Determining the Cycle Structure of Permutation Polynomials of Shape $X^t + \gamma \operatorname{Tr}(X^k)$

Dissertation

zur Erlangung des Akademischen Grades

doctor rerum naturalium
(Dr. rer. nat.)

von M. Sc. Daniel Gerike

geb. am 03.01.1990 in Schwalmstadt

genehmigt durch die Fakultät für Mathematik
der Otto-von-Guericke-Universität Magdeburg

Gutachter:
Prof. Dr. Gohar M. Kyureghyan
Universität Rostock

Prof. Dr. Alexander Pott
Otto-von-Guericke-Universität Magdeburg

Prof. Dr. Alev Topuzoğlu
Sabancı Üniversitesi

eingereicht am: 17.12.2019

Verteidigung am: 22.06.2020

Abstract

In this thesis we study the cycle structure of permutation polynomials. They play an important role in many applications of finite fields. Of particular note are combinatorial design theory, cryptography and coding theory.

An important application of permutation polynomials with known cycle structure in coding theory is their use as parts of turbo codes. In this context we want the permutations to be given as polynomials, because this reduces the implementation cost. But we also want to know their cycle structures, because they give us important algebraic and combinatorial properties of the permutations, which strongly influence the performance of the final code.

Currently we know the cycle structure only for a few simple classes of permutation polynomials. These are monomials, Dickson and linearized polynomials. We give a survey of these results. None of these classes make full use of the structure of a finite field and mainly depend on either the multiplicative or additive group of the field.

We focus on permutation polynomials of shape $X^t+\gamma \operatorname{Tr}_{q^n/q}(X^k) \in \mathbb{F}_{q^n}[X]$, where $\gamma \in \mathbb{F}_{q^n}$ and $1 \leq t, k \leq q^n-1$. In contrast to those classes, for which the cycle structure is already known, these depend on both the additive and multiplicative structure of a finite field, but still have a nice algebraic form. Permutation polynomials of this shape were first considered in 2008 by Charpin and Kyureghyan [5] for $q = 2$, where a complete classification was given. We show, that polynomials of shape $X^t+\gamma f(X)$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$, can only be permutations if $\gcd(t, q^n - 1) = 1$. In this case X^t is also a permutation, so for classification purposes it suffices to consider $t = 1$. In recent years Kyureghyan and Zieve [11], Ma and Ge [16] and Li, Qu, Chen, and Li [13] have constructed 24 infinite families of permutation polynomials of shape $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$.

We give the number of fixed points for all of these permutations. Further we show that permutation polynomials of shape $X + \gamma f(X)$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$, are precisely those that also permute any line $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^n}$. We give a condition on f, under which certain of these induced permutations on lines have the same cycle structure.

All 17 of the 24 infinite families, where n is fixed to 2 or 3 satisfy this condition. In particular, if $n = 2$, which holds for 15 of them, this allows us to ascertain the cycle structure by determining it on $\gamma\mathbb{F}_q$ and any one other line $\alpha + \gamma\mathbb{F}_q$. The cycle structure on $\gamma\mathbb{F}_q$ can be found easily, but getting the cycle structure on one of the other lines is still a very difficult problem. We solve it for two families completely and for one family in a special case.

For the other 7 families, where n is arbitrary, we need to use different techniques. By combining results on linear translators [12] and algebraic curves [7, 19] we determine the cycle structure of three of those families completely and of two more partially. The same methods also give us the cycle structure for all permutation polynomials of shape $X + \gamma \operatorname{Tr}_{2^n/2}(X^k)$, that is in the special case where $q = 2$. We ascertain the cycle structure of the last two families by showing that their cycle structure on any line $\alpha+\gamma\mathbb{F}_q$ is the same as the cycle structure of a simple linearized permutation polynomial over $\mathbb{F}_q$ with known cycle structure.

Additionally, we find the cycle structure of permutation polynomials of shape $X^{q^2+q+1} + \operatorname{Tr}_{q^3/q}(X)$, where q is odd, by explicitly computing their iterates. We get these polynomials by composing one of the 24 infinite families, $X+\operatorname{Tr}_{q^3/q}(X^{(q^2+1)/2})$, with monomial permutations, X^{q^2+q+1}.

Zusammenfassung

In dieser Dissertation befassen wir uns mit der Zyklenstruktur von Permutationspolynomen. Diese spielen eine wichtige Rolle in vielen Anwendungen von endlichen Körpern. Besonders zu beachten sind dabei kombinatorische Designs, Kryptographie und Kodierungstheorie.

Eine wichtige Anwendung von Permutationspolynomen mit bekannter Zyklenstruktur in der Kodierungstheorie ist deren Verwendung als Teile von Turbo-Codes. In diesem Zusammenhang möchten wir Permutationen in Polynomschreibweise vorliegen haben, denn dies reduziert die Implementationskosten. Zusätzlich möchten wir aber auch ihre Zyklenstruktur wissen, denn aus dieser erhalten wir wichtige algebraische und kombinatorische Eigenschaften der Permutationen, welche das Verhalten des fertigen Codes stark beeinflussen.

Momentan kennen wir nur die Zyklenstruktur einiger weniger Klassen von einfachen Permutationspolynomen. Diese sind Monome, Dickson und linearisierte Polynome. Wir geben eine Übersicht über diese Resultate. Keine dieser Klassen benutzt die vollständige Struktur eines Endlichen Körpers, sondern basieren hauptsächlich entweder auf der multiplikativen oder additiven Gruppe des Körpers.

