ON THE CYCLE STRUCTURE OF PERMUTATION POLYNOMIALS

by

AYÇA ÇEŞMELİOĞLU

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

Spring 2008

ON THE CYCLE STRUCTURE OF PERMUTATION POLYNOMIALS

APPROVED BY

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

Assoc. Prof. Dr. Wilfried Meidl .....
(Thesis Co-supervisor)

Assist. Prof. Dr. Cem Güneri .....

Assoc. Prof. Dr. Erkay Savaş .....

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

DATE OF APPROVAL: 17.06.2008

ON THE CYCLE STRUCTURE OF PERMUTATION POLYNOMIALS

Ayça Çeşmelioğlu

Mathematics, PhD Thesis, 2008

Thesis Supervisor: Prof. Dr. Alev Topuzoğlu
Thesis Co-supervisor: Assoc. Prof. Dr. Wilfried Meidl

Keywords: symmetric group on q letters, finite fields, permutation polynomials, monomials, Dickson polynomials, cycle decomposition, nonlinear pseudorandom number generators.

Abstract

L. Carlitz observed in 1953 that for any $a \in \mathbb{F}_q^*$, the transposition $(0\ a)$ can be represented by the polynomial

$$p_a(x) = -a^2(((x-a)^{q-2} + a^{-1})^{q-2} - a)^{q-2}$$

which shows that the group of permutation polynomials over $\mathbb{F}_q$ is generated by the linear polynomials $ax + b, a, b \in \mathbb{F}_q,\ a \neq 0$, and x^{q-2}.
Therefore any permutation polynomial over $\mathbb{F}_q$ can be represented as

$$\mathcal{P}_n = (\ldots((a_0x + a_1)^{q-2} + a_2)^{q-2} \ldots + a_n)^{q-2} + a_{n+1}, \text{ for some } n \geq 0.$$

In this thesis we study the cycle structure of permutation polynomials $\mathcal{P}_n$, and we count the permutations $\mathcal{P}_n$, $n \leq 3$, with a full cycle. We present some constructions of permutations of the form $\mathcal{P}_n$ with a full cycle for arbitrary n. These constructions are based on the so called binary symplectic matrices.

The use of generalized Fibonacci sequences over $\mathbb{F}_q$ enables us to investigate a particular subgroup of S_q, the group of permutations on $\mathbb{F}_q$. In the last chapter we present results on this special group of permutations.

PERMÜTASYON POLİNOMLARININ ÇEVRİM YAPISI ÜZERİNE

Ayça Çeşmelioğlu

Matematik, Doktora Tezi, 2008

Tez Danışmanı: Prof. Dr. Alev Topuzoğlu
Tez Eş Danışmanı: Doç. Dr. Wilfried Meidl

Anahtar Kelimeler: derecesi n olan simetrik grup, sonlu cisimler, permütasyon polinomları, birterimli polinomlar, Dickson polinomları, çevrim yapısı, doğrusal olmayan sözde rastgele sayı üreteçleri.

Özet

L. Carlitz $(0\ a)$ devriniminin

$$p_a(x) = -a^2(((x-a)^{q-2} + a^{-1})^{q-2} - a)^{q-2}$$

polinomu tarafından temsil edilebileceğini, dolayısıyla $\mathbb{F}_q$ üzerindeki permütasyon polinomlarının oluşturduğu grubun doğrusal polinomlar $ax + b, a, b \in \mathbb{F}_q, a \neq 0$ ve x^{q-2} tarafından gerildiğini göstermiştir. O halde $\mathbb{F}_q$ üzerindeki herhangi bir permütasyon polinomu en az bir n için

$$\mathcal{P}_n(x) = (\ldots((a_0x + a_1)^{q-2} + a_2)^{q-2} \ldots + a_n)^{q-2} + a_{n+1},$$

şeklinde yazılabilir.

Bu tezde, $n \leq 3$ için $\mathcal{P}_n$ şeklindeki permütasyon polinomlarının çevrim yapısı incelenmiş ve tam çevrime sahip olanların sayısıyla ilgili sonuçlar elde edilmiştir.

Herhangi bir n tek sayısı için, tam çevrime sahip $\mathcal{P}_n$ polinomlarının inşası için ikili simetrik matrisleri kullanan metodlar geliştirilmiştir.

$\mathbb{F}_q$ üzerinde tanımlı genelleştirilmiş Fibonacci dizilerinin kullanımı permütasyon polinomları grubunun belirli bir altgrubunu incelenmesine olanak sağlamıştır. Tezin son bölümünde bu özel altgrupla ilgili sonuçlar verilmiştir.

Aileme

ve

sevgili dedeme

Acknowledgments

First and foremost, I would like to thank my supervisor Prof. Dr. Alev Topuzoğlu for her motivation, guidance and encouragement throughout this thesis. Her contribution to my academic experience and my personality has been enormous. I also would like to thank my co-advisor Assoc. Prof. Dr. Wilfried Meidl who has not treated me only as a student, but also as a colleague and friend. I will always be grateful for his guidance, patience and invaluable friendship during every stage of this work. I would like to thank all the professors in Mathematics program for the knowledge they provided me during my studies at Sabancı University. I am especially thankful to Prof. Dr. Henning Stichenoth and Assist. Prof. Dr. Cem Güneri for their comments on the work for this thesis.

My parents and my sister have always motivated and supported me throughout my whole life, especially during the preparation of this thesis. I am deeply grateful to them for their endless love and care. I was fortunate to have Özgür Gül by my side for all these years at SabancıUniversity. I am thankful to him for his love, care, friendship and everything we shared . Last, but not least, I would like to thank all my friends in Mathematics programs for all the useful discussions we made and joyful moments we shared.

The last year for this work is supported by Yousef Jameel Scholarship.

Table of Contents

CHAPTER 1

INTRODUCTION

Throughout this thesis, $\mathbb{F}_q$ denotes the finite field with $q = p^r$ elements where p is a prime, $r \geq 1$ is an integer. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* if the polynomial function $f : c \mapsto f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a bijection. *Permutation polynomial* will be abbreviated as PP. We are concerned with the set of all PPs over $\mathbb{F}_q$, which is a group under composition and subsequent reduction modulo $x^q - x$. The group of PPs over $\mathbb{F}_q$ is isomorphic to S_q, the symmetric group on q letters.

PPs over finite fields have applications in many areas including cryptography, pseudorandom number generation and combinatorics. Despite the recent progress on this topic, there are still many open questions, see, for instance [23, 24, 34]. The following problems have attracted particular attention:

- Finding new classes of PPs.
- Determining the cycle structure of classes of PPs.
- Enumeration of special classes of PPs.

This thesis addresses the last two questions.

1.1. Some Classes of Permutation Polynomials

In this section we will review some of the known classes of PPs over $\mathbb{F}_q$.

Given an arbitrary polynomial $f(x) \in \mathbb{F}_q[x]$, it is 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 [19] for prime fields, which was then generalized in 1897 by Dickson [14] to arbitrary finite fields $\mathbb{F}_q$.

Theorem 1.1.1 *(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 $\leq q-2$.*

See [26, Chapter 7] for the proof.
As a corollary of Hermite's criterion, $f(x)$ 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 $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ 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 1.1.2 *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 [26, 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. We start by listing some well-known classes of PPs:

(1) Linear Polynomials: Every linear polynomial $ax + b \in \mathbb{F}_q[x]$, $a \neq 0$, is a PP of $\mathbb{F}_q$.

(2) Monomials: The monomial x^n permutes $\mathbb{F}_q$ if and only if $gcd(n, q-1) = 1$.

(3) Dickson polynomials of the 1st kind: For $a \in \mathbb{F}_q$, Dickson polynomials of the 1st kind are defined by the formula

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

Obviously, $deg(D_n(x,a)) = n$ and $D_n(x,0)$ is just the monomial x^n. The Dickson polynomial of the 1st kind $D_n(x,a)$ with $a \in \mathbb{F}_q^*$ is a PP of $\mathbb{F}_q$ if and only if $gcd(n, q^2-1) = 1$, see [25, Chapter 3] for a proof.

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

$$E_n(x,a) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-j}{j} (-a)^j x^{n-2j}. \tag{1.2}$$

From (1.2), it is easy to see that $deg(E_n(x,a)) = n$ and $E_n(x,0) = x^n$. It was shown by Matthews [30] 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 [10] 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 2nd kind that are PPs can be found in Coulter [12], Henderson and Matthews [17] and Henderson [18].

(5) Linearized Polynomials: Let $\mathbb{F}_{q^k}$ be the extension field of $\mathbb{F}_q$ of degree k. 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 $L(x)$, i.e. the $\mathbb{F}_q$-linear operator induced by $L(x)$ on $\mathbb{F}_{q^k}$ is nonsingular. See [26, Chapter 7].

Some other classes can be found in [26], Chapter 7. For some recent constructions we refer to the articles [2, 37, 38]

1.2. On the Cycle Structure of Permutations

Among the classes of PPs defined in the last section, the cycle structures of (**1**), (**2**) and partly of (**3**), (**5**) are known. We give the related results below. In the following, $\mathcal{N}_k(f)$ is used to denote the number of cycles of length k of the permutation corresponding to $f \in \mathbb{F}_q[x]$.

(1) For a linear permutation $ax + b \in \mathbb{F}_q[x]$, the cycle structure is as follows: If $a = 1, b \in \mathbb{F}_q^*$ then $f(x)$ has p^{r-1} cycles of length p. If $a \neq 1$ and s is the order of a in $\mathbb{F}_q$, then the permutation corresponding to the polynomial $f(x) = ax + b$ has a fixed point and $\frac{q-1}{s}$ cycles of length s.

(2) A monomial $g(x) = x^n$ which permutes $\mathbb{F}_q$ has a cycle of length m if and only if $q - 1$ has a divisor t such that the order of n modulo t is equal to m. Then $\mathcal{N}_m(g)$ satisfies

$$m\mathcal{N}_m(g) = gcd(q - 1, n^m - 1) - \sum_{\substack{i|m \\ i<m}} i\mathcal{N}_i(g).$$

See Ahmad [1] or Lidl and Mullen [22] for the proof.

(3) For Dickson polynomials of the 1st kind (1.1) which permute $\mathbb{F}_q$, the results about the cycle structure in the cases $a = 1$ and -1 are stated in the following theorems from [22].

Theorem 1.2.3 *$D_n(x, 1) \in \mathbb{F}_q[x]$ has a cycle of length m if and only if $q - 1$ or $q + 1$ has a divisor t such that $n^m \equiv \pm 1 \mod t$. Then $\mathcal{N}_m(D_n(x, 1))$ satisfies*

$$\begin{aligned} m\mathcal{N}_m(D_n(x,1)) &= [gcd(q+1, n^m+1) + gcd(q-1, n^m+1) \\ &+ gcd(q+1, n^m-1) + gcd(q-1, n^m-1)]/2 \\ &- \epsilon_1 - \sum_{\substack{i|m \\ i<m}} i\mathcal{N}_i(D_n(x,1)) \end{aligned}$$

where

$$\epsilon_1 = \begin{cases} 1 & \text{if } p = 2 \text{ or } p \text{ is odd and } n \text{ is even,} \\ 2 & \text{if } p \text{ is odd and } n \text{ is odd.} \end{cases}$$

Theorem 1.2.4 *Let $\nu_p(m)$ denote the largest power of p dividing m for $m \neq 0$ and set $\nu(0) = \infty$. If n and q are odd then $D_n(x, -1) \in \mathbb{F}_q[x]$ has a cycle of length m if and only if $q-1$ or $q+1$ has a divisor t such that $n^m \equiv 1 \mod t$ or $2(n^m+1) \equiv 0 \mod t$. Then $\mathcal{N}_m(D_n(x,-1))$ is given by*

$$\begin{aligned} m\mathcal{N}_m(D_n(x,-1)) &= [a_1 gcd(n^m+1, 2(q+1)) + a_2 gcd(n^m+1, q-1) \\ &+ a_3 gcd((n^m-1)/2, q+1) + gcd(n^m-1, q-1)]/2 \\ &- \epsilon_{-1} - \sum_{i|m, i<m} i\mathcal{N}_i(D_n(x,-1)) \end{aligned}$$

where

$$a_1 = \begin{cases} 1 & \text{if } \nu_2(n^m+1) = \nu_2(q+1), \\ 0 & \text{otherwise,} \end{cases} \quad a_2 = \begin{cases} 1 & \text{if } \nu_2(n^m+1) < \nu_2(q+1), \\ 0 & \text{otherwise,} \end{cases}$$

$$a_3 = \begin{cases} 1 & \text{if } \nu_2(n^m+1) > \nu_2(q+1), \\ 0 & \text{otherwise,} \end{cases}$$

$$\epsilon_{-1} = \begin{cases} 2 & \text{if } n^m \equiv 1 \mod 4 \text{ and } q \equiv 1 \mod 4, \\ 0 & \text{otherwise.} \end{cases}$$

See [22] for the proofs of these results.

(5) For the cycle structure of linearized polynomials over $\mathbb{F}_{q^k}$, the reader is referred to [32] since the results are too technical to state here.

Cycle structure of PPs is of theoretical interest but it is also needed for certain applications like generation of pseudorandom sequences.
Let $\psi(x) \in \mathbb{F}_q[x]$ be a polynomial of degree $d \geq 2$. The sequence (u_n) defined by the recurrence relation

$$u_{n+1} = \psi(u_n), n \geq 0, \tag{1.3}$$

with some initial value $u_0 \in \mathbb{F}_q$ is called a *nonlinear congruential pseudorandom number generator.*

In the following, we present some nonlinear pseudorandom number generators that have been considered in the literature. Note that when $\psi(x)$ is a PP of $\mathbb{F}_q$, the length

of the cycle containing s_0 in the cycle decomposition of $\psi(x)$ is the period length of the sequence (u_n) in (1.3) with the initial value u_0.

First, we describe a popular pseudorandom number generator which is especially used in cryptography.

The *power generator* over $\mathbb{F}_p$ is defined as

$$p_{n+1} = \psi(p_n),\ n = 1, 2, \cdots \tag{1.4}$$

for an initial value $p_0 \in \mathbb{F}_p^*$, where ψ is the monomial $\psi(x) = x^e \in \mathbb{F}_p[x]$.

Clearly, the power generator (p_n) becomes eventually periodic and it is purely periodic when $x^e \in \mathbb{F}_p[x]$ is a PP. Recall that $\psi(x) = x^e \in \mathbb{F}_p[x]$ is a PP when $gcd(e, p-1) = 1$. In [33], Shallit and Vasiga, in [9], Chou and Shparlinski proved some results about the preperiod, cycle length and their average values for the power generator. For further results on the properties of the power generator we refer to Shparlinski, [34, p.353].

Another example of nonlinear pseudorandom number generators is obtained by using a Dickson polynomial of the 1st kind $D_e(x, 1)$ in (1.1), namely $\psi(x) = D_e(x, 1) \in \mathbb{F}_p[x]$. Results on the quality of this generator with respect to applications in cryptology can be found in [4].

The *inversive pseudorandom number generator* is defined as

$$s_{n+1} = \psi(s_n) \tag{1.5}$$

where $\psi(x) = ax^{q-2} + b, n \geq 1$, and $a, b, s_0 \in \mathbb{F}_q$ with $a \neq 0$. The problem of constructing sequences (s_n) defined by (1.5) with the maximum possible period was first considered by Eichenauer and Lehn over the prime field $\mathbb{F}_p$ and in [15] it was shown that if $f(x) = x^2 - ax - b \in \mathbb{F}_p[x]$ is a primitive polynomial over $\mathbb{F}_p$ then (s_n) is a sequence of period p. In [16], Flahive and Niederreiter extended the result of Eichenauer and Lehn, by showing that (s_n) is a sequence of period p if and only if for the roots $\alpha, \beta \in \mathbb{F}_{p^2}$ of $f(x)$, $p+1$ is the smallest integer such that $(\frac{\alpha}{\beta})^{p+1} = 1$, i.e. $p+1$ is the order of $\frac{\alpha}{\beta}$. In [7], Chou proved the same statement for the sequences (s_n) over an arbitrary finite field $\mathbb{F}_q$ and in [8] he presented all possible period lengths for the inversive generator, i.e. the cycle structure of the permutation associated to $\psi(x) = ax^{q-2} + b \in \mathbb{F}_q[x]$.

Theorem 1.2.5 *Let $a, b \in \mathbb{F}_q$ with $ab \neq 0$ and $f(x)$ be the polynomial $f(x) = x^2 - bx - a \in \mathbb{F}_q[x]$.*

(1) If the polynomial $f(x)$ has a double root i.e. $f(x) = (x-\alpha)^2$ for some $\alpha \in \mathbb{F}_q$ then

(i) $\psi(\alpha) = \alpha$,

(ii) if $\alpha^{-1}s_0 \in \mathbb{F}_p \setminus \{1\}$ *then* $s_n = 0$ *for some* $n \geq 0$ *and the period length of* (s_n) *is* $p-1$,

(iii) if $\alpha^{-1}s_0 \in \mathbb{F}_q \setminus \mathbb{F}_p$ *then* $s_n \neq 0$ *for any* $n \geq 0$ *and the period length of* (s_n) *is* p.

(2) Suppose that the polynomial $f(x)$ has distinct roots in $\mathbb{F}_{q^2}$ i.e. $f(x) = (x-\alpha)(x-\beta)$ for some $\alpha, \beta \in \mathbb{F}_{q^2}$ and $o(m_f)$ denotes the order of the polynomial $m_f(x) = x^2 + (b^2/a+2)x + 1 \in \mathbb{F}_q[x]$.

(i) If $f(s_0) = 0$, *then* $\psi(s_0) = s_0$,

(ii) if p *is odd and* $o(m_f)$ *is even then the period length of the sequence* (s_n) *with* $s_0 = b/2$ *is* $o(m_f) - 1$ *and* $s_n = 0$ *for some* $n \geq 0$,

(iii) if both p *and* $o(m_f)$ *is odd then the period length of the sequence* (s_n) *with* $s_0 = b/2$ *is* $o(m_f)$ *and* $s_n \neq 0$ *for any* $n \geq 0$,

(iv) if $f(s_0) \neq 0$ *and* $s_0 \neq b/2$ *whenever* $p \neq 2$ *and the order* $o(M_f)$ *of the polynomial* $M_f(x) = x^2 - \left(2 + \frac{b^2+4a}{f(s_0)}\right)x + 1$ *divides* $o(m_f)$, *then* $s_n = 0$ *for some* $n \geq 0$ *and the period length of the sequence* (s_n) *is* $o(m_f) - 1$,

(v) if $f(s_0) \neq 0$ *and* $s_0 \neq b/2$ *whenever* $p \neq 2$ *and* $o(M_f)$ *does not divide* $o(m_f)$, *then* $s_n \neq 0$ *for any* $n \geq 0$ *and the period length of* (s_n) *is* $o(m_f)$.

The inversive generator is known to behave well according to most of the quality measures for randomness. These generators will be mentioned again in Chapter 2, since they can be considered as a special case of the PPs, that we study in this thesis. For a comprehensive survey on pseudorandom sequences and results about the related randomness measures, see [36].

In this thesis, we present results on the cycle structure of another large class of PPs and also give methods of constructing PPs over $\mathbb{F}_q$ with the largest possible cycle length.

1.3. Enumeration of Permutation Polynomials

It was mentioned in Section 1.1 that the enumeration of PPs with certain features is of interest. In particular finding the number of PPs of a fixed degree is a long standing open problem. Das [13], Konyagin and Pappalardi [20, 21], Malvenuto and Pappalardi [28] dealt with this problem and obtained the results which support the common belief that the vast majority of PPs are of degree $q-2$. Das showed the following result for the number of PPs of degree $p-2$ over the prime field in [13].

Theorem 1.3.6 *Let $N_p(p-2)$ be the number of PPs $f(x) \in \mathbb{F}_p[x]$ with $f(0)=0$ having degree $p-2$. Then*

$$\left| N_p(p-2) - \left(1-\frac{1}{p}\right)(p-1)! \right| \leq \left(1-\frac{1}{p}\right)\sqrt{\frac{1+(p-2)p^{p-1}}{p-1}}.$$

Let $N_{q,d}$ be the number of PPs over $\mathbb{F}_q$ of degree $< q-d-1$. Trivially, $N_q(1) = q(q-1)$ and $N_q(d) = 0$ for $d|q-1$. In [20], Konyagin and Pappalardi showed the following bound for $N_{q,1}$.

Theorem 1.3.7 *The number $N_{q,1}$ of PPs of degree $< q-2$ satisfies*

$$|N_{q,1} - (q-1)!| \leq \sqrt{\frac{2e}{\pi}} q^{q/2}.$$

Using the bound in Theorem 1.3.7, it is also possible to derive a bound for $N_p(p-2)$,

$$\left| N_p(p-2) - (1-\frac{1}{p})(p-1)! \right| \leq \sqrt{\frac{2e}{\pi}} p^{(p-2)/2}$$

which is asymptotically better for a factor proportional to $p^{1/2}$ than the bound in [13]. However Das also gives an algorithm to calculate the number of PPs of degree $p-2$.

As a continuation of their work, in [21] Konyagin and Pappalardi gave the following result.

Theorem 1.3.8 *Let $N_q(k_1, \ldots, k_d)$ be the number of PPs over $\mathbb{F}_q$ for which the coefficient of x^{k_i} is zero for all $1 \leq i \leq d$ where $0 < k_1 < \ldots < k_d \leq q-2$. Then*

$$\left| N_q(k_1, \ldots, k_d) - \frac{q!}{q^d} \right| < \left(1+\sqrt{\frac{1}{e}}\right)^q ((q-k_1-1))^q /2.$$

Note that $N_{q,d} = N_q(q-d-1,\ldots,q-2)$ and the result above can be used to obtain a bound for $N_{q,d}$.

In [29], Malvenuto and Pappalardi gave upper and lower bounds on the number $N_{q,[k]}$ of PPs over $\mathbb{F}_q$ of degree $q-k$ with a k-cycle where $3 \leq k \leq 6$.

