0}{\alpha_n\sqrt{d_0}} \\
&-\frac{\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n + (-\alpha_{n-1} + \beta_n)\sqrt{d_0} + d_0}{-\alpha_n\sqrt{d_0}} = 0 \\
\Rightarrow\quad &\frac{2d_0 + (\alpha_{n-1} - \beta_n)\sqrt{d_0}}{\alpha_n\sqrt{d_0}} + \frac{2d_0 + (-\alpha_{n-1} + \beta_n)\sqrt{d_0}}{\alpha_n\sqrt{d_0}} = 0 \\
\Rightarrow\quad &4d_0 = 0,
\end{aligned}$$

which implies $\mathrm{char}(\mathbb{F}_q) = 2$, a contradiction. □

Lemma 2.8. *The map φ defined in (2.12) is an involution.*

Proof. By Lemma 2.6, the image of φ belongs to $\mathbb{F}_q \setminus \{x_n\}$, and hence the map φ^2 is well-defined. Lemma 2.2 shows that φ is an involution. □

Now consider the following subsets of $\mathbb{F}_q \setminus \mathbf{O}_n$:

$$M := \Big\{ c \in \mathbb{F}_q \setminus \mathbf{O}_n \ : \ \varphi(c) \in \mathbf{O}_n \setminus \{x_n\} \Big\} \tag{2.13}$$

$$T := \Big\{ c \in \mathbb{F}_q \setminus \mathbf{O}_n \ : \ \varphi(c) \notin \mathbf{O}_n \text{ and } \varphi(c) = c \Big\}. \tag{2.14}$$

Obviously $M \cap T = \emptyset$. Also $|M| \leq |\mathbf{O}_n| - 1$, since φ is injective, and $|T| \leq 2$, by Lemma 2.4.

Lemma 2.9. *The restriction of F to the set*

$$D := \Big\{ c \in \mathbb{F}_q \setminus \mathbf{O}_n \ : \ \varphi(c) \notin \mathbf{O}_n \ \text{ and } \ \varphi(c) \neq c \Big\} \tag{2.15}$$

is $2-to-1$. In particular D has an even number of elements, $|D| = q - |\mathbf{O}_n| - |M| - |T|$.

Proof. First we show that $c \in D$ implies $\varphi(c) \in D$. For suppose $\varphi(c) \in M$, then $c = \varphi^2(c) \in \mathbf{O}_n$, a contradiction. Similarly, $\varphi(c) \notin T$ since $c \neq \varphi(c)$. By definition of D it follows that $\varphi(c) \in D$. By Lemma 2.2, $F(c) = F(\varphi(c))$, and since $c \neq \varphi(c)$ for each $c \in D$, the result follows. □

Lemma 2.10. $\varphi(D) = D$.

Proof. It follows from the above proof that $\varphi(D) \subset D$. Since φ is injective, the result follows. □

Lemma 2.11. *The restriction function $F_{|_M}$ is injective.*

Proof. This is an immediate consequence of the definition of M and Lemma 2.2. □

Lemma 2.12. *For each $c \in M$, there exists a unique $x_i \in \mathbf{O}_n \setminus \{x_n\}$, such that $\varphi(x_i) = c$.*

Proof. Take any $c \in M$. Then by definition of the set M, for some $i = 1, ..., n-1$ we have $\varphi(c) = x_i$, and hence, with $d_0 = (-1)^{n-1}c_0$,

$$\begin{aligned}
& -\frac{\alpha_n\beta_n c + \beta_n^2 - d_0}{\alpha_n^2 c + \alpha_n\beta_n} = -\frac{\beta_i}{\alpha_i} \\
\Rightarrow\ & \alpha_n\beta_n\alpha_i c + \beta_n^2\alpha_i - d_0\alpha_i = \alpha_n^2\beta_i c + \alpha_n\beta_n\beta_i \\
\Rightarrow\ & c(\alpha_n^2\beta_i - \alpha_n\beta_n\alpha_i) = -\alpha_n\beta_n\beta_i + \beta_n^2\alpha_i - d_0\alpha_i \\
\Rightarrow\ & c = \frac{-\alpha_n\beta_n\beta_i + \beta_n^2\alpha_i - d_0\alpha_i}{\alpha_n^2\beta_i - \alpha_n\beta_n\alpha_i}. \\
\Rightarrow\ & c = -\frac{\alpha_n\beta_n x_i + \beta_n^2 - d_0}{\alpha_n^2 x_i + \alpha_n\beta_n} \\
\Rightarrow\ & c = \varphi(x_i).
\end{aligned}$$

The uniqueness follows from the fact that φ is injective (Lemma 2.3). □

Lemma 2.13. *If $(\alpha_n x_i + \beta_n)(\alpha_n x_j + \beta_n) \neq (-1)^{n-1}c_0$ for all $i, j = 1, ..., n-1$ with $i \neq j$, then $M = \varphi\big(\mathbf{O}_n \setminus \{x_n\}\big)$.*

Proof. Let $x_i \in \mathbf{O}_n \setminus \{x_n\}$. It follows from Lemma 2.4 and the definition of M that $\varphi(x_i) \neq x_i$. If $\varphi(x_i) = x_j$ for some $j \neq i$, then

$$\begin{aligned}
-\frac{\alpha_n\beta_n x_i + \beta_n^2 - d_0}{\alpha_n^2 x_i + \alpha_n\beta_n} = x_j \quad &\Rightarrow \quad -\alpha_n\beta_n x_i - \beta_n^2 + d_0 = (\alpha_n^2 x_i + \alpha_n\beta_n)x_j \\
&\Rightarrow \quad \alpha_n^2 x_i x_j + \alpha_n\beta_n x_i + \beta_n\alpha_n x_j + \beta_n^2 = d_0.
\end{aligned}$$

But then $(\alpha_n x_i + \beta_n)(\alpha_n x_j + \beta_n) = d_0$, a contradiction. This shows that $\varphi(x_i) \notin \mathbf{O}_n$. It follows from Lemma 2.8 that $\varphi^2(x_i) = x_i$ and hence, in particular, $\varphi\big(\varphi(x_i)\big) \in \mathbf{O}_n \setminus \{x_n\}$. We have shown that $\varphi(x_i) \in M$ for each $x_i \in \mathbf{O}_n \setminus \{x_n\}$. □

Lemma 2.14. *The sets $F(D)$, $F(M)$, and $F(T)$ are pairwise disjoint.*

Proof. Suppose that for $F(y) = F(c)$ for some $c \in D$ and $y \in M$. Then by Lemma 2.2 we have $y = \varphi(c)$ and hence $y \in D$ by Lemma 2.10. This contradicts the assumption that $y \in M$. Hence $F(D) \cap F(M) = \emptyset$.

Similarly, if $F(c) = F(y)$ for $c \in D \cup M$ and $y \in T$ then by Lemma 2.2 we have $c = \varphi(y) = y$, a contradiction since $D \cup M$ and T are disjoint. □

Lemma 2.15. *If $|\mathbf{O}_n| = n$ then the following two conditions are equivalent:*

(i) $F(\mathbf{O}_n \setminus \{x_1\}) \cap F(\mathbb{F}_q \setminus \mathbf{O_n}) = \emptyset$,

(ii) for any $i \in \{2, ..., n\}$, the equation

$$(\alpha_n x + \beta_n)(\alpha_n x_{i-1} + \beta_n) = (-1)^{n-1} c_0 \frac{x - x_{i-1}}{x - x_i}$$

in the variable x has no solution c in $\mathbb{F}_q \setminus \mathbf{O_n}$.

Proof. Suppose that $F(\mathbf{O}_n \setminus \{x_1\}) \cap F(\mathbb{F}_q \setminus \mathbf{O_n}) \neq \emptyset$. Then for some c in $\mathbb{F}_q \setminus \mathbf{O_n}$, $x_i \in \mathbf{O}_n \setminus \{x_1\}$ we have $F(c) = F(x_i)$. Then by (2.6) and (2.10) we have $R_n(c) + c = R_n(x_{i-1}) + x_i$ which is equivalent to

$$\frac{\alpha_{n-1}c + \beta_{n-1}}{\alpha_n c + \beta_n} - \frac{\alpha_{n-1}x_{i-1} + \beta_{n-1}}{\alpha_n x_{i-1} + \beta_n} = x_i - c,$$

or

$$\begin{aligned} & \frac{\alpha_{n-1}\alpha_n c x_{i-1} + \alpha_{n-1}\beta_n c + \alpha_n \beta_{n-1} x_{i-1} + \beta_n \beta_{n-1}}{(\alpha_n c + \beta_n)(\alpha_n x_{i-1} + \beta_n)} \\ - \quad & \frac{\alpha_{n-1}\alpha_n c x_{i-1} + \alpha_n \beta_{n-1} c + \alpha_{n-1}\beta_n x_{i-1} + \beta_n \beta_{n-1}}{(\alpha_n c + \beta_n)(\alpha_n x_{i-1} + \beta_n)} = x_i - c. \end{aligned}$$

Then

$$\frac{\alpha_{n-1}\beta_n x_{i-1} + \alpha_n \beta_{n-1} x_{j-1} - \alpha_{n-1}\beta_n x_{j-1} - \alpha_n \beta_{n-1} x_{i-1}}{(\alpha_n c + \beta_n)(\alpha_n x_{i-1} + \beta_n)} = x_i - c$$

which is equivalent to

$$\begin{aligned} & \frac{(\alpha_{n-1}\beta_n - \alpha_n \beta_{n-1})(c - x_{i-1})}{(\alpha_n c + \beta_n)(\alpha_n x_{i-1} + \beta_n)} = x_i - c \\ \iff \quad & (-1)^n c_0 (c - x_{i-1}) = (\alpha_n c + \beta_n)(\alpha_n x_{i-1} + \beta_n)(x_i - c) \\ \iff \quad & (-1)^{n-1} c_0 \frac{c - x_{i-1}}{c - x_i} = (\alpha_n c + \beta_n)(\alpha_n x_{i-1} + \beta_n). \end{aligned}$$

Hence we may conclude that $F(\mathbf{O}_n \setminus \{x_1\}) \cap F(\mathbb{F}_q \setminus \mathbf{O_n}) = \emptyset$ if and only if

$$(-1)^{n-1} c_0 \frac{c - x_{i-1}}{c - x_i} \neq (\alpha_n c + \beta_n)(\alpha_n x_{i-1} + \beta_n)$$

for every c in $\mathbb{F}_q \setminus \mathbf{O_n}$, and $i \in \{2, .., n\}$. □

Lemma 2.16. *If $|\mathbf{O}_n| = n$, then the following two conditions are equivalent:*

(i) $|F(\mathbf{O}_n \setminus \{x_1\})| = n - 1$,

(ii) $(\alpha_n x_{i-1} + \beta_n)(\alpha_n x_{j-1} + \beta_n) \neq (-1)^{n-1} c_0 \frac{x_{j-1} - x_{i-1}}{x_j - x_i}$, *for all* $i, j \in \{2, ..., n\}$ *with* $i \neq j$.

Proof. Suppose that $F(x_i) = F(x_j)$ for some $i, j = 2, ..., n$ with $i \neq j$. Since all the poles in $\mathbf{O_n}$ are distinct, we have $R(x_{i-1}) + x_i = R(x_{j-1}) + x_j$ by Lemma 1.11. Hence

$$\begin{aligned}
& \frac{\alpha_{n-1}x_{i-1} + \beta_{n-1}}{\alpha_n x_{i-1} + \beta_n} - \frac{\alpha_{n-1}x_{j-1} + \beta_{n-1}}{\alpha_n x_{j-1} + \beta_n} = x_j - x_i \\
\iff \quad & \frac{\alpha_{n-1}\alpha_n x_{i-1}x_{j-1} + \alpha_{n-1}\beta_n x_{i-1} + \alpha_n\beta_{n-1}x_{j-1} + \beta_n\beta_{n-1}}{(\alpha_n x_{i-1} + \beta_n)(\alpha_n x_{j-1} + \beta_n)} \\
- \quad & \frac{\alpha_{n-1}\alpha_n x_{i-1}x_{j-1} + \alpha_{n-1}\beta_n x_{j-1} + \alpha_n\beta_{n-1}x_{i-1} + \beta_n\beta_{n-1}}{(\alpha_n x_{i-1} + \beta_n)(\alpha_n x_{j-1} + \beta_n)} = x_j - x_i \\
\iff \quad & \frac{\alpha_{n-1}\beta_n x_{i-1} + \alpha_n\beta_{n-1}x_{j-1} - \alpha_{n-1}\beta_n x_{j-1} - \alpha_n\beta_{n-1}x_{i-1}}{(\alpha_n x_{i-1} + \beta_n)(\alpha_n x_{j-1} + \beta_n)} = x_j - x_i \\
\iff \quad & \frac{(\alpha_{n-1}\beta_n - \alpha_n\beta_{n-1})(x_{i-1} - x_{j-1})}{(\alpha_n x_{i-1} + \beta_n)(\alpha_n x_{j-1} + \beta_n)} = x_j - x_i \\
\iff \quad & (-1)^n c_0(x_{i-1} - x_{j-1}) = (\alpha_n x_{i-1} + \beta_n)(\alpha_n x_{j-1} + \beta_n)(x_j - x_i) \\
\iff \quad & (-1)^{n-1} c_0 \frac{x_{j-1} - x_{i-1}}{x_j - x_i} = (\alpha_n x_{i-1} + \beta_n)(\alpha_n x_{j-1} + \beta_n).
\end{aligned}$$

Therefore for all $i, j \in \{2, ..., n\}$ with $i \neq j$

$$(-1)^{n-1} c_0 \frac{x_{j-1} - x_{i-1}}{x_j - x_i} \neq (\alpha_n x_{i-1} + \beta_n)(\alpha_n x_{j-1} + \beta_n)$$

if and only if $F(x_i) \neq F(x_j)$. This completes the proof. □

Lemma 2.17. *If* $|\mathbf{O}_n| = n$, *then the following two conditions are equivalent:*

(i) $F(x_i) \neq \frac{\alpha_{n-1}}{\alpha_n}$, *for all* $i \in \{2, ..., n\}$,

(ii) $\alpha_n x_i(\alpha_n x_{i-1} + \beta_n) \neq (-1)^n c_0$, *for all* $i \in \{2, ..., n\}$.

Proof. Suppose that $F(x_i) = \frac{\alpha_{n-1}}{\alpha_n}$ for some $i = 2, ..., n$. Since all the poles in $\mathbf{O_n}$ are distinct, we have $R(x_{i-1}) + x_i = \frac{\alpha_{n-1}}{\alpha_n}$ by Lemma 1.11. Hence

$$\begin{aligned}
& \frac{\alpha_{n-1}x_{i-1} + \beta_{n-1}}{\alpha_n x_{i-1} + \beta_n} + x_i = \frac{\alpha_{n-1}}{\alpha_n}, \\
\iff \quad & \frac{\alpha_n x_i x_{i-1} + \beta_n x_i + \alpha_{n-1}x_{i-1} + \beta_{n-1}}{\alpha_n x_{i-1} + \beta_n} = \frac{\alpha_{n-1}}{\alpha_n}, \\
\iff \quad & \alpha_n^2 x_i x_{i-1} + \alpha_n\beta_n x_i + \alpha_n\alpha_{n-1}x_{i-1} + \alpha_n\beta_{n-1} = \alpha_n\alpha_{n-1}x_{i-1} + \alpha_{n-1}\beta_n.
\end{aligned}$$

Then we get $-(\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n) = \alpha_n x_i(\alpha_n x_{i-1} + \beta_n)$. Therefore for $i \in \{2, ..., n\}$,

$$\alpha_n x_i(\alpha_n x_{i-1} + \beta_n) \neq (-1)^n c_0$$

if and only if $F(x_i) \neq \frac{\alpha_{n-1}}{\alpha_n}$. This completes the proof. □

Lemma 2.18. *If $|\mathbf{O}_n| = n$, then the following two conditions are equivalent:*

(i) $F(y) \neq \frac{\alpha_{n-1}}{\alpha_n}$, *for all* $y \in \mathbb{F}_q \setminus \mathbf{O}_n$,

(ii) $\alpha_n y(\alpha_n y + \beta_n) \neq (-1)^n c_0$.

Proof. Suppose that $F(y) = \frac{\alpha_{n-1}}{\alpha_n}$ for some $y \in \mathbb{F}_q \setminus \mathbf{O}_n$. Then we have

$$\begin{aligned} & \frac{\alpha_{n-1}y + \beta_{n-1}}{\alpha_n y + \beta_n} + y = \frac{\alpha_{n-1}}{\alpha_n}, \\ \iff \quad & \frac{\alpha_n y^2 + (\alpha_{n-1} + \beta_n)y + \beta_{n-1}}{\alpha_n y + beta_n} = \frac{\alpha_{n-1}}{\alpha_n}, \\ \iff \quad & \alpha_n\alpha_{n-1}y + \beta_n\alpha_{n-1} = \alpha_n^2 y^2 + \alpha_n(\alpha_{n-1} + beta_n)y + \beta_{n-1}\alpha_n. \end{aligned}$$

Then we have $-(\alpha_n\beta_{n-1} - \alpha_{n-1}\beta_n) = \alpha_n y(\alpha_n y + \beta_n)$. Therefore,

$$\alpha_n y(\alpha_n y + \beta_n) \neq (-1)^n c_0$$

if and only if $F(y) \neq \frac{\alpha_{n-1}}{\alpha_n}$, for all $y \in \mathbb{F}_q \setminus \mathbf{O}_n$. □

We now prove the main theorem of this section.

Theorem 2.19. *If $q > 2n + 1$ then there exists no complete mapping polynomial in $\mathcal{P}^{(1)}_{q,n}$.*

Proof. Let $f \in \mathcal{P}^{(1)}_{q,n}$ as in (2.11) be a complete mapping polynomial. Then, by Lemma 2.9, the set D must be empty. This means $0 = |D| = q - |\mathbf{O}_n| - |M| - |T|$, and since $|\mathbf{O}_n| \leq n$, $|M| \leq n - 1$, $|T| \leq 2$, we obtain the inequality $q \leq 2n + 1$. □

We recall the Chowla-Zassenhaus conjecture, proved by Cohen, see Theorem 1.43 above, stating that there is no complete mapping polynomial of degree d, when p is large with respect to d. We note the similarity of our result, relating the field size q to the Carlitz rank n of f in $\mathcal{P}^{(1)}_{q,n}$.

Theorem 2.19 motivates the question of finding methods for construction of complete mapping polynomials when $q \leq 2n+1$. The following theorem presents a partial answer to this question.

Theorem 2.20. *Let $f \in \mathcal{P}^{(1)}_{q,n}$, with distinct poles $x_1, x_2, \ldots, x_n$ in $\mathbb{F}_q$. Then f is a complete mapping polynomial if the following conditions are satisfied:*

(i) $(-1)^{n-1}c_0$ *is a square in* $\mathbb{F}_q$,

(ii) $\alpha_n y(\alpha_n y + \beta_n) \neq (-1)^n c_0$, *for all* $y \in \mathbb{F}_q \setminus \mathbf{O}_n$,

(iii) $\alpha_n x_i(\alpha_n x_{i-1} + \beta_n) \neq (-1)^n c_0$, *for all* $i \in \{2, ..., n\}$,

(iv) $(\alpha_n c + \beta_n)(\alpha_n x_{i-1} + \beta_n) \neq (-1)^{n-1} c_0 \frac{c - x_{i-1}}{c - x_i}$, *for every* $c \in \mathbb{F}_q \setminus \mathbf{O_n}$, *for all* $i \in \{2, ..., n\}$,

(v) $(-1)^{n-1} c_0 \frac{x_{j-1} - x_{i-1}}{x_j - x_i} \neq (\alpha_n x_{i-1} + \beta_n)(\alpha_n x_{j-1} + \beta_n)$, *for all* $i, j \in \{2, ..., n\}$ *with* $i \neq j$.