Unserer Schwerpunkt sind Permutationspolynome der Form $X + \gamma \operatorname{Tr}_{q^n/q}(X^k) \in \mathbb{F}_{q^n}[X]$, wobei $\gamma \in \mathbb{F}_{q^n}$ und $1 \leq t, k \leq q-1$. Im Gegensatz zu den Klassen, deren Zyklenstruktur uns bereits bekannt ist, basieren diese sowohl auf der additiven als auch der multiplikativen Struktur eines endlichen Körpers, haben aber trotzdem immer noch eine schöne Algebraische Form. Permutationspolynome dieser Art wurden ursprünglich im Jahr 2008 von Charpin und Kyureghyan [5] für den Fall $q = 2$ betrachtet und vollständig klassifiziert. Wir zeigen, dass Polynome der Form $X^t + \gamma f(x)$, wobei $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$, nur dann Permutationen sein können, wenn $\operatorname{ggT}(t, q^n - 1) = 1$. in diesem Fall ist X^t auch eine Permutation, sodass es für die Klassifikation genügt den Fall $t = 1$ zu betrachten. In den letzten Jahren haben Kyureghyan und Zieve [11], Ma und Ge [16] und Li, Qu, Chen und Li [13] insgesamt 24 unendliche Familien von Permutationspolynomen der Form $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ konstruiert.

Wir bestimmen die Anzahl der Fixpunkte aller dieser Permutationen. Weiter zeigen wir, dass die Permutationspolynome der Form $X + \gamma f(X^k)$, wobei $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$, genau diejenigen sind, die auch jede Gerade $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^n}$, permutieren. Wir zeigen: Wenn f eine besondere Eigenschaft erfüllt, dann haben bestimmte dieser auf Geraden induzierten Permutationen die selbe Zyklenstruktur.

Die 17 der 24 Familien, für die n die feste Zahl 2 oder 3 ist, erfüllen diese Eigenschaft. Insbesondere für $n = 2$, was bei 15 dieser Familien der Fall ist, erlaubt uns dies ihre Zyklenstruktur ermitteln indem wir sie auf $\gamma\mathbb{F}_q$ und einer beliebigen anderen Geraden $\alpha + \gamma\mathbb{F}_q$ bestimmen. Auf $\gamma\mathbb{F}_q$ kann die Zyklenstruktur einfach ge-

funden werden, aber die Zyklenstruktur auf einer der anderen Geraden zu erhalten ist weiterhin ein sehr schwieriges Problem. Wir lösen es für zwei Familien vollständig und für eine Familie in einem Spezialfall.

Für die restlichen 7 Familien, bei denen n beliebig ist, müssen wir andere Techniken benutzen. Durch die Kombination von Resultaten für lineare Translatoren [12] und algebraische Kurven [7, 19] bestimmen wir die Zyklenstruktur für drei dieser Familien vollständig und für zwei weitere teilweise. Mit den gleichen Methoden finden wir auch die Zyklenstruktur aller Permutationspolynome der Form $X+\gamma\,\mathrm{Tr}_{2^n/2}(X^k)$, also im Spezialfall $q = 2$. Die Zyklenstruktur der letzten zwei Familien bestimmen wir, indem wir zeigen, dass ihre Zyklenstruktur auf jeder Geraden $\alpha + \gamma\mathbb{F}_q$ die selbe ist wie die eines einfachen linearisierten Permutationspolynoms über $\mathbb{F}_q$, dessen Zyklenstruktur bekannt ist.

Zusätzlich ermitteln wir die Zyklenstruktur von Permutationspolynomen der Form $X^{q^2+q+1} + \mathrm{Tr}_{q^3/q}(X)$, wobei q ungerade ist, indem wir ihre Iterationen explizit berechnen. Diese Polynome erhalten wir, indem wir eine der 24 Familien, $X + \mathrm{Tr}_{q^3/q}(X^{(q^2+1)/2})$, mit einem Permutationsmonom, X^{q^2+q+1}, verknüpfen.

Contents

Introduction

Any map of a finite field into itself can be represented by a polynomial. If the map represented is a permutation, we call the polynomial a permutation polynomial. The cycle structure of a permutation polynomial is defined as the cycle structure of its associated permutation, which is a list of the cycle lengths and their multiplicities in the cycle decomposition of that permutation. Formal definitions of these concepts can be found in Chapter 1.

The cycle decomposition of a permutation contains information about its algebraic and combinatorial properties, e. g. its order and parity. Much of that information is retained in its cycle structure. A central challenge in the study of permutations over finite fields is finding connections between its polynomial representation and its combinatorial properties. Discovering the cycle structure of a permutation polynomial gives insight into this problem. The cycle structure of a permutation also uniquely determines to which conjugation class of the appropriate symmetric group it belongs. In this way knowing the cycle structure of a permutation polynomial over a finite field $\mathbb{F}_q$ is equivalent to knowing its conjugation class as an element of the symmetric group over $\mathbb{F}_q$. Finding the cycle structure of a class of permutation polynomials is a highly nontrivial problem. At present it is only solved for a few simple classes of permutation polynomials.