Theorem 1.3.9 *Let ϕ be the Euler ϕ-function. If $q \equiv 1 \mod k$ then*

$$N_{q,[k]} \geq \frac{\phi(k)}{k} q(q-1).$$

If the characteristic p of $\mathbb{F}_q$ satisfies $p > e^{(k-3)/e}$ then

$$N_{q,[k]} \leq \frac{(k-1)!}{k} q(q-1).$$

The authors also gave the complete formula for $N_{q,[k]}$ for the cases $k = 4, 5$ and partial formulas for $k = 6$.

In the next chapter of this thesis, we introduce a class of PPs, determine their cycle structure and present enumeration results for those with full cycle.

1.4. Generators for the Group of Permutation Polynomials of $\mathbb{F}_q$

L. Carlitz observed in 1953 that any transposition $(0\ a)$ for $a \in \mathbb{F}_q^*$ can be represented by the polynomial

$$p_a(x) = -a^2(((x-a)^{q-2} + a^{-1})^{q-2} - a)^{q-2}, \tag{1.6}$$

and hence 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 [6]. The result of Carlitz is the starting point for the work presented in this thesis.

The following results also stem from the work of Carlitz:

Theorem 1.4.10 *Let $q > 2$, c be a fixed primitive element of $\mathbb{F}_q$ and A_q denote the alternating group on q letters.*

(i) S_q can be generated by $cx, x+1$ and x^{q-2},

(ii) A_q *can be generated by its subgroups* $\{a^2x+b | a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$ *and* $\{(x^{q-2}+a)^{q-2} | a \in \mathbb{F}_q\}$,

(iii) A_q *can be generated by* $c^2x, x+1$ *and* $(x^{q-2}+1)^{q-2}$.

For proofs of the results above see Theorem 7.19, Theorem 7.21 in [26].

In [35], Stafford showed under which conditions on k, the group generated by the linear polynomials $ax+b,\ a \in \mathbb{F}_q^*,\ b \in \mathbb{F}_q$ and the monomial x^k where $\gcd(k, q-1) = 1$ is S_q.

Theorem 1.4.11 *Let* $1 < k < q-2$ *be an integer with* $gcd(k, q-1) = 1$. *Define* $G_k =< ax+b, x^k |\ a \in \mathbb{F}_q^*, b \in \mathbb{F}_q >$ *which is a subgroup of* S_q.

(i) If p *is odd and* k *is not a power of* p, *then* $G_k = S_q$.

(ii) If $p = 2$ *and* k *is not a power of* 2, *then* $G_k \supseteq A_q$. *Moreover,* $G_k = S_q$ *if and only if* x^k *is an odd permutation.*

This result specializes to the result of Carlitz when $k = q-2$.

Motivated by the result of Carlitz, a particular representation of PPs will be introduced in the next section.

1.5. Polynomials $\mathcal{P}_n(x)$

By Carlitz's observation mentioned in Section 1.4, it is seen that any PP can be written as a composition of the polynomials of the form $p_a(x)$ with $a \in \mathbb{F}_q^*$ given by (1.6). Based on this result we define a class of PPs over $\mathbb{F}_q$ in a recursive way as

$$\mathcal{P}_n(x) = (\mathcal{P}_{n-1}(x))^{q-2} + a_{n+1}, \text{ for } n \geq 1 \tag{1.7}$$

by setting $\mathcal{P}_0(x) = a_0x + a_1 \in \mathbb{F}_q[x]$ with $a_0 \neq 0$. Note that it is also possible to express $\mathcal{P}_n(x)$ as follows:

$$\mathcal{P}_n(x) = (\ldots((a_0x+a_1)^{q-2}+a_2)^{q-2}\ldots+a_n)^{q-2}+a_{n+1},\ n \geq 1, \tag{1.8}$$

where $a_i \neq 0$, for $i = 0, 2, \ldots, n$. Due to the result of Carlitz, any PP over $\mathbb{F}_q$ can be expressed as a $\mathcal{P}_n(x)$ for some $n \geq 0$. We write $\mathcal{P}_n(x) = \bar{P}_n(x)$ if $a_{n+1} \neq 0$ and $\mathcal{P}_n(x) = P_n(x)$ if $a_{n+1} = 0$, since it is more convenient to treat the cases $a_{n+1} = 0$ and $a_{n+1} \neq 0$ separately. For the polynomial

$$\bar{P}_n(x) = (\ldots((a_0x + a_1)^{q-2} + a_2)^{q-2} \ldots + a_n)^{q-2} + a_{n+1},$$

we consider

$$(\ldots((a_0x + a_1)^{-1} + a_2)^{-1} \ldots + a_n)^{-1} + a_{n+1},$$

i.e.

$$a_{n+1} + 1/(a_n + 1/(\ldots + a_2 + 1/(a_0x + a_1)\ldots)),$$

for which we can put

$$\bar{R}_n(x) = \frac{\alpha_{n+1}x + \beta_{n+1}}{\alpha_n x + \beta_n}, \tag{1.9}$$

where

$$\alpha_k = a_k\alpha_{k-1} + \alpha_{k-2} \quad \text{and} \quad \beta_k = a_k\beta_{k-1} + \beta_{k-2}, \tag{1.10}$$

for $k \geq 2$ and $\alpha_0 = 0, \alpha_1 = a_0, \beta_0 = 1, \beta_1 = a_1$. We remark here that α_k and β_k cannot both be zero.

For the polynomial $P_n(x)$, the fractional expansion and the related nth convergent $R_n(x) = \frac{\alpha_{n-1}x+\beta_{n-1}}{\alpha_n x+\beta_n}$ are obtained similarly.

We define the string $\mathbf{O}_n$ of *poles* as

$$\mathbf{O}_n = \{x_i : x_i = \frac{-\beta_i}{\alpha_i}, i = 1, \ldots, n\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}. \tag{1.11}$$

We note that any three consecutive elements of $\mathbf{O}_n$ are distinct. In fact, if $x_k = x_{k+1}$ for some $1 \leq k < n$ then $\frac{-\beta_k}{\alpha_k} = \frac{-\beta_{k+1}}{\alpha_{k+1}}$. Therefore

$$\begin{aligned} 0 &= \alpha_{k+1}\beta_k - \alpha_k\beta_{k+1} \\ &= (-1)^k(\alpha_1\beta_0 - \beta_1\alpha_0) \\ &= (-1)^k a_0 \end{aligned}$$

and this contradicts to the assumption that $a_0 \neq 0$.

If $x_{k-1} = x_{k+1}$ for some $1 < k < n$ then $\frac{-\beta_{k-1}}{\alpha_{k-1}} = \frac{-\beta_{k+1}}{\alpha_{k+1}} = -\frac{a_{k+1}\alpha_k+\alpha_{k-1}}{a_{k+1}\beta_k+\beta_{k-1}}$. Therefore

$$a_{k+1}\alpha_k\beta_{k-1} + \alpha_{k-1}\beta_{k-1} = a_{k+1}\alpha_{k-1}\beta_k + \alpha_{k-1}\beta_{k-1}$$

and

$$a_{k+1}(\alpha_k\beta_{k-1} - \beta_k\alpha_{k-1}) = 0.$$

Since $a_{k+1} \neq 0$, $\alpha_k\beta_{k-1} - \beta_k\alpha_{k-1} = 0$ gives a contradiction by using the previous paragraph.

For $x \in \mathbb{F}_q \backslash \mathbf{O}_n$, $R_n(x) = P_n(x)$ and $\bar{R}_n(x) = \bar{P}_n(x)$.

Related to the nth convergent $\bar{R}_n(x)$, the function $\bar{F}_n(x)$ is defined by

$$\bar{F}_n(x) = \begin{cases} \bar{R}_n(x) & \text{for } x \neq x_n \\ \alpha_{n+1}/\alpha_n & \text{when } x = x_n \in \mathbb{F}_q. \end{cases}$$

After defining the function $F_n(x)$ in a similar way, we put $\mathcal{F}_n(x) = \bar{F}_n(x)$ if $a_{n+1} \neq 0$, and $\mathcal{F}_n(x) = F_n(x)$ if $a_{n+1} = 0$. Since $\mathcal{R}_n(x)$ never takes the value α_{n+1}/α_n, $\mathcal{F}_n$ becomes a permutation of $\mathbb{F}_q$. The next lemma describes the relation between the values of $\mathcal{P}_n$ and $\mathcal{F}_n$ when the poles are distinct and are elements of $\mathbb{F}_q$.

Lemma 1.5.12 *If the poles $x_1, x_2, \ldots, x_n$ are distinct and in $\mathbb{F}_q$, then*

$$\mathcal{P}_n(x_i) = \begin{cases} \mathcal{F}_n(x_{i-1}) & \text{for} \quad 2 \leq i \leq n \\ \mathcal{F}_n(x_n) & \text{for} \quad i = 1 \end{cases}$$

for all $n \geq 2$. Therefore the permutation $\mathcal{P}_n = \mathcal{P}_n(x)$ can be expressed as a product of the n-cycle $(\mathcal{F}_n(x_{n-1}) \cdots \mathcal{F}_n(x_1)\ \mathcal{F}_n(x_n))$ with the permutation $\mathcal{F}_n(x)$, i.e.

$$\mathcal{P}_n(x) = (\mathcal{F}_n(x_{n-1}) \cdots \mathcal{F}_n(x_1)\ \mathcal{F}_n(x_n))\mathcal{F}_n(x), \tag{1.12}$$

(multiplying in right-to-left order).

Proof: The lemma can easily be proved by induction. Note that

$$\mathcal{F}_2(x) = \frac{a_0(a_2a_3 + 1)x + a_1a_2a_3 + a_1 + a_3}{a_0a_2x + a_1a_2 + 1}.$$

Substituting $x = x_1$, we have

$$\mathcal{F}_2(x_1) = a_3 \text{ and by definition, } \mathcal{F}_2(x_2) = \frac{\alpha_3}{\alpha_2}.$$

Recall that $\mathcal{P}_1(x) = (a_0x + a_1)^{q-2} + a_2$ and $\mathcal{F}_1(x) = \frac{a_0a_2x + a_1a_2 + 1}{a_0x + a_1}$. $\mathcal{P}_2(x)$ satisfies

$$\mathcal{P}_2(x_1) = (\mathcal{P}_1(x_1))^{q-2} + a_3 = (\mathcal{F}_1(x_1))^{q-2} + a_3 = \left(\frac{\alpha_2}{\alpha_1}\right)^{q-2} + a_3 = \frac{\alpha_3}{\alpha_2} = \mathcal{F}_2(x_2)$$

and

$$\mathcal{P}_2(x_2) = (\mathcal{P}_1(x_2))^{q-2} + a_3 = (\mathcal{F}_1(x_2))^{q-2} + a_3.$$

We have $\mathcal{F}_1(x_2) = 0$ and hence the desired equality is obtained.

For the rest of the proof the values of P_n will be considered, the case of $\bar{P}_n$ can be dealt with similarly. Suppose we have $P_{n-1}(x_i) = F_{n-1}(x_{i-1})$ for $2 \leq i \leq n-1$. Then we obtain

$$\begin{aligned} P_n(x_i) &= (P_{n-1}(x_i) + a_n)^{q-2} = (F_{n-1}(x_{i-1}) + a_n)^{q-2} \\ &= \left(\frac{\alpha_n x_{i-1} + \beta_n}{\alpha_{n-1} x_{i-1} + \beta_{n-1}}\right)^{q-2} = F_n(x_{i-1}) \end{aligned}$$

for $2 \leq i \leq n-1$. We have $P_{n-1}(x_n) = F_{n-1}(x_n)$ since all the poles in $\mathbf{O}_n$ are distinct, the pole x_n is not in $\mathbf{O}_{n-1}$. For $x = x_n$, we obtain

$$\begin{aligned} P_n(x_n) &= (P_{n-1}(x_n) + a_n)^{q-2} = (F_{n-1}(x_n) + a_n)^{q-2} = 0 \\ &= \frac{\alpha_{n-1} x_{n-1} + \beta_{n-1}}{\alpha_n x_{n-1} + \beta_n} = F_n(x_{n-1}). \end{aligned}$$

Finally, with the assumption that $P_{n-1}(x_1) = F_{n-1}(x_{n-1})$,

$$P_n(x_1) = (P_{n-1}(x_1) + a_n)^{q-2} = (F_{n-1}(x_{n-1}) + a_n)^{q-2} = \left(\frac{\alpha_{n-2}}{\alpha_{n-1}} + a_n\right)^{q-2} = \frac{\alpha_{n-1}}{\alpha_n}.$$

The equation (1.12) is immediate now, since P_n and F_n differ only at the poles. □

We will use Lemma 1.5.12 and results on the cycle decomposition of $\mathcal{F}_n$ to obtain the cycle decomposition of $\mathcal{P}_n$. The cycle decomposition of $\mathcal{F}_n$ can be obtained from the result of Chou on the inversive generator given in Theorem 1.2.5. Recall that the inversive generator (s_n) was defined in a recursive way by the polynomial $\psi(x) = ax^{q-2} + b$ with an initial element $s_0 \in \mathbb{F}_q$. Note that, $\psi(x)$ is $\mathcal{P}_1(x)$ with $a_1 = 0$.

Representation of PPs by polynomials of the form $\mathcal{P}_n(x)$ in (1.8) enables us to introduce a new approach to the enumeration of PPs. In Chapter 2, we present some enumeration results for the number of PPs of $\mathbb{F}_q$ of the form $\mathcal{P}_1(x)$ with a given cycle decomposition and also for the permutations $\mathcal{P}_2(x)$ and $P_3(x)$ with full cycle.

CHAPTER 2

CYCLE DECOMPOSITIONS OF $\mathcal{P}_2(x)$ AND $P_3(x)$

In this chapter, we give all the results about the cycle structure and the enumeration of the permutations $\mathcal{P}_2(x)$ and $P_3(x)$ with full cycle.
Recall that $\mathcal{P}_n(x)$ was introduced in (1.8) as

$$\mathcal{P}_n(x) = (\dots((a_0x + a_1)^{q-2} + a_2)^{q-2} \dots + a_n)^{q-2} + a_{n+1},\ n \geq 1$$

where $a_i \neq 0$ for all $i = 0, 2, 3, \cdots, n$ and Lemma 1.5.12 showed the close relation between the values of $\mathcal{P}_n(x)$ and $\mathcal{F}_n(x)$.
In the following section, we first define permutations of $\mathbb{F}_q$ based on nonconstant rational transformations, then present the results about the cycle structure of these permutations, which will be frequently used throughout this thesis.

2.1. Permutations defined by Rational Transformations and Their Cycle Structure

Let

$$R(x) = \frac{ax + b}{cx + d} \in \mathbb{F}_q(x), \quad c \neq 0, \tag{2.1}$$

be a nonconstant rational transformation. As before we define the permutation of $\mathbb{F}_q$ related to (2.1) as

$$F(x) = \begin{cases} R(x) & \text{if } x \neq \frac{-d}{c}, \\ \frac{a}{c} & \text{if } x = \frac{-d}{c}. \end{cases} \tag{2.2}$$

In this section, the cycle structure of this particular permutation will be considered. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

denote the matrix in $GL(2,q)$ associated with $R(x)$ in (2.1) (and at the same time with $F(x)$ in (2.2)). The cycle decomposition of the permutation F is closely related to the properties of the characteristic polynomial $f(x) = x^2 - \mathrm{tr}(A)x + \det(A)$ of the matrix A.

We define two sequences (A_n) and (B_n) over $\mathbb{F}_q$ recursively by using the matrix A,

$$\begin{pmatrix} A_{n+1} \\ B_{n+1} \end{pmatrix} = A \begin{pmatrix} A_n \\ B_n \end{pmatrix}, \quad A_0 = s_0, \;\; B_0 = 1, \tag{2.3}$$

for $s_0 \in \mathbb{F}_q$. Putting $s_n = F^n(s_0)$, $n \geq 0$, we observe that $s_n = A_n/B_n$ if $B_m \neq 0$ for $0 \leq m \leq n$, and $s_n = A_{n+1}/B_{n+1}$ if $B_m \neq 0$ for $0 \leq m \leq n-1$ and $B_n = 0$. From (2.3), it is easily seen that the sequences (A_n) and (B_n) satisfy

$$A_{n+1} = aA_n + bB_n \qquad \text{and} \qquad B_{n+1} = cA_n + dB_n \tag{2.4}$$

for all $n \geq 1$. Since $c \neq 0$, from the second equation in (2.4), we obtain

$$A_n = \frac{B_{n+1} - dB_n}{c} \tag{2.5}$$

and

$$\frac{A_n}{B_n} = \frac{-d}{c} + \frac{B_{n+1}}{cB_n}.$$

Inserting (2.5) into the first equation of (2.4), a second order recurrence relation is obtained for B_n,

$$B_{n+2} = \mathrm{tr}(A)B_{n+1} - \det(A)B_n$$

for $n \geq 0$ with $B_0 = 1, B_1 = cs_0 + d$. Note that the characteristic polynomial of the recurrence relation (B_n) satisfies, is the same as the characteristic polynomial $f(x) = x^2 - \mathrm{tr}(A)x + \det(A)$ of the matrix A. Suppose that $f(x)$ has roots $\alpha, \beta \in \mathbb{F}_{q^2}$. Solving the recurrence relation for (B_n) yields

$$B_n = \frac{\alpha^{n+1} - \beta^{n+1} + (cs_0 - a)(\alpha^n - \beta^n)}{\alpha - \beta} \tag{2.6}$$

and hence

$$\frac{A_n}{B_n} = -\frac{d}{c} + \frac{\alpha^{n+2} - \beta^{n+2} + (cs_0 - a)(\alpha^{n+1} - \beta^{n+1})}{c[\alpha^{n+1} - \beta^{n+1} + (cs_0 - a)(\alpha^n - \beta^n)]} \tag{2.7}$$

when $B_n \neq 0$ and $\alpha \neq \beta$

$$B_n = ((n+1)\alpha + (cs_0 - a))\,\alpha^{n-1} \tag{2.8}$$

which yields

$$\frac{A_n}{B_n} = -\frac{d}{c} + \frac{(n+2)\alpha^2 + (cs_0 - a)(n+1)\alpha}{c[(n+1)\alpha + (cs_0 - a)n]} \tag{2.9}$$

when $\alpha = \beta$ and $B_n \neq 0$.

The equations (2.7) and (2.9) above can also be expressed in the form

$$\frac{A_n}{B_n} = \frac{(\alpha^{n+1} - \beta^{n+1})s_0 - (\alpha^n - \beta^n)(ds_0 - b)}{\alpha^{n+1} - \beta^{n+1} + (\alpha^n - \beta^n)(cs_0 - a)}, \tag{2.10}$$

$$\frac{A_n}{B_n} = \frac{(n+1)\alpha s_0 - n(ds_0 - b)}{(n+1)\alpha + n(cs_0 - a)}, \tag{2.11}$$

which are sometimes more convenient to use in the following sections.

The result on the cycle decomposition of the permutation (2.2) is presented in the next theorem. In the following, $\mathrm{ord}(z)$ denotes the order of an element z in the multiplicative group of $\mathbb{F}_{q^2}$. Concerning the cycle decomposition of permutations τ of $\mathbb{F}_q$, we use the following notation. Consider a permutation τ of $\mathbb{F}_q$, which can be expressed as a product of disjoint cycles (or which is of the *type*),

$$\tau = \tau_1^{(1)}\ \tau_2^{(1)} \ldots\ \tau_{n_1}^{(1)}\ \tau_1^{(2)}\ \tau_2^{(2)} \ldots\ \tau_{n_2}^{(2)} \ldots \tau_1^{(s)}\ \tau_2^{(s)} \ldots\ \tau_{n_s}^{(s)} \tag{2.12}$$

where each $\tau_j^{(i)}$, $1 \leq j \leq n_i$, is a cycle of length l_i with $l_1 > l_2 > \ldots > l_s \geq 1$ and $n_1 l_1 + n_2 l_2 + \ldots + n_s l_s = q$. The cycle decomposition of a permutation of the type (2.12) will be denoted by

$$\mathcal{T}(\tau) = [n_1 \times l_1, n_2 \times l_2, \ldots, n_s \times l_s]$$

which means that in the cycle decomposition of τ there are n_1 cycles of length ℓ_1, n_2 cycles of length ℓ_2 and finally n_s cycles of length ℓ_s.

Theorem 2.1.1 below, which we express in a slightly generalized form, is essentially given in Theorem 1.2.5. The proof is presented here because it is a bit simpler than that in [8].

Theorem 2.1.1 *Let F be the permutation defined by (2.2), and let $f(x)$ be the characteristic polynomial of the matrix A associated with F. Let $\alpha, \beta \in \mathbb{F}_{q^2}$ be the roots of $f(x)$.*

(i) Suppose $f(x)$ is irreducible. If $k = \mathrm{ord}(\frac{\alpha}{\beta}) = \frac{q+1}{t}$, $1 \le t < \frac{q+1}{2}$, then

$$\mathcal{T}(F) = [(t-1) \times k, 1 \times (k-1)].$$

In particular F is a full cycle if $t = 1$.