(vi) $(\alpha_n x_i + \beta_n)(\alpha_n x_j + \beta_n) \neq (-1)^{n-1} c_0$ *for all* $i, j = 1, ..., n-1$ *with* $i \neq j$,

Moreover these conditions imply that $q = 2n + 1$.

Proof. The second and third conditions come from Lemmas 2.17 and 2.18. Condition (iv) comes from Lemma 2.15 and implies that $F(\mathbb{F}_q \setminus (\mathbf{O}_n \setminus \{x_1\})) \cap F(\mathbf{O}_n) = \emptyset$. Moreover, by Lemma 2.16, (v) implies that $|F(\mathbf{O}_n \setminus \{x_1\})| = n - 1$. The last condition implies that $|M| = n - 1$ and comes from Lemma 2.13. Finally the first condition implies that $|T| = 2$. Since the restriction of F to D is 2-to-1, D must be the empty set. This occurs exactly when $|M| + |T| = q - n$, which is equivalent to $n = (q-1)/2$. □

To illustrate the use of Theorem 2.20 we include some examples of complete mapping polynomials, which we obtained using the computer algebra package MAGMA [5], see Chapter 4.

2.3 The class $\mathcal{P}_{q,n}^{(2)}$

In this section we describe various constructions of complete mapping polynomials in $\mathcal{P}_{q,n}^{(2)}$, where $n \geq 3$. For this purpose we determine the permutations in $\mathcal{F}_{q,n}^{(2)}$, and hence study the polynomials $F(x) = f(x) + x$, where

$$f(x) = P_n(c_0, ..., c_{n-1}; x) \in \mathcal{P}_{q,n}^{(2)}. \tag{2.16}$$

Lemma 2.21. $F(x_1) = 0$.

Proof. Recall that the first pole x_1 is 0, since $\beta_1 = 0$. The proof is completely analogous to the proof of Lemma 2.1. □

Lemma 2.22. *If $|\mathbf{O}_n| = n$ and $\alpha_{n-1} \neq -\beta_n$, then for all $x_i, x_j \in \mathbf{O}_n$ with $x_i \neq x_j$,*

$$F(x_i) \neq F(x_j) \quad \Longleftrightarrow \quad \frac{x_i - x_j}{x_{i-1} - x_{j-1}} \neq -\frac{\alpha_{n-1}}{\beta_n}.$$

Proof. By equation (2.10), we have for all $x_i, x_j \in \mathbf{O}_n$ with $x_i \neq x_j$.

$$\begin{aligned} F(x_i) = F(x_j) \quad &\Longleftrightarrow \quad \mathcal{R}_n(x_{i-1}) - x_{i-1} + x_i = \mathcal{R}_n(x_{j-1}) - x_{j-1} + x_j, \\ &\Longleftrightarrow \quad \frac{\alpha_{n-1}}{\beta_n} x_{i-1} + \frac{\beta_{n-1}}{\beta_n} + x_i = \frac{\alpha_{n-1}}{\beta_n} x_{j-1} + \frac{\beta_{n-1}}{\beta_n} + x_j \\ &\Longleftrightarrow \quad \frac{\alpha_{n-1}}{\beta_n}(x_{i-1} - x_{j-1}) = x_j - x_i, \\ &\Longleftrightarrow \quad \frac{x_i - x_j}{x_{i-1} - x_{j-1}} = -\frac{\alpha_{n-1}}{\beta_n}. \end{aligned}$$

This completes the proof. □

Lemma 2.23. *If $|\mathbf{O}_n| = n$ and $\alpha_{n-1} \neq -\beta_n$ then for all $c \in \mathbb{F}_q \backslash \mathbf{O_n}$ and $2 \leq i \leq n-1$,*

$$F(x_i) \neq F(c) \quad \Longleftrightarrow \quad \frac{x_i - c}{x_{i-1} - c} \neq -\frac{\alpha_{n-1}}{\beta_n}.$$

Proof. For $i \in \{2, \ldots, n-1\}$ and $c \in \mathbb{F}_q \backslash \mathbf{O_n}$, by (2.8), we have

$$\begin{aligned} F(x_i) = F(c) \quad &\Longleftrightarrow \quad \mathcal{R}_n(x_{i-1}) - x_{i-1} + x_i = \mathcal{R}_n(c), \quad \text{for each } i, \\ &\Longleftrightarrow \quad \frac{\alpha_{n-1}}{\beta_n} x_{i-1} + \frac{\beta_{n-1}}{\beta_n} + x_i = (\frac{\alpha_{n-1}}{\beta_n} + 1)c + \frac{\beta_{n-1}}{\beta_n}, \\ &\Longleftrightarrow \quad \frac{\alpha_{n-1}}{\beta_n} x_{i-1} + x_i = (\frac{\alpha_{n-1}}{\beta_n} + 1)c, \\ &\Longleftrightarrow \quad \frac{\alpha_{n-1}}{\beta_n}(c - x_{i-1}) = x_i - c, \\ &\Longleftrightarrow \quad \frac{x_i - c}{x_{i-1} - c} = -\frac{\alpha_{n-1}}{\beta_n}, \quad i = 2, ..., n-1, \end{aligned}$$

which concludes the proof. □

Proposition 2.24. *Suppose $f(x) \in \mathcal{P}_{q,n}^{(2)}$ has distinct poles $x_1, \ldots, x_{n-1}, x_n = \infty$, and $F(x) = f(x) + x$. The polynomial $f(x)$ defined as in (2.16) is a complete mapping polynomial if $F(c) = 0$ implies $c = 0$, and the following two conditions are satisfied:*

(i) for all $2 \leq i, j \leq n-1$ with $i \neq j$,

$$\frac{x_i - x_j}{x_{i-1} - x_{j-1}} \neq -\frac{\alpha_{n-1}}{\beta_n},$$

(ii) for all $c \in \mathbb{F}_q \backslash \mathbf{O_n}$ and $2 \leq i \leq n-1$,

$$\frac{x_i - c}{x_{i-1} - c} \neq -\frac{\alpha_{n-1}}{\beta_n}.$$

Proof. We need to show that $F(x) = f(x) + x$ is a permutation polynomial. It immediately follows from the equation (2.8) that the restriction of F to $\mathbb{F}_q \backslash \mathbf{O_n}$ is injective. By Lemma 2.22 the restriction of F to $\mathbf{O_n} \setminus \{0\}$ is injective. By Lemma 2.23 the intersection of $F(\mathbb{F}_q \backslash \mathbf{O_n})$ with $F(\mathbf{O_n} \setminus \{0\})$ is empty. The hypothesis $F(c) = 0$ implies $c = 0$, concludes the proof. □

Theorem 2.25. *Let $\alpha_{n-1} \neq -\beta_n$, and $f \in \mathcal{P}^{(2)}_{q,n}$, with n distinct poles. Then f is a complete mapping polynomial if and only if for each $i \in \{1, \ldots, n-1\}$ there exists a unique $k(i) \in \{1, \ldots, n-1\} \setminus \{i-1, i\}$ s.t*

$$x_i + \frac{\alpha_{n-1}}{\beta_n} x_{i-1} = \left(1 + \frac{\alpha_{n-1}}{\beta_n}\right) x_{k(i)}, \tag{2.17}$$

where the indices $i = 1, \ldots, n-1$, should be calculated modulo $n-1$.

Proof. Suppose F is a permutation. By Lemma 2.23, for all $2 \leq i \leq n-1$,

$$\begin{aligned} & \frac{x_i - c}{x_{i-1} - c} \neq -\frac{\alpha_{n-1}}{\beta_n}, \quad \forall c \in \mathbb{F}_q \backslash \mathbf{O_n} \\ \iff \quad & \frac{x_i + \frac{\alpha_{n-1}}{\beta_n} x_{i-1}}{1 + \frac{\alpha_{n-1}}{\beta_n}} \neq c, \quad \forall c \in \mathbb{F}_q \backslash \mathbf{O_n}. \end{aligned}$$

This means that the expression on the left hand side must be a pole, i.e., there exists $k(i) \in \{1, \ldots, n-1\} \setminus \{i-1, i\}$ with

$$x_i + \frac{\alpha_{n-1}}{\beta_n} x_{i-1} = \left(1 + \frac{\alpha_{n-1}}{\beta_n}\right) x_{k(i)}.$$

Note that $k(i)$ should be different than $i-1$ and i, since all the poles are distinct. Now we show the uniqueness of $k(i)$. Suppose that for any $i \neq j$ there is a $k(i)$ with $k(i) \neq i, i-1$ and $k(i) \neq j, j-1$ such that

$$x_i + \frac{\alpha_{n-1}}{\beta_n} x_{i-1} = \big(1 + \frac{\alpha_{n-1}}{\beta_n}\big) x_{k(i)} \quad \text{and} \quad x_j + \frac{\alpha_{n-1}}{\beta_n} x_{j-1} = \big(1 + \frac{\alpha_{n-1}}{\beta_n}\big) x_{k(i)}.$$

Therefore we have

$$\begin{aligned} & x_i + \frac{\alpha_{n-1}}{\beta_n} x_{i-1} = x_j + \frac{\alpha_{n-1}}{\beta_n} x_{j-1} \\ \iff \quad & \frac{x_i - x_j}{x_{i-1} - x_{j-1}} = -\frac{\alpha_{n-1}}{\beta_n}. \end{aligned}$$

Hence F is not a permutation by Lemma 2.22, which contradicts to the assumption. Taking the summation of all the equalities for $i = 2, \ldots, n-1$ we obtain

$$\sum_{i=2}^{n-1} \left(x_i + \frac{\alpha_{n-1}}{\beta_n} x_{i-1}\right) = \sum_{i=2}^{n-1} \left(1 + \frac{\alpha_{n-1}}{\beta_n}\right) x_{k(i)}$$

which is equivalent to

$$\frac{\alpha_{n-1}}{\beta_n}x_1 + x_{n-1} + \sum_{i=2}^{n-2}\left(1+\frac{\alpha_{n-1}}{\beta_n}\right)x_i = \sum_{i=2}^{n-1}\left(1+\frac{\alpha_{n-1}}{\beta_n}\right)x_{k(i)}. \tag{2.18}$$

Since k is injective, all but one of the terms in the summation on the left hand side (for $i = 2, \ldots, n-2$) cancel with terms on the right hand side. What remains is

$$\frac{\alpha_{n-1}}{\beta_n}x_1 + x_{n-1} + \left(1+\frac{\alpha_{n-1}}{\beta_n}\right)x_r = \left(1+\frac{\alpha_{n-1}}{\beta_n}\right)(x_{k(s)} + x_{k(t)})$$

for some $r \in \{2, \ldots, n-2\}$ and $s, t \in \{2, \ldots, n-2\}$, with $k(s), k(t) \in \{1, n-1, r\}$. This leaves three possibilities for the set $\{k(s), k(t)\}$, namely $\{1, r\}$, $\{r, n-1\}$, and $\{1, n-1\}$. In the first case we obtain $x_{n-1} = x_1$, a contradiction. Similarly, in the second case we obtain

$$\frac{\alpha_{n-1}}{\beta_n}x_1 = \frac{\alpha_{n-1}}{\beta_n}x_{n-1},$$

which again leads to the contradiction $x_{n-1} = x_1$, since $\alpha_{n-1} \neq 0$, as $x_{n-1} \in \mathbb{F}_q$. In the remaining case we have

$$\frac{\alpha_{n-1}}{\beta_n}x_1 + x_{n-1} + \left(1+\frac{\alpha_{n-1}}{\beta_n}\right)x_r = \left(1+\frac{\alpha_{n-1}}{\beta_n}\right)(x_1 + x_{n-1}).$$

This implies that

$$x_1 + \frac{\alpha_{n-1}}{\beta_n}x_{n-1} = \left(1+\frac{\alpha_{n-1}}{\beta_n}\right)x_r.$$

Defining $k(1) = r$, gives the required result.

Conversely, suppose $F(x)$ is not a permutation. First we show that $F(x_j) = 0$ implies $x_j = 0$ (i.e. $j = 1$). Namely, if $F(x_j) = 0$, then by (2.10)

$$x_j + \frac{\alpha_{n-1}}{\beta_n}x_{j-1} + \frac{\beta_{n-1}}{\beta_n} = 0$$

which implies

$$x_j + \frac{\alpha_{n-1}}{\beta_n}x_{j-1} = \left(1+\frac{\alpha_{n-1}}{\beta_n}\right)\left(-\frac{\beta_{n-1}}{\beta_n + \alpha_{n-1}}\right). \tag{2.19}$$

But computing $x_{k(1)}$ from equation (2.17) we obtain exactly

$$x_{k(1)} = -\frac{\beta_{n-1}}{\beta_n + \alpha_{n-1}},$$

and hence from the injectivity of $k(i)$ and equation (2.19) we obtain $x_1 = x_j$. Now if $F(c) = 0$ for $c \in \mathbb{F}_q \setminus \mathbf{O}_n$, then by equation (2.8),

$$c = -\frac{\beta_{n-1}}{\beta_n + \alpha_{n-1}},$$

which equals $x_{k(1)}$, a contradiction. We have shown that $F(c) = 0$ implies $c = 0$. But then at least one of the two conditions from Proposition 2.24 is not satisfied. Suppose condition (i) does not hold. Then there exist $2 \leq i, j \leq n-1$ with $i \neq j$, such that

$$\frac{x_i - x_j}{x_{i-1} - x_{j-1}} = -\frac{\alpha_{n-1}}{\beta_n},$$

which implies $k(i) = k(j)$, a contradiction. On the other hand if the condition (ii) does not hold, then there exists some $c \in \mathbb{F}_q \backslash \mathbf{O_n}$ and some pole $x_i \in \mathbb{F}_q^*$ for which $F(c) = F(x_i)$ by Lemma 2.23. Solving for c this gives

$$c = \frac{x_i + \frac{\alpha_{n-1}}{\beta_n} x_{i-1}}{1 + \frac{\alpha_{n-1}}{\beta_n}},$$

which contradicts the existence of $k(i)$. □

The following lemma solves the recurrence relation which will be used in the proof of the next main theorem.

Lemma 2.26. *Let $n \geq 4$, $\mu, \nu \in \mathbb{F}_q$. If $x_{n-2} = \mu x_{n-1}$, and $x_{i-1} = \mu x_i + \nu x_{i+1}$ for $i = 1, \ldots, n-2$, then $x_{n-t} = G_t(\mu, \nu) x_{n-1}$, for $t = 1, \ldots, n-1$, and conversely, where*

$$G_t(\mu, \nu) = \sum_{i=1}^{\lceil t/2 \rceil} \binom{t-i}{i-1} \mu^{t-2i+1} \nu^{i-1}. \tag{2.20}$$

Proof. We give a proof by induction on t. One easily verifies the formula for $t = 1, 2$. Suppose $t \geq 3$ and (2.20) is satisfied for all $k < t$. Then

$$x_{n-t} = \mu x_{n-t+1} + \nu x_{n-t+2}$$

and by the induction hypothesis (here we use $n \geq 4$)

$$\begin{aligned} x_{n-t} &= \mu \left[\sum_{i=1}^{\lceil (t-1)/2 \rceil} \binom{t-1-i}{i-1} \mu^{t-2i} \nu^{i-1} x_{n-1} \right] + \nu \left[\sum_{i=1}^{\lceil (t-2)/2 \rceil} \binom{t-2-i}{i-1} \mu^{t-2i-1} \nu^{i-1} x_{n-1} \right] \\ &= \sum_{i=1}^{\lceil (t-1)/2 \rceil} \binom{t-1-i}{i-1} \mu^{t-2i+1} \nu^{i-1} x_{n-1} + \sum_{i=1}^{\lceil (t-2)/2 \rceil} \binom{t-2-i}{i-1} \mu^{t-2i-1} \nu^{i} x_{n-1}. \\ &= \sum_{i=1}^{\lceil (t-1)/2 \rceil} \binom{t-1-i}{i-1} \mu^{t-2i+1} \nu^{i-1} x_{n-1} + \sum_{i=2}^{\lceil t/2 \rceil} \binom{t-1-i}{i-2} \mu^{t-2i+1} \nu^{i-1} x_{n-1}. \end{aligned}$$

Now consider the coefficient of $\mu^{t-2i+1} \nu^{i-1} x_{n-1}$. For $i = 1$ this coefficient is

$$\binom{t-2}{0} = \binom{t-1}{0},$$

for $2 \leq i \leq \lceil (t-1)/2 \rceil$ it becomes

$$\binom{t-1-i}{i-1} + \binom{t-1-i}{i-2} = \binom{t-i}{i-1},$$

which is the same for $i = \lceil t/2 \rceil$ when t is even, while for t odd and $i = \lceil t/2 \rceil$ one obtains

$$\binom{t-1-(t/2+1/2)}{t/2+1/2-2} = 1 = \binom{t-(t/2+1/2)}{t/2+1/2-1}.$$

It follows that the coefficient of $\mu^{t-2i+1}\nu^{i-1}x_{n-1}$ equals $\binom{t-i}{i-1}$, for all $1 \leq i \leq \lceil t/2 \rceil$. The converse follows from the above calculations. □

For future reference we recall the relation (2.17) where k is the cycle $(1\ 2\ \ldots\ n-1)$, i.e.,

$$x_i + \frac{\alpha_{n-1}}{\beta_n} x_{i-1} = \left(1 + \frac{\alpha_{n-1}}{\beta_n}\right) x_{i+1}. \tag{2.21}$$

for $1 \leq i \leq n-1$, where indices are calculated modulo $n-1$.

Theorem 2.27. *For any $n \geq 4$ the polynomial*

$$H_n(x) = \sum_{j=0}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-j-2}{j} x^j (1+x)^j \tag{2.22}$$

has a root α in $\mathbb{F}_q^*$ if and only if there exist $x_1 = 0, x_2, \ldots, x_{n-1} \in \mathbb{F}_q$, satisfying (2.21), where $\alpha_{n-1}/\beta_n = \alpha$.

Proof. Let $\alpha \in \mathbb{F}_q^*$ be a root of the polynomial (2.22). Equivalently

$$\sum_{j=0}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-j-2}{j} \left[\left(-\frac{1}{\alpha}\right)^{-2} \left(1 + \frac{1}{\alpha}\right) \right]^j = 0,$$

and multiplying by $(-1/\alpha)^{n-2}$ we obtain

$$\sum_{j=0}^{\lceil \frac{n-1}{2} \rceil - 1} \binom{n-j-2}{j} \left(-\frac{1}{\alpha}\right)^{n-2-2j} \left(1 + \frac{1}{\alpha}\right)^j = 0.$$

Rewriting the summation gives

$$\sum_{i=1}^{\lceil \frac{n-1}{2} \rceil} \binom{n-i-1}{i-1} \left(-\frac{1}{\alpha}\right)^{n+1-2i} \left(1 + \frac{1}{\alpha}\right)^{i-1} = 0,$$

which is $G_{n-1}(-\alpha^{-1}, 1+\alpha^{-1}) = 0$, where $G_t(\mu, \nu)$ is defined by (2.20). Now choose $\beta_{n-1}, \beta_n, x_{n-1} \in \mathbb{F}_q^*$, put $\alpha_{n-1} = \beta_n \alpha$, and define $x_1, \ldots, x_{n-2}$ by (2.20), with $\mu =$

$-\beta_n/\alpha_{n-1}$ and $\nu = 1 + \beta_n/\alpha_{n-1}$. By the above, it follows that $x_1 = 0$. Applying Lemma 2.26, we obtain the recurrence relation (2.21).