The first article giving the cycle structure of an infinite family of permutation polynomials was published 50 years ago in 1969 by Ahmad [1]. In that article he determines the cycle structure of monomial permutations. Then about 20 years later, in 1988, Mullen and Vaughan [18] studied the cycle structure of linearized polynomials. Soon after, in 1991, the cycle structure of certain Dickson polynomials was ascertained by Lidl and Mullen [14]. For monomial, Dickson and linearized polynomials a classification into permutation and non-permutation polynomials is not difficult. None of these polynomials make use of the full structure of a finite field. For monomials only the multiplicative structure of the field is relevant. Dickson polynomials only use the ring structure of the field. Linearized polynomials depend solely on the vector space property of a finite field over a subfield. Finally, in 2008, Çeşmelioğlu, Meidl, and Topuzoğlu [4] studied a connection of the Carlitz rank and the cycle structure of permutation polynomials.

One important application of permutation polynomials with known cycle structure is in coding theory. There they can be used as interleavers, which are used in certain coding schemes to permute the components of a vector. In particular they are necessary for the construction of turbo codes. For this application we want the permutations given as polynomials, because these are easy to implement. Only the coefficients have to be stored. But we also have to know the cycle structure of

these permutations, because their combinatorial properties can drastically alter the performance of the final code. For more on this see Sakzad, Sadeghi, and Panario [23].

A class of permutation polynomials, whose properties need to be better understood is the class of permutation polynomials of shape $X^t + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ over F_{q^n}, where $\gamma \in \mathbb{F}_{q^n}^*$ and $1 \leq t, k \leq q^n - 1$. These permutation polynomials are interesting, because they make use of the full structure of a finite field by depending on both its additive and multiplicative structure but still have a rather simple algebraic form. We will determine the cycle structure of multiple infinite families of this shape, thereby giving the first results on cycle structures of permutation polynomials using the full structure of a finite field. Some of our results extend to a larger class of polynomials, where instead of $\operatorname{Tr}_{q^n/q}(X^k)$ any map $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ can be used.

Chapter 1 contains fundamental definitions and facts concerning permutations, cycle structure and permutation polynomials. Here we also state a well-known result, which will be used many times throughout the whole thesis: Two permutations have the same cycle structure precisely if they are conjugate.

In Chapter 2 we give a survey of previous results on the cycle structure of permutation polynomials. These are the cycle structures of monomials [1], Dickson polynomials $D_k(X, a)$ with $a = \pm 1$ [14] and linearized polynomials with coefficients in the subfield [17, 18, 20]. A connection between the Carlitz rank and the cycle structure of a permutation polynomial is studied in [4].

The class of polynomials of shape $X^t + \gamma f(X)$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$, is considered in the first part of Chapter 3. We show that if these polynomials are permutations, then necessarily $\gcd(t, q^n - 1) = 1$. Since in this case X^t is also a permutation polynomial $X^t + \gamma f(X)$ is a permutation if and only if $X + \gamma f(X^{t^{-1}})$ is. This shows, that for classification purposes we only have to study the case $t = 1$. By carefully considering the proof of this result it can be generalized to be applicable to many cases where we want to know if the sum of two maps is a permutation. Then a list (Theorem 3.4) of all currently known infinite families of permutation polynomials of shape $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ is given. It compiles the results of several recent articles [11–13, 16]. This list contains 24 cases, which we label (F_1) to (F_{24}). In Section 3.3 a result about linear translators [12] and a result on the number of rational places of certain algebraic curves [7, 19] are presented. These will be very useful to determine the cycle structure of a significant part of the permutation polynomials given in Theorem 3.4. After that we consider the special case, where $q = 2$, for which a complete classification into permutation polynomials and non-permutation polynomials was given in [5]. Using the results presented in Section 3.3 we can get the cycle structure for all permutation polynomials in this special case. At the end of the chapter the number of fixed points for all known infinite families of permutation polynomials of shape $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ is given. For most of them this can be done by computing the greatest common divisor of the exponent k and $q^n - 1$, which is the order of the multiplicative group of the finite field $\mathbb{F}_{q^n}$, but for some it is necessary to use the results from [7, 19].

Our general method to determine the cycle structure of one of the permutation polynomials in Theorem 3.4 depends on the extension degree n of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Therefore Chapter 4 is mainly about the cases, where this extension degree is 2 or 3 and Chapter 5 deals with the cases, where it is arbitrary.

In the first section of Chapter 4 the class $X + \gamma f(X)$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is again considered. We will see, that permutations of this shape are exactly those permutations, that also permute any line of the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$, which is parallel to the line $\gamma\mathbb{F}_q$. This will lead to a theorem, showing the following: If f is additionally 1-homogeneous, then the cycle structures of induced permutations on lines $\alpha + \gamma\mathbb{F}_q$, $\alpha \notin \mathbb{F}_q$, parallel to $\gamma\mathbb{F}_q$ are the same, if they are contained in the same 2-dimensional linear subspace of $\mathbb{F}_{q^n}$. All of the cases in Theorem 3.4 with $n \in \{2, 3\}$ fulfil this condition, which allows us to ascertain the cycle structure in cases with $n = 2$ by determining the cycle structure on only 2 lines. One of those lines has to be $\gamma\mathbb{F}_q$ and the second can be any other line parallel to it. Getting the cycle structure on $\gamma\mathbb{F}_q$ is no problem, but determining the cycle structure on one of those other lines is a challenge. We solve this for cases (F_2) and (F_{12}) completely and case (F_9) partially.