(ii) Suppose $\alpha, \beta \in \mathbb{F}_q$ and $\alpha \neq \beta$. If $k = \mathrm{ord}(\frac{\alpha}{\beta}) = \frac{q-1}{t}$, $t \ge 1$, then

$$\mathcal{T}(F) = [(t-1) \times k, 1 \times (k-1), 2 \times 1].$$

(iii) Suppose $f(x) = (x-\alpha)^2$, $\alpha \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, then

$$\mathcal{T}(F) = [(p^{r-1}-1) \times p, 1 \times (p-1), 1 \times 1].$$

Proof: We put $s_n = F^n(s_0)$ for $s_0 \in \mathbb{F}_q$. A fixed point $s_0 \in \mathbb{F}_q$ of $F(x)$, yields a cycle of length one. The equation $s_0 = F(s_0) = (as_0 + b)/(cs_0 + d)$, or equivalently $cs_0^2 + (d-a)s_0 - b = 0$ has two distinct solutions in $\mathbb{F}_q$ if the discriminant $\mathcal{D} = a^2 - 2ad + d^2 + 4bc$ is a nonzero square in $\mathbb{F}_q$. If $\mathcal{D} = 0$ there is only one solution and no solution if $\mathcal{D}$ is a nonsquare in $\mathbb{F}_q$. The term $\mathcal{D}$ is also the discriminant of the characteristic polynomial $f(x) = x^2 - \mathrm{tr}(A)x + \det(A)$ of the matrix A hence there are two cycles of length one if $f(x)$ has two distinct roots in $\mathbb{F}_q$, a cycle of length one if $f(x)$ has a double root, and none if $f(x)$ is irreducible.
For $\alpha \neq \beta$ and $s_0 = a/c$, we have $B_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}$ and equation (2.7) implies

$$\frac{A_n}{B_n} = -\frac{d}{c} + \frac{\alpha^{n+2} - \beta^{n+2}}{c(\alpha^{n+1} - \beta^{n+1})}\,. \tag{2.13}$$

If $\mathrm{ord}(\alpha/\beta) = k$, then $n = k-1$ is the smallest integer such that $B_n = 0$. Using (2.13), we have $s_{k-2} = -d/c$ and hence $s_{k-1} = F(-d/c) = a/c = s_0$. Therefore the cycle containing $s_0 = a/c$ is of length $k-1$.
If s_0 is not in the cycle containing a/c and hence $-d/c$, then from (2.10) it is easily seen that $B_n \neq 0$ and $s_n = A_n/B_n$ for all $n \ge 0$. In order to determine the length of such a cycle, we put $A_n/B_n = s_0$ in (2.7) and, obtain the condition

$$(as_0 + b)(\alpha^n - \beta^n) = s_0(cs_0 + d)(\alpha^n - \beta^n).$$

Therefore we have $n \equiv 0 \bmod k$ and thus the cycle has length k, or $as_0 + b = s_0(cs_0 + d)$ and s_0 is a fixed point of $F(x)$. This completes the proof of (i) and (ii).

In case $\alpha = \beta$ and $s_0 = a/c$, (2.9) yields

$$\frac{A_n}{B_n} = -\frac{d}{c} + \frac{n+2}{c(n+1)}\alpha. \tag{2.14}$$

From (2.14), it is easy to see that the smallest integer satisfying $s_n = -d/c$ is $n = p-2$ and with a similar argument used for the previous case one can also see that the cycle containing $s_0 = a/c$ is of length $p-1$. The only fixed point of F is $s_0 = (a-d)/(2c)$. This completes the proof for the case of a prime field. For $q = p^r$, $r > 1$, suppose that s_0 is not in the cycle of a/c and it is not the fixed point $(a-d)/(2c)$. Then we have $s_n = A_n/B_n$ for all $n \geq 0$, and by setting $A_n/B_n = s_0$ in (2.9) we get

$$(as_0 + b)n = s_0(cs_0 + d)n \Rightarrow n(cs_0^2 + (d-a)s_0 - b) = 0$$

and since s_0 is not the fixed point of $F(x)$, we obtain $n \equiv 0 \bmod p$. □

Remark 2.1.1 *The rational function $R(x)$ with $a = a_2, b = a_0^{-1}, c = 1, d = 0$, gives rise to the permutation $F(x)$ which coincides with $\mathcal{P}_1(x) = \bar{P}_1(x) = a_0x^{q-2} + a_2$. In [8] Chou focuses on this particular permutation which was introduced in Section 1.2. Theorem 2.1.1 gives the cycle structure of the polynomials $\bar{P}_1(x) = (a_0x + a_1)^{q-2} + a_2$ and $P_1(x) = (a_0x + a_1)^{q-2}$ for arbitrary values of a_0, a_1, a_2.*

The following lemma is an enumeration result on the permutations F of the type (2.2). For the rest of the thesis ϕ denotes the Euler ϕ-function.

Lemma 2.1.2 *Let $k > 1$ be a divisor of either $q+1$ or $q-1$. The number of monic quadratic polynomials $f(x) = x^2 - Tx + D \in \mathbb{F}_q[x]$ with two distinct roots $\alpha, \beta \in \mathbb{F}_{q^2}$ and ord$(\alpha/\beta) = k$ is given by $\frac{\phi(k)}{2}(q-1)$.*

Proof:

We have to distinguish two cases. If $f(x)$ is reducible, then first we choose an element $\delta \in \mathbb{F}_q^*$ of order $k|q-1$. There are $\phi(k)$ such elements. Then we choose an arbitrary element $\beta \in \mathbb{F}_q^*$ and set $\alpha = \delta\beta$. The polynomial $f(x) = (x-\alpha)(x-\beta) \in \mathbb{F}_q$ will then have the required properties and the number of these polynomials is $\frac{\phi(k)}{2}(q-1)$.

The number of irreducible polynomials $g(x) = x^2 + Cx + 1 \in \mathbb{F}_q[x]$ of order k is known to be $\phi(k)/2$, see [26, Theorem 3.5]. Suppose $g(\delta) = 0$. The polynomials $f(x) = x^2 - Tx + D = (x-\alpha)(x-\beta) \in \mathbb{F}_q[x]$ with $(T^2/D) - 2 = C$ are exactly the polynomials that satisfy $\alpha/\beta = \delta$ (see [7, Theorem 3]). Since $C \neq -2$, the parameter T can be chosen in $q-1$ different ways and then D is uniquely determined. □

Theorem 2.1.3 *Let F and k be as in Theorem 2.1.1. Suppose $q \geq 5$. The number of distinct permutations F with the given cycle decomposition is equal to $\phi(k)\frac{q-1}{2}q$ in the cases (i) and (ii) of Theorem 2.1.1, and is equal to $(q-1)q$ in the case (iii).*

Proof:

Without loss of generality we can assume that $c = 1$. Note that the matrix A, with fixed characteristic polynomial $f(x) = x^2 - (a+d)x + (ad-b)$, is then uniquely determined by the element $a \in \mathbb{F}_q$. The number of permutations with the given cycle decomposition is the product of the number of polynomials $f(x)$ with the number of choices for $a \in \mathbb{F}_q$. If $f(x)$ has distinct roots, then by Lemma 2.1.2, there are $\phi(k)\frac{q-1}{2}$ choices for the polynomial $f(x)$ where $k|q+1$ or $k|q-1$ according to whether $f(x)$ is irreducible or reducible. Once the characteristic polynomial $f(x)$ is fixed, there are q possible choices for a.

The formula for the case *(iii)* immediately follows from the fact that there are $q-1$ polynomials of the form $f(x) = (x-\alpha)^2$, $\alpha \in \mathbb{F}_q^*$ and q choices for $a \in \mathbb{F}_q$. □

Theorem 2.1.1 plays an important role in our study of the cycle structure of $\mathcal{P}_n$, $n \geq 2$. For $n \geq 1$, the rational transformation $\bar{R}_n(x)$ in (1.9) is of the form $R(x)$ in (2.1) and hence one can associate to it the characteristic polynomial

$$\bar{f}(x) = \bar{f}(n,x) = x^2 - (\alpha_{n+1} + \beta_n)x + \alpha_{n+1}\beta_n - \beta_{n+1}\alpha_n, \tag{2.15}$$

with α_k, β_k, $k \geq 1$, as in (1.10). Then the cycle decomposition of $\bar{F}_n(x)$ follows by Theorem 2.1.1 and one can determine the cycle structure of $\bar{P}_n$ by the use of Lemma 1.5.12 together with the positioning of the poles $x_1, \ldots, x_n$ in the cycles of $\bar{F}_n$. The same method also works for $P_n(x)$ with

$$f(x) = f(n,x) = x^2 - (\alpha_{n-1} + \beta_n)x + \alpha_{n-1}\beta_n - \alpha_n\beta_{n-1}. \tag{2.16}$$

2.2. Cycle Structure of $\mathcal{P}_2(x)$

In this section the cycle structure of the permutation

$$\mathcal{P}_2(x) = ((a_0x + a_1)^{q-2} + a_2)^{q-2} + a_3,\ a_0a_2 \neq 0$$

will be studied. Using the notation of (1.11), we have the poles $x_1 = -\frac{a_1}{a_0},\ x_2 = -\frac{a_1a_2+1}{a_0a_2}$ such that $x_1, x_2 \neq \infty$ and the corresponding rational function becomes

$$\mathcal{R}_2(x) = \frac{a_0(a_2a_3+1)x + a_1(a_2a_3+1) + a_3}{a_0a_2x + a_1a_2 + 1}. \tag{2.17}$$

By (1.12), we have

$$\mathcal{P}_2(x) = (\mathcal{F}_2(x_1)\ \mathcal{F}_2(x_2))\mathcal{F}_2(x) \tag{2.18}$$

with $\mathcal{F}_2(x) = \mathcal{R}_2(x)$ if $x \neq x_2$ and $\mathcal{F}_2(x_2) = (a_2a_3+1)/a_2$. The associated characteristic polynomial becomes

$$\bar{f}(x) = x^2 - (a_0(a_2a_3+1) + a_1a_2 + 1)x + a_0. \tag{2.19}$$

In the following, $\mathcal{C}(\tau, x)$ is used to refer to the cycle of the permutation $\tau \in S_q$ which contains $x \in \mathbb{F}_q$ and $\ell(\tau, x)$ denotes the length of $\mathcal{C}(\tau, x)$. We make the convention that when we write $y = \tau^n(x)$, the exponent n is chosen to be *minimal*.

Lemma 2.2.4 *Let F be a permutation of $\mathbb{F}_q$, $u, v \in \mathbb{F}_q$ and $P = (u\ v)F$ where multiplication is performed from right to left.*

(a) If $u = F^n(v)$ and $\ell(F, v) = l$, then $u \notin \mathcal{C}(P, v)$, $\ell(P, v) = n$ and $\ell(P, u) = l - n$.

(b) If $u \notin \mathcal{C}(F, v)$, $\ell(F, u) = k$ and $\ell(F, v) = l$, then $u \in \mathcal{C}(P, v)$ and $\ell(P, v) = k + l$.

Proof:

(a) Let $t_0 = v$ and $t_j = P^j(t_0)$. Then $t_n = v$, $t_j \neq v$ for $0 < j < n$ and $\ell(P, v) = n$. Hence $t_j \neq u$ for all $j \geq 0$, i.e. $u \notin \mathcal{C}(P, v)$. Let $s_0 = u$ and $s_j = P^j(s_0)$. Then $s_{l-n} = u$ and $s_j \neq u$, $0 < j < l - n$. Consequently, $\ell(P, u) = l - n$.

(b) Let $t_0 = v$ and $t_j = P^j(t_0)$, then we have $t_l = u$, $t_{k+l} = v$ and $t_j \neq v$ for $0 < j < k + l$.

□

First we consider the case where the polynomial in (2.19) has two distinct roots α, β.

Lemma 2.2.5 *Suppose $\bar{f}$ in (2.19) has two distinct roots $\alpha, \beta \in \mathbb{F}_{q^2}$ satisfying ord$(\frac{\alpha}{\beta}) = k$. Let $\gamma_0 = (\beta - 1)/(\alpha - 1) \in \mathbb{P}^1(\mathbb{F}_{q^2})$.*

(a) $x_1 \in \mathcal{C}(\mathcal{F}_2, x_2)$ *if and only if* $\gamma_0^k = 1$.

(b) When (2.19) *is reducible, the pole* x_1 *is a fixed point of* $\mathcal{F}_2$ *if and only if* $a_3 = -a_1/a_0$.

Proof:

(a) From the proof of Theorem 2.1.1, we see that the cycle which contains $\frac{a_2a_3+1}{a_2}$ is of length $k-1$, and (2.10) implies that $s_n = \mathcal{F}_2^n(s_0)$ with $s_0 = \frac{a_2a_3+1}{a_2}$ satisfies

$$s_n = \frac{a_2a_3+1}{a_2} - \frac{\alpha^n - \beta^n}{a_2(\alpha^{n+1} - \beta^{n+1})},\ 0 \le n \le k-2,$$

where $s_{k-2} = x_2$. Since $\mathcal{F}_2(x_1) = a_3$, $x_1 \in \mathcal{C}(\mathcal{F}_2, x_2)$ if and only if

$$a_3 = \mathcal{F}_2(x_1) = s_n = \frac{a_2a_3+1}{a_2} - \frac{\alpha^n - \beta^n}{a_2(\alpha^{n+1} - \beta^{n+1})} \tag{2.20}$$

for some $0 \le n \le k-2$. Equation (2.20) is equivalent to $\alpha^n(\alpha-1) = \beta^n(\beta-1)$ and $\alpha \ne 1$, which is equivalent to $(\frac{\alpha}{\beta})^n = \gamma_0$. Consequently, $x_1 \in \mathcal{C}(\mathcal{F}_2, x_2)$ if and only if $\gamma_0 \in \langle\frac{\alpha}{\beta}\rangle$, or $\gamma_0^k = 1$. We remark here that $\gamma_0 = (\frac{\alpha}{\beta})^n$ holds for some $n \le k-2$, and not for $n = k-1$, since $(\frac{\alpha}{\beta})^{k-1} = \frac{\beta}{\alpha}$.

(b) The second assertion follows immediately by equating $x_1 = \frac{-a_1}{a_0}$ and $\mathcal{F}_2(x_1) = a_3$.

□

The length ℓ_i of a cycle $\tau_j^{(i)}$ in (2.12) depends on the values of some parameters in some cases below and hence the ordering of the ℓ_i's varies. The notation $\underline{\mathcal{T}}(\tau)$ is used when the ordering $\ell_1 > \ldots > \ell_s$ does not necessarily hold.

Theorem 2.2.6 *Suppose that the polynomial* $\bar{f}$ *in* (2.19) *has two distinct roots* $\alpha, \beta \in \mathbb{F}_{q^2}$ *satisfying* $\mathrm{ord}(\frac{\alpha}{\beta}) = k$. *Let* $k = \frac{q+1}{t}$, $1 \le t < (q+1)/2$, *when* $\bar{f}(x)$ *is irreducible and* $k = \frac{q-1}{t}$, $1 \le t \le (q-1)/2$, *for* $\alpha, \beta \in \mathbb{F}_q$. *Put* $\gamma_0 = (\beta-1)/(\alpha-1) \in \mathbb{P}^1(\mathbb{F}_{q^2})$.

1. *If* $\gamma_0^k \ne 1$ *and* $\bar{f}(x)$ *is irreducible, then* $\mathcal{T}(\mathcal{P}_2) = [1 \times (2k-1), (t-2) \times k]$. *In particular* $\mathcal{P}_2$ *is a full cycle if* $k = (q+1)/2$.

2. *If* $\gamma_0^k \ne 1$ *and* $\bar{f}(x)$ *is reducible, then*

   (a) $\mathcal{T}(\mathcal{P}_2) = [1 \times (2k-1), (t-2) \times k, 2 \times 1]$, *when* $a_3 \ne -a_1/a_0$,

   (b) $\mathcal{T}(\mathcal{P}_2) = [t \times k, 1 \times 1]$, *when* $a_3 = -a_1/a_0$.

3. *If* $\gamma_0^k = 1$ *and* $\bar{f}(x)$ *is irreducible, then* $\underline{\mathcal{T}}(\mathcal{P}_2) = [(t-1) \times k, 1 \times n, 1 \times (k-n-1)]$ *for some integer* $1 \leq n \leq k-2$.

4. *If* $\gamma_0^k = 1$ *and* $\bar{f}(x)$ *is reducible, then* $\underline{\mathcal{T}}(\mathcal{P}_2) = [(t-1) \times k, 1 \times n, 1 \times (k-n-1), 2 \times 1]$ *for some integer* $1 \leq n \leq k-2$.

Proof: Equation (2.18) implies that the cycle decomposition of $\mathcal{P}_2(x)$ is the same as the cycle decomposition of $\mathcal{F}_2(x)$ given in Theorem 2.1.1, except for the cycles containing x_1, x_2.

Recall that x_2 is in the unique cycle of $\mathcal{F}_2$ of length $k-1$. Therefore, the cycle decomposition of $\mathcal{P}_2(x)$ is obtained by Lemma 2.2.4 if we know the location of x_1 in the cycle decomposition of $\mathcal{F}_2(x)$. The condition for x_1 to be in the cycle of length $k-1$ is given by Lemma 2.2.5(a) when $\bar{f}(x)$ is reducible, $\mathcal{F}_2$ has two fixed points and Lemma 2.2.5(b) gives the condition for x_1 to be one. The claim for all possible cases then follows immediately. □

Remark 2.2.2 *The exact cycle decomposition of* $\mathcal{P}_2(x)$*, in the cases (3) and (4) of Theorem 2.2.6 is determined by the smallest integer* n *for which* $(\alpha/\beta)^n = \gamma_0$ *is satisfied. Hence one encounters the problem of evaluating a discrete logarithm.*

Theorem 2.2.7 *Suppose that the polynomial* $\bar{f}(x)$ *in (2.19) has a double root* $\alpha \neq 0$.

1. *If* $\alpha = 1$*, then* $a_0 = 1$*,* $a_3 = -a_1/a_0$ *and* $\mathcal{T}(\mathcal{P}_2) = [p^{r-1} \times p\ ]$*. In particular, if* $r = 1$*, then* $\mathcal{P}_2$ *is a full cycle of length* $q = p$.

2. *If* $\alpha \in \mathbb{F}_p \setminus \{1\}$*, then* $\underline{\mathcal{T}}(\mathcal{P}_2) = [(p^{r-1}-1) \times p, 1 \times n, 1 \times p - n - 1, 1 \times 1]$*, where* $n = \alpha/(1-\alpha)$.

3. *If* $r > 1$ *and* $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$*, then* $\mathcal{T}(\mathcal{P}_2) = [1 \times (2p-1), (p^{r-1}-2) \times p, 1 \times 1]$.

Proof: *(1)* If $\bar{f}(x) = (x-1)^2$, from (2.19), it is easily seen that $a_0 = 1$ and $a_3 = -a_1/a_0$. Thus x_1 is a fixed point of $\mathcal{F}_2$ by Lemma 2.2.5(b). The assertion follows by Theorem 2.1.1 and Lemma 2.2.4.

(2) If $x_1 \in \mathcal{C}(\mathcal{F}_2, x_2)$ then by Theorem 2.1.1 and Lemma 2.2.4, the claimed cycle decomposition is obtained. Hence $\mathcal{F}_2(x_1) = a_3$ and $\mathcal{F}_2(x_2) = (a_2a_3 + 1)/a_2$ are in the same cycle. Thus $s_0 = \mathcal{F}_2(x_2)$ would yield $\mathcal{F}_2(x_1) = s_n$ for some $n \geq 1$. Therefore

(2.14) gives the condition

$$a_3 = \frac{a_2a_3+1}{a_2} - \frac{n}{a_2(n+1)\alpha} \text{ or equivalently } \alpha = \frac{n}{n+1}$$

for some $0 \le n \le p-2$. Hence x_1, x_2 are in the same cycle if and only if $\alpha \in \mathbb{F}_p \setminus \{1\}$. Therefore the cycle decomposition above follows with $n = \alpha/(1-\alpha)$.

(3) By using Theorem 2.1.1 and its proof, it is easy to see that in the cycle decomposition of $\mathcal{F}_2$, the possible cycle lengths are $p, p-1, 1$, and $\ell(\mathcal{F}_2, x_1) = p$ if and only if $x_1 \notin \mathcal{C}(\mathcal{F}_2, x_2)$ and x_1 is not a fixed point. From the proofs of *(1)*, *(2)*, one can see that this is equivalent to $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$. In this case, Lemma 2.2.4(b) implies that the cycle of length $p-1$ (containing x_2) and the cycle of length p, which contains x_1, join up to form a cycle of length $2p-1$. □

2.3. Enumeration of PPs of the Form $\mathcal{P}_2(x)$ with Full Cycle

The connection between the permutations $\mathcal{P}_n$ and $\mathcal{F}_n$ brings up the question of whether or not a one-to-one correspondence can be formed between the set of permutations $\mathcal{P}_n$ and specific subsets of the set $\mathcal{S}_R$ of all formal expressions $\mathcal{S}_R = \{R(x) = (ax+b)/(cx+d) : (a,b,c,d) \in \mathbb{F}_q^4\}$.

As expected, there is a one-to-one correspondence only if n is small, namely for $\mathcal{P}_1$, $\mathcal{P}_2$, and P_3. In the case of $P_1(x) = (a_0x+a_1)^{q-2} = F_1(x)$, one needs to consider the subset $\mathcal{S}_R^{(1)} = \{1/(a_0x+a_1) : a_0 \neq 0, a_1 \in \mathbb{F}_q\}$. The identification $a = 1/a_2, b = a_1/(a_0a_2), d = (a_1a_2+1)/(a_0a_2)$ describes a one-to-one correspondence between the set of permutations of the form P_2 and the set of rational transformations $(ax+b)/(x+d)$ with $a \neq 0$. The permutation P_2 is then given by $P_2(x) = ((a_0x+a_1)^{q-2} + a_2)^{q-2} = (a\ 0)\frac{ax+b}{x+d}$, where a, b, d are defined as above.

Proposition 2.3.8 *Let $q > 5$. There is a one-to-one correspondence between the set of permutations of the form $\bar{P}_2$ and the set of the formal expressions $(ax+b)/(cx+d)$ with $c \neq 0$, $ad-bc \neq 0$ and $a-ad+bc \neq 0$.*

Proof:

Equating (2.17) with the formal expression $\frac{ax+b}{cx+d}$, we obtain

$$a = a_0(a_2a_3 + 1), b = a_1(a_2a_3 + 1) + a_3, c = a_0a_2, d = a_1a_2 + 1.$$

Then it follows immediately that $c = a_0a_2 \neq 0$, $a - (ad - bc) = a_0a_2a_3 \neq 0$, and $ad - bc = a_0 \neq 0$. For given a, b, c, d satisfying the above conditions, one gets the unique solution of the above system of equations as

$$a_0 = -D, a_1 = \frac{(1-d)D}{c}, a_2 = -\frac{c}{D} \text{ and } a_3 = \frac{a-D}{c},$$

with $D = ad - bc$. Consider the set $\Delta = \{(a, b, c, d) \in \mathbb{F}_q^4 \mid c \neq 0, ad - bc \neq 0, a - (ad - bc) \neq 0\}$. The cardinality of Δ and the set of all possible expressions for $\bar{P}_2$ is $q(q-1)^3$.