Conversely, if there exists $x_1 = 0, x_2, \ldots, x_{n-1} \in \mathbb{F}_q$, $\alpha_{n-1}, \beta_n \in \mathbb{F}_q^*$ satisfying (2.21), then by Lemma 2.26 for $t = n-1$ we obtain

$$0 = x_1 = \sum_{i=1}^{\lceil \frac{n-1}{2} \rceil} \binom{n-i-1}{i-1} \left(-\frac{1}{\alpha}\right)^{n+1-2i} \left(1+\frac{1}{\alpha}\right)^{i-1},$$

where $\alpha = \alpha_{n-1}/\beta_n \in \mathbb{F}_q^*$. It follows from the equivalent statements at the start of the proof that α is a root of the polynomial (2.22). □

Theorem 2.28. *If $H_n(\alpha) = 0$ with $\alpha \in \mathbb{F}_q^*$ and $x_{n-1} \in \mathbb{F}_q^*$ such that the x_i's defined by*

$$x_{n-t} = G_t(-\alpha^{-1}, 1+\alpha^{-1})x_{n-1},$$

for $t \in \{2, \ldots, n-1\}$ are all distinct, then there exists a complete mapping polynomial $f(x) \in \mathcal{P}_{q,n}^{(2)}$ with poles $x_1 = 0, x_2, \ldots, x_{n-1}, x_n = \infty$.

Proof. It follows from the hypothesis, Lemma 2.26 and Theorem 2.27 that the x_i's are all distinct and satisfy the recurrence relations (2.21) with $\alpha_{n-1}/\beta_n = \alpha$. Moreover, since -1 is not a root of the polynomial $H_n(x)$, it follows that $\alpha_{n-1} \neq -\beta_n$. Applying Theorem 2.25 finishes the proof. □

Example 2.29. Take $q = 73$ and $n = 9$. Then we have

$$H_9(x) = 4x^3(1+x)^3 + 10x^2(1+x)^2 + 6x(1+x) + 1.$$

We choose $\alpha = 19$ as one of the roots of the polynomial $H_9(x)$ in $\mathbb{F}_{73}$. Then the polynomial $G_t(-\alpha^{-1}, 1+\alpha^{-1})$ becomes

$$\sum_{i=1}^{\lceil \frac{t}{2} \rceil} \binom{t-i}{i-1} (23)^{t-2i+1} (51)^{i-1}.$$

Put $R_9(x) = 19x + 1$ giving $x_8 = 23$. By using above theorem, we obtain

$$\begin{aligned}
x_7 &= G_2(23,51)x_8 = 23.23 = 18,\\
x_6 &= G_3(23,51)x_8 = -4.23 = -19,\\
x_5 &= G_4(23,51)x_8 = 59.23 = 43,\\
x_4 &= G_5(23,51)x_8 = 58.23 = 20,\\
x_3 &= G_6(23,51)x_8 = 36.23 = 25,\\
x_2 &= G_7(23,51)x_8 = -10.23 = -11,
\end{aligned}$$

which are all distinct. Now we use a procedure given in [3] which enables us constructing P_9 with R_9 and the poles $x_1, \ldots, x_9$ are prescribed. Since $R_9(x) = 19x + 1$, we have $\alpha_8 = 19\epsilon$, $\beta_8 = \epsilon$ and $\beta_9 = \epsilon$ where $\epsilon \neq 0$. Now we will use the relations (2.2) from before

$$\alpha_{i-2} = \alpha_i - c_{i-1}\alpha_{i-1} \quad \text{and} \quad \beta_{i-2} = \beta_i - c_{i-1}\beta_{i-1}$$

for $i \in \{2, \ldots, n-1\}$, to determine the coefficients $c_8, c_7, \ldots, c_0$ in the definition of $f(x)$, where $F(x) = f(x) + x$. These relations imply that for all $i \in \{2, \ldots, 8\}$,

$$\frac{\beta_{i-2}}{\alpha_{i-2}} = \frac{\beta_i - c_{i-1}\beta_{i-1}}{\alpha_i - c_{i-1}\alpha_{i-1}}$$

and hence

$$-x_{i-2} = \frac{\beta_i - c_{i-1}\beta_{i-1}}{\alpha_i - c_{i-1}\alpha_{i-1}}$$

or equivalently

$$-x_{i-2}\big(\alpha_i - c_{i-1}\alpha_{i-1}\big) = \beta_i - c_{i-1}\beta_{i-1}$$

and finally

$$c_{i-1} = \frac{\beta_i + x_{i-2}\alpha_i}{\beta_{i-1} + x_{i-2}\alpha_{i-1}}. \tag{2.23}$$

Therefore we get

$$c_8 = \frac{\beta_9 + x_7\alpha_9}{\beta_8 + x_7\alpha_8} = \frac{\epsilon}{\epsilon + 50\epsilon} = -10,$$

and $\alpha_7 = \alpha_9 - c_8\alpha_8 = 44\epsilon$, $\beta_7 = \beta_9 - c_8\beta_8 = 11\epsilon$. Recursively we calculate the exact values for $c_7, \ldots, c_2$, and values for $\alpha_6, \beta_6, \ldots, \alpha_1, \beta_1$ as multiples of ϵ. Then we can find c_2 which is equal to β_3. The identity $\beta_2 = c_1\beta_1 + \beta_0 = -\epsilon = 1$ then yields the value for $\epsilon = -1$. From $\alpha_0 = 0$, we have $c_1 = \alpha_2/\alpha_1 = 22$. Finally, we have $c_0 = \alpha_1$. Hence we get a polynomial

$$f(x) = P_9(-19, 22, -11, 23, -11, 23, -11, 23, -10; x)$$

which is a complete mapping polynomial over $\mathbb{F}_{73}$.

2.3.1 $n = 4$

In this section we focus on the smallest case: $n = 4$. We start by giving a necessary and sufficient condition for the existence of complete mapping polynomials in the class $\mathcal{P}^{(2)}_{q,4}$.

Theorem 2.30. *There exists a complete mapping polynomial $f \in \mathcal{P}_{q,4}^{(2)}$ with distinct poles $x_1, x_2, x_3, x_4 = \infty$ satisfying (2.21) if and only if the polynomial $1 + x + x^2$ has a root α in $\mathbb{F}_q^*$.*

Proof. For $n = 4$, the polynomial (2.22), becomes

$$H_4(x) = \sum_{j=0}^{1} \binom{2-j}{j} x^j (1+x)^j = 1 + x + x^2. \tag{2.24}$$

Now suppose $\alpha \in \mathbb{F}_q^*$ is a root of $H_4(x)$. Applying Theorem 2.27 we obtain $x_1 = 0, x_2, x_3 \in \mathbb{F}_q$ satisfying the recurrence relations (2.21) with $\alpha_{n-1}/\beta_n = \alpha$, i.e.,

$$x_1 = 0, \ x_2 = (1+\alpha)\, x_3.$$

It follows that for any choice of $x_3 \in \mathbb{F}_q^*$, the elements x_1, x_2, x_3 are distinct. By Theorem 2.25 we obtain a complete mapping polynomial $f \in \mathcal{P}_{q,4}^{(2)}$ with poles $x_1, x_2, x_3, x_4 = \infty$ satisfying (2.21), where $\alpha_{n-1}/\beta_n = \alpha$.

Conversely, if $f \in \mathcal{P}_{q,4}^{(2)}$ with poles $x_1, x_2, x_3, x_4 = \infty$ satisfying (2.21) is a complete mapping polynomial then by Theorem 2.27, the polynomial $H_4(x)$ must have a root $\alpha \in \mathbb{F}_q^*$. □

Theorem 2.30 yields explicit constructions of complete mapping polynomials in $\mathcal{P}_{q,4}^{(2)}$ for $q \equiv 1 \mod 3$ and $q = 3^s$.

Theorem 2.31. *If $q = 3^s$ or $q \equiv 1 \bmod 3$, then any polynomial of the form*

$$\left(\left(\left(\left(\frac{\alpha^3}{(1+\alpha)^2} x \right)^{q-2} + c \right)^{q-2} + \frac{1}{\alpha c} \right)^{q-2} - \frac{\alpha c}{1+\alpha} \right)^{q-2} \in \mathcal{P}_{q,4}^{(2)} \tag{2.25}$$

is a complete mapping polynomial over $\mathbb{F}_q$ where $c \in \mathbb{F}_q^*$ is arbitrary, $\alpha = 1$ if $q = 3^s$ and it is a primitive 3^{rd} root of unity if $q \equiv 1 \bmod 3$.

Proof. If $char(\mathbb{F}_q) = 3$, then $1 + x + x^2 = (x-1)^2$. So $\alpha = 1$ is a root in $\mathbb{F}_q$. When $(q, 3) = 1$, then $1 + x + x^2 = Q_3$ is the 3^{rd} cyclotomic polynomial over $\mathbb{F}_q$ and it has a root α in $\mathbb{F}_q$ whenever $q \equiv 1 \mod 3$. In both cases Thm 2.30 applies and hence there exists a complete mapping polynomial in $f \in \mathcal{P}_{q,4}^{(2)}$ with poles $x_4 = \infty$, and x_1, x_2, x_3 satisfying the recurrence relations (2.21),

$$x_i + \alpha x_{i-1} = (1+\alpha) x_{i+1}.$$

Let $F \in \mathcal{F}_{q,4}^{(2)}$ with $F(x) = f(x) + x$. Then

$$F(x) = \left(\left((c_0 x)^{q-2} + c_1 \right)^{q-2} + c_2 \right)^{q-2} + c_3 \Bigg)^{q-2} + x,$$

for some $c_0, c_1, c_2, c_3 \in \mathbb{F}_q^*$. From (2.2) and (2.3) one obtains

$$x_1 = 0,\ x_2 = -\frac{1}{c_1 c_0},\ x_3 = -\frac{c_2}{c_0(c_2 c_1 + 1)}.$$

From the recurrence relations between the poles we then obtain

$$x_2 = (1+\alpha)x_3 \quad \text{which implies} \quad c_2 = \frac{1}{\alpha c_1}.$$

We also know that $\alpha_4 = 0$, which implies that $c_3(c_1 c_2 + 1) + c_1 = 0$. Substituting the expression obtained for c_2 above, gives

$$c_3 = \frac{-\alpha c_1}{1+\alpha}.$$

Finally, recall that $\alpha = \dfrac{\alpha_3}{\beta_4}$, which means

$$\alpha = \frac{c_0(c_1 c_2 + 1)}{c_3 c_2 + 1},$$

and this implies

$$c_0 = \frac{\alpha^3}{(1+\alpha)^2}.$$

We have obtained the coefficients c_0, c_1, c_2, c_3 in terms of α and $c_1 \in \mathbb{F}_q^*$, which gives the formula (2.25) for $f(x) \in \mathcal{P}_{q,4}^{(2)}$, where $c = c_1 \in \mathbb{F}_q^*$ is arbitrary. □

2.3.2 $n = 5$

Also for the case $n = 5$ we obtain a necessary and sufficient condition for the existence of complete mapping polynomials in the class $\mathcal{P}_{q,5}^{(2)}$. For this case we will obtain explicit constructions of complete mapping polynomials in $\mathcal{P}_{q,5}^{(2)}$ for $q \equiv 1 \mod 4$.

Theorem 2.32. *There exists a complete mapping polynomial $f \in \mathcal{P}_{q,5}^{(2)}$ with distinct poles $x_1, x_2, x_3, x_4, x_5 = \infty$ satisfying (2.21) if and only if the polynomial $2x^2 + 2x + 1$ has a root α in $\mathbb{F}_q^*$.*

Proof. For $n = 5$, the polynomial (2.22), becomes

$$H_5(x) = \sum_{j=0}^{1} \binom{3-j}{j} x^j (1+x)^j = 2x^2 + 2x + 1. \tag{2.26}$$

Now suppose $\alpha \in \mathbb{F}_q^*$ is a root of $H_5(x)$. Applying Theorem 2.27 we obtain $x_1 = 0, x_2, x_3, x_4 \in \mathbb{F}_q$ satisfying the recurrence relations (2.21) with $\alpha_{n-1}/\beta_n = \alpha$, i.e.,

$$x_1 = 0,\ x_2 = (1+\alpha)\, x_3,\ x_3 = (1+\alpha)\, x_4 - \alpha x_2.$$

Solving for x_2 and x_3 in function of α and x_4 we obtain

$$x_1 = 0,\ x_2 = \frac{(1+\alpha)^2}{\alpha^2+\alpha+1} x_4,\ x_3 = \frac{1+\alpha}{\alpha^2+\alpha+1} x_4. \tag{2.27}$$

It follows that for any choice of $x_4 \in \mathbb{F}_q^*$, the elements x_1, x_2, x_3, x_4 are distinct. By Theorem 2.25, we obtain a complete mapping polynomial $f \in \mathcal{P}_{q,5}^{(2)}$ with poles $x_1, x_2, x_3, x_4, x_5 = \infty$ satisfying (2.21), where $\alpha_{n-1}/\beta_n = \alpha$.

Conversely, if $f \in \mathcal{P}_{q,5}^{(2)}$ with poles $x_1, x_2, x_3, x_4, x_5 = \infty$ satisfying (2.21) is a complete mapping polynomial then by Theorem 2.27, the polynomial $H_5(x)$ must have a root $\alpha \in \mathbb{F}_q^*$. □

In the next theorem we explicitly determine the coefficients c_0, c_2, c_3, c_4 in function of the root α of $H_5(x)$ and the first coefficient $c_1 \in \mathbb{F}_q^*$.

Theorem 2.33. *Let $q \equiv 1 \bmod 4$. Any polynomial of the form*

$$\left(\left(\left(\left(-\frac{(\alpha+1)^2}{\alpha c^2}x\right)^{q-2} + c\right)^{q-2} + \frac{1}{\alpha c}\right)^{q-2} - \frac{(2\alpha+1)\alpha c}{(\alpha+1)^2}\right)^{q-2} + \frac{(\alpha+1)^2}{\alpha^2 c}\right)^{q-2} \tag{2.28}$$

in $\mathcal{P}_{q,5}^{(2)}$ is a complete mapping polynomial over $\mathbb{F}_q$ where $\alpha \in \mathbb{F}_q$ is a root of $2x^2+2x+1$ and $c \in \mathbb{F}_q^*$ is arbitrary.

Proof. Since $q \equiv 1 \mod 4$, by Euler's criterion, the polynomial $2x^2+2x+1$ has a root $\alpha \in \mathbb{F}_q^*$. By Theorem 2.32, there exists a complete mapping polynomial in $f \in \mathcal{P}_{q,5}^{(2)}$ with poles $x_5 = \infty$, and x_1, x_2, x_3, x_4 satisfying the recurrence relations in (2.21),

$$x_i + \alpha x_{i-1} = (1+\alpha) x_{i+1}.$$

Let $F \in \mathcal{F}_{q,5}^{(2)}$ with $F(x) = f(x) + x$. Then

$$F(x) = \left(\left(\left((c_0 x)^{q-2} + c_1\right)^{q-2} + c_2\right)^{q-2} + c_3\right)^{q-2} + c_4\Big)^{q-2} + x,$$

for some $c_0, c_1, c_2, c_3, c_4 \in \mathbb{F}_q^*$. From (2.2) and (2.3) one can get

$$x_1 = 0,\ x_2 = -\frac{1}{c_1 c_0},\ x_3 = -\frac{c_2}{c_0(c_2 c_1 + 1)},\ x_4 = -\frac{c_3 c_2 + 1}{c_0\big(c_3(c_2 c_1 + 1) + c_1\big)}.$$

From the recurrence relations between the poles we first obtain

$$x_2 = (1+\alpha)x_3 \quad \text{which implies} \quad c_2 = \frac{1}{\alpha c_1}.$$

Now to find c_3 we consider the relation between the poles for $i = 4$. We obtain $x_4 = -\alpha x_3$ and by substituting $c_2 = \frac{1}{\alpha c_1}$ we get

$$c_3 = -\frac{c_1\alpha(2\alpha+1)}{(\alpha+1)^2}.$$

We also know that $\alpha_5 = 0$, which implies

$$c_4 = \frac{c_2c_1 + 1}{c_3c_2c_1 + c_3 + c_1}$$

Substituting c_2 and c_3 by the expression obtained above, gives

$$c_4 = \frac{(\alpha+1)^2}{c_1\alpha^2}.$$

To determine the coefficient c_0, we recall that $\alpha = \dfrac{\alpha_4}{\beta_5}$, which means

$$\alpha = \frac{c_0(c_3(c_2c_1+1)+c_1}{c_4(c_3c_2+1)+c_2}$$

which gives

$$c_0 = -\frac{(\alpha+1)^2}{c_1^2}.$$

Hence we have obtained the coefficients c_0, c_1, c_2, c_3, c_4 in terms of α and $c_1 \in \mathbb{F}_q^*$, which gives the formula (2.28) for $f(x) \in \mathcal{P}_{q,5}^{(2)}$, where $c = c_1 \in \mathbb{F}_q^*$ is arbitrary. □

2.3.3 $n = 6$

As in the case $n = 4$ and $n = 5$ we obtain the following necessary and sufficient condition for the existence of complete mapping polynomials in the class $\mathcal{P}_{q,6}^{(2)}$.

Theorem 2.34. *There exists a complete mapping polynomial $f \in \mathcal{P}_{q,6}^{(2)}$ with distinct poles $x_1, x_2, x_3, x_4, x_5, x_6 = \infty$ satisfying (2.21) if and only if the polynomial $x^4 + 2x^3 + 4x^2 + 3x + 1$ has a root α in $\mathbb{F}_q^*$.*

Proof. For $n = 6$, the polynomial (2.22), becomes

$$H_6(x) = \sum_{j=0}^{2} \binom{4-j}{j} x^j(1+x)^j = x^4 + 2x^3 + 4x^2 + 3x + 1. \tag{2.29}$$

Now suppose $\alpha \in \mathbb{F}_q^*$ is a root of $H_6(x)$. Note that $\alpha \neq -1$. Applying Theorem 2.27 we obtain $x_1 = 0, x_2, x_3, x_4, x_5 \in \mathbb{F}_q$ satisfying the recurrence relations (2.21) with $\alpha_{n-1}/\beta_n = \alpha$, i.e.,

$$x_1 = 0,\ x_2 = \frac{\alpha}{1+\alpha} x_5,\ x_3 = (1+\alpha)\, x_4 - \alpha x_2,\ x_4 = (1+\alpha)\, x_5 - \alpha x_3.$$

Writing all poles in terms of α and x_5 gives

$$x_1 = 0,\ x_2 = \frac{\alpha}{1+\alpha} x_5,\ x_3 = \frac{\alpha}{(1+\alpha)^2} x_5,\ x_4 = -\frac{1}{\alpha} x_5. \tag{2.30}$$

Clearly $x_2 \neq x_5$. We may conclude that for any choice of $x_5 \in \mathbb{F}_q^*$, the elements x_1, x_2, x_3, x_4, x_5 are distinct.

By Theorem 2.25, we obtain a complete mapping polynomial $f \in \mathcal{P}_{q,6}^{(2)}$ with poles $x_1, x_2, x_3, x_4, x_5, x_6 = \infty$ satisfying (2.21), where $\alpha_{n-1}/\beta_n = \alpha$.

Conversely, if $f \in \mathcal{P}_{q,6}^{(2)}$ with poles $x_1, x_2, x_3, x_4, x_5, x_6 = \infty$ satisfying (2.21) is a complete mapping polynomial then by Theorem 2.27, the polynomial $H_6(x)$ must have a root $\alpha \in \mathbb{F}_q^*$. □

The following theorem gives an explicit formula for a family of complete mapping polynomials in $\mathcal{P}_{q,6}^{(2)}$.