Chapter 5 contains results on the cases of Theorem 3.4, where the extension degree is arbitrary. A permutation polynomial in one of these cases always has one of two properties. Either γ is a 0-linear translator of $\mathrm{Tr}_{q^n/q}(X^k)$, which allows us to use the results presented in Section 3.3 to find the cycle structure, or the cycle structure is the same on any line parallel to $\gamma\mathbb{F}_q$, including $\gamma\mathbb{F}_q$, which is also the same as the cycle structure of a linearized permutation polynomial on $\mathbb{F}_q$. For most of the cases with this property the cycle structure can then be determined using the results from [17, 18, 20].

Finally Chapter 6 deals with a method we call shifting the exponent. A composition of two permutations is still a permutation. This allows one to consider permutations $X^t + \gamma\,\mathrm{Tr}_{q^n/q}(X)$ instead of permutations $X + \gamma\,\mathrm{Tr}_{q^n/q}(X^k)$, where $t \equiv q^m k^{-1} \pmod{q^n - 1}$. This means we consider a permutation where the *exponent* was *shifted* from the monomial inside of the trace-function to the monomial outside of the trace-function. In case (F_{16}) this leads to a permutation with an interesting cycle structure, which can be determined by explicitly computing its iterates.

Table A summarizes our current knowledge on the cycle structure of the 24 families of permutation polynomials given in Theorem 3.4.

Table A: Overview of determined cycle structures and conjectures

Case	**Cycle Structure**	**Reference**
(F_1)	Conjecture	Conjecture 4.4
(F_2)	Determined Completely	Theorem 4.14
(F_3)	Conjecture	Conjecture 4.4
(F_4)	open	–
(F_5)	open	–
(F_6)	open	–
(F_7)	open	–
(F_8)	open	–
(F_9)	Determined Partially / Conjecture	Theorem 4.25 / Conjecture 4.4
(F_{10})	open	–
(F_{11})	open	–
(F_{12})	Determined Completely	Theorem 4.20
(F_{13})	open	–
(F_{14})	Conjecture	Conjecture 4.4
(F_{15})	Conjecture	Conjecture 4.4
(F_{16})	after Exponent Shifting	Theorems 6.5, 6.6 and 6.8
(F_{17})	open	–
(F_{18})	Determined Completely	Theorem 5.3
(F_{19})	Determined Completely	Theorem 5.5
(F_{20})	Determined Completely	Theorem 5.7
(F_{21})	Determined Partially	Theorem 5.15
(F_{22})	Determined Completely	Theorem 5.11
(F_{23})	Determined Completely	Theorem 5.13
(F_{24})	Determined Partially	Theorem 5.18

Chapter 1

Fundamental Definitions and Properties

This chapter contains some fundamental facts about permutations, cycle structure and permutation polynomials. In the first part the definition for the cycle structure of a permutation is given and notations for it are introduced. We will further see an important criterion that allows us to tell if two permutations have the same cycle structure without having to determine it. The second part contains the definition of permutation polynomials and an example that shows some simple methods to determine the cycle structure of one.

1.1 Permutations and Cycle Structure

It is well known that any permutation can be written uniquely (up to reordering) as a product of disjoint cycles. This is called *cycle decomposition*.

Definition 1.1. The *cycle structure* of a permutation lists the multiplicity of each cycle length in its cycle decomposition.

If a permutation has (i. e. its cycle decomposition contains) exactly n_1 cycles of length l_1, n_2 cycles of length l_2, ... and n_r cycles of length l_r where $l_1 < l_2 < \cdots < l_r$, we write its cycle structure as $l_1^{n_1} l_2^{n_2} \dots l_r^{n_r}$. Sometimes we will allow $n_i = 0$, to simplify notations. For an example of this, see the following definition.

Definition 1.2. Let $\pi : A \to A$ be a permutation of the set A that also permutes a subset B of A. We will denote the cycle structure of π (on A) by $\mathrm{CS}(\pi)$ and the cycle structure of π on B, i. e. $\pi\big|_B$, by $\mathrm{CS}_B(\pi)$.

We define an addition of cycle structures as follows. Let $c_1 = l_1^{n_1} l_2^{n_2} \dots l_r^{n_r}$ and $c_2 = l_1^{m_1} l_2^{m_2} \dots l_r^{m_r}$, where $n_i, m_i = 0$ is allowed. Then we write

$$c_1 + c_2 = l_1^{n_1+m_1} l_2^{n_2+m_2} \dots l_r^{n_r+m_r}.$$

Remark 1.1. Let $A = B \cup C$, where $B \cap C = \emptyset$. If the permutation $\pi : A \to A$ also permutes B and C then $\mathrm{CS}(\pi) = \mathrm{CS}_B(\pi) + \mathrm{CS}_C(\pi)$.

For a finite set A we denote the symmetric group defined over A by S_A.

Definition 1.3. Let A and B be finite sets of the same size. The permutations $F \in S_A$ and $G \in S_B$ are called *conjugate* if there exists a bijection $\varphi : A \to B$, such that $F = \varphi^{-1} \circ G \circ \varphi$.

The next well known fact will be very useful later, because it allows us to find the cycle structure of a permutation, by determining the cycle structure of a conjugate.