Now that a one-to-one correspondence is established between the set $\mathcal{S}_{\bar{R}}^{(2)} = \{R(x) = (ax + b)/(cx + d) : (a, b, c, d) \in \Delta\}$, and the set $\mathcal{S}_{\bar{P}_2} = \{(((a_0x + a_1)^{q-2} + a_2)^{q-2} + a_3 : a_0a_2a_3 \neq 0\}$, it remains to show that two elements $\bar{P}_2(x) = ((a_0x+a_1)^{q-2}+a_2)^{q-2}+a_3$ and $\bar{P}_2'(x) = ((a_0'x+a_1')^{q-2}+a_2')^{q-2}+a_3'$ of $\mathcal{S}_{\bar{P}_2}$ induce the same permutation if and only if $a_i = a_i'$ for $i = 0, 1, 2, 3$. Clearly, if $\bar{P}_2$ and $\bar{P}_2'$ correspond to rational transformations $\bar{R}_2 \neq \bar{R}_2'$ and $q > 5$, then the permutations are different. Now suppose that $\bar{P}_2$, $\bar{P}_2'$ are mapped to the same rational function (but distinct elements of $\mathcal{S}_{\bar{R}}^{(2)}$), i.e. $\bar{R}_2 = (ax + b)/(cx + d)$ and $\bar{R}_2' = (\epsilon ax + \epsilon b)/(\epsilon cx + \epsilon d)$, $\epsilon \neq 1$, by the injection above. Then the corresponding poles are given by $x_1 = -a_1/a_0 = \frac{1-d}{c}, x_1' = -a_1'/a_0' = \frac{1-\epsilon d}{\epsilon c}$ and $x_2 = x_2' = -b/a$. Hence by (2.18), $\bar{P}_2$ and $\bar{P}_2'$ induce different permutations.

□

The following corollary is an easy consequence of Theorem 2.1.1

Corollary 2.3.9 *The permutation $\mathcal{P}_2$ is a full cycle if and only if*

(1) (i) the polynomial $f(x)$ in (2.19) is irreducible,

(ii) the roots $\alpha, \beta \in \mathbb{F}_{q^2}$ of $f(x)$ satisfy ord$(\alpha/\beta) = (q + 1)/2$,

(iii) $\gamma_0 = (\beta - 1)/(\alpha - 1)$ satisfies $\gamma_0^{(q+1)/2} \neq 1$, or

(2) $\mathbb{F}_q$ is a prime field and $f(x) = (x - 1)^2$ (then $a_0 = 1$, $a_3 = -a_1$).

Proof: In case of *(1)*, Theorem 2.1.1 implies that $\mathcal{F}_2$ is composed of two cycles $\mathcal{C}_1, \mathcal{C}_2$ of lengths $(q+1)/2$ and $(q-1)/2$, respectively. The pole x_2 lies in the cycle $\mathcal{C}_2$. The parameter γ_0 introduced in Lemma 2.2.5 is related to the distribution of the poles, more precisely, $x_1 \in \mathcal{C}_2$ also if and only if $\gamma_0^{(q+1)/2} = 1$. Hence by the condition *(1-iii)* and Lemma 2.2.5(a) $x_1 \in \mathcal{C}_1$, $x_2 \in \mathcal{C}_2$ and (2.18) implies that $\mathcal{C}_1, \mathcal{C}_2$ join together to yield a full cycle.

For the case *(2)*, Theorem 2.1.1 (*iii*) implies that $\mathcal{F}_2$ is composed of a fixed point and a cycle of length $p-1$ which contains x_2. Since $a_0 = 1$, $a_3 = -a_1$, we have x_1 as the fixed point by Lemma 2.2.5(b) and (2.18) implies that the two cycles join up to give $\mathcal{P}_2$, which is a cycle of length p. □

Lemma 2.3.10 *Suppose $f(x) = x^2 - Tx + D \in \mathbb{F}_q[x]$ is irreducible with roots $\alpha, \beta \in \mathbb{F}_{q^2}$, and let $\gamma_0 = (\beta - 1)/(\alpha - 1)$. Then*

(i) $ord(\gamma_0)$ divides $q+1$,

(ii) $\gamma_0 \neq 1$ and $\gamma_0 \neq \beta/\alpha$.

Proof: (*i*) With $\beta = \alpha^q$ and the observation that

$$\gamma_0^{q+1} = \left(\frac{\beta - 1}{\alpha - 1}\right)^{q+1} = \left(\frac{\beta^q - 1}{\alpha^q - 1}\right)\left(\frac{\beta - 1}{\alpha - 1}\right) = 1,$$

assertion (*i*) follows.
(*ii*) Easily follows from the assumption $\alpha \neq \beta$. □

Theorem 2.3.11 *Let $q > 5$. The number of distinct permutations of the form $\mathcal{P}_2(x) = ((a_0x + a_1)^{q-2} + a_2)^{q-2} + a_3 \in \mathbb{F}_q[x]$ with full cycle is*
$\frac{1}{4}\phi(\frac{q+1}{2})(q+1)q(q-1)$ when $q = p^r$ for a prime p with $r > 1$, and
$\frac{1}{4}\phi(\frac{p+1}{2})(p+1)p(p-1) + p(p-1)$ when $q = p$ is prime.

Proof: We first count those $\mathcal{P}_2$ which satisfy condition *(1)* of Proposition 2.3.9.
We fix a polynomial $g(x) = (x - \delta)(x - \delta^{-1})$ with $\mathrm{ord}(\delta) = (q+1)/2$. Among the $q-1$ polynomials $f_i(x) = x^2 - T_ix + D_i = (x - \alpha_i)(x - \beta_i)$, $i = 1, \ldots, q-1$ with $\alpha_i/\beta_i = \delta$ (see the proof of Lemma 2.1.2), we need to count the ones, which satisfy $ord(\frac{\beta_i - 1}{\alpha_i - 1}) \nmid (q+1)/2$.

We put $\gamma_{0(i)} = \frac{\beta_i - 1}{\alpha_i - 1}$ and show that $\gamma_{0(i)} \neq \gamma_{0(j)}$ for $i \neq j$. If $\gamma_{0(i)} = \gamma_{0(j)}$, then $\alpha_j\beta_i - \alpha_j - \beta_i = \alpha_i\beta_j - \alpha_i - \beta_j$. Multiplying both sides by $\delta = \alpha_i/\beta_i = \alpha_j/\beta_j$ yields

$\alpha_i\delta + \alpha_j = \alpha_j\delta + \alpha_i$ which is equivalent to $\alpha_i(\delta - 1) = \alpha_j(\delta - 1)$. Hence we have $\alpha_i = \alpha_j$ and therefore $\beta_i = \beta_j$, i.e. $i = j$. Consequently, the sets $\tilde{\Gamma} = \{\gamma_{0(i)}, i = 1, \ldots, q-1\}$ and $\Gamma = \{\eta \in \mathbb{F}_{q^2} : \eta^{q+1} = 1, \eta \neq 1, \eta \neq \delta^{-1}\}$ are the same by Lemma 2.3.10. The cardinality of the set $\Gamma_0 = \{\eta \in \Gamma : ord(\eta) | (q+1)/2\}$ is easily seen to be $(q+1)/2 - 2$ and hence $|\Gamma \setminus \Gamma_0| = (q+1)/2$. Therefore, exactly $(q+1)/2$ polynomials in $\{f_i(x), i = 1, \ldots, q-1\}$ satisfy $\mathrm{ord}(\alpha_i/\beta_i) = \mathrm{ord}(\delta) = (q+1)/2$ and $\gamma_{0(i)}^{(q+1)/2} \neq 1$. Given such a polynomial $f_i(x) = x^2 - T_i x + D_i$, the coefficient a_0 in (2.19) is uniquely determined by $a_0 = D_i$, we have q choices for $a_1 \in \mathbb{F}_q$ and $q-1$ choices for $a_2 \in \mathbb{F}_q^*$. The coefficient a_3 is then uniquely determined by $T = a_0(a_2a_3 + 1) + a_1a_2 + 1$. Since we have $\frac{\phi((q+1)/2)}{2}$ distinct choices for the polynomial $g(x)$, we obtain $\frac{\phi(\frac{q+1}{2})}{2}\frac{q+1}{2}q(q-1)$ for the total number of permutations $\mathcal{P}_2(x)$ with full cycle in case $q = p^r, r > 1$. (Note that here we use the one-to-one correspondence between the parameters (a_0, a_1, a_2, a_3) describing $\mathcal{P}_2$ and permutations induced by them).

For the case that $\mathbb{F}_q = \mathbb{F}_p$ is a prime field we additionally obtain permutations $\mathcal{P}_2$ with a full cycle if $f(x) = (x-1)^2$. As can be seen easily we then have

$$\mathcal{P}_2(x) = ((x + a_1)^{p-2} + a_2)^{p-2} - a_1$$

for some arbitrary $a_1 \in \mathbb{F}_q$ and $a_2 \in \mathbb{F}_q^*$. □

2.4. Cycle Structure of $\mathcal{P}_3(x)$

In this section we determine the cycle structure of the permutations of the form $\mathcal{P}_3(x)$. Recall that $\mathcal{P}_3(x)$ is defined as

$$\mathcal{P}_3(x) = (((a_0x + a_1)^{q-2} + a_2)^{q-2} + a_3)^{q-2} + a_4 \in \mathbb{F}_q[x]$$

with $a_i \neq 0$ for $i = 0, 2, 3$.

We have the poles $x_1 = -\frac{a_1}{a_0}, x_2 = -\frac{a_1a_2+1}{a_0a_2}, x_3 = -\frac{a_1(a_2a_3+1)+a_3}{a_0(a_2a_3+1)}$ by (1.11) and the corresponding rational function $\mathcal{R}_3(x)$ is given by

$$\mathcal{R}_3(x) = \frac{(a_0a_4(a_2a_3 + 1) + a_0a_2)x + a_1a_4(a_2a_3 + 1) + a_3a_4 + a_1a_2 + 1}{a_0(a_2a_3 + 1)x + a_1(a_2a_3 + 1) + a_3}. \qquad (2.21)$$

First, we assume that $a_2a_3+1 \neq 0$ hence $x_3 \in \mathbb{F}_q$. Then the relation between the cycle structure of $\mathcal{P}_3(x)$ and $\mathcal{F}_3(x)$ is given by Lemma 1.5.12 as

$$\mathcal{P}_3(x) = (\mathcal{F}_3(x_2)\mathcal{F}_3(x_1)\mathcal{F}_3(x_3))\mathcal{F}_3(x) \tag{2.22}$$

If $a_2a_3 + 1 = 0$ then the last pole becomes $x_3 = \infty$ and this case will be investigated at the end of this section.

The permutations $P_3(x)$ and $\bar{P}_3(x)$ are both obtained as products of 3-cycles and permutations defined by the rational transformations of the form (2.21) with $a_4 = 0$ and $a_4 \neq 0$, respectively. We study only the cycle structure of the PPs of $\mathbb{F}_q$ of the form

$$P_3(x) = (((a_0x + a_1)^{q-2} + a_2)^{q-2} + a_3)^{q-2}, \quad a_0a_2a_3 \neq 0 \tag{2.23}$$

in this section, since the cycle structure of $\bar{P}_3(x)$ can be obtained by applying the same method. The characteristic polynomial in (2.16) associated with

$$R_3(x) = \frac{a_0a_2x + a_1a_2 + 1}{a_0(a_2a_3+1)x + a_1(a_2a_3+1) + a_3} \tag{2.24}$$

becomes

$$f(x) = x^2 - (a_0a_2 + a_1(a_2a_3+1) + a_3)x - a_0 \tag{2.25}$$

and F_3 denotes the permutation corresponding to R_3.

The following lemmas are needed for the analysis of the cycle decomposition of P_3. The integers n, m which appear in Lemmas 2.4.12, 2.4.13 are again chosen to be minimal.

Lemma 2.4.12 *Let F be a permutation of $\mathbb{F}_q$, $u, v, w \in \mathbb{F}_q$ and $P = (u\ v\ w)F$. Suppose that $u = F^n(w)$ and $\ell(F, w) = l$.*

1. *If $v = F^m(w)$, then*
   (a) u, v, w lie in distinct cycles of P and $\ell(P, u) = l - n$, $\ell(P, v) = n - m$, $\ell(P, w) = m$ if $m < n$,
   (b) u, v, w are in the same cycle of P with length l if $m > n$.

2. *If $v \notin \mathcal{C}(F, w)$ and $\ell(F, v) = k$, then $v \in \mathcal{C}(P, w)$, $u \notin \mathcal{C}(P, w)$ and $\ell(P, w) = k+n$, $\ell(P, u) = l - n$.*

Proof: *(1)* Let $u = F(y_1), v = F(y_2)$ and $w = F(y_3)$, then $P(y_1) = v, P(y_2) = w$ and $P(y_3) = u$. If $m < n$, then $P(x)$ has the following three types of cycles: $(w\ F(w)\ \ldots\ y_2)$, $(v = F^m(w)\ F(v)\ \ldots\ y_1)$ and $(u = F^n(w)\ F(u)\ \ldots\ y_3)$ of lengths m, $n-m$ and $l-n$, respectively.

If $m > n$ then the cycle of $F(x)$ of length l containing u, v, w becomes the cycle

$$(w\ F(w)\ \ldots\ y_1\ v\ F(v)\ \ldots\ y_3\ u\ F(u)\ \ldots\ y_2)$$

of P, again of length l.

For the proof of *(2)*, as in the proof of *(1)*, we assume $u = F(y_1), v = F(y_2)$ and $w = F(y_3)$. Then $P(y_1) = v, P(y_2) = w$ and $P(y_3) = u$ and $P(x)$ has the cycles $(w\ F(w)\ \ldots\ y_1\ v\ \ldots\ y_2)$, $(u = F^n(w)\ \ldots\ y_3)$. □

Remark 2.4.3 *It is possible that both F and P are full cycles. Suppose that F is a full cycle. It follows by Lemma 2.4.12(1.b) that $P = (u\ v\ w)F = (v\ w)(u\ w)F$ is also a full cycle if and only if $m > n$ where $u = F^n(w)$ and $v = F^m(w)$.*

Lemma 2.4.13 *Let u, v, w, F, P be as in Lemma 2.4.12. Suppose that $u \notin \mathcal{C}(F, w)$, $\ell(F, u) = k$ and $\ell(F, w) = l$.*

1. *If $v \notin \mathcal{C}(F, u)$, $v \notin \mathcal{C}(F, w)$ and $\ell(F, v) = j$, then u, v, w are in the same cycle of P, of length $k + l + j$.*

2. *If $v = F^n(u)$, then $u \in \mathcal{C}(P, w)$ with $\ell(P, u) = \ell(P, w) = l + n$ and $v \notin \mathcal{C}(P, w)$ with $\ell(P, v) = k - n$.*

3. *If $v = F^n(w)$, then $v \in \mathcal{C}(P, u)$ with $\ell(P, u) = \ell(P, v) = k + l - n$ and $w \notin \mathcal{C}(P, u)$ with $\ell(P, w) = n$.*

Proof: The proof is very similar to the proof of Lemma 2.4.12 and hence omitted. □

Now we turn our attention to the permutation P_3. By the lemmas given above, it turns out that, for determining the cycle decomposition of P_3, the location of the elements $F_3(x_1), F_3(x_2), F_3(x_3)$, i.e. x_1, x_2, x_3 in the cycles of F_3 relative to each other is of ultimate importance. In the following lemma we consider the problem of locating the poles within the cycles of F_3.

Lemma 2.4.14 *Suppose that the polynomial $f(x)$ in (2.25) has two distinct roots $\alpha, \beta \in \mathbb{F}_{q^2}$ with $\mathrm{ord}(\frac{\alpha}{\beta}) = k$. Let $\gamma_1 = (\beta - a_3)/(\alpha - a_3), \gamma_2 = (a_2\beta + 1)/(a_2\alpha + 1), \gamma_3 = (\beta - a_1)/(\alpha - a_1) \in \mathbb{P}^1(\mathbb{F}_{q^2})$. Then*

(i) $x_1 \in \mathcal{C}(F_3, x_3)$ if and only if $\gamma_1^k = 1$,

(ii) $x_2 \in \mathcal{C}(F_3, x_3)$ if and only if $\gamma_2^k = 1$,

(iii) the poles x_1, x_2, x_3 lie in different cycles of F_3 if and only if $\gamma_1^k \neq 1$, $\gamma_2^k \neq 1$ and $\gamma_3^k \neq 1$.

Proof: Note that for $s_0 = a_2/(a_2a_3 + 1)$, we obtain by (2.10) that

$$s_n = \frac{1}{a_2a_3 + 1}\left(a_2 + \frac{\alpha^n - \beta^n}{\alpha^{n+1} - \beta^{n+1}}\right),\ 0 \leq n \leq k - 2. \tag{2.26}$$

Recall that x_3 is in the cycle of length $k - 1$ by the proof of Theorem 2.1.1.
(i) Obviously $F_3(x_3) = \frac{a_2}{a_2a_3+1}$ is in the cycle of length $k - 1$. Consequently by (2.26), the pole $x_1 = -\frac{a_1}{a_0}$ is contained in this cycle if and only if

$$x_1 = \frac{1}{a_2a_3 + 1}\left(a_2 + \frac{\alpha^n - \beta^n}{\alpha^{n+1} - \beta^{n+1}}\right),$$

for some $0 \leq n \leq k - 2$. This is equivalent to

$$\begin{aligned} \alpha^n(a_0 + (a_1a_2a_3 + a_1 + a_0a_2)\alpha) - \beta^n(a_0 + (a_1a_2a_3 + a_1 + a_0a_2)\beta) &= 0 \\ \alpha^n(-\alpha\beta + (\alpha + \beta - a_3)\alpha) - \beta^n(-\alpha\beta + (\alpha + \beta - a_3)\beta) &= 0 \end{aligned}$$

and

$$\alpha^{n+1}(\alpha - a_3) = \beta^{n+1}(\beta - a_3) \ \text{ and } \ \alpha \neq a_3$$

for some $0 \leq n \leq k - 2$. This implies $(\alpha/\beta)^n = (\beta - a_3)/(\alpha - a_3)$ for $1 \leq n \leq k - 1$ and so $\frac{\beta - a_3}{\alpha - a_3} \in \left\langle \frac{\alpha}{\beta} \right\rangle$, hence $(\frac{\beta - a_3}{\alpha - a_3})^k = 1$.
(ii) can be obtained similarly from the condition

$$x_2 = \frac{1}{a_2a_3 + 1}\left(a_2 + \frac{\alpha^n - \beta^n}{\alpha^{n+1} - \beta^{n+1}}\right)$$

for some $0 \leq n \leq k - 2$.
(iii) If $\gamma_1^k, \gamma_2^k \neq 1$ then neither x_1, nor x_2 is in the cycle of length $k - 1$. Now we note that $F_3(x_2) = 0$ and $F_3(x_1) = 1/a_3$. Consequently, $x_1 \in \mathcal{C}(F_3, x_2)$ if and only if $1/a_3 = F_3^n(0)$ for some $0 \leq n \leq k - 1$. With (2.10) we get

$$\frac{(a_1a_2 + 1)(\alpha^n - \beta^n)}{(\alpha^{n+1} - \beta^{n+1}) - a_0a_2(\alpha^n - \beta^n)} = \frac{1}{a_3}$$

for some $0 \leq n \leq k-1$, which is equivalent to

$$(\frac{\alpha}{\beta})^n = \frac{\alpha - a_1}{\beta - a_1} = 1/\gamma_3$$

for some $0 \leq n \leq k-1$. □

Theorem 2.4.15 *Suppose that $f(x)$ in (2.25) is irreducible with roots $\alpha, \beta \in \mathbb{F}_{q^2}$. Let $k = \mathrm{ord}(\frac{\alpha}{\beta}) = \frac{q+1}{t}$, $1 \leq t < \frac{q+1}{2}$, and $\gamma_1 = (\beta - a_3)/(\alpha - a_3), \gamma_2 = (a_2\beta + 1)/(a_2\alpha + 1), \gamma_3 = (\beta - a_1)/(\alpha - a_1)$.*

(1) If $\gamma_1^k = \gamma_2^k = 1$ then

(a) $\mathcal{T}(P_3) = [(t-1) \times k, 1 \times (k-1)\,]$, in particular P_3 is a full cycle if $k = q+1$, or

(b) $\underline{\mathcal{T}}(P_3) = [(t-1) \times k, 1 \times m, 1 \times (k-n-1), 1 \times (n-m)]$

for some integers $1 \leq m < n \leq k-2$.

(2) If $\gamma_1^k \neq 1$ and $\gamma_2^k = 1$ then $\mathcal{T}(P_3) = [1 \times (k+n), (t-2) \times k, 1 \times (k-n-1)]$ for some integer $1 \leq n \leq k-2$.

(3) If $\gamma_1^k, \gamma_2^k, \gamma_3^k \neq 1$ then $\mathcal{T}(P_3) = [1 \times (3k-1), (t-3) \times k]$. In particular P_3 is a full cycle if 3 divides $q+1$ and $k = (q+1)/3$.

(4) If $\gamma_1^k, \gamma_2^k \neq 1$ and $\gamma_3^k = 1$ then $\mathcal{T}(P_3) = [1 \times (k+n-1), (t-2) \times k, 1 \times (k-n)]$ for some integer $1 \leq n \leq k-1$.