Theorem 2.35. *Any polynomial of the form*

$$f(x) = P_6\left(\frac{\alpha^5}{(\alpha+1)^4}, c, \frac{1}{c\alpha}, \frac{c}{1+\alpha}, \frac{1}{c\alpha}, -\frac{c\alpha}{1+\alpha}; x\right) \ \in\ \mathcal{P}_{q,6}^{(2)} \tag{2.31}$$

is a complete mapping polynomial over $\mathbb{F}_q$ if $\alpha \in \mathbb{F}_q$ is a root of $x^4 + 2x^3 + 4x^2 + 3x + 1$ and $c \in \mathbb{F}_q^*$ is arbitrary.

Proof. If the polynomial $x^4 + 2x^3 + 4x^2 + 3x + 1$ has a root $\alpha \in \mathbb{F}_q^*$ then by Theorem 2.34, there exists a complete mapping polynomial in $f \in \mathcal{P}_{q,6}^{(2)}$ with poles $x_6 = \infty$, and x_1, x_2, x_3, x_4, x_5 satisfying the recurrence relations in (2.21),

$$x_i + \alpha x_{i-1} = (1+\alpha) x_{i+1}.$$

Let $F \in \mathcal{F}_{q,6}^{(2)}$ with $F(x) = f(x) + x$. Then

$$F(x) = \left(\left(\left(\left(\left((c_0 x)^{q-2} + c_1\right)^{q-2} + c_2\right)^{q-2} + c_3\right)^{q-2} + c_4\right)^{q-2} + c_5\right)^{q-2} + x,$$

for some $c_0, c_1, c_2, c_3, c_4, c_5 \in \mathbb{F}_q^*$. From (2.2) and (2.3) one can get

$$x_1 = 0, \quad x_2 = -\frac{1}{c_1 c_0}, \quad x_3 = -\frac{c_2}{c_0(c_2c_1+1)}, \quad x_4 = -\frac{c_3c_2+1}{c_0\big(c_3(c_2c_1+1)+c_1\big)}$$

and

$$x_5 = -\frac{c_4(c_3c_2+1)+c_2}{c_0\big(c_4c_3(c_2c_1+1)+c_4c_1+c_2c_1+1\big)}.$$

Similarly as above we obtain

$$x_2 = (1+\alpha)x_3 \quad \text{which implies} \quad c_2 = \frac{1}{\alpha c_1}.$$

Now to find c_3 we consider the relation $x_3 + \alpha x_2 = (1+\alpha)x_4$ and by substituting $c_2 = \dfrac{1}{\alpha c_1}$ we get

$$c_3 = \frac{c_1}{1+\alpha}.$$

By substituting c_2 and c_3 to the equation

$$x_4 + \alpha x_3 = (1+\alpha)x_5$$

we get $c_4 = \dfrac{1}{c_1\alpha}$. We also know that $\alpha_6 = 0$, which implies that

$$c_5 = \frac{c_0\big(c_3(c_2c_1+1)+c_1\big)}{c_0\big(c_4c_3(c_2c_1+1)+c_4c_1+c_2c_1+1\big)}.$$

Substituting the expressions we obtained for c_2, c_3 and c_4 above, we get

$$c_5 = -\frac{c_1\alpha}{1+\alpha}.$$

Recall that $\alpha = \dfrac{\alpha_5}{\beta_6}$, which means

$$c_0 = \frac{\alpha^5}{(1+\alpha)^4}.$$

Hence we have obtained the coefficients $c_0, c_1, c_2, c_3, c_4, c_5$ in terms of α and $c_1 \in \mathbb{F}_q^*$, which gives the formula (2.31) for $f(x) \in \mathcal{P}_{q,6}^{(2)}$, where $c = c_1 \in \mathbb{F}_q^*$ is arbitrary. □

Corollary 2.36. *Let $p = 5$ or $p \equiv \pm 1 \mod 10$ and $q = p^s$ be a square. Then any polynomial of the form (2.31) is a complete mapping polynomial over $\mathbb{F}_q$, where $\alpha \in \mathbb{F}_q$ is a root of $x^4 + 2x^3 + 4x^2 + 3x + 1$ and $c \in \mathbb{F}_q^*$ is arbitrary.*

Proof. We only need to prove that the polynomial $H_6(x) = x^4 + 2x^3 + 4x^2 + 3x + 1$ has a root $\alpha \in \mathbb{F}_q$ if q is as in the hypothesis. It is easy to see that H_6 factorizes over $\mathbb{F}_{q^2}$ as $H_6(x) = (x^2 + x + d)(x^2 + x + d^{-1})$, where $d = \frac{3\pm\sqrt{5}}{2}$. If $p = \pm 1 \mod 5$ then d is in $\mathbb{F}_p$. Note that since p is odd, this means that $p \equiv \pm 1 \mod 10$. In this case $x^2 + x \pm d \in \mathbb{F}_p[x]$, being a quadratic, has roots in $\mathbb{F}_{p^2}$. Hence if q is a square, its roots are in $\mathbb{F}_q$. □

Remark 2.37. It is possible to deal with the case of characteristic 2 along the same lines. One needs to consider the trace function to determine the number of zeros of a quadratic equations. More precisely, for the equation $x^2 + ax + b = 0$, substitute $x \mapsto ay$. Then

$$a^2y^2 + a^2y + b = 0 \quad \Rightarrow \quad y^2 + y + a^{-2}b = 0,$$

has 2 solutions if $Tr(a^{-2}b) = 0$ and no solution otherwise. However we leave out this case since Carlitz rank has been studied only in odd characteristic so far.

Remark 2.38. Above we gave construction of complete mapping polynomials satisfying $|\mathbf{O_n}| = n$. Note that there are also examples of complete mappings with $|\mathbf{O_n}| < n$. For instance, take $q = 17$ and $n = 6$ the polynomial

$$f(x) = P_6(-1, 10, 3, -3, 6, -4; x)$$

is a complete mapping polynomials where $x_2 = x_5 = 12$.

CHAPTER 3

On Value Sets of a Class of Polynomials

As mentioned in Section 1.3, value sets of polynomials $f(x)$ are usually studied in relation to the degree of $f(x)$. In this thesis, we study value sets in relation with the Carlitz rank. In particular, we will study the spectrum of classes of polynomials $f(x)+x$, where $f(x)$ is a PP of Carlitz rank at most n.

3.1 The Spectrum $v(\mathcal{F}_{q,n}^{(1)})$

In this section, the spectrum of the class $\mathcal{F}_{q,n}^{(1)}$ is studied. First, we give some results for $n=1$ and $n=2$.

Theorem 3.1. *If $F(x) \in \mathcal{F}_{q,1}$, then*

$$v(\mathcal{F}_{q,1}) = \begin{cases} \frac{q+1}{2} & \text{if } q \equiv 1 \mod 4, \\ \frac{q-1}{2}, \frac{q+3}{2} & \text{if } q \equiv 3 \mod 4. \end{cases}$$

Proof. Let $F(x)$ be in $\mathcal{F}_{q,1}$. Then $F(x) = (c_0 x)^{q-2} + x$. Note that $F(x)$ has a unique pole which is 0 and clearly $F(0) = 0$. For $c \in \mathbb{F}_q^*$, we have a rational function $F(c) = \frac{c_0 c^2 + 1}{c_0 c}$. Obviously $\pm\sqrt{-c_0^{-1}}$ are zeros of F.

Let $c \in \mathbb{F}_q^*$. We show that there is a unique $y \neq c$ with $F(c) = F(y)$, whenever $c \neq \pm\sqrt{c_0^{-1}}$. Namely, for $c \neq 0$, we have

$$\begin{aligned} F(c) = F(y) &\Rightarrow c_0 c^2 y + y = a_0 c y^2 + c \\ &\Rightarrow c_0 c y (c - y) = (c - y) \\ &\Rightarrow y = \frac{1}{c_0 c}, \quad \text{since } c \neq y. \end{aligned}$$

Therefore $y = \frac{1}{c_0 c} \neq c$ if $c \neq \pm\sqrt{c_0^{-1}}$.

If c_0 and $-c_0$ are both squares in $\mathbb{F}_q$ (which implies $q \equiv 1 \bmod 4$), then we get three times $F(c) = 0$, once $F(c) = \pm 2\sqrt{c_0^{-1}}$ and twice any other value. This implies $|V_F| = 3 + (q-5)/2 = (q+1)/2$.

If c_0 and $-c_0$ are both nonsquares in $\mathbb{F}_q$ (that is $q \equiv 1 \bmod 4$ again), then we get once $F(c) = 0$ and any other value attained twice. Thus the size of the value set is again $1 + (q-1)/2 = (q+1)/2$.

If c_0 is a square and $-c_0$ is nonsquare in $\mathbb{F}_q$ (that is $q \equiv 3 \bmod 4$), then $F(c) = 0$ and $F(c) = \pm 2\sqrt{c_0^{-1}}$ are attained once and each other value twice. Therefore we have $|V_F| = 3 + (q-3)/2 = (q+3)/2$. If c_0 is a nonsquare and $-c_0$ is a square in $\mathbb{F}_q$ (thus $q \equiv 3 \bmod 4$), then we get three times $F(c) = 0$, and any other value is attained twice. Then the size of the value set is $1 + (q-3)/2 = (q-1)/2$. □

Theorem 3.2. *If $F(x) \in \mathcal{F}_{q,2}$, then*

$$v(\mathcal{F}_{q,2}) = \Big\{(q-1)/2,\ (q+1)/2,\ (q+3)/2,\ (q+5)/2\Big\}.$$

Proof. Consider $F(x) = \big((c_0 x)^{q-2} + c_1\big)^{q-2} + x$, where $c_0, c_1 \neq 0$. The poles are $x_1 = 0$, $x_2 = -1/(c_0 c_1)$. Hence when $c \neq 0$ and $c \neq -1/(c_0 c_1)$,

$$F(c) = \big((c_0 c)^{-1} + c_1\big)^{-1} + c = \frac{c_0 c_1 c^2 + (c_0+1)c}{c_0 c_1 c + 1} = \frac{c\big(c_0 c_1 c + (c_0+1)\big)}{c_0 c_1 c + 1},$$

$F(0) = 1/c_1$, $F\big(-1/c_0 c_1\big) = -1/(c_0 c_1)$. Let $c \in \mathbb{F}_q^*$ and $c \neq -1/(c_0 c_1)$. We show that there is a unique $y \neq c$ with $F(c) = F(y)$, whenever

$$c \neq \frac{\mp\sqrt{-c_0} - 1}{c_0 c_1}.$$

Namely, for $c \neq 0$, and $c \neq -1/(c_0 c_1)$,

$$\begin{aligned} F(c) = F(y) \ &\Rightarrow \quad \big(c_0^2 c_1^2 cy + c_0 c_1 (c+y) + (c_0+1)\big)(c-y) = 0 \\ &\Rightarrow \qquad y(c_0^2 c_1^2 c + c_0 c_1) + c_0 c_1 c + c_0 + 1 = 0. \end{aligned}$$

Therefore we get

$$y = -\frac{c_0 c_1 c + c_0 + 1}{c_0^2 c_1^2 c + c_0 c_1}.$$

Note that $c = -\frac{c_0+1}{c_0 c_1}$ implies $y = 0$ but y can not be equal to the one of the poles so in this case we should exclude $c = -\frac{c_0+1}{c_0 c_1}$.

$$\text{If } \ y = c \ \ \Rightarrow \ \ -\frac{c_0 c_1 c + c_0 + 1}{c_0^2 c_1^2 c + c_0 c_1} = c \ \ \Rightarrow \ \ (c_0 c_1 c + 1)^2 = -c_0 \ \ \Rightarrow \ \ c = \frac{\mp\sqrt{-c_0} - 1}{c_0 c_1}.$$

Hence $y \neq c$ only if

$$c \neq \frac{\mp\sqrt{-c_0} - 1}{c_0 c_1}.$$

Now let us consider the poles of F. Note that $F(0) = 1/c_1 = F(c)$ occurs when

$$\frac{1}{c_1} = \frac{c_0 c_1 c^2 + (c_0 + 1)c}{c_0 c_1 c + 1} \quad \Rightarrow \quad c_0 c_1^2 c^2 + c_1 c - 1 = 0$$

i.e

$$c = \frac{-1 \mp \sqrt{1 + 4c_0}}{2c_0 c_1}.$$

Similarly $F\big(-1/(c_0 c_1)\big) = -1/(c_0 c_1) = F(c)$ occurs when

$$\frac{-1}{c_0 c_1} = \frac{c_0 c_1 c^2 + (c_0 + 1)c}{c_0 c_1 c + 1} \quad \Rightarrow \quad c_0^2 c_1^2 c^2 + (c_0^2 c_1 + 2c_0 c_1)c + 1 = 0,$$

i.e,

$$c = \frac{-(c_0 + 1) \pm \sqrt{c_0(4 + c_0)}}{2c_0 c_1}.$$

Now we determine the values of $|V_F|$. First let $c_0 \neq -1$.

Suppose that $-c_0, 1+4c_0, c_0(4+c_0)$ are all squares in $\mathbb{F}_q$. Then F attains the values 0, and

$$\frac{\mp 2c_0 + (c_0 - 1)(\sqrt{-c_0})}{c_0 c_1 \sqrt{-c_0}}$$

once each and any other value twice. Thus the size of the value set is $1+2+(q-5)/2 = (q+1)/2$.

If $-c_0$ is a square and one of $1 + 4c_0$, then $c_0(4 + c_0)$ is a nonsquare in $\mathbb{F}_q$. Then both values $F(c) = 0$, and

$$F(c) = \frac{\mp 2c_0 + (c_0 - 1)(\sqrt{-c_0})}{c_0 c_1 \sqrt{-c_0}}$$

are attained once, one of the values $1/c_1$, $-1/(c_0 c_1)$ is attained once and any other value twice. Hence $|V_F| = 1 + 2 + 1 + (q-5)/2 = (q+3)/2$.

Suppose that $-c_0$ is a square in $\mathbb{F}_q$ and $1 + 4c_0$, $c_0(4 + c_0)$ are nonsquares in $\mathbb{F}_q$. Then 0,

$$\frac{\mp 2c_0 + (c_0 - 1)(\sqrt{-c_0})}{c_0 c_1 \sqrt{-c_0}},$$

$-1/(c_0 c_1)$ and $1/c_1$ are all attained once each, and any other value is attained twice. Thus $|V_F| = 1 + 2 + 1 + 1 + (q-5)/2 = (q+5)/2$.

Suppose that $-c_0$ is a nonsquare in $\mathbb{F}_q$, and $1 + 4c_0$, $c_0(4 + c_0)$ are squares in $\mathbb{F}_q$. Then F attains the value 0 once and any other value twice. Hence the size of the value set is $1 + (q-3)/2 = (q-1)/2$.

Suppose that $-c_0$ is a nonsquare in $\mathbb{F}_q$ and one of $1+4c_0$, $c_0(4+c_0)$ is a square in $\mathbb{F}_q$. Then 0 is attained once, one of the values $1/c_1$, $-1/(c_0c_1)$ is attained once and any other value twice. Therefore $|V_F| = 1+1+(q-3)/2 = (q+1)/2$.

Suppose that $-c_0$, $1+4c_0$, $c_0(4+c_0)$ are all nonsquares in $\mathbb{F}_q$. Then we have $F(c) = 0$, $F(c) = 1/c_1$ and $F(c) = -1/(c_0c_1)$ once each and any other value twice. Thus $|V_F| = 1+1+1+(q-3)/2 = (q+3)/2$.

Now let $c_0 = -1$. Then $-c_0 = 1$ is always a square in $\mathbb{F}_q$. Note that in this case $F(c) \neq 0$, for each $c \in \mathbb{F}_q^*$. If -3 is a square in $\mathbb{F}_q$ then F attains the value $1/c_1$ four times, the value $4/c_1$ once and any other value twice. Therefore $|V_F| = 1+1+(q-5)/2 = (q-1)/2$. If -3 is a nonsquare in $\mathbb{F}_q$ then $1/c_1$ is attained twice and $4/c_1$ is attained once and any other value is attained twice. Thus $|V_F| = 1+1+(q-3)/2 = (q+1)/2$. This completes the proof. □

Theorem 3.3. *For every $F \in \mathcal{F}_{q,n}^{(1)}$,*

$$\lceil \frac{q-n}{2} \rceil \leq |V_F| \leq \frac{q+2n+1}{2}.$$

Proof. By the arguments presented in Section 2.2, the maximal cardinality of the value set for F is attained when $|M| = n-1$, $(-1)^{n-1}c_0$ is square in $\mathbb{F}_q$, $|F(\mathbf{O}_n)| = n$ and $F(\mathbf{O}_n) \cap F(\mathbb{F}_q \setminus \mathbf{O}_n) = \emptyset$. Therefore

$$\max(|V_F|) = n+2+(n-1)+\frac{q-n-2-(n-1)}{2} = \frac{q+2n+1}{2}.$$

If n is odd, then the minimum value is attained if the sets T and M are empty and $F(\mathbf{O}_n) \subset F(\mathbb{F}_q \setminus \mathbf{O}_n)$, in which case

$$\min(|V_F|) = \frac{q-n}{2}$$

If n is even, then $q-n$ is odd, which implies (since $|D|$ is even), that at least one element belongs to $\mathbb{F}_q \setminus (\mathbf{O}_n \cup D)$. Therefore

$$\min(|V_F|) = 1+\frac{q-1-n}{2} = \frac{q+1-n}{2}.$$

Hence

$$\lceil \frac{q-n}{2} \rceil \leq |V_F| \leq \frac{q+2n+1}{2},$$

for every $F \in \mathcal{F}_{q,n}^{(1)}$. □

3.2 The Spectrum $v(\mathcal{F}_{q,n}^{(2)})$

In this section, the spectrum of the class $\mathcal{F}_{q,n}^{(2)}$ is studied. We start by determining the spectrum of $\mathcal{F}_{q,3}^{(2)}$.

3.2.1 $v(\mathcal{F}_{q,3}^{(2)})$

Theorem 3.4. *If $F \in \mathcal{F}_{q,3}^{(2)}$, $F(x) = f(x) + x$ with $f(x) = P_3(c_0, c_1, c_2; x)$ then*

$$|V_F| = \begin{cases} 3 & \text{if} \quad c_0c_1^2 = 1, \\ q-2 & \text{otherwise.} \end{cases}$$

Proof. Take $F \in \mathcal{F}_{q,3}^{(2)}$. Then $\alpha_3 = 0$, which means that $c_2c_1 + 1 = 0$, i.e., $c_2 = -\frac{1}{c_1}$. Therefore we have the polynomial $F \in \mathcal{F}_{q,3}^{(2)}$ is of the form

$$F(x) = \left(((c_0x)^{q-2} + c_1)^{q-2} - \frac{1}{c_1}\right)^{q-2} + x,$$

and the corresponding rational function

$$\mathcal{R}_n(x) = \frac{\alpha_2 x + \beta_2}{\beta_3} + x = (-c_0c_1^2 + 1)x - c_1 \tag{3.1}$$

since $\alpha_2 = c_1c_0$, $\beta_2 = 1$ and $\beta_3 = c_2 = -\frac{1}{c_2}$. By Lemmas 2.9 and 2.21, we have

$$F(x_1) = 0, \quad F(x_2) = \mathcal{R}_n(x_1) + x_2 = -\frac{c_0c_1^2 + 1}{c_0c_1},$$

where $x_1 = 0$ and $x_2 = -\frac{1}{c_0c_1}$.

If $c_0c_1^2 = 1$ then by equation (3.1) we obtain $F(y) = -c_1$ for all $y \neq x_1, x_2$, or equivalently F behaves as a constant polynomial except at two points x_1, x_2. We also have $F(x_2) = -\frac{c_0c_1^2+1}{c_0c_1} = -2c_1$. Therefore, $V_F = \{0, -c_1, -2c_1\}$. Hence $|V_F| = 3$.