Proposition 1.1. *Let A and B be finite sets of the same size. The permutations $F \in S_A$ and $G \in S_B$ have the same cycle structure if and only if they are conjugate.*

Remark 1.2. Let A be a finite set and $F, G \in S_A$. Since $F \circ G = G^{-1} \circ G \circ F \circ G$, we know that $G \circ F$ and $F \circ G$ always have the same cycle structure. In particular if we consider a finite field $\mathbb{F}_q$ and $F \in S_{\mathbb{F}_q}$, then for $a \in \mathbb{F}_q^*, b \in \mathbb{F}_q$ the permutations $x \mapsto F(ax + b)$ and $x \mapsto aF(x) + b$ have the same cycle structure.

1.2 Permutation Polynomials

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. Given a univariate polynomial $F(X) \in \mathbb{F}_q[X]$, its *associated map* F is defined by

$$F : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto F(x).$$

The associated maps of polynomials $F(X)$ and $G(X)$ are equal on $\mathbb{F}_q$ if and only if $F(X) \equiv G(X) \pmod{X^q - X}$. In particular, the associated maps of two different polynomials of degree less than q are different. The number of different maps of $\mathbb{F}_q$ into itself is q^q, which is also the number of different polynomials of degree less than q in $\mathbb{F}_q[X]$.

This shows that any map g of $\mathbb{F}_q$ into itself is the associated map of a unique polynomial over $\mathbb{F}_q$ of degree less than q, which is called the reduced polynomial of g.

Using Lagrange interpolation we can give a formula for the reduced polynomial $g(X)$ of the map g:

$$g(X) = \sum_{x \in \mathbb{F}_q} g(x)(1 - (X - x)^{q-1}).$$

Definition 1.4. A polynomial over $\mathbb{F}_q$ is called a *permutation polynomial* of $\mathbb{F}_q$ if it induces a permutation on $\mathbb{F}_q$.

The cycle structure of a permutation polynomial is the cycle structure of its induced permutation.

We will denote the cycle structure of a permutation polynomial $F(X)$ as $\mathrm{CS}(F)$.

Definition 1.5. Let $a \in \mathbb{F}_q^*$. The *(multiplicative) order* $\mathrm{ord}(a)$ of a is the smallest positive integer m, such that $a^m = 1$.

Let us now take a look at an example, which clarifies the notation and contains basic steps used to determine the cycle structure.

Example 1.1. Let p be the characteristic of $\mathbb{F}_q$ and $F(X) = aX + b \in \mathbb{F}_q(X)$, $a \neq 0$. Then

$$\mathrm{CS}(F) = \begin{cases} 1^q, & a = 1, b = 0, \\ p^{q/p}, & a = 1, b \neq 0, \\ 1^1 \operatorname{ord}(a)^{(q-1)/\operatorname{ord}(a)}, & a \neq 1. \end{cases}$$

Proof. If $a = 1, b = 0$, then F is the identity map on $\mathbb{F}_q$.

If $a = 1, b \neq 0$, then the n-th iterate of $F(X)$ is $F^n(X) = X + nb$, so for any $x \in \mathbb{F}_q$, we see that $F^n(x) = x$ if and only if $p \mid n$ and all cycles are of length p.

If $a \neq 1$, then $F^n(X) = a^n X + \frac{a^n - 1}{a-1} b$. We see that F has one fixed point $-\frac{b}{a-1}$ and for all other $x \in \mathbb{F}_q$, that $F^n(x) = x$ if and only if $\operatorname{ord}(a) \mid n$, so all other cycles are of length $\operatorname{ord}(a)$. □

Often it is easier to only consider monic polynomials or polynomials with no constant term. So naturally the question arises, if it is enough to consider such polynomials, when determining cycle structures. That is, we want to know the following:

Let $F(X) \in \mathbb{F}_q[X]$ be a permutation polynomial and $a \in \mathbb{F}_q^*$. Is it sufficient to know the cycle structure of $F(X)$ if one wants to determine the cycle structure of $aF(X)$ or of $a + F(X)$?

In general the answer is no. Consider for example the permutation polynomials $2X$ and $3X$ over $\mathbb{F}_5$. It is easy to see that $\mathrm{CS}(2X) = 1^1 4^1 = \mathrm{CS}(3X)$ but

$$\mathrm{CS}(3 \cdot (2X)) = \mathrm{CS}(X) = 1^5 \neq 1^1 2^2 = \mathrm{CS}(4X) = \mathrm{CS}(3 \cdot (3X)).$$

Similarly, if we consider $X + 2$ and $X + 3$ over $\mathbb{F}_5$, then $\mathrm{CS}(X + 2) = 5^1 = \mathrm{CS}(X + 3)$ but

$$\mathrm{CS}(3 + (X + 2)) = \mathrm{CS}(X) = 1^5 \neq 5^1 = \mathrm{CS}(X + 1) = \mathrm{CS}(3 + (X + 3)).$$

In contrast the cycle structure of iterates is easily determined, if one knows the cycle structure of the original permutation.