(5) If $\gamma_1^k = 1$ and $\gamma_2^k \neq 1$ then $\mathcal{T}(P_3) = [1 \times (2k-n-1), (t-2) \times k, 1 \times n]$ for some integer $1 \leq n \leq k-2$.

Proof: If we put $u = F_3(x_2), v = F_3(x_1)$ and $w = F_3(x_3)$, and recall that $P_3(x) = (F_3(x_2)\ F_3(x_1)\ F_3(x_3))F_3(x)$, then the theorem follows from Lemmas 2.4.12, 2.4.13, 2.4.14, and Theorem 2.1.1 on the cycle decomposition of $F_3(x)$. □

Remark 2.4.4 *The exact values for the parameters m and n are given by the relative positions of the three poles when they are in the same cycle of F_3. These relative positions are essentially described by the integers n_i for which we have $\gamma_i = (\alpha/\beta)^{n_i}$, $i = 1, 2, 3$. Their identification, as in the case of $\mathcal{P}_2$, requires the evaluation of discrete logarithms.*

If $f(x)$ is reducible over $\mathbb{F}_q$, then F_3 has fixed points, i.e. cycles of length one, which have to be taken into consideration. F_3 has two fixed points when the roots of $f(x)$ are distinct and has only one fixed point when $f(x)$ has a double root.

Lemma 2.4.16 *Suppose that $f(x)$ in (2.25) is reducible over $\mathbb{F}_q$. Then*

(i) the pole x_1 is a fixed point of $F_3(x)$ if and only if $a_3 = -\frac{a_0}{a_1}$,

(ii) the pole x_2 is a fixed point of $F_3(x)$ if and only if $a_2 = -\frac{1}{a_1}$.

Proof: The pole x_1 is a fixed point of $F_3(x)$ if and only if $-\frac{a_1}{a_0} = \frac{1}{a_3} = F_3(x_1)$. Hence the condition in part (i) follows. $F_3(x_2) = 0$ and hence x_2 is a fixed point of $F_3(x)$ if and only if $-\frac{a_1a_2+1}{a_0a_2} = 0$. □

Remark 2.4.5 *Suppose that $f(x)$ in (2.25) has distinct roots $\alpha, \beta \in \mathbb{F}_q$ and γ_1, γ_2 are as in Lemma 2.4.14. For $i = 1, 2$, $\gamma_i^k \neq 1$ when x_i is not a fixed point. The pole x_3, which is always in the cycle of F_3 of length $k-1$, is not a fixed point of F_3 unless $k = 2$.*

Theorem 2.4.17 *Suppose that $f(x)$ in (2.25) has two distinct roots $\alpha, \beta \in \mathbb{F}_q$. Let $k = \mathrm{ord}(\frac{\alpha}{\beta}) = \frac{q-1}{t}$, $1 \leq t \leq \frac{q-1}{2}$, and $\gamma_1 = (\beta - a_3)/(\alpha - a_3), \gamma_2 = (a_2\beta + 1)/(a_2\alpha + 1), \gamma_3 = (\beta - a_1)/(\alpha - a_1)$, $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{P}^1(\mathbb{F}_q)$.*

(1)-(5) If $a_3 \neq -a_0/a_1$ and $a_2 \neq -1/a_1$, then $\mathcal{T}(P_3)$ is the same as in the cases (1)-(5) of Theorem 2.4.15, except that, in each case P_3 has two more cycles of length 1 (here of course, $k = \frac{q-1}{t}$, not $\frac{q+1}{t}$ as in Theorem 2.4.15).

(6) If $a_3 = -a_0/a_1$ and $a_2 = -1/a_1$, then $\mathcal{T}(P_3) = [1 \times (k+1), (t-1) \times k]$. In particular P_3 is a full cycle if $k = q - 1$.

(7) (a) If $a_3 = -a_0/a_1$ and $\gamma_2^k = 1$ or
(b) if $a_2 = -1/a_1$ and $\gamma_1^k = 1$,
then $\underline{\mathcal{T}}(P_3) = [(t-1) \times k, 1 \times n, 1 \times (k-n), 1 \times 1]$, with $2 \leq n \leq k-1$ in the case of (a) and $1 \leq n \leq k-2$ in the case of (b).

(8) If $a_3 = -a_0/a_1$, $a_2 \neq -1/a_1$, $\gamma_2^k \neq 1$ or $a_3 \neq -a_0/a_1$, $a_2 = -1/a_1$, $\gamma_1^k \neq 1$ then $\mathcal{T}(P_3) = [1 \times 2k, (t-2) \times k, 1 \times 1]$.

Proof: The assertion follows as in the proof of Theorem 2.4.15, by using Lemmas 2.4.12, 2.4.13, 2.4.14, 2.4.16, with $u = F_3(x_2), v = F_3(x_1)$, $w = F_3(x_3)$ and by Theorem 2.1.1. □

Now we focus on the case where the polynomial $f(x)$ in (2.19) has a double root $\alpha \in \mathbb{F}_q^* = \mathbb{F}_{p^r}^*$. We recall that in this case, $\mathcal{T}(F_3) = [(p^{r-1}-1) \times p, 1 \times (p-1), 1 \times 1]$. We will use the following lemma.

Lemma 2.4.18 *Suppose that $f(x)$ in (2.25) has a double root $\alpha \in \mathbb{F}_q^*$. Then*

(i) $x_1 \in \mathcal{C}(F_3, x_3)$ if and only if $\alpha/a_3 \in \mathbb{F}_p \setminus \{1\}$,

(ii) $x_2 \in \mathcal{C}(F_3, x_3)$ if and only if $-a_2\alpha \in \mathbb{F}_p \setminus \{1\}$,

(iii) $x_1 \in \mathcal{C}(F_3, x_2)$ if and only if $a_1/\alpha \in \mathbb{F}_p \setminus \{1\}$.

Proof: For $s_0 = a_2/(a_2a_3+1)$, the equation (2.11) can be written as

$$\frac{A_n}{B_n} = \frac{1}{a_2a_3+1}\left(a_2 + \frac{n}{\alpha(n+1)}\right) = \frac{1}{a_0(a_2a_3+1)}\left(a_0a_2 - \alpha\frac{n}{n+1}\right). \tag{2.27}$$

If we set $s_n = F_3^n(s_0)$, then $s_n = \frac{A_n}{B_n}$ in (2.27) for $n = 0, 1, \ldots, p-2$.

(i) From (2.27) we obtain that x_1 is in the cycle of length $p-1$, i.e. in the cycle that contains x_3, if and only if

$$F_3(x_1) = \frac{1}{a_3} = \frac{a_2}{a_2a_3+1} + \frac{n}{(n+1)\alpha}\cdot\frac{1}{a_2a_3+1} \quad \text{or} \quad \frac{n}{n+1} = \frac{\alpha}{a_3}$$

for some $0 \le n \le p-2$. This is equivalent to $\alpha/a_3 \in \mathbb{F}_p \setminus \{1\}$.

(ii) The analogous condition for x_2 is

$$F_3(x_2) = 0 = \frac{a_2}{a_2a_3+1} + \frac{n}{(n+1)\alpha}\cdot\frac{1}{a_2a_3+1} \quad \text{or} \quad \frac{n}{n+1} = -a_2\alpha.$$

(iii) Since $F_3(x_2) = 0$ and $F_3(x_1) = 1/a_3$, one can obtain the condition for x_1, x_2 to be in the same cycle, by setting $s_0 = 0$ in (2.11). This yields

$$\frac{1}{a_3} = \frac{(a_1a_2+1)n}{(n+1)\alpha - a_0a_2n} \quad \text{or} \quad na_1 = \alpha(n-1)$$

for some $1 \le n \le p-1$. □

Remark 2.4.6 *If $r = 1$, $\mathbb{F}_q$ is a prime field, then $\alpha = a_3$ if and only if x_1 is a fixed point of $F_3(x)$ and hence by Lemma 2.4.16, $a_3 = -a_0/a_1$. Similarly $\alpha = -1/a_2$ implies that*

x_2 is a fixed point and $a_2 = -1/a_1$. Using $\alpha^2 = -a_0$ and $2\alpha = a_0a_2 + a_1(a_2a_3+1) + a_3$, it can be shown that these equivalences also hold if $\mathbb{F}_q$ is not a prime field. Consequently $\ell(F_3, x_1) = p$ if and only if $\alpha/a_3 \in \mathbb{F}_q \backslash \mathbb{F}_p$ and $\ell(F_3, x_2) = p$ if and only if $-a_2\alpha \in \mathbb{F}_q \backslash \mathbb{F}_p$. Moreover one easily obtains that $\alpha = a_1$ implies that either x_1 or x_2 is fixed point of $F_3(x)$.

Theorem 2.4.19 *Suppose that $f(x)$ in (2.25) has a double root $\alpha \in \mathbb{F}_q^* = \mathbb{F}_{p^r}^*$.*

(1) If $\alpha/a_3 \in \mathbb{F}_p \setminus \{1\}$ and $-a_2\alpha \in \mathbb{F}_p \setminus \{1\}$ then
(a) $\mathcal{T}(P_3) = [(p^{r-1}-1) \times p, 1 \times (p-1), 1 \times 1]$, or
(b) $\underline{\mathcal{T}}(P_3) = [(p^{r-1}-1) \times p, 1 \times m, 1 \times (p-n-1), 1 \times (n-m), 1 \times 1]$ for some integers $1 \le m < n \le p-2$.

(2) If $\alpha = -1/a_2$ and $\alpha/a_3 \in \mathbb{F}_p \setminus \{1\}$, or $\alpha = a_3$ and $-a_2\alpha \in \mathbb{F}_p \setminus \{1\}$, then $\mathcal{T}(P_3) = [(p^{r-1}-1) \times p, 1 \times n, 1 \times (p-n)]$ for some integer $1 \le n \le p-2$ in the first case and $2 \le n \le p-1$ in the second case.

(3) If $r \ge 2$, $\alpha/a_3 \in \mathbb{F}_p \setminus \{1\}$ and $-a_2\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$ then
$\mathcal{T}(P_3) = [1 \times (2p-n-1), (p^{r-1}-2) \times p, 1 \times n, 1 \times 1]$ for some integer $1 \le n \le p-2$.

(4) If $r \ge 2$, $\alpha/a_3 \in \mathbb{F}_q \setminus \mathbb{F}_p$ and $-a_2\alpha \in \mathbb{F}_p \setminus \{1\}$ then
$\mathcal{T}(P_3) = [1 \times (p+n), (p^{r-1}-2) \times p, 1 \times (p-n-1), 1 \times 1]$ for some integer $1 \le n \le p-2$.

(5) If $r \ge 2$, and $\alpha = a_3$ and $-a_2\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$, or $\alpha/a_3 \in \mathbb{F}_q \setminus \mathbb{F}_p$ and $\alpha = -1/a_2$, then
$\mathcal{T}(P_3) = [1 \times 2p, (p^{r-1}-2) \times p]$.

(6) If $r \ge 2$, $-a_2\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$ and $a_1/\alpha \in \mathbb{F}_p \setminus \{1\}$ or $a_1 = 0$, then
$\underline{\mathcal{T}}(P_3) = [(p^{r-1}-2) \times p, 1 \times (p+n-1), 1 \times (p-n), 1 \times 1]$ for some integer $1 \le n \le p-1$.

(7) If $r \ge 2$, $\alpha/a_3 \in \mathbb{F}_q \setminus \mathbb{F}_p$, $-a_2\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$, $a_1/\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$ and $a_1 \ne 0$, then
$\mathcal{T}(P_3) = [1 \times (3p-1), (p^{r-1}-3) \times p, 1 \times 1]$.

Proof: The theorem follows from Lemmas 2.4.12, 2.4.13, 2.4.16, 2.4.18, the remark thereafter, and Theorem 2.1.1. □

Finally we consider the case where $a_2a_3 + 1 = 0 = \alpha_3$, i.e. $x_3 = \infty$ or equivalently

$$P_3(x) = (((a_0x + a_1)^{q-2} + a_2)^{q-2} - \frac{1}{a_2})^{q-2}. \tag{2.28}$$

The function $R_3(x)$ reduces to the linear polynomial

$$R_3(x) = -a_2(a_0a_2x + a_1a_2 + 1), \tag{2.29}$$

in this case thus $F_3(x) = R_3(x)$ for all $x \in \mathbb{F}_q$. From Equation (2.28) one sees that $P_3(x_1) = 0$ and $P_3(x_2) = -a_2$. Therefore

$$P_3(x) = \begin{cases} F_3(x) & x \neq x_1, x_2 \\ F_3(x_2) = 0 & x = x_1 \\ F_3(x_1) = -a_2 & x = x_2. \end{cases} \tag{2.30}$$

and

$$P_3(x) = (F_3(x_1)\ F_3(x_2))F_3(x) = (-a_2\ 0)F_3(x), \tag{2.31}$$

hence the cycle decomposition of $P_3(x)$ can easily be determined by Lemma 2.2.4. We note that $F_3(x) = ax + b$ is a full cycle when $r = 1$ i.e. $\mathbb{F}_q$ is a prime field, $a = 1$ and $b \neq 0$. If $a \neq 1$ and k is the order of a in $\mathbb{F}_q$, then $F_3(x)$ has one fixed point $\wp = b/(1 - a)$ and $\mathcal{T}(F_3) = [(q - 1)/k \times k, 1 \times 1]$. The following proposition gives the conditions for P_3 to be a full cycle. The cycle decomposition of P_3 in the cases where it is not a full cycle can easily be obtained by an argument, similar to that used previously.

Proposition 2.4.20 *Let* $P_3(x) = (((a_0x + a_1)^{q-2} + a_2)^{q-2} - \frac{1}{a_2})^{q-2}$, $a_0a_2 \neq 0$. *The permutation* P_3 *is a full cycle if and only if* $ord(-a_0a_2^2) = q-1$ *and one of the following holds:* $a_1 = a_0a_2$ *or* $a_1 = -1/a_2$.

Proof: Note that the fixed point $\wp$ of F_3 is equal to x_1 if and only if $a_1 = a_0a_2$ and $\wp$ is equal to x_2 if and only if $a_1 = -1/a_2$. Then the proof follows from Lemma (2.2.4) and the previous paragraph. □

Remark 2.4.7 *Since* $x_3 = \infty$ *yields* $P_3 = (-a_2\ 0)F_3$, *where* F_3 *is a linear function, by putting* $F_3(x) = x$ *(i.e* $a_0 = -1/a_2^2$ *and* $a_1 = -1/a_2$ *in (2.28)) and* $-a_2 = a$ *we get* $P_3(x) = p_a(x)$, *the transposition (1.6), described by Carlitz.*

2.5. Enumeration of Permutations of the form $P_3(x)$ with Full Cycle

In this section we count the number of $P_3(x)$ with full cycle. First we give a result establishing a one-to-one correspondence between $P_3(x)$ and a certain subset of $\mathbb{F}_q^4$ (or formal expressions of the form $(ax+b)/(cx+d)$).

Proposition 2.5.21 *Let $q > 5$. There is a one-to-one correspondence between the set of PPs of the form P_3 and the set of the formal expressions $(ax+b)/(cx+d)$ with $a \neq 0$, $ad-bc \neq 0$ and $c+ad-bc \neq 0$.*

Proof: We put

$$a = a_0a_2, b = a_1a_2 + 1, c = a_0(a_2a_3 + 1), d = a_1(a_2a_3 + 1) + a_3$$

by considering (2.24). Then it immediately follows that $a = a_0a_2 \neq 0$, $c + ad - bc = a_0a_2a_3 \neq 0$, and $ad - bc = -a_0 \neq 0$. For given a, b, c, d satisfying the above conditions, one gets the unique solution of the above system of equations as

$$a_0 = -D, a_1 = \frac{(1-b)D}{a}, a_2 = -\frac{a}{D} \text{ and } a_3 = \frac{c+D}{a},$$

with $D = ad - bc$. Note that the cardinality of the set $\Delta = \{(a, b, c, d) \in \mathbb{F}_q^4 \mid a \neq 0, ad - bc \neq 0, c + ad - bc \neq 0\}$ (and that of the set of possible expressions for P_3) is $q(q-1)^3$.

Now that a one-to-one correspondence is established between the set $\mathcal{S}_R^{(3)} = \{R(x) = (ax+b)/(cx+d) : (a, b, c, d) \in \Delta\}$, and the set $\mathcal{S}_{P_3} = \{(((a_0x+a_1)^{q-2}+a_2)^{q-2}+a_3)^{q-2} : a_0a_2a_3 \neq 0\}$, it remains to show that two elements $P_3(x) = (((a_0x + a_1)^{q-2} + a_2)^{q-2} + a_3)^{q-2}$ and $P_3'(x) = (((a_0'x+a_1')^{q-2}+a_2')^{q-2}+a_3')^{q-2}$ of $\mathcal{S}_{P_3}$ induce the same permutation if and only if $a_i = a_i'$ for $i = 0, 1, 2, 3$. Clearly, if P_3 and P_3' correspond to rational transformations $R_3 \neq R_3'$ and $q > 5$, then the permutations are different. Now suppose that P_3, P_3' are mapped to the same rational function (but distinct elements of $\mathcal{S}_R^{(3)}$), i.e. $R_3 = (ax+b)/(cx+d)$ and $R_3' = (\epsilon ax+\epsilon b)/(\epsilon cx+\epsilon d)$, $\epsilon \neq 1$, by the injection above. Then the corresponding poles are given by $x_1 = -a_1/a_0 = \frac{1-b}{a}, x_1' = -a_1'/a_0' = \frac{1-\epsilon b}{\epsilon a}$ and clearly $x_2 = x_2' = -b/a$ and $x_3 = x_3' = -d/c$ (if $c = 0$, then $x_3 = x_3'$ is the pole at infinity). Hence by (2.22), (2.31), P_3 and P_3' induce different permutations.

□

Remark 2.5.8 *The set of permutations P_3 with $x_3 \neq \infty$, i.e. $a_2a_3+1 \neq 0$, corresponds to the set $\mathcal{S}_R^{(3')} = \{R(x) = (ax+b)/(cx+d) : (a,b,c,d) \in \Delta, c \neq 0\}$, which is of cardinality $q(q-1)^2(q-2)$.*
We emphasize that if $(a_0,a_1,a_2,a_3) \neq (a_0',a_1',a_2',a_3')$, then the permutations induced by P_3, P_3' and also by $\bar{P}_2$, $\bar{P}_2'$, are actually distinct. This is not true anymore for $\bar{P}_3$.

For $u,v \in \mathbb{F}_q^*$, the transposition $(u\ v)$, for instance, can be expressed as $\bar{P}_3$ for both choices of $a_0 = -1/(u-v)^2$, $a_1 = -ua_0$, $a_2 = v-u$, $a_3 = 1/(u-v)$, $a_4 = v$, and $a_0' = a_0$, $a_1' = -va_0$, $a_2' = -a_2$, $a_3' = -a_3$, $a_4' = u$.

The following remark collects all possible full cycle cases for $P_3(x)$ which are given in Theorems 2.4.15, 2.4.17 and Proposition 2.31.

Remark 2.5.9 *The permutation P_3 in (2.23) is a full cycle if and only if one of the following conditions (1)-(4) is satisfied.*

(1) (i) The polynomial $f(x)$ in (2.25) is irreducible,

(ii) the roots $\alpha,\beta \in \mathbb{F}_{q^2}$ of $f(x)$ satisfy ord$(\alpha/\beta) = q+1$ so that F_3 is a full cycle, and

(iii) the pole x_1 lies between the poles x_2, x_3 in the cycle F_3.

(2) (i) The polynomial $f(x)$ in (2.25) is irreducible,

(ii) 3 divides $q+1$, and the roots $\alpha,\beta \in \mathbb{F}_{q^2}$ of $f(x)$ satisfy ord$(\alpha/\beta) = (q+1)/3$, i.e. F_3 is composed of 2 cycles of length $(q+1)/3$ and 1 cycle of length $(q-2)/3$,

(iii) the elements $\gamma_1 = (\beta-a_3)/(\alpha-a_3), \gamma_2 = (a_2\beta+1)/(a_2\alpha+1), \gamma_3 = (\beta-a_1)/(\alpha-a_1) \in \mathbb{F}_{q^2}$ satisfy $\gamma_1^{(q+1)/3}, \gamma_2^{(q+1)/3}, \gamma_3^{(q+1)/3} \neq 1$, i.e. the poles x_1, x_2, x_3 are in distinct cycles of F_3.

(3) (i) The polynomial $f(x)$ in (2.25) has two distinct roots $\alpha,\beta \in \mathbb{F}_q$,

(ii) ord$(\alpha/\beta) = q-1$, i.e. F_3 is composed of one cycle of length $q-2$ and two cycles of length 1,

(iii) $a_2a_3+1 \neq 0$, i.e. the pole x_3 is in $\mathbb{F}_q$,

(iv) $a_3 = -a_0/a_1$ and $a_2 = -1/a_1$, i.e. x_1, x_2 are the fixed points of F_3.

(4) (i) $a_2a_3+1 = 0$, i.e. $F_3(x)$ is linear,

(ii) $ord(-a_0a_2^2) = q-1$, *and*

(iii) either $a_1 = a_0a_2$ *or* $a_2 = -1/a_1$, *i.e. either* x_1 *or* x_2 *is the fixed point of* F_3.

Before we give the results about the number of P_3 with full cycle, we present a lemma on some simple properties of the parameters $\gamma_1, \gamma_2, \gamma_3$ introduced in Theorem 2.4.15.

Lemma 2.5.22 *Suppose* $f(x) = x^2 - Tx + D \in \mathbb{F}_q[x]$ *is irreducible with roots* $\alpha, \beta \in \mathbb{F}_{q^2}$, *and let* γ_i, $i = 1, 2, 3$ *be defined as in Section 2.4. Then*

(i) $ord(\gamma_i)$ *divides* $q+1$ *for* $i = 1, 2, 3$,

(ii) $\gamma_i \neq 1$ *and* $\gamma_i \neq \beta/\alpha$ *for* $i = 1, 2$ *and* $\gamma_3 \neq 1$,

(iii) $\gamma_1 = \gamma_2$ *if and only if* $a_2a_3 + 1 = 0$, *and* $\gamma_2 = \gamma_3$ *if and only if* $a_1a_2 + 1 = 0$.