Now consider the case $c_0c_1^2 = -1$. Then $F(x_1) = F(x_2) = 0$ for the poles $x_1 = 0$ and $x_2 = -\frac{1}{c_0c_1} = c_1$. By Equation (3.1), we have $F(y) = 2y - c_1$ for each $y \in \mathbb{F}_q^* \setminus \{x_2\}$. The multiplicity of the element 0 in the value set is 3 since the equation $2x - c_1 = 0$ has exactly one solution in $\mathbb{F}_q \setminus \{x_1, x_2\}$. Therefore, we have

$$V_F = \{0, 0, 0, u_1, u_2, ..., u_{q-3}\},$$

where $u_i = F(y_i)$ for $i \in \{1, \ldots, q-3\}$ and $y_i \in \mathbb{F}_q^* \setminus \{x_2\}$. Hence $|V_F| = q - 2$.

Next, assume that $c_0c_1^2 \neq \pm 1$. Then $F(x_1) \neq F(x_2)$ and $F(y) = (-c_0c_1^2+1)y - c_1$ for $y \neq x_1, x_2$. Hence for each $i = 1, 2$, there exists a unique $y \in \mathbb{F}_q \setminus \{x_1, x_2\}$ s.t. $F(x) = F(x_i)$. Therefore,

$$V_F = \left\{0, 0, -\frac{-c_0c_1^2-1}{c_0c_1}, -\frac{-c_0c_1^2-1}{c_0c_1}, v_1, v_2, ..., v_{q-4}\right\},$$

where $v_i = F(y_i)$ for $i \in \{1, \ldots, q-4\}$ and $y_i \in \mathbb{F}_q^* \setminus \{x_2\}$. Hence $|V_F| = q-2$. □

Corollary 3.5. *The spectrum of the family $\mathcal{F}_{q,3}^{(2)}$ is*

$$v\left(\mathcal{F}_{q,3}^{(2)}\right) = \{3, q-2\}.$$

Corollary 3.6. *Any polynomial $F \in \mathcal{F}_{q,3}^{(2)}$ of the form*

$$F(x) = \left(\left(\left(\frac{1}{c^2}x\right)^{q-2} + c\right)^{q-2} - \frac{1}{c}\right)^{q-2} + x,$$

where $c \in \mathbb{F}_q^*$, has the value set $V_F = \{0, -c, -2c\}$.

Proof. The polynomial of this form is obtained in the case $c_0c_1^2 = 1$ in the proof of the previous theorem, and so is the value set $V_F = \{0, -c, -2c\}$. □

3.2.2 $v(\mathcal{F}_{q,4}^{(2)})$

Next we study the spectrum of the class of polynomials $\mathcal{F}_{q,4}^{(2)}$. First we collect some general properties of polynomials in this class which will be used in the proof of the main theorems of this section.

Let $F(x) \in \mathcal{F}_{q,4}^{(2)}$. Then $\alpha_4 = 0$, which means that $c_3(c_2c_1+1) + c_1 = 0$. Therefore

$$c_3 = -\frac{c_1}{c_2c_1+1}.$$

So $F(x)$ is of the form

$$F(x) = \left(\left((c_0x)^{(q-2)} + c_1\right)^{(q-2)} + c_2\right)^{(q-2)} - \frac{c_1}{c_2c_1+1}\Bigg)^{q-2} + x,$$

where $c_0, c_1, c_2 \in \mathbb{F}_q^*$. Here the corresponding rational function is

$$\mathcal{R}_n(x) = \left(\frac{\alpha_3}{\beta_4} + 1\right)x + \frac{\beta_3}{\beta_4} = \Big(c_0(c_2c_1+1)^2 + 1\Big)x + c_2(c_2c_1+1), \tag{3.2}$$

since $\alpha_3 = c_0(c_2c_1+1)$, $\beta_3 = c_2$ and

$$\beta_4 = c_3c_2 + 1 = \frac{1}{c_2c_1+1}.$$

Therefore the poles are

$$x_1 = 0, x_2 = -\frac{1}{c_0c_1}, \quad \text{and} \quad x_3 = -\frac{c_2}{c_0(c_2c_1+1)}. \tag{3.3}$$

By Lemmas 2.9 and 2.21, we have

$$F(x_1) = 0, \quad F(x_2) = c_2(c_2c_1+1) + x_2, \tag{3.4}$$

$$F(x_3) = \frac{1}{c_3} + x_3 = -\frac{c_2c_1+1}{c_1} + x_3. \tag{3.5}$$

Theorem 3.7. *If $F(x) \in \mathcal{F}_{q,4}^{(2)}$ is of the form $F(x) = f(x) + x$, where $f(x) = P_4(c_0, c_1, c_2, c_3; x)$, with $c_0 = -1/(c_2c_1+1)^2$, then*

$$|V_F| = \begin{cases} 2 & \textit{if} \quad c_1c_2 \in \{-2, -1/2, 1\} \quad \textit{and } \mathrm{char}(\mathbb{F}_q) = 3, \\ 3 & \textit{if} \quad c_1c_2 \in \{-2, -1/2, 1\} \quad \textit{and } \mathrm{char}(\mathbb{F}_q) \neq 3, \\ 4 & \textit{otherwise.} \end{cases}$$

Proof. Since

$$c_0 = -\frac{1}{(c_2c_1+1)^2},$$

it follows that $\mathcal{R}_n(x)$ is constant: $\mathcal{R}_n(x) = c_2(c_2c_1+1)$. Then for $y \in \mathbb{F}_q \setminus \mathbf{O}_n$ we get

$$F(y) = \mathcal{R}_n(y) = c_2(c_2c_1+1),$$

whereas for the poles we have

$$F(x_2) = \mathcal{R}_n(x_1) - x_1 + x_2 = c_2(c_2c_1+1) + \frac{(c_2c_1+1)^2}{c_1} = \frac{(c_2c_1+1)(2c_2c_1+1)}{c_1},$$

and

$$F(x_3) = \mathcal{R}_n(x_2) - x_2 + x_3 = \frac{c_1^2c_2^2 - 1}{c_1},$$

where

$$x_2 = \frac{(c_1c_2+1)^2}{c_1}, \quad x_3 = c_2(c_1c_2+1).$$

One easily verifies that $F(y)$ can not coincide with $F(x_1), F(x_2)$ and $F(x_3)$ since c_2c_1+1 can not be equal to zero.

If $c_1c_2 = -1/2$, then we have $F(x_1) = F(x_2) = 0$, $F(x_3) = 3c_2/2$, where $x_1 = 0$, $x_2 = -c_2/2$, $x_3 = c_2/2$ and $F(y) = c_2/2$ for $y \in \mathbb{F}_q \setminus \{x_1, x_2, x_3\}$. Therefore, $V_F = \{0, c_2/2, 3c_2/2\}$, which has size three for $\mathrm{char}(\mathbb{F}_q) \neq 3$.

If $c_1c_2 = 1$, then we have $F(x_1) = F(x_3) = 0$, $F(x_2) = 6c_2$, where $x_1 = 0$, $x_2 = 4c_2$, $x_3 = 2c_2$ and $F(y) = 2c_2$, for $y \in \mathbb{F}_q \setminus \{x_1, x_2, x_3\}$. Therefore, $V_F = \{0, 2c_2, 6c_2\}$, which has size three for $\mathrm{char}(\mathbb{F}_q) \neq 3$.

If $c_1c_2 = -2$, then we have $F(x_1) = 0$, $F(x_2) = F(x_3) = -3c_2/2$, where $x_1 = 0$, $x_2 = c_2/2$, $x_3 = -c_2$ and $F(y) = -c_2$ for $y \in \mathbb{F}_q \setminus \{x_1, x_2, x_3\}$. Therefore, $V_F = \{0, -c_2, -3c_2/2\}$, which has size three for $\mathrm{char}(\mathbb{F}_q) \neq 3$.

If $c_1c_2 \notin \{-2, -1/2, 1\}$ then the values of $F(x_1)$, $F(x_2)$, $F(x_3)$ are pairwise distinct and different from $F(y)$ for $y \in \mathbb{F}_q \setminus \{x_1, x_2, x_3\}$, and we have

$$V_F = \{0, \frac{(c_2c_1+1)(2c_2c_1+1)}{c_1}, \frac{c_1^2c_2^2-1}{c_1}, c_2(c_2c_1+1)\},$$

which has cardinality four. □

Theorem 3.8. *If $F(x) \in \mathcal{F}_{q,4}^{(2)}$ is of the form $F(x) = f(x) + x$, where $f(x) = P_4(c_0, c_1, c_2, c_3; x)$, with $c_0 \neq -1/(c_2c_1+1)^2$, then $|V_F| \in \{q-3, q-2, q\}$.*

Proof. Since

$$c_0 \neq -\frac{1}{(c_2c_1+1)^2}$$

the rational function $\mathcal{R}_n(x)$ is a linear function. Observe that $F(x_1) = 0 = \mathcal{R}_n(y)$ if $y = \gamma_1(c_0, c_1, c_2)$, where

$$\gamma_1(c_0, c_1, c_2) = -\frac{c_2(c_2c_1+1)}{c_0(c_2c_1+1)^2+1} \tag{3.6}$$

and $\gamma_1(c_0, c_1, c_2) \neq x_1$ since $c_2c_1 + 1$ can not be zero. If $\gamma_1(c_0, c_1, c_2) = x_3$, then

$$-\frac{c_2(c_2c_1+1)}{c_0(c_2c_1+1)^2+1} = -\frac{c_2}{c_0(c_2c_1+1)},$$

and hence

$$c_0(c_2c_1+1)^2 = c_0(c_2c_1+1)^2 + 1,$$

which gives a contradiction. If $\gamma_1(c_0, c_1, c_2) = x_2$, then

$$-\frac{c_2(c_2c_1+1)}{c_0(c_2c_1+1)^2+1} = -\frac{1}{c_0c_1},$$

or equivalently

$$c_0c_2c_1(c_2c_1+1) = c_0(c_2^2c_1^2+2c_2c_1+1)+1,$$

which implies $c_0(c_2c_1+1)+1=0$. Therefore, if $c_0=\delta_1(c_1,c_2)$, where

$$\delta_1(c_1,c_2) = -\frac{1}{c_2c_1+1}, \tag{3.7}$$

then $\gamma_1(c_0,c_1,c_2)=x_2$ in which case there exists no element $y\in\mathbb{F}_q^*\setminus\{x_2,x_3\}$ such that $F(x_1)=F(y)=0$.

Now suppose $F(x_2)=\mathcal{R}_n(y)$. Then we have $y=\gamma_2(c_0,c_1,c_2)$, where

$$\gamma_2(c_0,c_1,c_2) = -\frac{1}{c_0c_1(c_0(c_2c_1+1)^2+1)}. \tag{3.8}$$

It clear that $\gamma_2(c_0,c_1,c_2)\neq x_1$. If $\gamma_2(c_0,c_1,c_2)=x_2$, then we have

$$-\frac{1}{c_0^2c_1(c_2c_1+1)+c_0c_1} \;=\; -\frac{1}{c_0c_1},$$

which gives a contradiction since $c_0(c_2c_1+1)\neq 0$. The condition $\gamma_2(c_0,c_1,c_2)=x_3$ is satisfied for $c_0=\delta_2(c_1,c_2)$, where

$$\delta_2(c_1,c_2) = \frac{1}{c_1c_2(c_2c_1+1)^2}. \tag{3.9}$$

Finally if $F(x_3)=\mathcal{R}_n(y)$, then we have

$$\Big(c_0(c_2c_1+1)^2+1\Big)y + c_2(c_2c_1+1) = -\frac{c_2c_1+1}{c_1} - \frac{c_2}{c_0(c_2c_1+1)}$$

and hence $y=\gamma_3(c_0,c_1,c_2)$, where

$$\gamma_3(c_0,c_1,c_2) = -\frac{c_0(c_2c_1+1)^3+c_2c_1}{c_0c_1(c_2c_1+1)(c_0(c_2c_1+1)^2+1)}. \tag{3.10}$$

We have $\gamma_3(c_0,c_1,c_2)=x_1$ for $c_0=\delta_3(c_1,c_2)$, where

$$\delta_3(c_1,c_2) = -\frac{c_1c_2}{(c_2c_1+1)^3}, \tag{3.11}$$

whereas straightforward calculations show that the conditions $\gamma_3(c_0,c_1,c_2)=x_2$ and $\gamma_3(c_0,c_1,c_2)=x_3$ both lead to the same contradiction $0=1$. It follows that for each $i\in\{1,2,3\}$,

(i) $\mathcal{R}_n(\gamma_i(c_0,c_1,c_2)) = F(x_i)$,

(ii) $\gamma_i(c_0,c_1,c_2)\in\{x_1,x_2,x_3\}$ if and only if $c_0=\delta_i(c_1,c_2)$, and

(iii) $\gamma_i(\delta_i(c_1,c_2),c_1,c_2) = x_{i+1}$, where the indices $i = 1,2,3$ should be calculated modulo 3.

(iv) there exists an element $y \in \mathbb{F}_q^* \setminus \mathbf{O}_n$ such that $F(x_i) = F(y)$ if and only if $c_0 \neq \delta_i(c_1,c_2)$.

Moreover, we see that $\delta_1(c_1,c_2) = \delta_2(c_1,c_2)$, if and only if $-(c_1c_2)^2 = (c_1c_2+1)$, which can only happen when -3 is a square in $\mathbb{F}_q$, i.e., for $q = 3^h$ or $q \equiv 1 \mod 3$. Exactly the same condition is valid for $\delta_2(c_1,c_2) = \delta_3(c_1,c_2)$, and $\delta_1(c_1,c_2) = \delta_3(c_1,c_2)$. In this case for each $i = 1,2,3$, it follows from property (iv) there is no $y \in \mathbb{F}_q \setminus \mathbf{O}_n$ for which $F(y) = F(x_i)$. Therefore we obtain $|V_F| = q$. If $c_0 = \delta_1(c_1,c_2)$, then $F(x_1) \neq F(x_2)$, $F(x_1) \neq F(x_3)$. Also $F(x_2) = F(x_3)$ if and only if $(c_1c_2+1)^2 = -1$ which can only occur when $q \equiv 1 \mod 4$. Suppose this holds, i.e. $F(x_2) = F(x_3)$. Then $-(c_1c_2)^2 \neq (c_1c_2+1)$, and hence $\delta_i(c_1,c_2) \neq \delta_j(c_1,c_2)$ for each $i \neq j$. Also $\gamma_2(\delta_1(c_1,c_2),c_1,c_2) = \gamma_3(\delta_1(c_1,c_2),c_1,c_2)$, and it follows from properties (i)-(iv) that $|V_F| = q-2$. If $F(x_2) \neq F(x_3)$, i.e. $(c_1c_2+1)^2 \neq -1$ and $-(c_1c_2)^2 \neq (c_1c_2+1)$, then

$$\gamma_2(\delta_1(c_1,c_2),c_1,c_2), \gamma_3(\delta_1(c_1,c_2),c_1,c_2) \in \mathbb{F}_q \setminus \mathbf{O}_n,$$

and again applying the above properties, this time we obtain $|V_F| = q-2$. The same argument holds for the other two case $c_0 = \delta_i(c_1,c_2)$, $i = 2,3$. If on the other hand $c_0 \notin \{\delta_i(c_1,c_2) : i = 1,2,3\}$, then

$$\gamma_i(c_0,c_1,c_2) \in \mathbb{F}_q \setminus \mathbf{O}_n, \quad \text{for all } i = 1,2,3,$$

in which case $|V_F| = q-3$. □

Examining the different cases in the proof of the above theorems, we can determine the spectrum of the class of polynomials $\mathcal{F}_{q,4}^{(2)}$.

Corollary 3.9. *The spectrum of the family $\mathcal{F}_{q,4}^{(2)}$ is*

$$v(\mathcal{F}_{q,4}^{(2)}) = \begin{cases} \{2,4,q-3,q-2,q\} & \text{if } \mathrm{char}(\mathbb{F}_q) = 3, \\ \{3,4,q-3,q-2,q\} & \text{if } \mathrm{char}(\mathbb{F}_q) \neq 3 \text{ and } q \equiv 1 \mod 3, \\ \{3,4,q-3,q-2\} & \text{otherwise.} \end{cases}$$

Theorem 3.10. *Any polynomial* $F \in \mathcal{F}_{q,4}^{(2)}$ *of the form*

$$F(x) = \left(\left(\left((-\frac{1}{(c_2c_1+1)^2}x)^{q-2} + c_1 \right)^{q-2} + c_2 \right)^{q-2} - \frac{c_1}{c_2c_1+1} \right)^{q-2} + x$$

where $c_1, c_2 \in \mathbb{F}_q^*$ *with* $c_1c_2 \notin \{-2, -1/2, 1\}$*, has value set*

$$V_F = \left\{ 0, \frac{(c_1c_2+1)(2c_1c_2+1)}{c_1}, -\frac{c_1c_2+1}{c_1}, c_2(c_2c_1+1) \right\},$$

and $|V_F| = 4$*.*

Proof. It follows from the proof of Theorem 3.7 that if $c_1c_2 \notin \{-2, -1/2, 1\}$ then we have that $F(x_i) \neq F(x_j)$ for all $i \neq j$. The explicit value set follows from the end of the proof Theorem 3.7. □

Theorem 3.11. *If* $\mathrm{char}(\mathbb{F}_q) \neq 3$ *and* $q \not\equiv 1 \mod 3$ *then any polynomial* $F \in \mathcal{F}_{q,4}^{(2)}$ *of the form*

$$F(x) = \left(\left(\left(\left(\frac{-x}{c_2c_1+1} \right)^{q-2} + c_1 \right)^{q-2} + c_2 \right)^{q-2} - \frac{c_1}{c_2c_1+1} \right)^{q-2} + x$$

where $c_1, c_2 \in \mathbb{F}_q^*$*, has* $|V_F| = q-2$*.*

Proof. The polynomial $F(x)$ is of the form $f(x) + x$ where $f(x) = P_4(c_0, c_1, c_2, c_3; x)$ with

$$c_0 = \frac{-1}{c_2c_1+1}.$$

Note that this equals $\delta_1(c_1, c_2)$ as defined in (3.7). It follows from the proof of Theorem 3.8 that $|V_F| \in \{q-2, q\}$.

The condition $\mathrm{char}(\mathbb{F}_q) \neq 3$ and $q \not\equiv 1 \mod 3$ implies that $\delta_i(c_1, c_2) \neq \delta_j(c_1, c_2)$ for $i \neq j$, where δ_i is as defined in (3.7), (3.9), (3.11). This implies that

$$\gamma_2(c_0, c_1, c_2), \gamma_3(c_0, c_1, c_2) \in \mathbb{F}_q \setminus \mathbf{O}_n,$$

and hence $|V_F| = q-2$. □

Theorem 3.12. *If* $F(x) \in \mathcal{F}_{q,4}^{(2)}$ *is of the form* $F(x) = f(x) + x$*, where* $f(x) = P_4(c_0, c_1, c_2, c_3; x)$*, with* $c_1, c_2 \in \mathbb{F}_q^*$ *arbitrary and*

$$c_0 \notin \left\{ -\frac{1}{c_2c_1+1}, \frac{1}{c_1c_2(c_2c_1+1)^2}, -\frac{c_1c_2}{(c_2c_1+1)^3} \right\}$$

then $|V_F| = q-3$*.*

Proof. The proof easily follows from the proof of Theorem 3.8; the excluded values for c_0 are the values $\delta_i(c_1, c_2)$, $i = 1, 2, 3$ as defined in (3.7), (3.9), (3.11). □

3.2.3 $v(\mathcal{F}_{q,n}^{(2)})$

Theorem 3.13. *If $F \in \mathcal{F}_{q,n}^{(2)}$ with n distinct poles, then*

$$|V_F| \in \{2, 3, 4, 5, \ldots, n, q-n+1, q-n+2, \ldots, q-2, q\}.$$

Proof. Let $F \in \mathcal{F}_{q,n}^{(2)}$ with n distinct poles. Then there are $n-1$ poles which lie in $\mathbb{F}_q$ and $q-n+1$ elements in $\mathbb{F}_q \setminus \mathbf{O}_n$. If $\alpha_{n-1} = -\beta_n$ then we have the following

$$F(x_1) = 0, \quad F(y) = x_{n-1} \neq 0 \ \text{ for every } \ y \in \mathbb{F}_q \setminus \mathbf{O}_n.$$

In the pole part, the number of different images lies between 2 and $n-1$. Since there is a fixed value for the non-poles, we have $2 \leq |V_F| \leq n$.