Proposition 1.2. *Let F be permutation with $\mathrm{CS}(F) = l_1^{n_1} l_2^{n_2} \dots l_r^{n_r}$, then the cycle structure of its m-th iteration $F^m = \underbrace{F \circ \dots \circ F}_{m}$ is*

$$\mathrm{CS}(F^m) = \sum_{j=1}^{r} \left(\frac{l_j}{\gcd(l_j, m)} \right)^{n_j \gcd(l_j, m)}.$$

Proof. Since the cycles in a cycle decomposition are disjunct, it suffices to consider a single cycle $(x_1\ x_2\ \dots\ x_l)$. Now

$$(x_1\ x_2\ \dots\ x_l)^m = (x_1\ x_{m+1}\ x_{2m+1}\ \dots\ x_{(k-1)m+1})(\dots)\dots,$$

where the indices are elements of the residue class ring $\mathbb{Z}_l$ and k is the smallest integer, s. t. $km + 1 \equiv 1 \pmod{l}$. This means $km = \operatorname{lcm}(l, m)$ and so $k = l/\gcd(l, m)$. Since this holds similarly for every element of the cycle, $(x_1\ x_2\ \dots\ x_l)^m$ only has cycles of length k. Then the number of these cycles has to be $l/k = \gcd(l, m)$. □

Chapter 2

Permutation Polynomials with Known Cycle Structures

This chapter contains a survey of permutation polynomials whose cycle structure has been determined. These are monomials, Dickson polynomials and linearized polynomials. In all of these cases a simple condition exists to determine if a given polynomial is a permutation polynomial or not. In Section 2.4 we take a look at a paper that studies connections between the Carlitz rank and the cycle structure of a permutation polynomial. This study was inspired by a result of Carlitz [2] from 1953, which states, that any permutation polynomial over a finite field $\mathbb{F}_q$ can be written as a composition of polynomials $\alpha X + \beta$ and X^{q-2}, where $\alpha, \beta \in \mathbb{F}_q$, $\alpha \neq 0$.

2.1 Monomials

In 1969 Ahmad [1] determined the cycle structure of monomial permutations. To state his results we will use the following notation.

Notation 2.1. Let k and t be positive integers. We denote by $\mathrm{ord}_t(k)$ the order of k modulo t, i. e. the smallest positive integer m with $k^m \equiv 1 \pmod{t}$.

The following proposition, which classifies monomials, is well known. It is derived from the fact, that the multiplicative group of a finite field is cyclic and the image set of the power map $x \mapsto x^k$ on a cyclic group with n elements is the subgroup with $n/\gcd(k, n)$ elements. Proofs for these properties can be found in [15, pp. 7, 50, 351].

Proposition 2.1. *The monomial $X^k \in \mathbb{F}_q[X]$ is a permutation polynomial if and only if $\gcd(k, q-1) = 1$.*

The following theorem gives the cycle structure for all monomial permutations.

Theorem 2.2. *The permutation polynomial X^k , $\gcd(k, q-1) = 1$, has a cycle of length m on $\mathbb{F}_q^*$ if and only if $m = \mathrm{ord}_t(k)$, where $t \mid (q-1)$. The number N_m of those cycles satisfies*

$$m \cdot N_m = \gcd(k^m - 1, q-1) - \sum_{i \mid m, i \neq m} i \cdot N_i, \;\; N_1 = \gcd(k-1, q-1).$$

Remark 2.1. On $\mathbb{F}_q$, X^k has the additional fixed point 0 and thus $N_1 + 1$ fixed points in total.

2.2 Dickson Polynomials

In 1991 Lidl and Mullen [14] determined the cycle structure of Dickson polynomials $D_k(X, a)$ with $a = \pm 1$. Since the Dickson polynomials $D_k(X, 0)$ are monomials, together with the previous section the cycle structure for all Dickson polynomials $D_k(X, a)$ with $a \in \{-1, 0, 1\}$ is known. These are exactly the cases in which the Dickson polynomials with a fixed a are a subgroup of the symmetric group. A proof for this can be found in [15, pp. 359–360]. This means in these cases the iterates of the permutation polynomials are again Dickson polynomials with the same parameter a. So it is not surprising, that these are exactly the cases where the cycle structure could be determined. For further information about these cycle structures see also Rubio, Mullen, Corrada, and Castro [22].

Definition 2.2 (Dickson polynomial)**.** Let $a \in \mathbb{F}_q$. The polynomial

$$D_k(X, a) = \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{k}{k-j} \binom{n-j}{j} (-a)^j X^{k-2j}$$

over $\mathbb{F}_q$ is called *Dickson polynomial (of the first kind) of degree k.*

Remark 2.2. A Dickson polynomial with $a = 0$ is a monomial, $D_k(X, 0) = X^k$.

The following well known result classifies Dickson polynomials. A proof can be found in [15, p. 356].

Proposition 2.3. *Let $a \in \mathbb{F}_q^*$. The Dickson polynomial $D_k(X, a) \in \mathbb{F}_q[X]$ is a permutation polynomial if and only if* $\gcd(k, q^2 - 1) = 1$.

The following theorem gives the cycle structure for Dickson permutation polynomials $D_k(X, 1)$.

Theorem 2.4. *Let $q = p^s$ be a prime power. The permutation polynomial $D_k(X, 1)$,* $\gcd(k, q^2 - 1) = 1$*, has a cycle of length m on $\mathbb{F}_q$ if and only if $m = \operatorname{ord}_t(k)$ or if m is the smallest positive integer with $k^m \equiv -1 \pmod{t}$, where $t \mid q - 1$ or $t \mid q + 1$. The number N_m of those cycles satisfies*

$$\begin{aligned} & m \cdot N_m \\ &= \frac{\gcd(q+1, k^m+1) + \gcd(q-1, k^m+1) + \gcd(q+1, k^m-1) + \gcd(q-1, k^m-1)}{2} \\ &\quad - \varepsilon - \sum_{i \mid m, i < m} i \cdot N_i \end{aligned}$$

where

$$\varepsilon = \begin{cases} 1, & p = 2 \text{ or } p \text{ odd and } k \text{ even}, \\ 2, & p \text{ odd and } k \text{ odd}. \end{cases}$$

To state the next theorem we need the following definition.