Proof: (i) With $\beta = \alpha^q$ and the observation that

$$\gamma_1^{q+1} = \left(\frac{\beta - a_3}{\alpha - a_3}\right)^{q+1} = \left(\frac{\beta^q - a_3^q}{\alpha^q - a_3^q}\right)\left(\frac{\beta - a_3}{\alpha - a_3}\right) = 1,$$

the assertion follows for γ_1 and also similarly for γ_2, γ_3.
(ii) Follows from the assumptions $a_2 \neq 0$, $a_3 \neq 0$ and $\alpha \neq \beta$.
(iii) Trivial. □

Theorem 2.5.23 *Let* $q > 5$. *The number of distinct permutations of the form* $P_3(x) = (((a_0x + a_1)^{q-2} + a_2)^{q-2} + a_3)^{q-2} \in \mathbb{F}_q[x]$ *with full cycle is*
$\frac{1}{4}\phi(q+1)(q-1)^2(q-2) + 3\phi(q-1)(q-1)$, *if* $3 \nmid (q+1)$ *and*
$\frac{1}{4}\phi(q+1)(q-1)^2(q-2) + 3\phi(q-1)(q-1) + \frac{1}{9}\phi\left(\frac{q+1}{3}\right)(q-1)(q+1)^2$, *if* $3 \mid (q+1)$.

The proof consists of four parts, corresponding to each condition in Remark 2.5.9.
Proof: We start with case *(1)* of Remark 2.5.9 and fix a polynomial $f(x) = x^2 - Tx + D \in \mathbb{F}_q[x]$ with roots $\alpha, \beta \in \mathbb{F}_{q^2}$ satisfying $ord(\frac{\alpha}{\beta}) = q+1$. Then any associated rational function of the form $R(x) = (ax+b)/(cx+d)$ satisfies $a + d = T$ and $ad - bc = D$. We recall that the corresponding permutation is always a full cycle. This cycle can be expressed as $(s_0\ s_1\ \ldots\ s_{q-1})$ with $s_0 = a/c, s_{q-1} = -d/c = x_3$. Equation (2.10) shows that

$$s_n = \frac{a}{c} - D\frac{\alpha^n - \beta^n}{c(\alpha^{n+1} - \beta^{n+1})}$$

for $0 \leq n \leq q-2$. In order that the pole x_1 lies between x_2 and x_3, we fix a pair of integers (j_1, j_2) with $0 \leq j_2 < j_1 \leq q-2$, and put $s_{j_1} = x_1, s_{j_2} = x_2$. Since $x_1 = -a_1/a_0 = (1-b)/a$ and $x_2 = -b/a$, we have $s_{j_2+1} = R(-b/a) = 0$ and $s_{j_1+1} = R((1-b)/a) = a/(D+c)$. Here we note that $D + c \neq 0$. Consequently we have

$$s_{j_2+1} = 0 = \frac{a}{c} - D\frac{\alpha^{j_2+1} - \beta^{j_2+1}}{c(\alpha^{j_2+2} - \beta^{j_2+2})},$$

which uniquely yields $a = D(\alpha^{j_2+1} - \beta^{j_2+1})/(\alpha^{j_2+2} - \beta^{j_2+2})$. We note that $a \neq 0$, otherwise $\alpha^{j_2+1} = \beta^{j_2+1}$ which contradicts with $\mathrm{ord}(\alpha/\beta) = q+1$. With

$$s_{j_1+1} = \frac{a}{D+c} = \frac{a}{c} - D\frac{\alpha^{j_1+1} - \beta^{j_1+1}}{c(\alpha^{j_1+2} - \beta^{j_1+2})}$$

we obtain

$$c = a((\alpha^{j_1+2} - \beta^{j_1+2})/(\alpha^{j_1+1} - \beta^{j_1+1})) - D.$$

Finally, we get $d = T - a$ and $b = \frac{ad-D}{c}$. Hence with the choice of the characteristic polynomial $f(x)$ and the positions j_1, j_2 for the poles x_1, x_2 in the cycle of F_3, we obtain a, b, c, d uniquely, where $a \neq 0, ad - bc + c \neq 0$, and of course $ad - bc \neq 0$. It is easy to see that different choices of the triples $f(x), j_1, j_2$ give different elements of the set Δ, defined in the proof of Remark 2.5.21. By the same proposition we know that in order to enumerate the set of permutations P_3 satisfying condition *(1)* of Proposition 2.5.9, it is sufficient to count the possible choices for $f(x), j_1, j_2$. But there are $\frac{\phi(q+1)}{2}(q-1)$ choices for f and $(q-1)(q-2)/2$ choices for the pairs (j_1, j_2).

We now turn our attention to the third case of Remark 2.5.9. In this case P_3 is of the form

$$P_3(x) = (((a_0x + a_1)^{q-2} - \frac{1}{a_1})^{q-2} - \frac{a_0}{a_1})^{q-2}, \tag{2.32}$$

and the associated characteristic polynomial is given by

$$f(x) = x^2 - (a_1 - \frac{a_0}{a_1})x - a_0. \tag{2.33}$$

It is sufficient to determine the number of choices for the pair (a_0, a_1), $a_0a_1 \neq 0$, for which the roots α, β of the polynomial (2.33) satisfy $\mathrm{ord}(\alpha/\beta) = q-1$. We recall that there are $\frac{\phi(q-1)(q-1)}{2}$ polynomials $f(x) = x^2 - Tx + D$ with distinct roots α, β satisfying $\mathrm{ord}(\alpha/\beta) = q-1$. For a fixed polynomial $f(x)$ with these properties, a_0 in (2.33) is determined to be $a_0 = -D \neq 0$. With $T = a_1 - \frac{a_0}{a_1}$ we get exactly two nonzero solutions for a_1, namely

$$a_1 = \frac{T \pm \sqrt{T^2 - 4D}}{2}.$$

Clearly T^2-4D is a nonzero square in $\mathbb{F}_q$ since $f(x)$ has two distinct roots in $\mathbb{F}_q$. Thus we have $\phi(q-1)(q-1)$ permutations P_3 of the form (2.32) with a full cycle.

We now consider the fourth case of Remark 2.5.9. First suppose that $a_1 = a_0a_2$, i.e. x_1 is the unique fixed point of the linear function $F_3(x) = R_3(x)$ given in (2.29). Then we require $ord(-a_0a_2^2) = ord(-\frac{a_1^2}{a_0}) = q-1$. For each of the $\phi(q-1)$ choices for $-a_1^2/a_0$ we have $q-1$ choices for a_1. The coefficients a_0 and a_2 are then uniquely determined as nonzero elements of $\mathbb{F}_q$, and hence a_3 is uniquely given by $a_2a_3+1=0$. When x_2 is the fixed point of F_3 we similarly get the same number, $\phi(q-1)(q-1)$.

Therefore in case $a_2a_3+1=0$, the total number of $P_3(x)$ with full cycle is given by $2\phi(q-1)(q-1)$. This completes the proof of the theorem if 3 does not divide $q+1$.

Finally we assume that 3 divides $q+1$ and consider the case *(2)* of Remark 2.5.9. For each of the $\frac{\phi(\frac{q+1}{3})}{2}(q-1)$ distinct irreducible polynomials $f(x) = x^2 - Tx + D = (x-\alpha)(x-\beta)$ with $ord(\frac{\alpha}{\beta}) = \frac{q+1}{3}$ we can determine the number of permutations P_3 as follows. By (2.25) the parameters a_0, a_1, a_2, a_3 satisfy $a_0 = -D$ and $a_0a_2 + a_1(a_2a_3 + 1) + a_3 = T$. We also recall that $a_2a_3 \neq 0$. Hence we have $q-1$ choices for a_2. The parameter a_1 is uniquely determined by

$$a_1 = \frac{T + Da_2 - a_3}{a_2a_3 + 1}, \tag{2.34}$$

if and only if $a_3 \neq -1/a_2$. Consequently, for each f we obtain precisely $(q-1)(q-2)$ possible parameters (a_0, a_1, a_2, a_3), and hence distinct permutations P_3. We therefore have the cardinality of the set S_F of permutations P_3, satisfying the conditions *(2-i, ii)* of Remark 2.5.9:

$$|S_F| = \frac{\phi(\frac{q+1}{3})}{2}(q-1)^2(q-2).$$

We recall that for $P_3 \in S_F$, the permutation F_3 is composed of exactly 3 cycles.
Our aim, of course, is to obtain the cardinality of the set $S = \{P_3 \in S_F : \gamma_i^{(q+1)/3} \neq 1, i = 1,2,3\}$, i.e. we wish to enumerate $P_3 \in S_F$, for which the poles x_1, x_2, x_3 lie in distinct cycles of F_3. For this purpose, we evaluate $|S_F \setminus S|$ by considering the partition:

$$S_F \setminus S = S_{1,3} \cup S_{2,3} \cup S_{1,2} \cup S_{1,2,3}, \tag{2.35}$$

where $S_{i,j}$ is the set referring to the case of the two poles x_i, x_j being in the same cycle of F_3, which does not contain the third pole, $1 \leq i < j \leq 3$. The set $S_{1,2,3}$, obviously refers to the remaining P_3 with all three poles lying in the same cycle of F_3.

In parts *(i)-(iv)* below, we calculate the cardinalities of the four sets in (2.35), partitioning $S_F \setminus S$.

(i): We recall that this case is equivalent with $\gamma_1^{(q+1)/3} = 1$ and $\gamma_2^{(q+1)/3} \neq 1$, which implies $\gamma_3^{(q+1)/3} \neq 1$. Since we have $\gamma_1 \neq 1, \frac{\beta}{\alpha}$ by Lemma 2.5.22, out of the $\frac{q+1}{3}$ elements of $\mathbb{F}_{q^2}$ whose order divides $(q+1)/3$, γ_1 can have only $\frac{q+1}{3} - 2$ values. For each choice of $\gamma_1 = (\beta - a_3)/(\alpha - a_3)$ we uniquely obtain $a_3 = (\alpha\gamma_1 - \beta)/(\gamma_1 - 1)$. Note that a_3 is in fact an element of $\mathbb{F}_q$. Now γ_2 is among the $2(q+1)/3$ elements of $\mathbb{F}_{q^2}$ whose order divides $q+1$ but not $(q+1)/3$. The coefficient a_2 is then uniquely given by $a_2 = (\gamma_2 - 1)/(\beta - \alpha\gamma_2)$, again an element in $\mathbb{F}_q$. Since $a_0 = -D$ is determined by $f(x)$, we finally obtain a_1 by equation (2.34) which is well-defined by Lemma 2.5.22. Therefore $|S_{1,3}| = \tau_1 = \phi(\frac{q+1}{3})(q-1)\frac{(q+1)(q-5)}{9}$.

(ii): This case is essentially the same as (i), with γ_1, γ_2 are interchanged. Hence $|S_{2,3}| = \tau_2 = \tau_1 = \phi(\frac{q+1}{3})(q-1)\frac{(q+1)(q-5)}{9}$.

(iii): This case applies for $\gamma_2^{(q+1)/3} \neq 1$ and $\gamma_3^{(q+1)/3} = 1$. Then $\gamma_1^{(q+1)/3} \neq 1$ follows. Since we only have to exclude $\gamma_3 = 1$, we have $\frac{q-2}{3}$ choices for γ_3, each choice uniquely defines $a_1 = (\alpha\gamma_3 - \beta)/(\gamma_3 - 1) \in \mathbb{F}_q$. For γ_2 we have $2(q+1)/3$ choices, again each choice uniquely determines a_2. From $T = a_0a_2 + a_1(a_2a_3 + 1) + a_3$ we obtain $a_3 = (T - a_1 - a_0a_2)/(a_1a_2 + 1)$ which by Lemma 2.5.22 is well-defined since $\gamma_2 \neq \gamma_3$. Consequently, $|S_{1,2}| = \tau_3 = \phi(\frac{q+1}{3})(q-1)\frac{(q+1)(q-2)}{9}$.

(iv): This is equivalent to $\gamma_1^{(q+1)/3} = \gamma_2^{(q+1)/3} = 1$ and consequently also $\gamma_3^{(q+1)/3} = 1$. Again by choosing γ_1 and γ_2 appropriately we obtain a_3 and a_2, respectively, and then by equation (2.34) we get a_1. Here we need to exclude the possibility $\gamma_2 = \gamma_1$ in order to avoid $a_2a_3 + 1 = 0$. Consequently for each of the $(q-5)/3$ possible choices for γ_1 we have exactly $(q-8)/3$ choices for γ_2. This yields $|S_{1,2,3}| = \tau_4 = \phi(\frac{q+1}{3})\frac{(q-1)(q-5)(q-8)}{18}$.

Finally we can calculate

$$|S| = \frac{\phi(\frac{q+1}{3})}{2}(q-1)^2(q-2) - \sum_{i=1}^{i=4}\tau_i = \phi(\frac{q+1}{3})(q-1)\frac{(q+1)^2}{9},$$

and the proof is complete. □

CHAPTER 3

CONSTRUCTIONS OF P_n WITH FULL CYCLE

In this chapter we consider the construction of permutations P_n with given number of cycles, where we focus on the most interesting case of permutations with full cycle. We first introduce some preliminaries in the first two sections.

3.1. Multiplication by Transpositions

Cohn and Lempel determined the number of distinct cycles obtained by multiplying a single cycle of length m by a sequence of symbol-disjoint transpositions in [11]. Beck generalized this result to arbitrary transpositions in [5]. We use the main results of [5] which will be presented in this section.

We fix a cycle $\tau = (s_0\ s_1\ \ldots\ s_{m-1})$ and consider the set T of transpositions of the set $\{s_0, s_1, \ldots, s_{m-1}\}$. For two transpositions $\sigma_1 = (s_{i_1}\ s_{j_1})$, $\sigma_2 = (s_{i_2}\ s_{j_2}) \in T$ we define $(\sigma_1 \wedge \sigma_2)_\tau = \sigma_1 \wedge \sigma_2$ by

$$\sigma_1 \wedge \sigma_2 = \begin{cases} 1 & \text{if } \sigma_1\sigma_2\tau \text{ is a full cycle,} \\ 0 & \text{if } \sigma_1\sigma_2\tau \text{ is not a full cycle,} \end{cases}$$

where the multiplication, again, is performed from right-to-left. The next definition associates a binary matrix to a sequence $\sigma_1, \sigma_2, \ldots, \sigma_k$ of k transpositions in T (cf. [5]). The *link relation matrix* of the transpositions $\sigma_1, \sigma_2, \ldots, \sigma_k \in T$ is defined to be the binary, symmetric $k \times k$-matrix $L(\sigma_1, \sigma_2, \ldots, \sigma_k) = (L_{ij})$, where

$$L_{ji} = L_{ij} = \sigma_i \wedge \sigma_j \text{ if } 1 \leq i < j \leq k \text{ and } L_{ii} = 0 \text{ for } i = 1, \ldots k.$$

We remark that for the definition of $\wedge$, the ordering of the transpositions is crucial. The following proposition is the main theorem of [5]. As usual null(A) denotes the dimension of the null space of the matrix A.

Proposition 3.1.1 *The number of cycles in the cycle decomposition of* $\sigma_1\sigma_2\ldots\sigma_k\tau$ *is given by* null $(L(\sigma_1,\sigma_2,\ldots,\sigma_k))+1$.

An easy consequence of the above result is that the product $\sigma_1\sigma_2\ldots\sigma_k\tau$ is a full cycle if and only if the matrix $L(\sigma_1,\sigma_2,\ldots,\sigma_k)$ is invertible.

Example 3.1.1 *Lemma 2.4.12(1.b) shows that* $(s_{i_1},s_j)(s_{i_2},s_j)\tau$ *is a full cycle if and only if* $s_j=\tau^k(s_{i_1}), s_j=\tau^m(s_{i_2})$ *and* $m>k$, *in other words,* $\tau=(..s_{i_2}...s_{i_1}...s_j..)$. *In this case we have* $(s_{i_1},s_j)\wedge(s_{i_2},s_j)=1$ *and the corresponding link relation matrix is*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We close this section with some remarks on link relation matrices.

Each link relation matrix has zeros in the main diagonal. We call a binary, symmetric matrix with zero diagonal a *binary symplectic matrix* in accordance with [27, Chapter 15]. From [27, p.436], one can see that there are exactly

$$N(k,k)=2^{\frac{k}{2}(\frac{k}{2}-1)}\prod_{i=1}^{k/2}(2^{k+1-2i}-1)$$

invertible binary symplectic $k\times k$-matrices if k is even and there is none if k is odd.

We define two canonical invertible binary symplectic matrices which we will use in the construction of $P_n(x)$ with full cycle.
For an even integer k, let $K=(K_{ij})$ be the $k\times k$-matrix defined by

$$K_{2t,2t-1}=K_{2t-1,2t}=1,\quad t=1,2,\ldots,k/2$$

and $K_{ij}=0$ for the remaining entries. Then K is in block diagonal form with $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ as blocks. Evidently each row and each column of K contains exactly one nonzero element, and K is invertible. We call this matrix the *canonical invertible symplectic* $k\times k$*-matrix of type I*. Now again for an even integer k, we define another $k\times k$-matrix $M=(M_{ij})$ over $\mathbb{F}_2$ by

$$M_{ij}=1 \text{ if and only if } i+j\leq k+1 \text{ and } i\neq j.$$

Clearly M is an invertible binary symplectic matrix. We call the matrix M the *canonical invertible symplectic $k \times k$-matrix of type II.*

3.2. Link Relation Matrices and Ordering of the Poles

Suppose that for a given $P_n(x)$ the poles defined by (1.11) are distinct elements of $\mathbb{F}_q$. Recall that by Lemma 1.5.12 we have

$$P_n(x) = (F_n(x_{n-1}) \ \dots \ F_n(x_1) \ F_n(x_n))F_n(x),$$

which can also be written as

$$\begin{aligned} P_n(x) &= (F_n(x_1) \ F_n(x_n))(F_n(x_2) \ F_n(x_n)) \dots (F_n(x_{n-1}) \ F_n(x_n))F_n(x) \\ &:= \sigma_1\sigma_2 \dots \sigma_{n-1}F_n(x). \end{aligned} \tag{3.1}$$

If $F_n(x) = \tau$ is a full cycle, then the number of cycles in the cycle decomposition of $P_n(x)$ is determined by the rank of the link relation matrix $L(\sigma_1, \sigma_2, \dots, \sigma_{n-1})$. By the example following the Proposition 3.1.1 we see that $\sigma_{i_1} \wedge \sigma_{i_2} = 1$ for $i_1 < i_2$ if and only if $F_n(x_n) = \tau^k(F_n(x_{i_1})), F_n(x_n) = \tau^m(F(x_{i_2}))$ and $m > k$ or equivalently $x_n = \tau^k(x_{i_1}), x_n = \tau^m(x_{i_2})$ and $m > k$ (where again the exponents k, m are minimal). The ordering of the poles in τ therefore determines the link relation matrix $L(\sigma_1, \sigma_2, \dots, \sigma_{n-1})$. Unfortunately, not all invertible binary symplectic matrices give a proper ordering of the poles for the construction of $P_n(x)$ with full cycle when $F_n(x)$ is a full cycle. In Section 3.5 we deal with the problem of identifying the appropriate matrices for this construction.

Example 3.2.2 *Suppose that n is odd, $\tau = F_n(x)$ is a full cycle and the poles in τ are ordered as follows:*

$$x_2, x_1, x_4, x_3, \dots, x_{2t}, x_{2t-1}, \dots, x_{n-1}, x_{n-2}, x_n.$$

If i is even, then there is no j such that $i < j$ and x_j appears before x_i in τ. Thus the ith row of the link relation matrix L contains only zeros after the main diagonal.

If i is odd, then x_{i+1} is the only pole with larger index that lies before x_i and hence $L_{i,i+1} = 1$ is the only 1 in the ith row after the main diagonal. Therefore this ordering of the poles corresponds to the canonical invertible symplectic $(n-1)\times(n-1)$-matrix of type I.

Example 3.2.3 *For an odd integer n we consider the canonical invertible symplectic $(n-1)\times(n-1)$-matrix M of type II. We regard it as $L(\sigma_1, \sigma_2 \ldots, \sigma_{n-1})$, corresponding to (3.1), and determine the ordering of the poles in $\tau = F_n(x) = (s_0\ s_1 \ldots s_{q-1})$ where $s_{q-1} = x_n$. All entries in the first row are 1 except for M_{11}. Thus the poles $x_i = s_{j_i}$, $2 \le i \le n-1$, all appear before $x_1 = s_{j_1}$, i.e. $j_i < j_1$ for all $2 \le i \le n-1$. For the elements in the second row of M we have $M_{2j} = 1$, $3 \le j \le n-2$, and $M_{2,n-1} = 0$. Thus other than x_1, x_{n-1} is the only pole which lies between x_2 and x_n, i.e. $j_2 < j_{n-1}$ and $j_i < j_2$ for $3 \le i \le n-2$. With a similar argument we see that $x_1, \ldots, x_{i-1}$ and $x_{n-1}, \ldots, x_{n-(i-1)}$ all lie between x_i and x_n, $i = 3, \ldots, (n+1)/2$. Consequently we obtain the ordering*

$$x_{(n+1)/2}, x_{(n-1)/2}, x_{(n+3)/2}, x_{(n-3)/2}, \ldots, x_{n-2}, x_2, x_{n-1}, x_1, x_n$$

of the poles in accordance with the matrix M.

3.3. Constructing P_n with Prescribed Poles

Let $x_1, x_2, \ldots, x_n$ be fixed poles in $\mathbb{F}_q$, not necessarily distinct. Note however that x_i, x_{i+1}, x_{i+2}, $1 \le i \le n-2$, are always distinct.