Now let $\alpha_{n-1} \neq -\beta_n$. Then the restriction of the function defined by F to the non-pole elements is represented by a linear polynomial. Hence there are $q-n+1$ distinct values for the non-poles. The image of a pole might coincide with the image of another pole or with the image of a non-pole, so as a minimum we have the same number $q-n+1$. But when some images of poles are not contained in the set of images of non-poles, then $|V_F|$ may take the values $q-n+1, q-n+2, \ldots, q-2$.

Assume that $|V_F|$ has size $q-1$. This means that there $q-2$ distinct elements appear once, 1 element b_1 appears twice and one element b_0 does not appear. Now consider the sum of the values of images of F, i.e.

$$\sum_{c=0}^{q-1} F(c) = \sum_{c=0}^{q-1} \Big(f(c) + c \Big) = \sum_{c=0}^{q-1} f(c) + \sum_{c=0}^{q-1} c.$$

Since $f(x)$ and x are permutation polynomials, i.e.,

$$\sum_{c=0}^{q-1} f(c) \equiv 0 \pmod{q} \quad \text{and} \quad \sum_{c=0}^{q-1} c \equiv 0 \pmod{q},$$

and

$$\sum_{c=0}^{q-1} F(c) = b_1 + \sum_{c \in \mathbb{F}_q \setminus \{b_0\}} c = b_1 - b_0$$

which gives a contradiction. Hence the value set of F can not contain exactly $q-1$ values. The case where q is attained is studied in the 2nd Chapter, Section 2.3. □

Remark 3.14. The theorem above shows that there is a gap in the spectrum of $\mathcal{F}_{q,n}^{(2)}$ between n and $q-n+1$. Note that this gap is large if q is large with respect to n. The

second gap, between permutation and non permutation polynomials, between $q-2$ and q, is independent of n for any choice of q. Moreover, as we have seen for $n=3$ and $n=4$, this gap can in general not be enlarged.

In the following section we study the permutation polynomials $f(x)$ for which $F(x)=f(x)+x$ attains the minimum cardinality of value set where $F \in \mathcal{F}_{q,n}^{(2)}$.

3.3 Minimal Value Polynomials in $\mathcal{F}_{q,n}^{(2)}$

In this section we are interested in the construction of minimal value set polynomials in the class $\mathcal{F}_{q,n}^{(2)}$, $n \geq 3$. This means that we are studying polynomials $F(x)=f(x)+x$, with $|V_F| \in \{2,3\}$, where

$$f(x) = P_n(c_0, ..., c_{n-1}; x) \in \mathcal{P}_{q,n}^{(2)},$$

and $f(x)$ has set of poles $\mathbf{O}_n$ with the first $n-1$ poles $x_1 = 0, x_2, \ldots, x_{n-1} \in \mathbb{F}_q$ and the last pole $x_n = \infty$. With the α_i's and β_i's defined as in (2.2), this implies that $\alpha_n = 0$. Then $f(x)$ has associated rational fraction

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

and similarly for $F(x)$ we have the rational function

$$\mathcal{R}_n(x) = \left(\frac{\alpha_{n-1}}{\beta_n} + 1\right)x + \frac{\beta_{n-1}}{\beta_n}. \tag{3.12}$$

We also recall that if $|\mathbf{O_n}| = n$ then $F(x_1) = 0$, see Lemma 2.21. We start with the following easy lemma.

Lemma 3.15. *If $F(x) \in \mathcal{P}_{q,n}^{(2)}$ has n distinct poles and $\alpha_{n-1} = -\beta_n$, then $F(c) = x_{n-1}$ is constant for each $c \in \mathbb{F}_q \setminus \mathbf{O}_n$.*

Proof. By the assumption and by (2.8), we have

$$F(c) = \mathcal{R}_n(c) = \frac{\beta_{n-1}}{\beta_n} = -\frac{\beta_{n-1}}{\alpha_{n-1}},$$

and hence $F(c) = x_{n-1}$, by definition of the poles. □

Lemma 3.16. *If the poles $x_1, x_2, ..., x_{n-1}$ in $\mathbb{F}_q$ are distinct and $\alpha_{n-1} = -\beta_n$, then*

$$F(x_i) = x_{n-1} - x_{i-1} + x_i \quad \textit{for } 2 \leq i \leq n-1.$$

Proof. This immediately follows from (2.10, and

$$\mathcal{R}_n(x) = \left(\frac{\alpha_{n-1}}{\beta_n} + 1\right) x + \frac{\beta_{n-1}}{\beta_n} = \frac{\beta_{n-1}}{\beta_n} = -\frac{\beta_{n-1}}{\alpha_{n-1}} = x_{n-1},$$

that

$$F(x_i) = x_{n-1} - x_{i-1} + x_i \quad \text{for } 2 \leq i \leq n-1.$$

□

Lemma 3.17. *If $|\mathbf{O}_n| = n$ and $\alpha_{n-1} = -\beta_n$, then the following statements are equivalent:*

(i) $x_i = (1-i)x_{n-1}$ for all $1 \leq i \leq n-2$;

(ii) $F(x_i) = 0$ for all $1 \leq i \leq n-2$.

Proof. By Lemma 3.16, we have

$$F(x_i) = x_{n-1} - x_{i-1} + x_i \quad \text{for } 2 \leq i \leq n-1.$$

Therefore if $x_i = (1-i)x_{n-1}$ for all $1 \leq i \leq n-2$, then for any $j \in \{2, \ldots, n-2\}$ we obtain

$$F(x_j) = x_{n-1} - (2-j)x_{n-1} + (1-j)x_{n-1} = 0.$$

Since also $F(x_1) = 0$, property (ii) of the lemma follows.

Conversely if $F(x_i) = 0$ for all $1 \leq i \leq n-2$, then $x_i = x_{i-1} - x_{n-1}$ for all $1 \leq i \leq n-2$, and hence for each $j \in \{1, \ldots, n-2\}$ it follows that

$$x_j = x_{j-1} - x_{n-1} = x_{j-2} - 2x_{n-1} = \ldots = x_1 - (j-1)x_{n-1} = (1-j)x_{n-1},$$

which completes the proof. □

Remark 3.18. We note that the requirement $|\mathbf{O}_n| = n$ and any of the two equivalent conditions from the above lemma imply that $n-3 < \mathrm{char}(\mathbb{F}_q)$. The same holds for the conditions in Theorem 3.20.

Lemma 3.19. *If $|\mathbf{O}_n| = n$ and $\alpha_{n-1} = -\beta_n$, then $x_{n-2} = (3-n)x_{n-1} \iff F(x_{n-1}) = (n-1)x_{n-1}$.*

Proof. The proof is immediate from Lemma 3.16 □

Theorem 3.20. *Let* $\mathbf{O}_n = \{x_1, \ldots, x_n\}$, *where* $x_1 = 0$, $x_n = \infty$, *and* $|\mathbf{O}_n| = n$. *If* $x_i = (1-i)x_{n-1}$ *for* $1 \leq i \leq n-2$, *then there exists a minimal value set polynomial* $F(x) \in \mathcal{P}^{(2)}_{q,n}$ *with set of poles* $\mathbf{O}_n$.

Proof. Here we use a slight modification of a procedure given in [3], in order to obtain $F(x)$ where $R_n(x)$ and the poles are prescribed.

Consider a polynomial $F(x) \in \mathcal{P}^{(2)}_{q,n}$ with prescribed set of poles $\mathbf{O}_n$ and with associated rational fraction

$$R_n(x) = \frac{ax+b}{-a} = \frac{\epsilon a x + \epsilon b}{-\epsilon a},$$

$\epsilon \neq 0$, and define

$$\alpha_{n-1} = \epsilon a,\ \beta_{n-1} = \epsilon b,\ \beta_n = -\epsilon a.$$

Then we know the exact value for $x_{n-1} = -b/a$ since

$$x_{n-1} = -\frac{\beta_{n-1}}{\alpha_{n-1}}.$$

All the other poles x_i for $1 \leq i \leq n-2$ are obtained by the formula $x_i = (1-i)x_{n-1}$.

Equation (2.23) allow us to recursively calculate the exact values for $c_{n-1}, c_{n-2}, \ldots, c_2$, and values for $\alpha_{n-2}, \beta_{n-2}, \ldots, \alpha_1, \beta_1$ as multiples of ϵ. In the final step c_2, c_1, c_0, and ϵ are calculated as follows. From $\alpha_0 = 0$, $\beta_0 = 1$ and $\alpha_2 = c_1\alpha_1 + \alpha_0$ we have $c_1 = \alpha_2/\alpha_1$. The identity $\beta_2 = c_1\beta_1 + \beta_0 = 1$ then yields the value for ϵ. Then we can find c_2 which is equal to β_3. Finally, we have $c_0 = \alpha_1$. Hence we construct a minimal value polynomial $F \in \mathcal{P}^{(2)}_{q,n}$ with value set

$$V_F = \{0, 0, ..., 0, (n-1)x_{n-1}, x_{n-1}\}.$$

This completes the proof. □

Remark 3.21. We note that if $\mathrm{char}(\mathbb{F}_q)$ divides $n-1$, then for F as in the above theorem we obain $|V_F| = 2$, otherwise $|V_F| = 3$. Now, since the conditions already imply that $\mathrm{char}(\mathbb{F}_q) > n-3$ (see Remark 3.18), the case $|V_F| = 2$ only occurs for $\mathrm{char}(\mathbb{F}_q) = n-1$.

Remark 3.22. Note that the proof of Theorem 3.20 gives a procedure to construct the minimal value set polynomial.

Corollary 3.23. *For all $a, b \in \mathbb{F}_q^*$ and $n \geq 3$ with $\mathrm{char}(\mathbb{F}_q) > n-3$, a polynomial $F(x) \in \mathcal{F}_{q,n}^{(2)}$ can be constructed with value set $V_F = \{0, -b/a, (n-1)(-b/a)\}$.*

Proof. It suffices to define $x_{n-1} = -b/a$, and apply the procedure described in the proof of Theorem 3.20. □

We now illustrate Remark 3.22 with an example.

Example 3.24. Assume that $p = 13$, $n = 5$, $\alpha_5 = 0$ and $\alpha_4 = -\beta_5$. Let

$$R_n(x) = \frac{9\epsilon x + 8\epsilon}{4\epsilon}.$$

As the initial values we have

$$\alpha_4 = 9\epsilon, \quad \beta_4 = 8\epsilon, \quad \beta_5 = 4\epsilon.$$

First one can calculate the last pole $x_4 = -8/9 = 2$. Also it is known that the first pole is always zero. The other poles $x_3 = 9$, $x_2 = 11$ are obtained by the formula $x_i = (1-i)x_{n-1}$ for $i = 2, 3$. Also, we have

$$c_4 = \frac{\beta_5 + x_3\alpha_5}{\beta_4 + x_3\alpha_4} = 11,$$

and hence

$$\alpha_3 = \alpha_5 - c_4\alpha_4 = 5\epsilon, \quad \beta_3 = \beta_5 - c_4\beta_4 = 7\epsilon.$$

We obtain recursively

$$c_3 = \frac{\beta_4 + x_2\alpha_4}{\beta_3 + x_2\alpha_3} = 12, \quad \alpha_2 = \alpha_4 - c_3\alpha_3 = \epsilon, \quad \beta_2 = \beta_4 - c_3\beta_3 = 2\epsilon,$$

Therefore $\epsilon = 7$ since we must have $\beta_2 = 1$. It follows that $c_2 = \beta_3 = 10$. Then

$$\alpha_1 = \alpha_3 - c_2\alpha_2 = -5\epsilon = 4, \quad c_1 = \frac{\alpha_2}{\alpha_1} = 5 \quad \text{and} \quad c_0 = \alpha_1 = 4.$$

Finally we obtain the polynomial $F(x) = f(x) + x$ given by given by

$$F(x) = \Big(\Big(\big(((4x)^{q-2} + 5)^{q-2} + 10\big)^{q-2} + 12\Big)^{q-2} + 11\Big)^{q-2} + x.$$

whose value set has size three since $|V_F| = |V_1| + |V_2| = 2 + 1 = 3$, where $V_1 = \{F(x_i) : x_i \in \mathbf{O}_n\}$ and $V_2 = \{F(c) \ : \ c \in \mathbb{F}_q \setminus \mathbf{O}_n\}$.

Theorem 3.25. *For any $n \geq 3$, $n-3 < \mathrm{char}(\mathbb{F}_q) \neq n-1$, there exists $F \in \mathcal{F}_{q,n}^{(2)}$ s.t. $|V_F| = 3$.*

Proof. Put $\alpha_n = 0$ and $\alpha_{n-1} = -\beta_n$, and consider $\mathcal{R}_n(x) = R_n(x) + x = x_{n-1}$. Put $x_i = (1-i)x_{n-1}$ for $i = 1, ..., n-2$. Now apply Theorem 3.20 to obtain the required polynomial $F \in \mathcal{F}_{q,n}^{(2)}$. □

CHAPTER 4

Examples

We emphasise that with regard to applications, see Remark 1.18, these complete mapping polynomials are easy to implement thanks to their Carlitz rank representation. Moreover, the tables with examples illustrate that these complete mapping polynomials also satisfy the required properties (iii) and (iv), as explained in Remark 1.18.

4.1 Complete mapping polynomials in $\mathcal{P}_{q,n}^{(1)}$

In this section we list some examples of complete mapping polynomials in the class $\mathcal{P}_{q,n}^{(1)}$ which were found by an algorithm based on Theorem 2.20. The computations were done by the use of the computer algebra system MAGMA [5].

Table 4.1. The following table contains examples of complete mapping polynomials $f(x) \in \mathcal{P}_{q,n}^{(1)}$. The first column indicates the prime power q, the second column indicates the integer $n = (q-1)/2$. We only list one example for each value of q.

q	n	$f(x)$
11	5	$5x^8 + 5x^7 + 5x^6 + 4x^4 + 2x^3 + 5x^2 + 9x + 5$
13	6	$10x^{10} + 5x^9 + 5x^8 + 8x^7 + 12x^6 + 7x^5 + 2x^4 + 6x^3 + 4x^2 + 4x + 3$
17	8	$7x^{14} + 13x^{13} + 3x^{12} + 14x^9 + 10x^8 + 5x^7 + x^6 + 6x^5 + 2x^4 + 2x^3$ $+5x^2 + 13x + 3$
19	9	$14x^{16} + 13x^{15} + 5x^{14} + 12x^{13} + 9x^{12} + 11x^{11} + 3x^{10} + 8x^9 + 10x^8$ $+6x^7 + 6x^6 + 6x^5 + 10x^4 + 4x^3 + 18x^2 + 2x + 4$

q	n	$f(x)$
23	11	$14x^{20} + 18x^{19} + 21x^{18} + 4x^{16} + 11x^{15} + 18x^{13} + 21x^{12} + 11x^{11} + 19x^{10}$
		$+5x^9 + 6x^8 + 9x^6 + 4x^5 + 3x^3 + 11x^2 + 3$
25	12	$u^{16}x^{22} + u^9x^{21} + u^9x^{20} + u^{15}x^{19} + u^{16}x^{18} + u^8x^{17} + u^{17}x^{16}$
		$+u^7x^{15} + u^{20}x^{14} + u^{17}x^{13} + u^5x^{12} + u^5x^{11} + 4x^{10} + u^{11}x^9$
		$+u^8x^8 + u^9x^7 + u^8x^5 + u^4x^4 + u^{13}x^3 + u^9x^2 + u^8x + u$
27	13	$ux^{24} + u^{21}x^{23} + ux^{22} + u^{25}x^{21} + u^8x^{20} + u^5x^{19} + u^{23}x^{18}$
		$+u^{20}x^{17} + 2x^{16} + u^{22}x^{15} + u^6x^{14} + 2x^{13} + u^{14}x^{11} + u^2x^{10}$
		$+u^{12}x^9 + u^{20}x^8 + u^9x^7 + u^{10}x^6 + u^{12}x^5 + u^2x^4 + 2x^3$
		$+u^7x^2 + u^{25}x + u^2$
29	14	$15x^{26} + 26x^{23} + 25x^{22} + 13x^{21} + 6x^{20} + 5x^{19} + 9x^{18} + 24x^{17} + 19x^{16}$
		$+16x^{15} + 3x^{14} + 7x^{13} + 3x^{12} + 23x^{11} + 15x^{10} + 24x^9 + 25x^8 + 19x^7$
		$+8x^6 + 28x^5 + 9x^4 + 6x^3 + 23x + 4$

4.2 Complete mapping polynomials in $\mathcal{P}_{q,4}^{(2)}$

For $n = 4$ we list examples of complete mapping polynomials in $\mathcal{P}_{q,4}^{(2)}$ for $q \equiv 1 \mod 3$, obtained by Theorem 2.31, i.e.,

$$f(x) = \left(\left(\left(\left(\frac{\alpha^3}{(1+\alpha)^2} x \right)^{q-2} + c \right)^{q-2} + \frac{1}{\alpha c} \right)^{q-2} - \frac{\alpha c}{1+\alpha} \right)^{q-2},$$

where $q \equiv 1 \mod 3$, $\alpha \in \mathbb{F}_q$ is a root of $x^2 + x + 1$ and $c \in \mathbb{F}_q^*$ is arbitrary.

In the Tables 4.2 and 4.3, the first column gives the value of q, the second column gives the values for the root α and the coefficient $c \in \mathbb{F}_q^*$. The last column gives the complete mapping polynomial $f(x) \mod x^q - x$ corresponding to α and c. The examples illustrate that the reduced degree of $f(x)$ is always large compared to q, in fact in the table below, all the examples have reduced degree $q - 3$, the largest possible degree. We note that in the table the coefficient c was randomly picked from the nonzero elements of $\mathbb{F}_q$. From our data for other values of c, it seems that the polynomials do not substantially differ, in terms of degree or weight. For this reason we only listed one complete mapping polynomial for each prime, although different choices for $c \in \mathbb{F}_q^*$ do give different polynomials.

4.3 Complete mapping polynomials in $\mathcal{P}_{q,5}^{(2)}$

For $n = 5$ we list examples of complete mapping polynomials in $\mathcal{P}_{q,5}^{(2)}$ for $q \equiv 1 \mod 4$, obtained by Theorem 2.33, i.e.,

$$f(x) = \left(\left(\left(\left(-\frac{(\alpha+1)^2}{\alpha c^2}x\right)^{q-2} + c\right)^{q-2} + \frac{1}{\alpha c}\right)^{q-2} - \frac{(2\alpha+1)\alpha c}{(\alpha+1)^2}\right)^{q-2} + \frac{(\alpha+1)^2}{\alpha^2 c}\Bigg)^{q-2}$$

where $\alpha \in \mathbb{F}_q$ is a root of $H_5(x) = 2x^2 + 2x + 1$ and $c \in \mathbb{F}_q^*$ is arbitrary.