Definition 2.3. Let $\nu_p(m)$ denote the highest power of p dividing m. By convention let $\nu_p(0) = \infty$.

The following theorem gives the cycle structure for Dickson permutation polynomials $D_k(X, -1)$.

Theorem 2.5. *The permutation polynomial $D_k(X, -1)$, $\gcd(k, q^2 - 1) = 1$, has a cycle of length m on $\mathbb{F}_q$ if and only if $m = \mathrm{ord}_t(k)$ or m is the smallest positive integer with $2(k^m + 1) \equiv 0 \pmod{t}$, where $t \mid q - 1$ or $t \mid q + 1$. The number N_m of those cycles satisfies*

$$m \cdot N_m = \frac{\delta + \gcd(q - 1, k^m - 1)}{2} - \varepsilon - \sum_{i \mid m, i \neq m} i \cdot N_i,$$

where

$$\varepsilon = \begin{cases} 2, & k^m \equiv 1 \text{ and } q \equiv 1 \pmod 4, \\ 0, & \text{otherwise}, \end{cases}$$

$$\delta = \begin{cases} \gcd(q - 1, k^m + 1), & \nu_2(k^m + 1) < \nu_2(q + 1), \\ \gcd(2(q + 1), k^m + 1), & \nu_2(k^m + 1) = \nu_2(q + 1), \\ \gcd(q + 1, (k^m - 1)/2), & \nu_2(k^m + 1) > \nu_2(q + 1). \end{cases}$$

2.3 Linearized Polynomials

In 1988 Mullen and Vaughan [18] determined the cycle structure of q-linearized permutation polynomials with coefficients in the subfield $\mathbb{F}_q$. We use notations similar to those of [15, pp. 107–124].

Definition 2.4. Let $\mathbb{F}_{q^n}$ be the extension field of $\mathbb{F}_q$ with q^n elements. A polynomial of shape

$$L(X) = \sum_{j=0}^{m} \alpha_j X^{q^j} \in \mathbb{F}_{q^n}[X]$$

is called a *q-linearized polynomial* or *q-polynomial* over $\mathbb{F}_{q^n}$.

Definition 2.5. A polynomial of the form $A(X) = L(X) + \alpha$, where $L(X)$ is a q-polynomial over $\mathbb{F}_{q^n}$ and $\alpha \in \mathbb{F}_{q^n}$, is called a *$q$-affine polynomial* or *affine q-polynomial* over $\mathbb{F}_{q^n}$.

Remark 2.3.

1. The associated map of a q-linearized polynomial L is an $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^n}$, i. e. a linear map of $\mathbb{F}_{q^n}$ seen as an n-dimensional vector space over $\mathbb{F}_q$.

2. The reduced polynomial of an $\mathbb{F}_q$-linear map is a q-linearized polynomial with $m < n$.

Definition 2.6. The polynomials

$$\Lambda(X) = \sum_{j=0}^{m} \alpha_j X^j \quad \text{and} \quad L(X) = \sum_{j=0}^{m} \alpha_j X^{q^j}$$

over $\mathbb{F}_{q^n}$ are called *q-associates* of each other. More specifically, $\Lambda(X)$ is the *conventional q-associate* of $L(X)$ and $L(X)$ is the *linearized q-associate* of $\Lambda(X)$.

If all coefficients of $L(X)$ are elements of $\mathbb{F}_q$, we consider $\Lambda(X)$ to be in $\mathbb{F}_q[X]$.

The following proposition, classifying q-linearized polynomials with coefficients in the subfield $\mathbb{F}_q$, is well known. A proof can be found in [3].

Proposition 2.6. *A q-linearized polynomial $L(X) \in \mathbb{F}_{q^n}[X]$ with coefficients in $\mathbb{F}_q$ is a permutation polynomial if and only if its conventional q-associate $\Lambda(X) \in \mathbb{F}_q[X]$ and $X^n - 1$ are coprime.*

The following example gives a family of linearized permutation polynomials.

Example 2.1. Let a be a primitive element of $\mathbb{F}_4$. Then $X + aX^4 \in \mathbb{F}_{4^n}[X]$ is a permutation polynomial if and only if $3 \nmid n$.

Proof. We want to show that $\gcd(X^n + 1, aX + 1) = 1$ in $\mathbb{F}_4[X]$, if and only if $3 \nmid n$. Then the claim in the example follows from Proposition 2.6.

Because $aX + 1$ is irreducible, $\gcd(X^n + 1, aX + 1) = 1$ holds if and only if $aX + 1 \nmid X^n + 1$. This is equivalent to $X + a^{-1} \nmid X^n + 1$, which is the case precisely if $\mathrm{ord}(a) \nmid n$. Since a is a primitive element of $\mathbb{F}_4$, we know $\mathrm{ord}(a) = 3$ and therefore that $\gcd(X^n + 1, aX + 1) = 1$ if and only if $3 \nmid n$. □

The following theorem, which summarizes the first part of [18], gives a method to determine the cycle structure of q-linearized permutation polynomials with coefficients in the subfield $\mathbb{F}_q$. It is not easy to apply to specific families of linearized permutation polynomials, e. g. Example 2.1, but can be used to efficiently compute the cycle structure of a given linearized permutation polynomial using a computer algebra system, e. g. SAGE or MAGMA. For a demonstration of this see Example 2.2, Example 2.3 and Table 2.1.