For the rational function $R_n(x) = (ax+b)/(cx+d)$, associated with P_n, we have $x_n = -d/c$ and $x_{n-1} = -b/a$. Since w.l.o.g. we can put $c = 1$ and thus $d = -x_n$, we have $q-1$ choices for $R_n(x)$. As can be seen below, any one of these possible choices for $R_n(x) = (ax+b)/(x+d) = (\epsilon ax + \epsilon b)/(\epsilon x + \epsilon d)$ uniquely defines $P_n(x)$.
The construction procedure starts with the initial values

$$\alpha_n = \epsilon, \beta_n = \epsilon d, \alpha_{n-1} = \epsilon a, \beta_{n-1} = \epsilon b$$

where $d = -x_n$ and a, b are fixed elements of $\mathbb{F}_q$ such that $x_{n-1} = -b/a$ and ϵ is a variable. By the identity

$$a_i = \frac{\beta_i + x_{i-2}\alpha_i}{\beta_{i-1} + x_{i-2}\alpha_{i-1}}, \quad i = 3, \ldots, n, \tag{3.2}$$

which follows by (1.10) and (1.11), we obtain the unique value for a_n,

$$a_n = \frac{\epsilon d + x_{n-2}\epsilon}{\epsilon b + x_{n-2}\epsilon a} = \frac{d + x_{n-2}}{b + x_{n-2}a}.$$

Then we can express $\alpha_{n-2} = \alpha_n - a_n\alpha_{n-1}$ and $\beta_{n-2} = \beta_n - a_n\beta_{n-1}$, again as multiples of ϵ. Similarly one obtains by the equation (3.2) the exact values for $a_{n-1}, \ldots, a_3$, and values for $\alpha_{n-3}, \beta_{n-3}, \ldots, \alpha_1, \beta_1$ as multiples of ϵ. In the final step a_2, a_1, a_0 and ϵ are calculated:
From $\alpha_0 = 0$, $\beta_0 = 1$ and $\alpha_2 = a_2\alpha_1 + \alpha_0$ we first obtain $a_2 = \alpha_2/\alpha_1$. The identity $\beta_2 = a_2\beta_1 + \beta_0 = a_2\beta_1 + 1$ then yields the value for ϵ. Finally, we have $a_1 = \beta_1$ and $a_0 = \alpha_1$.

Remark 3.3.1 *An obvious modification of this algorithm also works when some $x_i = \infty$, see [3].*

3.4. Constructions of P_n with Full Cycle

In this section we present two constructions of P_n with full cycle. We first consider the case where n is *odd*.
The main idea here is to choose a rational linear transformation $R(x) = R_n(x)$ such that the corresponding permutation $F_n(x)$ is a full cycle, and then to position the poles $x_1, x_2, \ldots, x_{n-1}, x_n$ in this cycle in such a way that the link relation matrix corresponding to the product of transpositions

$$(F_n(x_1)\ F_n(x_n))(F_n(x_2)\ F_n(x_n)) \ldots (F_n(x_{n-1})\ F_n(x_n)) \tag{3.3}$$

is invertible. Proposition 3.1.1 implies in this case that the permutation $P_n(x)$ in (3.1) is a full cycle.

First we choose an irreducible polynomial $f(x) = x^2 - \mathrm{tr}(A)x + \det(A) \in \mathbb{F}_q[x]$, of order $q+1$ to serve as the characteristic polynomial of the matrix A associated with $R(x) = R_n(x) = (ax+b)/(cx+d)$. Theorem 2.1.1 guarantees that the corresponding permutation $F_n(x)$ is a full cycle, i.e. $(s_0 \ \ldots \ s_{q-1})$. It also follows by the proof of Theorem 2.1.1 that the cycle starting with $s_0 = a/c$ satisfies $s_{q-1} = x_n = -d/c$. Now we choose a suitable invertible $(n-1)\times(n-1)$ link relation matrix $L(\sigma_1, \sigma_2, \ldots, \sigma_{n-1})$, which exists since $n-1$ is even. We position the poles $x_1 = s_{j_1}, x_2 = s_{j_2}, \ldots, x_{n-1} = s_{j_{n-1}}, x_n = s_{q-1}$ according to the matrix $L(\sigma_1, \sigma_2, \ldots, \sigma_{n-1})$. We use this ordering to find the matrix A. Since we should have $x_{n-1} = -b/a$, from $F_n(-b/a) = 0$, $x_{n-1} = s_{j_{n-1}}$ and (2.10) we obtain the condition

$$s_{j_{n-1}+1} = \frac{a}{c} - \frac{\det(A)}{c} \cdot \frac{\alpha^{j_{n-1}+1} - \beta^{j_{n-1}+1}}{\alpha^{j_{n-1}+2} - \beta^{j_{n-1}+2}} = 0, \tag{3.4}$$

where $\alpha, \beta \in \mathbb{F}_{q^2}$ are the roots of $f(x)$. The equation (3.4) yields

$$a = \det(A) \cdot \frac{\alpha^{j_{n-1}+1} - \beta^{j_{n-1}+1}}{\alpha^{j_{n-1}+2} - \beta^{j_{n-1}+2}}.$$

We note that $a \in \mathbb{F}_q$. Then $d = \mathrm{tr}(A) - a$, and for each $q-1$ choices of $b \in \mathbb{F}_q^*$ we obtain a unique value for $c = (ad - \det(A))/b$. Now the values $s_0 = a/c$, $s_{j_{n-1}} = x_{n-1} = -b/a$ and $s_{q-1} = x_n = -d/c$ can be evaluated. The values of the remaining poles $x_i = s_{j_i}$, $i = 1, \ldots, n-2$, can be obtained from (2.10) with $s_0 = a/c$, and $P_n(x)$ can then be determined with the procedure described in Section 3.3.

Example 3.4.4 *$q = 11$, $n = 5$:*
We choose the irreducible characteristic polynomial $f(x) = x^2 - 8x + 6$, for which the roots α and $\beta = \alpha^{11}$ satisfy ord$(\alpha/\beta) = q+1 = 12$. We fix the position of the poles as

$$s_1 = x_3, s_4 = x_2, s_6 = x_4, s_8 = x_1$$

where $s_0 = a/c$, $s_{10} = x_5$ and the matrix A is as specified in the construction above. This particular ordering of the poles corresponds to the canonical invertible symplectic 4×4-matrix of type II. From $x_4 = s_6$ we obtain

$$a = \det(A) \cdot \frac{\alpha^7 - \beta^7}{\alpha^8 - \beta^8} = 6$$

and thus $d = 2$. We choose $b = 1$ and calculate $c = (ad - \det(A))/b = 6$. Consequently

$$R(x) = R_5(x) = \frac{6x+1}{6x+2} = \frac{x+2}{x+4}$$

is the rational function associated with our permutation $P_5(x)$. *Therefore* $x_4 = -b/a = 9$, $x_5 = -d/c = 7$ *and with (2.10) for* $s_0 = a/c = 1$, *we obtain* $x_1 = 6, x_2 = 10, x_3 = 5$. *We can now apply the algorithm of Section 3.3 to determine* $P_5(x)$:
As initial values we have

$$\alpha_5 = \epsilon, \beta_5 = 4\epsilon, \alpha_4 = \epsilon, \beta_4 = 2\epsilon.$$

Recursively we obtain

$$a_5 = \frac{\beta_5 + x_3\alpha_5}{\beta_4 + x_3\alpha_4} = 6, \quad \alpha_3 = \alpha_5 - a_5\alpha_4 = 6\epsilon,\ \beta_3 = \beta_5 - a_5\beta_4 = 3\epsilon,$$

$$a_4 = \frac{\beta_4 + x_2\alpha_4}{\beta_3 + x_2\alpha_3} = 7, \quad \alpha_2 = \alpha_4 - a_4\alpha_3 = 3\epsilon,\ \beta_2 = \beta_4 - a_4\beta_3 = 3\epsilon,$$

$$a_3 = \frac{\beta_3 + x_1\alpha_3}{\beta_2 + x_1\alpha_2} = 5, \quad \alpha_1 = \alpha_3 - a_3\alpha_2 = 2\epsilon,\ \beta_1 = \beta_3 - a_3\beta_2 = 10\epsilon.$$

Finally we get $a_2 = \alpha_2/\alpha_1 = 7$, *and the equation* $\beta_2 = a_2\beta_1 + 1$ *yields* $3\epsilon = 7 \cdot 10\epsilon + 1$ *and therefore* $\epsilon = 10$. *Hence* $a_1 = \beta_1 = 1$, $a_0 = \alpha_1 = 9$, *and our permutation* $P_5(x)$, *which is a full cycle, is given by*

$$P_5(x) = (((((9x+1)^9 + 7)^9 + 5)^9 + 7)^9 + 6)^9.$$

Now we consider the case where n is *even*. We choose an irreducible characteristic polynomial $f(x) = x^2 - \mathrm{tr}(A)x + \det(A) \in \mathbb{F}_q[x]$ of order $(q+1)/2$ with roots $\alpha, \beta \in \mathbb{F}_{q^2}$, with the additional property that

$$\left(\frac{\beta - 1}{\alpha - 1}\right)^{(q+1)/2} \neq 1.$$

Accordingly we fix a matrix A and a rational function $R(x) = R_n(x) = (ax+b)/(cx+d)$. By Theorem 2.1.1 and Lemma 2.2.5(a), the associated permutation $F_n(x)$ has one cycle of length $(q-1)/2$ that contains the pole $-d/c$ and one cycle of length $(q+1)/2$ that contains the pole $-b/a$. Since $F_n(-b/a) = 0$ we consider the cycle $\tau = (s_0\ s_1\ \ldots\ s_{(q-1)/2})$, where $s_0 = 0$ and $s_{q-1/2} = -b/a$. We choose an appropriate invertible $(n-2) \times (n-2)$ link relation matrix that we correspond to the product of transpositions

$$(F_n(x_1)\ F_n(x_{n-1}))(F_n(x_2)\ F_n(x_{n-1}))\ldots(F_n(x_{n-2})\ F_n(x_{n-1})).$$

According to this link relation matrix we choose the positions of the poles $x_1 = s_{j_1}, x_2 = s_{j_2}, \ldots, x_{n-2} = s_{j_{n-2}}$, all in the cycle τ. The values for the poles $x_1 = s_{j_1}, x_2 =$

$s_{j_2}, \ldots, x_{n-2} = s_{j_{n-2}}$ can be calculated by the equation (2.10) with $s_0 = 0$. The permutation $P_n(x)$ is then obtained by the procedure described in Section 3.3.

We note that we can write

$$P_n(x) = (F_n(x_1)\ F_n(x_n))(F_n(x_2)\ F_n(x_n)) \ldots (F_n(x_{n-1})\ F_n(x_n))F_n(x)$$

$$= (F_n(x_{n-1})\ F_n(x_n))(F_n(x_1)\ F_n(x_{n-1}))(F_n(x_2)\ F_n(x_{n-1})) \ldots (F_n(x_{n-2})\ F_n(x_{n-1}))F_n(x)$$

$$:= \tau_n\tau_1\tau_2 \ldots \tau_{n-2}F_n(x).$$

With our choice of the poles, the transpositions $\tau_1, \ldots, \tau_{n-2}$ only act on the cycle τ containing $x_{n-1} = -b/a$. Since we chose the corresponding link relation matrix to be invertible, by Proposition 3.1.1 the product of these transpositions transform the cycle of length $(q+1)/2$ into another cycle of length $(q+1)/2$. The cycle of length $(q-1)/2$ is unchanged. The last transposition $\tau_n = (F_n(x_{n-1})\ F_n(x_n))$ joins up the two cycles, resulting in the full cycle $P_n(x)$.

Example 3.4.5 *$q = 17$, $n = 6$:*
The roots α, β of the irreducible polynomial $x^2 + x + 8$ satisfy ord$(\alpha/\beta) = (q+1)/2 = 9$ and $((\beta - 1)/(\alpha - 1))^9 = 6(\alpha + 1) \neq 1$. We choose the corresponding rational function $R(x) = R_6(x) = (x + 7)/(x + 15)$, which yields the poles $x_6 = 2$ and $x_5 = 10$. The associated permutation $F_6(x)$ has then a cycle of length 9 of the form $(s_0, s_1, \ldots, s_8)$ with $s_0 = 0$ and $s_8 = x_5 = 10$. We choose the remaining poles to be

$$s_1 = x_2, s_3 = x_1, s_4 = x_4, s_6 = x_3$$

which corresponds to the canonical invertible symplectic 4×4-matrix of type I. By (2.10), for $s_0 = 0$ we obtain $x_1 = 14, x_2 = 5, x_3 = 15$ and $x_4 = 6$. Applying the algorithm of Section 3.3 we obtain

$$P_6(x) = ((((((4x + 12)^{15} + 9)^{15} + 10)^{15} + 3)^{15} + 5)^{15} + 16)^{15},$$

which is the full cycle $(1, 9, 12, 7, 13, 8, 11, 2, 0, 5, 6, 3, 10, 16, 15, 4, 14)$.

3.5. Matrices, which are Suitable for Construction of Permutations with Full Cycle

Given a polynomial $f(x) = x^2 - \mathrm{tr}(A)x + \det(A) \in \mathbb{F}_q[x]$ of order $q+1$ and an invertible binary symplectic matrix, can we always choose an ordering of poles $x_1, x_2, \ldots, x_n$ in the cycle of $F(x)$ which allows a construction of $P_n(x)$ with a full cycle as in Section 3.4? The answer is "no". In this section we will characterize the matrices which enable such a construction.

Recall that for the $(n-1) \times (n-1)$ link relation matrix $L(\sigma_1, \ldots, \sigma_{n-1}) = (\ell_{ij})$, we have

$$\ell_{ij} = \begin{cases} 1 & \text{if } x_n = F_n^k(x_i), x_n = F_n^m(x_j) \text{ with } m > k, \\ 0 & \text{if } x_n = F_n^k(x_i), x_n = F_n^m(x_j) \text{ with } m < k, \end{cases}$$

for any $1 \leq i < j \leq n-1$. We remark here that $x_n = F_n^k(x_i)$ always means that k is the minimal number satisfying this equality. We arrange the elements in the full cycle $F_n(x)$ so that the pole x_n is the last element of the cycle.

The invertible binary symplectic matrices which are not suitable for the construction of $P_n(x)$ with full cycle are characterized in the following proposition.

Proposition 3.5.2 *Let n be an odd integer and L be an $(n-1) \times (n-1)$ invertible binary symplectic matrix. L does not correspond to an ordering of poles $x_1, \ldots, x_n$ in a cycle if and only if for some integers i, j, k with $1 \leq i < j < k \leq n-1$ we have $l_{ij} = 0, l_{ik} = 1, l_{jk} = 0$ or $l_{ij} = 1, l_{ik} = 0, l_{jk} = 1$.*

Proof: Suppose L satisfies $l_{ij} = 0, l_{ik} = 1, l_{jk} = 0$ for some integers $1 \leq i < j < k \leq n-1$. From $l_{ij} = 0$, we see that the poles are arranged in the order $\ldots, x_i, \ldots, x_j, \ldots, x_n$ and since $l_{ik} = 1$ the poles x_i, x_k, x_n will be ordered as $\ldots, x_k, \ldots, x_i, \ldots, x_n$. Hence we have the ordering $\ldots, x_k, \ldots, x_i, \ldots, x_j, \ldots, x_n$ which contradicts to the entry $l_{jk} = 0$. For the other case we have $l_{ij} = 1, l_{ik} = 0, l_{jk} = 1$. The poles are ordered as $\ldots, x_j, \ldots, x_i, \ldots, x_n$ since $l_{ij} = 1$ and $l_{ik} = 0$ implies $\ldots, x_i, \ldots, x_k, \ldots, x_n$ which

gives $\ldots, x_j, \ldots, x_i, \ldots, x_k, \ldots, x_n$. On the other hand $x_{jk} = 1$ yields the ordering $\ldots, x_k, \ldots, x_j, \ldots, x_n$ which is a contradiction.

There are $2^3 = 8$ choices for the entries l_{ij}, l_{ik}, l_{jk} for $1 \leq i < j < k \leq n-1$ but the number of permutations of the poles x_i, x_j, x_k, x_n is $3! = 6$ with x_n always located at the end. This shows us that there are only two cases given by the proposition which do not correspond to an ordering of the poles. □

Some Examples: The following 4×4 matrices are types of invertible binary symplectic matrices which can not be used to order the poles $x_1, \ldots, x_5$.

$$K = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad L = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

For the first matrix we have $k_{12} = 0, k_{13} = 1, k_{23} = 0$, for the second matrix $l_{12} = 0, l_{14} = 1, l_{24} = 0$ and for the third matrix $m_{12} = 1, m_{13} = 0, m_{23} = 1$.

In the following part we present some examples of $(n-1) \times (n-1)$ invertible binary symplectic matrices which are suitable for the construction of $P_n(x)$ with full cycle when n is an odd integer. The first two types of matrices are actually the invertible binary symplectic matrices introduced in Section 3.1.

TYPE 1

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Corresponding ordering of the poles:

$x_2, x_1, x_4, x_3, ..., x_{2t}, x_{2t-1}, ..., x_{n-1}, x_{n-2}, x_n,$ for all $3 \leq t \leq (n-3)/2$.

TYPE 2

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Corresponding ordering of the poles:

$x_{(n+1)/2}, x_{(n-1)/2}, x_{(n+3)/2}, x_{(n-3)/2}, ..., x_{n-2}, x_{(2}, x_{n-1}, x_1, x_n.$

TYPE 3

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Corresponding ordering of the poles:

$x_{n-2}, x_2, x_{n-3}, x_3, ..., x_{(n+1)/2}, x_{(n-1)/2}, x_{n-1}, x_1, x_n.$

TYPE 4

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Corresponding ordering of the poles:

$x_{n-1}, x_1, x_{n-2}, x_2, ..., x_{(n+1)/2}, x_{(n-1)/2}, x_n.$

TYPE 5

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Corresponding ordering of the poles:

$x_2, x_4, ..., x_{n-1}, x_1, x_3, ...x_{n-2}, x_n$.

TYPE 6

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Corresponding ordering of the poles:

$x_{n-1}, x_{n-2}, x_{n-3}, ..., x_3, x_2, x_1, x_n$.

TYPE 7

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Corresponding ordering of the poles:

$x_2, x_{n-1}, x_3, x_{n-2}, ..., x_{(n+3)/2}, x_{(n+1)/2}, x_1, x_n$.

TYPE 8

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Corresponding ordering of the poles:

$x_{(n+1)/2}, x_1, x_{(n+3)/2}, x_2, ..., x_{n-2}, x_{(n-1)/2}, x_n.$

TYPE 9

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Corresponding ordering of the poles:

$x_{n-1}, x_{n-3}, ..., x_4, x_2, x_1, x_3, ..., x_{n-2}, x_n.$

CHAPTER 4

PERMUTATIONS ASSOCIATED WITH GENERALIZED FIBONACCI SEQUENCES

Let p be an odd prime and $q = p^r$ where $r \geq 1$. In this chapter we consider the PPs of the form (1.8) with $a_0 = 1, a_{n+1} = 0$ and $a_i = a$ for all $1 \leq i \leq n$ where $a \in \mathbb{F}_q^*$. Consequently, our PPs are of the form

$$P_{a,n}(x) = (\ldots((x+a)^{q-2}+a)^{q-2}\ldots+a)^{q-2} \in \mathbb{F}_q[x]. \tag{4.1}$$

One can see immediately that $R_{a,n}(x)$ takes the form

$$R_{a,n}(x) = a + 1/(a + 1/(\ldots + a + 1/(x+a)\ldots)),$$

and hence the connection of $P_{a,n}(x)$ to the generalized Fibonacci sequences becomes evident. Recall that the generalized Fibonacci sequence (G_n) is defined as $G_{n+2} = aG_{n+1} + G_n$ for all $n \geq 0$ with $a \in \mathbb{F}_q^*, G_0 = 0, G_1 = 1$.

4.1. Cycle Structure

Let η be the real valued function on $\mathbb{F}_q^*$ defined as

$$\eta(c) = \begin{cases} 1 & \text{if } c \text{ is a square in } \mathbb{F}_q, \\ -1 & \text{otherwise.} \end{cases}$$

η is a multiplicative character of $\mathbb{F}_q$ called the *quadratic character* of $\mathbb{F}_q$.

Theorem 4.1.1 *Let $P_{a,n}$ be the permutation defined by (4.1) and $f(x)$ be the polynomial $f(x) = x^2 - ax - 1 \in \mathbb{F}_q[x]$ with the roots $\alpha, \beta \in \mathbb{F}_{q^2}$. Let $k = \mathrm{ord}(\frac{\alpha}{\beta})$ when $\alpha \neq \beta$ and η be the quadratic character of $\mathbb{F}_q$.*

(a) If $\eta(a^2+4) = -1$ then

$$\tau(P_{a,n}) = [(\frac{q+1}{k} - 1)\mathrm{gcd}(k,n) \times \frac{k}{\mathrm{gcd}(k,n)}, \mathrm{gcd}(k-1,n) \times \frac{k-1}{\mathrm{gcd}(k-1,n)}].$$

(b) If $\eta(a^2+4) = 1$ then

$$\tau(P_{a,n}) = [(\frac{q-1}{k} - 1)\mathrm{gcd}(k,n) \times \frac{k}{\mathrm{gcd}(k,n)}, \mathrm{gcd}(k-1,n) \times \frac{k-1}{\mathrm{gcd}(k-1,n)}, 2 \times 1].$$

(c) If $a^2 + 4 = 0$ then

$$\tau(P_{a,n}) = [(p^{r-1} - 1)\mathrm{gcd}(p,n) \times \frac{p}{\mathrm{gcd}(p,n)}, \mathrm{gcd}(p-1,n) \times \frac{p-1}{\mathrm{gcd}(p-1,n)}, 1 \times 1].$$

Proof:

The polynomial $P_{a,n}(x)$ can be written as the composition of the permutation $P_{a,1}(x) = (x+a)^{q-2} \in \mathbb{F}_q[x]$ as $(P_{a,1})^n(x) = P_{a,n}(x)$. Hence, the cycle structure of the permutation $P_{a,n}(x)$ is fully determined by the cycle structure of $P_{a,1}(x)$, i.e. $\tau(P_{a,n}) = \tau(P_{a,1}^n)$.