In the Tables 4.4 and 4.5, the first column gives the value of q, the second column gives the values for the root α and the coefficient $c \in \mathbb{F}_q^*$, and the last column gives the complete mapping polynomial $f(x) \mod x^q - x$ corresponding to α and c. The examples illustrate that the reduced degree of $f(x)$ is always large compared to q, in fact in the table below, all the examples have reduced degree $q - 4$.

4.4 Complete mapping polynomials in $\mathcal{P}_{q,6}^{(2)}$

For $n = 6$ we list examples of complete mapping polynomials in $\mathcal{P}_{q,6}^{(2)}$ for $p = 5$ or $p \equiv \pm 1 \mod 10$ and $q = p^s$ where q is a square, obtained by Theorem 2.35 and Corollary 2.36, in case q is not a prime, i.e.,

$$f(x) = P_6\left(\frac{\alpha^5}{(\alpha+1)^4}, c, \frac{1}{c\alpha}, \frac{c}{1+\alpha}, \frac{1}{c\alpha}, -\frac{c\alpha}{1+\alpha}; x\right) \in \mathcal{P}_{q,6}^{(2)}$$

where $\alpha \in \mathbb{F}_q$ is a root of $H_6(x) = x^4 + 2x^3 + 4x^2 + 3x + 1$ and $c \in \mathbb{F}_q^*$ is arbitrary. In the Tables 4.6 and 4.7, the first column gives the value of q, the second column gives the values for the root α and the coefficient $c \in \mathbb{F}_q^*$, and the last column gives the complete mapping polynomial $f(x) \mod x^q - x$ corresponding to α and c. Again, the examples illustrate that the reduced degree of $f(x)$ is always large compared to q, in fact in the table below, all the examples have reduced degree $q - 5$, except the trivial example for $q = 5$.

Table 4.2. Examples of complete mapping polynomials in the class $\mathcal{P}_{p,4}$ where p is a prime, $p \leq 61$, $p = 3$ or $p \equiv 1 \mod 3$.

p	$[\alpha, c]$	$f(x)$
3	$[1, 1]$	x^1
7	$[2, 3]$	$6x^4 + 4x^3 + x^2$
13	$[3, 3]$	$x^{10} + 2x^9 + 7x^8 + 7x^7 + 9x^6 + x^4 + 2x^3 + 7x^2 + 10x$
19	$[7, 12]$	$18x^{16} + 6x^{15} + 14x^{14} + 15x^{13} + 8x^{12} + 18x^{10} + 6x^9 + 14x^8 + 15x^7$ $+8x^6 + 18x^4 + 6x^3 + 14x^2 + 3x$
31	$[5, 14]$	$2x^{28} + 25x^{27} + 12x^{26} + 13x^{25} + 18x^{24} + 8x^{22} + 7x^{21} + 17x^{20} + 21x^{19}$ $+10x^{18} + x^{16} + 28x^{15} + 6x^{14} + 22x^{13} + 9x^{12} + 4x^{10} + 19x^9 + 24x^8$ $+26x^7 + 5x^6 + 16x^4 + 14x^3 + 3x^2 + 16x$
37	$[10, 27]$	$36x^{34} + 9x^{33} + 20x^{32} + 21x^{31} + 11x^{30} + 36x^{28} + 9x^{27} + 20x^{26} + 21x^{25}$ $+11x^{24} + 36x^{22} + 9x^{21} + 20x^{20} + 21x^{19} + 11x^{18} + 36x^{16} + 9x^{15} + 20x^{14}$ $+21x^{13} + 11x^{12} + 36x^{10} + 9x^9 + 20x^8 + 21x^7 + 11x^6 + 36x^4 + 9x^3$ $+20x^2 + 31x$
43	$[6, 27]$	$39x^{40} + 29x^{39} + 39x^{38} + 36x^{37} + 42x^{36} + 22x^{34} + 34x^{33} + 22x^{32} + 17x^{31}$ $+27x^{30} + 8x^{28} + 28x^{27} + 8x^{26} + 14x^{25} + 2x^{24} + 42x^{22} + 18x^{21} + 42x^{20}$ $+9x^{19} + 32x^{18} + 27x^{16} + 30x^{15} + 27x^{14} + 15x^{13} + 39x^{12} + 2x^{10} + 7x^9$ $+2x^8 + 25x^7 + 22x^6 + 32x^4 + 26x^3 + 32x^2 + 19x$
61	$[13, 16]$	$34x^{58} + 57x^{57} + 35x^{56} + 41x^{55} + 57x^{54} + 20x^{52} + 12x^{51} + 17x^{50} + 60x^{49}$ $+12x^{48} + x^{46} + 25x^{45} + 10x^{44} + 3x^{43} + 25x^{42} + 58x^{40} + 47x^{39} + 31x^{38}$ $+52x^{37} + 47x^{36} + 9x^{34} + 42x^{33} + 29x^{32} + 27x^{31} + 42x^{30} + 34x^{28} + 57x^{27}$ $+35x^{26} + 41x^{25} + 57x^{24} + 20x^{22} + 12x^{21} + 17x^{20} + 60x^{19} + 12x^{18} + x^{16}$ $+25x^{15} + 10x^{14} + 3x^{13} + 25x^{12} + 58x^{10} + 47x^9 + 31x^8 + 52x^7 + 47x^6$ $+9x^4 + 42x^3 + 29x^2 + 40x$

Table 4.3. Examples of complete mapping polynomials in the class $\mathcal{P}_{q,4}$ where q is a prime power, and q is not a prime, $q \leq 121$, $q = 3^s$ or $q \equiv 1 \mod 3$.

q	$[\alpha, c]$	$f(x)$
9	$[1, u^7]$	$u^3x^6 + u^5x^4 + u^7x^2 + 1x$
25	$[u^8, u^{10}]$	$3x^{22} + u^{23}x^{21} + u^{16}x^{20} + u^{15}x^{19} + u^2x^{18} + 2x^{16} + u^{11}x^{15} + u^4x^{14} + u^3x^{13}$ $+u^{14}x^{12} + 3x^{10} + u^{23}x^9 + u^{16}x^8 + u^{15}x^7 + u^2x^6 + 2x^4 + u^{11}x^3 + u^4x^2$ $+u^{17}x$
27	$[1, u^2]$	$u^{20}x^{24} + u^{16}x^{22} + u^{12}x^{20} + u^8x^{18} + u^4x^{16} + x^{14} + u^{22}x^{12} + u^{18}x^{10}$ $+u^{14}x^8 + u^{10}x^6 + u^6x^4 + u^2x^2 + 1x$
49	$[2, u^{31}]$	$u^3x^{46} + u^{36}x^{45} + u^{29}x^{44} + u^{46}x^{43} + u^{23}x^{42} + u^9x^{40} + u^{42}x^{39} + u^{35}x^{38}$ $+u^4x^{37} + u^{29}x^{36} + u^{15}x^{34} + x^{33} + u^{41}x^{32} + u^{10}x^{31} + u^{35}x^{30} + u^{21}x^{28}$ $+u^6x^{27} + u^{47}x^{26} + 2x^{25} + u^{41}x^{24} + u^{27}x^{22} + u^{12}x^{21} + u^5x^{20} + u^{22}x^{19}$ $+u^{47}x^{18} + u^{33}x^{16} + u^{18}x^{15} + u^{11}x^{14} + u^{28}x^{13} + u^5x^{12} + u^{39}x^{10} + 6x^9$ $+u^{17}x^8 + u^{34}x^7 + u^{11}x^6 + u^{45}x^4 + u^{30}x^3 + u^{23}x^2$
81	$[1, u^{56}]$	$u^{72}x^{78} + 2x^{76} + u^8x^{74} + u^{56}x^{72} + u^{24}x^{70} + u^{72}x^{68} + 2x^{66} + u^8x^{64} + u^{56}x^{62}$ $+u^{24}x^{60} + u^{72}x^{58} + 2x^{56} + u^8x^{54} + u^{56}x^{52} + u^{24}x^{50} + u^{72}x^{48} + 2x^{46}$ $+u^8x^{44} + u^{56}x^{42} + u^{24}x^{40} + u^{72}x^{38} + 2x^{36} + u^8x^{34} + u^{56}x^{32} + u^{24}x^{30}$ $+u^{72}x^{28} + 2x^{26} + u^8x^{24} + u^{56}x^{22} + u^{24}x^{20} + u^{72}x^{18} + 2x^{16} + u^8x^{14} + u^{56}x^{12}$ $+u^{24}x^{10} + u^{72}x^8 + 2x^6 + u^8x^4 + u^{56}x^2 + 1x$
121	$[u^{40}, 7]$	$6x^{118} + u^{102}x^{117} + 2x^{116} + u^{114}x^{115} + 2x^{114} + 7x^{112} + u^{78}x^{111} + 6x^{110} + u^{90}x^{109}$ $+6x^{108} + 10x^{106} + u^{54}x^{105} + 7x^{104} + u^{66}x^{103} + 7x^{102} + 8x^{100} + u^{30}x^{99} + 10x^{98}$ $+u^{42}x^{97} + 10x^{96} + 2x^{94} + u^6x^{93} + 8x^{92} + u^{18}x^{91} + 8x^{90} + 6x^{88} + u^{102}x^{87}$ $+2x^{86} + u^{114}x^{85} + 2x^{84} + 7x^{82} + u^{78}x^{81} + 6x^{80} + u^{90}x^{79} + 6x^{78} + 10x^{76} + u^{54}x^{75}$ $+7x^{74} + u^{66}x^{73} + 7x^{72} + 8x^{70} + u^{30}x^{69} + 10x^{68} + u^{42}x^{67} + 10x^{66} + 2x^{64} + u^6x^{63}$ $+8x^{62} + u^{18}x^{61} + 8x^{60} + 6x^{58} + u^{102}x^{57} + 2x^{56} + u^{114}x^{55} + 2x^{54} + 7x^{52} + u^{78}x^{51}$ $+6x^{50} + u^{90}x^{49} + 6x^{48} + 10x^{46} + u^{54}x^{45} + 7x^{44} + u^{66}x^{43} + 7x^{42} + 8x^{40} + u^{30}x^{39}$ $+10x^{38} + u^{42}x^{37} + 10x^{36} + 2x^{34} + u^6x^{33} + 8x^{32} + u^{18}x^{31} + 8x^{30} + 6x^{28} + u^{102}x^{27}$ $+2x^{26} + u^{114}x^{25} + 2x^{24} + 7x^{22} + u^{78}x^{21} + 6x^{20} + u^{90}x^{19} + 6x^{18} + 10x^{16} + u^{54}x^{15}$ $+7x^{14} + u^{66}x^{13} + 7x^{12} + 8x^{10} + u^{30}x^9 + 10x^8 + u^{42}x^7 + 10x^6 + 2x^4 + u^6x^3$ $+8x^2 + u^{37}x$

Table 4.4. Examples of complete mapping polynomials in the class $\mathcal{P}_{p,5}$ where p is a prime, $p \leq 61$, $p \equiv 1 \mod 4$.

p	$[\alpha, c]$	$f(x)$
5	$[1, 4]$	$3x^1$
13	$[2, 1]$	$7x^9 + 2x^8 + 5x^7 + 10x^6 + 5x^5 + 6x^4 + 8x^3 + 3x^2 + 3x$
17	$[6, 9]$	$16x^{13} + 15x^{12} + 6x^{11} + 6x^{10} + 2x^9 + 15x^8 + 13x^7 + 13x^6 + 14x^5$ $+15x^4 + 7x^3 + 7x^2$
29	$[8, 4]$	$8x^{25} + 12x^{24} + 4x^{23} + 3x^{22} + 10x^{21} + 26x^{20} + 21x^{19} + 23x^{18} + 20x^{17}$ $+8x^{16} + 7x^{15} + 27x^{14} + 10x^{13} + 27x^{12} + 4x^{11} + 3x^{10} + 22x^9 + 15x^8$ $+27x^7 + 13x^6 + 6x^5 + 18x^4 + 24x^3 + 18x^2 + 19x$
37	$[15, 14]$	$19x^{33} + 28x^{32} + 18x^{31} + 23x^{30} + 32x^{29} + 3x^{28} + 14x^{27} + 22x^{26} + 10x^{25}$ $+36x^{24} + 34x^{23} + 27x^{22} + 21x^{21} + 25x^{20} + 33x^{19} + 36x^{18} + 31x^{17} + 4x^{16}$ $+4x^{15} + x^{14} + 36x^{13} + 11x^{12} + 3x^{11} + 10x^{10} + 34x^9 + 21x^8 + 23x^7$ $+15x^6 + 11x^5 + 30x^4 + 19x^3 + 14x^2 + 6x$
41	$[4, 2]$	$2x^{37} + 16x^{36} + 39x^{35} + 33x^{34} + 4x^{33} + 37x^{32} + 26x^{31} + 22x^{30} + 39x^{29}$ $+x^{28} + 22x^{27} + 6x^{26} + 3x^{25} + 10x^{24} + 36x^{23} + 21x^{22} + 34x^{21} + 18x^{20}$ $+2x^{17} + 16x^{16} + 39x^{15} + 33x^{14} + 4x^{13} + 37x^{12} + 26x^{11} + 22x^{10} + 39x^9$ $+x^8 + 22x^7 + 6x^6 + 3x^5 + 10x^4 + 36x^3 + 21x^2 + 38x$
53	$[11, 38]$	$19x^{49} + 26x^{48} + 32x^{47} + 47x^{46} + 3x^{45} + 26x^{44} + 24x^{43} + 22x^{42} + 7x^{41}$ $+26x^{40} + 26x^{39} + 15x^{38} + 6x^{37} + 26x^{36} + 52x^{35} + 30x^{34} + 46x^{33} + 26x^{32}$ $+19x^{31} + 13x^{30} + 36x^{29} + 26x^{28} + 14x^{27} + 4x^{26} + 12x^{25} + 26x^{24} + 2x^{23}$ $+46x^{22} + 18x^{21} + 26x^{20} + 5x^{19} + 9x^{18} + 43x^{17} + 26x^{16} + 44x^{15} + 5x^{14}$ $+50x^{13} + 26x^{12} + 21x^{11} + 6x^{10} + 35x^9 + 26x^8 + 40x^7 + 19x^6 + 52x^5$ $+26x^4 + 22x^3 + 29x^2 + 19x$
61	$[5, 42]$	$2x^{57} + 31x^{56} + 22x^{55} + 18x^{54} + 31x^{53} + 17x^{52} + 12x^{51} + 32x^{50} + 57x^{49}$ $+29x^{48} + 15x^{47} + 40x^{46} + 12x^{45} + 10x^{44} + 38x^{43} + 20x^{42} + 4x^{41} + 35x^{40}$ $+58x^{39} + 53x^{38} + 32x^{37} + 31x^{36} + 17x^{35} + 25x^{34} + 20x^{33} + 17x^{32} + 24x^{31}$ $+3x^{30} + 59x^{29} + 29x^{28} + 35x^{27} + 12x^{26} + 56x^{25} + 10x^{24} + 51x^{23} + 14x^{22}$ $+57x^{21} + 35x^{20} + 39x^{19} + 43x^{18} + 39x^{17} + 31x^{16} + 26x^{15} + 49x^{14} + 52x^{13}$ $+17x^{12} + 39x^{11} + 43x^{10} + 31x^9 + 29x^8 + 60x^7 + 38x^6 + 50x^5 + 10x^4$ $+52x^3 + 37x^2 + 52x$

Table 4.5. Examples of complete mapping polynomials in the class $\mathcal{P}_{q,5}$ where q is a prime power but not a prime, $q \leq 121$, $q \equiv 1 \mod 4$.

q	$[\alpha, c]$	$f(x)$
9	$[u^5, u^2]$	$u^2x^5 + 2x^4 + u^6x^3 + 2x^2 + u^5x$
25	$[1, 2]$	$2x^{21} + x^{20} + 2x^{17} + x^{16} + 2x^{13} + x^{12} + 2x^9 + x^8 + 2x^5 + x^4 + 3x$
49	$[u^{10}, u^{22}]$	$u^{36}x^{45} + u^{42}x^{44} + 5x^{43} + u^{30}x^{42} + u^{28}x^{41} + u^2x^{40} + 6x^{39} + u^{14}x^{38} + u^{44}x^{37}$
		$+u^{10}x^{36} + 2x^{35} + u^6x^{34} + u^{20}x^{33} + u^{18}x^{32} + 4x^{31} + u^{22}x^{30} + u^{26}x^{28} + 3x^{27}$
		$+u^{46}x^{26} + u^4x^{25} + u^{34}x^{24} + u^{36}x^{21} + u^{42}x^{20} + 5x^{19} + u^{30}x^{18} + u^{28}x^{17}$
		$+u^2x^{16} + 6x^{15} + u^{14}x^{14} + u^{44}x^{13} + u^{10}x^{12} + 2x^{11} + u^6x^{10} + u^{20}x^9 + u^{18}x^8$
		$+4x^7 + u^{22}x^6 + u^{26}x^4 + 3x^3 + u^{46}x^2 + u^3x$
81	$[u^{50}, u^{11}]$	$u^{64}x^{77} + u^{75}x^{76} + u^6x^{75} + u^{57}x^{74} + u^{39}x^{72} + u^{72}x^{69} + u^3x^{68} + u^{14}x^{67}$
		$+u^{65}x^{66} + u^{47}x^{64} + x^{61} + u^{11}x^{60} + u^{22}x^{59} + u^{73}x^{58} + u^{55}x^{56} + u^8x^{53}$
		$+u^{19}x^{52} + u^{30}x^{51} + ux^{50} + u^{63}x^{48} + u^{16}x^{45} + u^{27}x^{44} + u^{38}x^{43} + u^9x^{42}$
		$+u^{71}x^{40} + u^{24}x^{37} + u^{35}x^{36} + u^{46}x^{35} + u^{17}x^{34} + u^{79}x^{32} + u^{32}x^{29} + u^{43}x^{28}$
		$+u^{54}x^{27} + u^{25}x^{26} + u^7x^{24} + 2x^{21} + u^{51}x^{20} + u^{62}x^{19} + u^{33}x^{18} + u^{15}x^{16}$
		$+u^{48}x^{13} + u^{59}x^{12} + u^{70}x^{11} + u^{41}x^{10} + u^{23}x^8 + u^{56}x^5 + u^{67}x^4 + u^{78}x^3$
		$+u^{49}x^2 + u^{50}x$
121	$[u^9, u^{79}]$	$u^{70}x^{117} + u^{53}x^{116} + 5x^{115} + u^{19}x^{114} + u^2x^{113} + u^{57}x^{112} + u^4x^{111} + u^{95}x^{110}$
		$+u^{102}x^{109} + u^{61}x^{108} + u^{20}x^{107} + u^{111}x^{106} + u^{46}x^{105} + u^{65}x^{104} + 9x^{103} + u^{43}x^{102}$
		$+u^{38}x^{101} + u^{69}x^{100} + u^{52}x^{99} + u^{23}x^{98} + u^{66}x^{97} + u^{73}x^{96} + u^{116}x^{95} + u^{87}x^{94}$
		$+u^{34}x^{93} + u^{77}x^{92} + 6x^{91} + u^{79}x^{90} + u^{81}x^{88} + u^{16}x^{87} + u^{107}x^{86} + u^{18}x^{85}$
		$+u^{85}x^{84} + u^{104}x^{83} + u^{75}x^{82} + u^{94}x^{81} + u^{89}x^{80} + u^{110}x^{77} + u^{93}x^{76} + u^{88}x^{75}$
		$+u^{59}x^{74} + u^{42}x^{73} + u^{97}x^{72} + u^{44}x^{71} + u^{15}x^{70} + u^{22}x^{69} + u^{101}x^{68} + 10x^{67}$
		$+u^{31}x^{66} + u^{86}x^{65} + u^{105}x^{64} + u^{112}x^{63} + u^{83}x^{62} + u^{78}x^{61} + u^{109}x^{60} + u^{92}x^{59}$
		$+u^{63}x^{58} + u^{106}x^{57} + u^{113}x^{56} + 8x^{55} + u^7x^{54} + u^{74}x^{53} + u^{117}x^{52} + u^{28}x^{51}$
		$+u^{119}x^{50} + ux^{48} + u^{56}x^{47} + u^{27}x^{46} + u^{58}x^{45} + u^5x^{44} + 4x^{43} + u^{115}x^{42} + u^{14}x^{41}$
		$+u^9x^{40} + u^{30}x^{37} + u^{13}x^{36} + u^8x^{35} + u^{99}x^{34} + u^{82}x^{33} + u^{17}x^{32} + 7x^{31}$
		$+u^{55}x^{30} + u^{62}x^{29} + u^{21}x^{28} + u^{100}x^{27} + u^{71}x^{26} + u^6x^{25} + u^{25}x^{24} + u^{32}x^{23}$
		$+u^3x^{22} + u^{118}x^{21} + u^{29}x^{20} + 2x^{19} + u^{103}x^{18} + u^{26}x^{17} + u^{33}x^{16} + u^{76}x^{15}$
		$+u^{47}x^{14} + u^{114}x^{13} + u^{37}x^{12} + u^{68}x^{11} + u^{39}x^{10} + u^{41}x^8 + 3x^7 + u^{67}x^6$
		$+u^{98}x^5 + u^{45}x^4 + u^{64}x^3 + u^{35}x^2 + u^{37}x$

Table 4.6. Examples of complete mapping polynomials in the class $\mathcal{P}_{p,6}$ where p is a prime, $p \leq 71$.

p	$[\alpha, c]$	$f(x)$
5	$[2, 1]$	$2x^1$
11	$[1, 7]$	$4x^6 + 2x^5 + 5x^4 + 3x^3 + 5x^2 + 7x$
31	$[6, 16]$	$15x^{26} + 2x^{25} + 20x^{24} + 4x^{23} + 6x^{22} + 18x^{21} + 3x^{20} + 6x^{19} + 20x^{18}$ $+7x^{16} + 20x^{15} + 19x^{14} + 28x^{13} + 11x^{12} + 18x^{11} + 26x^{10} + 25x^9 + 11x^8$ $+9x^6 + 9x^5 + 23x^4 + 30x^3 + 14x^2 + 1x$
41	$[12, 19]$	$35x^{36} + 9x^{35} + 37x^{34} + 11x^{33} + 18x^{32} + 5x^{31} + 14x^{30} + 26x^{29} + 25x^{28}$ $+3x^{26} + 28x^{25} + 4x^{24} + 34x^{23} + 37x^{22} + 5x^{20} + 38x^{19} + 5x^{18} + 4x^{16}$ $+21x^{15} + 14x^{14} + 32x^{13} + 30x^{12} + 4x^{11} + 4x^{10} + 12x^9 + 21x^8 + 36x^6$ $+2x^5 + 6x^4 + 9x^3 + 11x^2 + 21x$
61	$[6, 57]$	$57x^{56} + 52x^{55} + 58x^{54} + 6x^{53} + 42x^{52} + 49x^{51} + 6x^{50} + 6x^{49} + 21x^{48}$ $+35x^{46} + 59x^{45} + 9x^{44} + 52x^{43} + 59x^{42} + 60x^{41} + 5x^{40} + 32x^{39} + 51x^{38}$ $+19x^{36} + 34x^{35} + 29x^{34} + 51x^{33} + 52x^{32} + 24x^{30} + 46x^{29} + 39x^{28} + 18x^{26}$ $+6x^{25} + 49x^{24} + 32x^{23} + 41x^{22} + 14x^{21} + 58x^{20} + 21x^{19} + 43x^{18} + 13x^{16}$ $+44x^{15} + 18x^{14} + 26x^{13} + 60x^{12} + 34x^{11} + 14x^{10} + 17x^9 + 29x^8 + 41x^6$ $+49x^5 + 20x^4 + 16x^3 + 51x^2 + 32x$
71	$[11, 5]$	$59x^{66} + 18x^{65} + 69x^{64} + 44x^{63} + 2x^{62} + 4x^{61} + 35x^{60} + 61x^{59} + 3x^{58}$ $+30x^{56} + 65x^{55} + 15x^{54} + 60x^{53} + 35x^{52} + 40x^{51} + 36x^{50} + 60x^{49} + 53x^{48}$ $+41x^{46} + 24x^{45} + 6x^{44} + 13x^{43} + 49x^{42} + 65x^{41} + 21x^{40} + 49x^{39} + 35x^{38}$ $+18x^{36} + 2x^{35} + 25x^{34} + 24x^{33} + 14x^{32} + 33x^{31} + 63x^{30} + 21x^{29} + 15x^{28}$ $+54x^{26} + 43x^{25} + 59x^{24} + 13x^{23} + 49x^{22} + 19x^{21} + 34x^{20} + 7x^{19} + 5x^{18}$ $+19x^{16} + x^{15} + 8x^{14} + 48x^{13} + 28x^{12} + 6x^{11} + 38x^{10} + 15x^9 + 31x^8$ $+63x^6 + 60x^5 + 31x^4 + 11x^3 + 36x^2 + 57x$

Table 4.7. Examples of complete mapping polynomials in the class $\mathcal{P}_{q,6}$ where q is a prime power but not a prime, $q \leq 121$, $p = 5$ or $p \equiv \pm 1 \mod 10$ and $q = p^s$ where q is a square.

q	$[\alpha, c]$	$f(x)$
25	$[2, u^{20}]$	$u^{20}x^{20} + 4x^{16} + u^4x^{12} + u^{20}x^8 + 4x^4 + 2x$
81	$[u^2, u^{16}]$	$u^{60}x^{76} + u^{19}x^{75} + u^{17}x^{73} + u^{56}x^{72} + u^{15}x^{71} + u^{14}x^{70} + u^{13}x^{69} + u^{12}x^{68}$ $+u^{10}x^{66} + u^9x^{65} + u^{48}x^{64} + u^7x^{63} + u^{46}x^{62} + u^4x^{60} + u^{43}x^{59} + u^{42}x^{58}$ $+x^{56} + u^{78}x^{54} + u^{75}x^{51} + u^{33}x^{49} + u^{32}x^{48} + u^{69}x^{45} + u^{68}x^{44} + u^{67}x^{43}$ $+u^{26}x^{42} + u^{25}x^{41} + u^{64}x^{40} + u^{60}x^{36} + u^{19}x^{35} + u^{17}x^{33} + u^{56}x^{32} + u^{15}x^{31}$ $+u^{14}x^{30} + u^{13}x^{29} + u^{12}x^{28} + u^{10}x^{26} + u^9x^{25} + u^{48}x^{24} + u^7x^{23} + u^{46}x^{22}$ $+u^4x^{20} + u^{43}x^{19} + u^{42}x^{18} + x^{16} + u^{78}x^{14} + u^{75}x^{11} + u^{33}x^9 + u^{32}x^8 + u^{69}x^5$ $+u^{68}x^4 + u^{67}x^3 + u^{26}x^2 + u^{18}x$
121	$[1, u^{26}]$	$u^{74}x^{116} + x^{115} + u^{94}x^{114} + u^{80}x^{113} + u^{90}x^{112} + u^{88}x^{111} + u^{74}x^{110} + u^{54}x^{106}$ $+u^{100}x^{105} + u^{74}x^{104} + 10x^{103} + u^{70}x^{102} + u^{68}x^{101} + u^{54}x^{100} + u^{34}x^{96} + u^{80}x^{95}$ $+u^{54}x^{94} + u^{40}x^{93} + u^{50}x^{92} + 5x^{91} + u^{34}x^{90} + u^{14}x^{86} + 10x^{85} + u^{34}x^{84} + u^{20}x^{83}$ $+u^{30}x^{82} + u^{28}x^{81} + u^{14}x^{80} + u^{114}x^{76} + u^{40}x^{75} + u^{14}x^{74} + x^{73} + u^{10}x^{72}$ $+u^8x^{71} + u^{114}x^{70} + u^{94}x^{66} + u^{20}x^{65} + u^{114}x^{64} + u^{100}x^{63} + u^{110}x^{62} + 6x^{61}$ $+u^{94}x^{60} + u^{74}x^{56} + x^{55} + u^{94}x^{54} + u^{80}x^{53} + u^{90}x^{52} + u^{88}x^{51} + u^{74}x^{50}$ $+u^{54}x^{46} + u^{100}x^{45} + u^{74}x^{44} + 10x^{43} + u^{70}x^{42} + u^{68}x^{41} + u^{54}x^{40} + u^{34}x^{36}$ $+u^{80}x^{35} + u^{54}x^{34} + u^{40}x^{33} + u^{50}x^{32} + 5x^{31} + u^{34}x^{30} + u^{14}x^{26} + 10x^{25} + u^{34}x^{24}$ $+u^{20}x^{23} + u^{30}x^{22} + u^{28}x^{21} + u^{14}x^{20} + u^{114}x^{16} + u^{40}x^{15} + u^{14}x^{14} + x^{13}$ $+u^{10}x^{12} + u^8x^{11} + u^{114}x^{10} + u^{94}x^6 + u^{20}x^5 + u^{114}x^4 + u^{100}x^3 + u^{110}x^2$ $+7x$

Bibliography

[1] A. Akbary, D. Ghioca, Q. Wang, *On permutation polynomials of prescribed shape, Finite Fields and Their Applications*, **15**, (2009), 195-206.

[2] A. Akbary, D. Ghioca, Q. Wang, *On constructing permutations of finite fields, Finite Fields and Their Applications*, **17**, (2011), 51-67.

[3] E. Aksoy, A.Çeşmelioğlu, W. Meidl, A. Topuzoğlu, *On the Carlitz Rank of a permutation polynomial, Finite Fields and Their Applications*, **15**, (2009), 428-440.

[4] A. Biró, *On polynomials over prime fields taking only two values on the multiplicative group, Finite Fields and Their Applications*, **6**, (2000), no.4, 302-308.

[5] W. Bosma, J. Cannon, C. Playoust, *The Magma Algebra System I. the user language, J. Symbolic Computation*, vol. 24, (1997), 235-265.

[6] C. Blondeau, A. Canteaut, P. Charpin, *Differential properties of power functions, Int. J. Information and Coding Theory*, **1**, (2010), 149-170.

[7] C. Blondeau, A. Canteaut, P. Charpin, *Differential properties of* $x \to x^{2^t-1}$, *IEEE Trans. Inform. Theory*, **57**, (2011), 8127-8137.

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

[9] C. Bracken, G. Leander, *A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree*, *Finite Fields and Their Applications*, **16**, (2010), 231-242.

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

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

[12] P. Charpin, G. Kyureghyan, *Cubic monomial bent functions: a subclass of* $\mathcal{M}$*, SIAM J. Discrete Math*, **22**, (2), (2008), 650-665.

[13] P. Charpin, G. Kyureghyan, *When does* $G(x) + \gamma Tr(H(x))$ *permute* $\mathbb{F}_{p^n}$*? Finite Fields and Their Applications*, **15**, (2009), 615-632.

[14] W.-S. Chou, J. Gomez-Galderon, G. L. Mullen, *Value sets of Dickson polynomials over finite fields, J. Number Theory*, **30**, (1988), 334-344.

[15] S. Chowla, H. Zassenhaus, *Some conjectures concerning finite fields*, Norske Vid. Selsk. Forh. (Trondheim), **41**, (1968), 34-35.

[16] S. D. Cohen, *The distribution of polynomials over finite field, Acta Arith.*, **17**, (1970), 255-271.

[17] S. D. Cohen, *Dickson polynomials of the second kind that are permutations, Canad. J. Math.*, **46**, no.2 (1994), 225-238.

[18] S. D. Cohen, *Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials*, *Canad. Math. Bull.*, **33**, (1990), 230-234.

[19] R. S. Coulter, R. W. Matthews, *On the permutation behaviour of Dickson polynomials of the second kind, Finite Fields and Their Applications*, **8**, no. 4 (2002), 519-530.

[20] T. W. Cusick, *Value sets of some polynomials over finite fields* $\mathrm{GF}(2^{2m})$*, SIAM J. Comput.*, **27**, (1998), no.1, 120-131.

[21] T. W. Cusick, *Polynomials over base 2 finite fields with evenly distributed values, Finite Fields and Their Applications*, **11**, (2005), no. 2, 278-291.

[22] T. W. Cusick, P. Müller, *Wan's bound for the value sets of polynomials*, *Finite Fields and Their Applications*, **233**, (1996), 69-72.

[23] A. Çeşmelioğlu, *On the cycle structure of permutation polynomials, Ph.D. thesis, Sabancı University, İstanbul,* (2008).

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

[25] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, *Permutations of finite fields with prescribed properties, J. of Computational and Applied Mathematics*, **259**, (2014), 536-545.

[26] P. Das, G.L. Mullen, *Value sets of polynomials and the Cauchy Davenport theorem, Finite fields with Applications to Coding Theory, Cryptography and Related Areas*, (2002), 80-85.

[27] L. E. Dickson, *The analytic representation of substitutions on a power of a prime letters with a discussion of the linear group, Annals of Mathematics*, **11**, (1896-1897), 65-120, 161-183.

[28] J. Gomez-Calderon, J. D. Madden, *Polynomials with small value set over finite fields, J. of Number Theory*, **28**, (1988), no.2, 167-188.

[29] D. Gomez-Perez, A. Ostafe, A. Topuzoğlu, *On the Carlitz rank of permutations of $\mathbb{F}_q$ and pseudorandom sequences, Journal of Complexity*, **30**, (2014), 279-289.

[30] X. Guangkui, X. Cao, *Complete permutation polynomials over finite fields of odd characteristic, Finite Fields and Their Applications*, **31**, (2015), 228-240.

[31] R. Guralnick, D. Wan, *Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, Israel J. Math.*, **101**, (1997), 255-287.

[32] M. Henderson, *A note on the permutation behaviour of the Dickson polynomials of the second kind, Bull. Austral. Math. Society*, **56**, no.3, (1997), 499-505.

[33] M. Henderson, R. Matthews, *Dickson polynomials of the second kind which are permutation polynomials over a finite field, New Zealand J. Math.*, **27**, no.2 (1998), 227-244.

[34] C. Hermite, *Sur les fonctions de sept lettres, C. R. Acad. Sciences,* **57**, (1863), 750-757; Oevres **2**, Gauthier-Villars, Paris, (1908), 200-208.

[35] X. D. Hou, *Permutation polynomials over finite fields - A survey of recent advances, Finite Fields and Their Applications*, **32**, (2015), 82-119.

[36] R. Lidl, G. L. Mullen, G. Turnwald, *Dickson Polynomials, Pitman Monographs and Surveys in Pure and Applied Mathematics*, **65**, (1993).

[37] R. Lidl, H. Niederreiter, *Finite fields, 2nd Edition, Encyclopedia of Mathematics and its Applications,* **20**, *Cambridge University Press, Cambridge*, ISBN 0521392314, (1997).

[38] H. B. Mann, *The construction of orthogonal Latin squares*, *Annals of Math. Statistics*, **13**, (1942), 418-423.

[39] M. Matsui, *Linear cryptanalysis method for DES cipher,* Advances in Cryptography - Eurocrypt'93, Lect. Notes Computer Science, **765**, (1993), 386-397.

[40] R. Matthews, *Permutation Polynomials in one and several variables, Ph.D. thesis, University of Tasmania, Hobart*, (1982).

[41] K. McCann, K. S. Williams, *The distribution of the residues of a quartic polynomial. Glasgow Math. J.*, **8**, (1967), 67-88.

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

[43] G. L. Mullen, *Permutation Polynomials over Finite Fields, Finite Fields, Coding Theory, and Advances in Communications and Computing*, Marcel Dekker, NY, (1993), 131-151.

[44] G. L. Mullen, H. Niederreiter, *Dickson polynomials over finite fields and complete mappings, Canada Math. Bulletin*, **30**, (1987), 19-27.

[45] G. L. Mullen, D. Panario, *Handbook of finite fields, Discrete Mathematics and its Applications*, ISBN 9781439873786, Chapman and Hall / CRC Press, (2013).

[46] G. L. Mullen, D. Wan, Q. Wang, *Value sets of polynomial maps over finite fields, Quart. J. Math.*, **64**, **4**, (2013), 1191-1196.

[47] G. L. Mullen, D. Wan, Q. Wang, *An index bound on value sets of polynomial maps over finite fields, Applications of Algebra and Number Theory*, (2014), 280-296.

[48] A. Muratovic-Ribic, E. Pasalic, *A note on complete mapping polynomials over finite fields and their applications in cryptography, Finite Fields and Their Applications*, **25**, (2014), 306-315.

[49] H. Niederreiter, K. H. Robinson, *Complete mappings of finite fields, J. Aust. Math. Society*, A 33, no.2, (1982), 197-212.

[50] H. Niederreiter, A. Winterhof, *Cyclotomic R-orthomorphisms of finite fields*, *Discrete Mathematics*, **295**, (2005), 161-171.

[51] K. Nyberg, *Differentially uniform mappings for cryptography, Eurocrypt'93, Lect. Notes Comput. Science*, **765**, Springer-Verlag, New York, (1993), 55-64.

[52] F. Pausinger, A. Topuzoğlu, *Permutations of finite fields and uniform distribution modulo 1*, *Algebraic Curves and Finite Fields*, edited by H. Niederreiter, A. Ostafe, D. Panario and A. Winterhof, Radon Series on Applied and Computational Mathematics 16, (2014), 145-157.

[53] I. E. Shparlinski, *Finite fields: theory and computation The meeting point of number theory, computer science, coding theory and cryptography, Mathematics and its Applications*, **477**, (1999).

[54] A. Topuzoğlu, *Carlitz rank of permutations of finite fields:*, *Jornal of Symbolic Computation*, **64**, (2014), 53-66.

[55] Z. Tu, X. Yeng, C. Li, T. Helleseth, *Two classes of permutation polynomials having the form* $(x^{2^m} + x + \delta)^s + x$, *Finite Fields and Their Applications*, **31**, (2015), 12-24.

[56] Z. Tu, X. Yeng, Y. Jiang, *Permutation polynomials of the form* $(x^{p^m} - x + \delta)^s + L(x)$ *over the finite field* $\mathbb{F}_q^{2m}$ *of odd characteristic, Finite Fields and Their Applications*, **34**, (2015), 20-35.

[57] Z. Tu, X. Zeng, L. Hu, *Several classes of complete permutation polynomials, Finite Fields and Their Applications*, **25**, (2014), 182-193.

[58] D. Wan, P. J.-S. Shiue, C. S. Chen, *Value Sets of Polynomials over Finite Fields*, *Proc. Amer. Math. Soc.*, **119**, (1993), 711-717.

[59] D. Wan, *A p-adic lifting lemma and its application to permutation polynomials, Finite Fields, Coding Theory and Advances in Communications and Computing*, (1993), 209-216.

[60] A. Winterhof, *Generalizations of complete mappings of finite fields and some applications*, *Journal of Symbolic Computation*, **64**, (2014), 42-52.

[61] G. Wu, N. Li, T. Helleseth, Y. Zhang, *Some classes of monomial complete permutation polynomials over finite fields of characteristic two, Finite Fields and Their Applications*, **28**, (2014), 148-165.

[62] Z. Zha, L. Hu, X. Cao, *Constructing permutations and complete permutations over finite fields via subfield-valued polynomials*, *Finite Fields and Their Applications*, **31**, (2015), 162-177.

[63] M. Zieve, *On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, Proc. Amer. Math. Society*, **137**, (2009), 2209-2216.