Recall that $P_{a,1}(x) = F_{a,1}(x)$ for all $x \in \mathbb{F}_q$, where $F_{a,1}(x)$ is the permutation defined by the rational transformation $R_{a,1}(x) = \frac{1}{x+a} \in \mathbb{F}_q(x)$. The characteristic polynomial associated with $R_{a,1}(x)$ is the polynomial $f(x) = x^2 - ax - 1 \in \mathbb{F}_q[x]$ and the conditions *(a),(b),(c)* correspond to $f(x)$ being irreducible, having distinct roots and having a double root in $\mathbb{F}_q$, respectively. By Theorem 2.1.1, one obtains the cycle decomposition of $P_{a,1}$ for the cases *(a),(b),(c)* as follows:

(a) $\tau(P_{a,1}) = [(\frac{q+1}{k} - 1) \times k, 1 \times (k-1)]$,

(b) $\tau(P_{a,1}) = [(\frac{q-1}{k} - 1) \times k, 1 \times (k-1), 2 \times 1]$,

(c) $\tau(P_{a,1}) = [(p^{r-1} - 1) \times p, 1 \times (p-1), 1 \times 1]$.

We write $P_{a,1}$ as a product of disjoint cycles as

$$P_{a,1} = C_1 C_2 \ldots C_s$$

where $s = \frac{q-1}{k}$, $s = \frac{q+1}{k}$ and $s = p^{r-1}$ in the cases *(a),(b),(c)* respectively. We arrange the cycles so that $\ell(C_1) = k-1, \ell(C_j) = k$ for $2 \leq j \leq s$ in the first two cases and

$\ell(C_1) = p-1, \ell(C_j) = p$ for $2 \leq j \leq s$ in the last case. Since the cycles $C_1, C_2, \ldots, C_s$ are disjoint, we have $P_{a,n} = P_{a,1}^n = C_1^n C_2^n \ldots C_s^n$.

We only have to show that for a cycle $C = (\sigma_1 \sigma_2 \ldots \sigma_{\ell(C)})$ of length $\ell(C)$, $\tau(C^n) = \left[gcd(n, \ell(C)) \times \frac{\ell(C)}{gcd(n,\ell(C))}\right]$. Then the proof follows for all the cases of the theorem.

Let t be the length of the cycle C_{σ_1} containing σ_1 in the cycle decomposition of C^n, i.e. $C_{\sigma_1} = (\sigma_1 \sigma_{n+1} \ldots \sigma_{(t-1)n+1})$ with the indices written modulo $\ell(C)$. It is clear that the cycles of C^n are all of the same length t and the order of C^n is $t = \frac{\ell(C)}{gcd(\ell(C),n)}$.

□

Remark 4.1.1 *The case (c) of the theorem occurs if and only if* $q \equiv 1 \mod 4$ *and* $a = 2\gamma$ *where* $\gamma \in \mathbb{F}_q$ *satisfies* $\gamma^2 + 1 = 0$. *Hence, we do not have the case (c) of Theorem 4.1.1 in case* $q \equiv 3 \mod 4$.

Corollary 4.1.2 *Let* G_a *be the subgroup generated by* $P_{a,1}(x) = (x+a)^{q-2} \in \mathbb{F}_q[x]$ *and* $f(x) = x^2 - ax - 1 \in \mathbb{F}_q[x]$.

(i) Suppose that $q \equiv 3 \mod 4$ *or* $a^2 + 4 \neq 0$. *If for the roots* $\alpha, \beta \in \mathbb{F}_q$ *of* $f(x)$ *we have* $ord(\frac{\alpha}{\beta}) = k > 1$ *then*

$$|G_a| = \begin{cases} k-1 & \text{if k=q+1 or k=q-1,} \\ k(k-1) & \text{otherwise.} \end{cases}$$

(ii) If $q \equiv 1 \mod 4$ *and* $a = 2\gamma$ *where* $\gamma \in \mathbb{F}_q$ *satisfies* $\gamma^2 + 1 = 0$ *then*

$$|G_a| = \begin{cases} p-1 & \text{if r=1,} \\ p(p-1) & \text{otherwise.} \end{cases}$$

Proof: The proof follows from the arguments used in the proof of Theorem 4.1.1. □

The following corollary is an easy consequence of Theorem 4.1.1 and Remark 4.1.1.

Corollary 4.1.3 *Suppose that* $a \in \mathbb{F}_p$ *and* $q = p$. *Then* $|G_a| = p$ *if and only if* $p \equiv 3 \mod 4$ *and* $ord(\frac{\alpha}{\beta}) = p + 1$.

4.2. Generalized Fibonacci Sequences and Poles of $P_{a,n}$

Recall that the generalized Fibonacci sequence (G_n) is defined as $G_{n+2} = aG_{n+1} + G_n$ for all $n \geq 0$ with $a \in \mathbb{F}_q^*, G_0 = 0, G_1 = 1$.

Lemma 4.2.4 *The rational function $R_{a,n}(x)$ associated to $P_{a,n}(x)$ satisfies*

$$R_{a,n}(x) = \frac{G_{n-1}x + G_n}{G_n x + G_{n+1}}$$

for all $n \geq 1$.

Proof:

For $n = 1$,

$$R_{a,1}(x) = \frac{1}{x+a} \quad \text{and} \quad \frac{G_0 x + G_1}{G_1 x + G_2} = \frac{1}{x+a}. \tag{4.2}$$

Hence the claim is true for this case.

Suppose that $R_{a,n-1}(x) = \frac{G_{n-2}x + G_{n-1}}{G_{n-1}x + G_n}$. Then

$$\begin{aligned} R_{a,n}(x) &= \frac{1}{a + R_{a,n-1}(x)} = \frac{1}{a + \frac{G_{n-2}x + G_{n-1}}{G_{n-1}x + G_n}} \\ &= \frac{G_{n-1}x + G_n}{(aG_{n-1} + G_{n-2})x + aG_n + G_{n-1}} = \frac{G_{n-1}x + G_n}{G_n x + G_{n+1}}. \end{aligned}$$

□

Consequently, the string of poles is given by $\mathbf{O}_{a,n} = \{x_i : x_i = -\frac{G_{i+1}}{G_i}, i = 1, \ldots, n\} \subset \mathbb{P}^1(\mathbb{F}_q)$.

The polynomial $f(x) = x^2 - ax - 1 \in \mathbb{F}_q[x]$ is the characteristic polynomial of the shortest recurrence relation satisfied by the sequence (G_n). If $f(x)$ in Theorem 4.1.1 has distinct roots $\alpha, \beta \in \mathbb{F}_{q^2}$, then G_n is of the form

$$G_n = c_1\alpha^n + c_2\beta^n.$$

From the initial values G_0, G_1, we derive the formula

$$G_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},\ n \geq 0,$$

and therefore

$$\mathbf{O}_{a,n} = \{x_i : x_i = -\frac{G_{i+1}}{G_i} = -\frac{\alpha^{i+1} - \beta^{i+1}}{\alpha^i - \beta^i}, i = 1, \ldots, n\}.$$

If $\text{ord}(\frac{\alpha}{\beta}) = k$ then $G_k = 0$ and hence $x_{k-1} = 0, x_k = \infty$.

If $a^2 + 4 = 0$ i.e. the polynomial $f(x)$ has a double root $\alpha \in \mathbb{F}_q$, then G_n is of the form

$$G_n = (c_1 + c_2 n)\alpha^n$$

and we obtain the formula

$$G_n = n\left(\frac{a}{2}\right)^{n-1}, n \geq 0.$$

The string of poles is then

$$\mathbf{O}_{a,n} = \{x_i : x_i = -\frac{G_{i+1}}{G_i} = \frac{-(i+1)}{i}\frac{a}{2}, i = 1, \ldots, n\}$$

for all $n \geq 1$ with $x_{p-1} = 0$ and $x_p = \infty$, i.e.

$$\mathbf{O}_{a,n} \subseteq \{\alpha\frac{a}{2} \in \mathbb{F}_q : \alpha \in \mathbb{F}_p \setminus \{p-1\}\} \cup \{\infty\}$$

with equality for all $n \geq p$.

The following lemma is an easy generalization of *d'Ocagne's identity* for Fibonacci sequences

Lemma 4.2.5 *$G_{n+1}G_j - G_nG_{j+1} = (-1)^{j+1}G_{n-j}$ for all $n \geq j \geq 0$.*

Proof:

For $n \geq j$ we have

$$\begin{aligned} G_{n+1}G_j - G_nG_{j+1} &= (aG_n + G_{n-1})G_j - G_n(aG_j + G_{j-1}) \\ &= -(G_nG_{j-1} - G_{n-1}G_j) \\ &= -(G_{j-1}(aG_{n-1} + G_{n-2}) - G_{n-1}(aG_{j-1} + G_{j-2})) \\ &= (-1)^2(G_{n-1}G_{j-2} - G_{j-1}G_{n-2}). \end{aligned}$$

By repeating this process, we obtain the equality

$$(-1)^j(G_{n-j+1}G_0 - G_1G_{n-j}) = (-1)^{j+1}G_{n-j}.$$

□

Proposition 4.2.6 *Let $f(x) = x^2 - ax - 1 \in \mathbb{F}_q[x]$ and $\alpha, \beta \in \mathbb{F}_{q^2}$ be the roots of $f(x)$ with $\alpha \neq \beta$. Let $k = \mathrm{ord}(\frac{\alpha}{\beta})$. Then*

(a) the poles $x_1, \ldots, x_k$ associated to $P_{a,k}$ are all distinct,

(b) $x_{rk+j} = x_j$ for all $r \geq 1$ and $1 \leq j \leq k$,

(c) the poles x_i for $i = 1, .., n-1, n+1, ..., k$ are not the fixed points of $F_{a,n}(x)$ for any $1 \leq n \leq k-1$.

Proof:

(a) Assume that $x_i = x_j$ for some $1 \leq i \neq j < k$. Then

$$x_i = -\frac{G_{i+1}}{G_i} = -\frac{G_{j+1}}{G_j}, \text{ and}$$

$$G_{i+1}G_j - G_iG_{j+1} = 0.$$

Without loss of generality, suppose that $j \leq i$. Then we can write the equality as

$$(-1)^{j+1}G_{i-j} = 0$$

by using Lemma 4.2.5, which implies $G_{i-j} = 0$. This contradicts the fact that k is the smallest integer with $G_k = 0$. For $j < k$, we have $x_j \neq \infty$, otherwise $G_j = 0$ which is again a contradiction.

(b) $(\frac{\alpha}{\beta})^k = 1$ implies

$$G_{rk} = \frac{\alpha^{rk} - \beta^{rk}}{\alpha - \beta} = \frac{(\beta^k)^r - (\beta^k)^r}{\alpha - \beta} = 0 \tag{4.3}$$

for all $r \geq 1$. Lemma 4.2.5 and (4.3) gives

$$G_{rk+j+1}G_j - G_{j+1}G_{rk+j} = (-1)^{j+1}G_{rk} = 0.$$

Then we have

$$x_{rk+j} = -\frac{G_{rk+j+1}}{G_{rk+j}} = -\frac{G_{j+1}}{G_j} = x_j.$$

(c) Note that $F_{a,n}(x) = R_{a,n}(x)$ for all $x \in \mathbb{F}_q \setminus \{x_n\}$ where x_n is the pole of the rational transformation $R_{a,n}(x)$. Since

$$F_{a,n}(x) = x \iff R_{a,n}(x) = x \quad \text{for } x \in \mathbb{F}_q \setminus \{x_n\},$$

the fixed points of $F_{a,n}(x)$ other than x_n are the roots of the polynomial $g(x) = x^2 + ax - 1 \in \mathbb{F}_q[x]$.

$$\begin{aligned} g\left(-\frac{G_{i+1}}{G_i}\right) &= \left(-\frac{G_{i+1}}{G_i}\right)^2 + a - \frac{G_{i+1}}{G_i} - 1 = \frac{G_{i+1}^2 - aG_{i+1}G_i - G_i^2}{G_i^2} \\ &= \frac{G_{i+1}(G_{i+1} - aG_i) - G_i^2}{G_i^2} = \frac{G_{i+1}G_{i-1} - G_i^2}{G_i^2} \\ &= \frac{(-1)^i}{G_i^2} \end{aligned}$$

where the last equality follows by the generalization of Cassini's identity. Hence x_i is not a root of $g(x)$ for $i = 1, ..., n-1, n+1, ..., k$.
For $x = x_n = \frac{-G_{n+1}}{G_n}$, we obtain $F_{a,n}(x_n) = \frac{-G_{n-1}}{G_n}$, and hence x_n is a fixed point if and only if $G_{n+1} + G_{n-1} = 0$. □

In this chapter, we worked on the cycle structure and the string of poles of a certain subset of $\mathcal{P}_n(x)$, namely, the set of polynomials $P_{a,n}(x)$ for $n \geq 1$. When we impose conditions on the coefficients a_i for $0 \leq i \leq n$, the requirements for having a certain cycle structure became easier to check and also the set of polynomials we worked on is a cyclic subgroup of the group of PPs over $\mathbb{F}_q$.

Recall that for a permutation $p(x)$ over $\mathbb{F}_q$, it is always possible to find $\mathcal{P}_n(x)$ such that $p(x) = \mathcal{P}_n(x)$ with $n \geq 0$. The minimal n satisfying the equality is called the *Carlitz rank* of $p(x)$ which is denoted by $Crk(p(x))$, see [3]. In other words, $Crk(p(x))$ is the minimum number of inversions needed to obtain $p(x)$. In [3], a method was presented to determine the Carlitz rank of permutations. As observed in [3], it is not possible to write $\mathcal{P}_n(x)$ as $\mathcal{P}_m(x)$ for $m < n < \frac{q-1}{2}$, when the poles are distinct. In our example, the relation of the poles $x_1, \cdots, x_n$ with the generalized Fibonacci sequence enabled us to determine the string of poles completely for any $n \geq 1$. If $f(x)$ has a double root then the poles $x_1, \cdots, x_p$ are distinct and if $f(x)$ has distinct roots $\alpha, \beta \in \mathbb{F}_{q^2}$ with $k = ord(\frac{\alpha}{\beta})$ then the poles $x_1, \cdots, x_k$ are distinct by Proposition 4.2.6(a). By using the results in [3], we obtain that

$$Crk(P_{a,n}(x)) = n, \text{ when } n \leq \min\left\{p+1, \frac{q-1}{2}\right\}.$$

in case $f(x)$ has a double root and

$$Crk(P_{a,n}(x)) = n, \text{ when } n \leq \min\left\{k+1, \frac{q-1}{2}\right\}.$$

when $f(x)$ has distinct roots.

A natural extension of the results in this chapter would be to impose other conditions on the coefficients a_i, for $0 \leq i \leq n+1$, of $\mathcal{P}_n(x) \in \mathbb{F}_q[x]$ and study the cycle structure of the resulting PPs.

Bibliography

[1] Ahmad, S. *Cycle structure of automorphisms of finite cyclic groups. J. Combinatorial Theory* **6** (1969) 370–374.

[2] Akbary, A., Alaric, S. and Wang, Q. *On some classes of permutation polynomials. Int. J. Number Theory* **4** no. 1 (2008), 121–133.

[3] Aksoy, E., Çeşmelioğlu, A., Meidl, W. and Topuzoğlu, A. *On the Carlitz Rank of a permutation polynomial. submitted.*

[4] Aly, H. and Winterhof, A. *On the linear complexity profile of nonlinear cogruential pseudorandom number generators with Dickson polynomials. Des. Codes Cryptogr.* **39** no.2 (2006) 155–162.

[5] Beck, I. *Cycle decomposition by transpositions. J. Combinatorial Theory Ser. (A)* **23** no. 2 (1977), 198–207.

[6] Carlitz, L. *Permutations in a finite field. Proc. Amer. Math. Soc.* **4** (1953) 538.

[7] Chou, W.-S. *On inversive maximal period polynomials over finite fields. Appl. Algebra Eng. Comm. Comput.* **6** (1995) 245–250.

[8] Chou, W.-S. *The period lengths of inversive pseudorandom vector generations. Finite Fields Appl.* **1** (1995) 126–132.

[9] Chou, W.-S. and Shparlinski, I. E. *On the cycle structure of repeated exponentiation modulo a prime. J. Number Theory* **107** no. 2 (2004) 345–356.

[10] Cohen, S. D. *Dickson polynomials of the second kind that are permutations. Canad. J. Math.* **46** no. 2 (1994), 225–238.

[11] Cohn, M. and Lempel, A. *Cycle decomposition by disjoint transpositions. J. Combinatorial Theory Ser. (A)* **13** no. 2 (1972), 83–89.

[12] Coulter, R. S. and Matthews, R. W. *On the permutation behaviour of Dickson polynomials of the second kind. Finite Fields Appl.* **8** no. 4 (2002), 519–530.

[13] Das, P. *The number of permutation polynomials of a given degree over a finite field. Finite Fields Appl.* **8** (2002) 478-490.

[14] Dickson, L. E. *The analytic representation of substitutions on a power of a prime letters with a discussion of the linear group.* Ann. of Math. **11** (1897) 65-120, 161-183.

[15] Eichenauer, J. and Lehn, J. A non-linear congruential pseudo random number generator, *Statist. Papers* **27** (1986), 315–326 .

[16] Flahive, M. and Niederreiter, H. *On inversive congruential generators for pseudo-random numbers. Finite Fields, Coding Theory and Advances in Communications and Computing, (Las Vegas,NV,1991)*, 75–80, Lecture Notes in Pure and Appl. Math., **141**, Marcel-Dekker, New York, 1993.

[17] Henderson, M. and Matthews, R. *Dickson polynomials of the second kind which are permutation polynomials over a finite field. New Zealand J. Math.* **27** no. 2 (1998), 227–244.

[18] Henderson, M. *A note on the permutation behaviour of the Dickson polynomials of the second kind. Bull. Austral. Math. Soc.* **56** no. 3 (1997), 499–505.

[19] Hermite, C. *Sur les fonctions de sept lettres.* C. R. Acad. Sci. Paris, **57** (1863) 750-757; Oevres Vol.2, Gauthier-Villars, Paris, (1908) 200-208.

[20] Konyagin, S. and Pappalardi, F. *Enumerating Permutation Polynomials Over Finite Fields by Degree. Finite Fields Appl.* **8** (2002) 548-553.

[21] Konyagin, S. and Pappalardi, F. *Enumerating Permutation Polynomials Over Finite Fields by Degree II.* F*Finite Fields Appl.* **12** (2006) 26-37.

[22] Lidl, R. and Mullen, G. L. *Cycle structure of Dickson permutation polynomials. Math. J. Okayama Univ.* **33** (1991) 1–11.

[23] Lidl, R. and Mullen, G. L. *When Does a Polynomial over a Finite Field Permute the Elements of the Field. The American Mathematical Montly* **95**, No.3 (1988) 243-246.

[24] Lidl, R. and Mullen, G. L. *When Does a Polynomial over a Finite Field Permute the Elements of the Field, II. The American Mathematical Montly* **100**, No.1 (1993) 71-74.

[25] Lidl, R., Mullen, G. L. and Turnwald, G. *Dickson Polynomials Pitman Monographs and Surveys in Pure and Applied Mathematics* **65**, (1993).

[26] Lidl, R. and Niederreiter, H. *Finite fields.* 2nd Ed. *Encyclopedia of Mathematics and its Applications* **20**, Cambridge University Press, Cambridge (1997).

[27] MacWilliams, F. J. and Sloane, N. J. A. *The theory of error correcting codes.* North Holland Mathematical Library, no.16, Amsterdam-New York-Oxford, (1977)

[28] Malvenuto, C. and Pappalardi, F. *Enumerating Permutation Polynomials I: Permutations with Non-Maximal Degree. Finite Fields Appl.* **8** (2002) 531-547.

[29] Malvenuto, C. and Pappalardi, F. *Enumerating Permutation Polynomials II: k-cycles with minimal degree. Finite Fields Appl.* **10** (2004) 72-96.

[30] Matthews, R. *Permutation Polynomials in one and several variables.* Ph.D. thesis, University of Tasmania, Hobart, (1982).

[31] Mullen, G. L. *Permutation Polynomials over Finite Fields.* Finite Fields, Coding Theory, and Advances in Communications and Computing, Marcel Dekker, NY, (1993) 131-151.

[32] Mullen, G. L. and Vaughan, T. P. *Cycles of linear permutations over a finite field. Linear Algebra Appl.* **108** (1988) 63–82.

[33] Vasiga, T. and Shallit, J. *On the iteration of certain quadratic maps over GF(p) Discrete Mathematics* **277** (2004) 219–240

[34] Shparlinski, I. E. *Finite fields: theory and computation The meeting point of number theory, computer science, coding theory and cryptography. Mathematics and its Applications* **477**, Kluwer Academic Publishers, Dordrecht (1999).

[35] Stafford, R. M. *Groups of permutation polynomials over finite fields*, *Finite Fields Appl.* **4**, (1998) 450-452.

[36] Topuzoğlu, A. and Winterhof, A. *Pseudorandom sequences, in* "Topics in Geometry, Coding Theory and Cryptography", (A. Garcia and H. Stichtenoth, Eds.) Algebra and Applications, **6**, (2007) 135-166, Springer-Verlag.

[37] Yuan, J. and Ding, C. *Four classes of permutation polynomials of* $\mathbb{F}_{2^m}$, *Finite Fields Appl.* **13**, no.4 (2007) 869–876.

[38] Yuan, J., Ding, C., Wang, H. and Pieprzyk, J. *Permutation polynomials of the form* $(x^p - x + \delta)^s + L(x)$, *Finite Fields Appl.* **14**, no.2 (2008) 482–493.