Theorem 2.7. *Let q be a power of the prime p and $L(X) \in \mathbb{F}_{q^n}[X]$ be a q-linearized permutation polynomial with coefficients in $\mathbb{F}_q$. Let $\Lambda(X) \in \mathbb{F}_q[X]$ be the conventional q-associate of $L(X)$. Let $n = p^t n_1$, where $\gcd(n_1, p) = 1$. Let the factorization of $X^n - 1 \in \mathbb{F}_q[X]$ be*

$$X^n - 1 = (X^{n_1} - 1)^{p^t} = \prod_{i=1}^{l} \Gamma_i(X)^{p^t}$$

where the $\Gamma_i(X)$ are distinct monic irreducible polynomials over $\mathbb{F}_q$. For any i, let $G_i(X) \in \mathbb{F}_{q^n}[X]$ be the linearized q-associate of $\Gamma_i(X)$.

Let $W_i = \ker(G_i), W_i^{(j)} = \ker(G_i^j)$, *then* $\mathbb{F}_{q^n} = \bigoplus_{i=1}^{l} W_i^{(p^t)}$ *and* L *also permutes any subspace* $W_i^{(j)}$.

The cycle structure of L *can be determined in the following way:*

1. *If the cycle structures of* $L\big|_{W_i^{(p^t)}}$ *are*

$$\mathrm{CS}_{W_i^{(p^t)}}(L) = s_{i1}^{m_{i1}} s_{i2}^{m_{i2}} \dots s_{ir_i}^{m_{ir_i}}$$

then the cycle structure of L *is*

$$CS(L) = \sum_{k \in K} S_k^{M_k}$$

where

$$\begin{aligned} K &= \{1, \dots, r_1\} \times \{1, \dots, r_2\} \times \cdots \times \{1, \dots, r_l\} \\ S_k &= \mathrm{lcm}(s_{1k_1}, s_{2k_2}, \dots, s_{lk_l}) \\ M_k &= \frac{\prod_{i=1}^{l} s_{ik_i} m_{ik_i}}{S_k} \end{aligned}$$

2. *Let* $1 \le i \le l$, $\mathbb{F}_{q^m}$ *be the splitting field of* $\Gamma_i(X)$, $\omega \in \mathbb{F}_{q^m}^*$ *a root of* $\Gamma_i(X)$, $j = \mathrm{ord}(\Lambda(\omega))$ *and* s *the largest positive integer such that* $\Gamma_i(X)^s \mid \Lambda(X)^j - 1$. *Then for the cycle structure of* L *on* $W_i^{(p^t)}$ *the following holds:*

   a) *If* $p^t = 1$ *then*

$$CS_{W_i^{(p^t)}}(L) = 1^1 j^{(q^m-1)/j}.$$

   b) *If* $s \ge p^t > 1$, *then*

$$CS_{W_i^{(p^t)}}(L) = 1^1 j^{(q^d-1)/j},$$

   where $d = \dim(W_i^{(p^t)})$.

   c) *If* $s < p^t$ *let* r *be such that* $p^{r-1}s < p^t \le p^r s$,

$$U_e = \begin{cases} \{0\}, & e = -1, \\ W_i^{(p^e s)}, & 0 \le e \le r-1, \\ W_i^{(p^t)}, & e = r \end{cases}$$

   and $d_e = \dim(U_e)$. *Then*

$$CS_{W_i^{(p^t)}}(L) = 1^1 j^{(q^{d_0}-q^{d-1})/j} (pj)^{(q^{d_1}-q^{d_0})/(pj)} \dots (p^r j)^{(q^{d_r}-q^{d_{r-1}})/(p^r j)}.$$

The following two examples show how Theorem 2.7 can be used to determine the cycle structure of a family of linearized permutation polynomials. Note that the permutation polynomials considered in Example 2.2 are a small subset of the family described in Example 2.1. Example 2.3 shows that this general description of the cycle structure can not be easily extended to the whole family.

Example 2.2. Let a be a primitive element of $\mathbb{F}_4$. Then the cycle structure of the permutation polynomial $L(X) = X + aX^4 \in \mathbb{F}_{4^{2^t}}[X]$ is

$$\mathrm{CS}(L) = 1^1 3^1 6^2 12^{20} \dots (2^t \cdot 3)^{(4^{2^t} - 4^{2^{t-1}})/(2^t \cdot 3)}.$$

Proof. With the notations of Theorem 2.7 we have $p = 2$, $n = 2^t$, so $n_1 = 1$ and $\Lambda(X) = aX + 1$. Further $X^n + 1 = (X + 1)^{2^t}$, so we only have 1 factor. This means we can determine the cycle structure using only part 2 of Theorem 2.7.

Now $\Gamma_1(X) = X + 1$ and its splitting field is $\mathbb{F}_4$, $\omega = 1$ is a root of Γ_1, so

$$j = \mathrm{ord}(\Lambda(1)) = \mathrm{ord}(a + 1) = 3.$$

Since $\Lambda(X)^j - 1 = X(X + 1)(X + a)$ we get $s = 1$. This means we are in case (c) of part 2 of Theorem 2.7, i. e. $s < 2^t$. Because $2^{t-1} \cdot 1 < 2^t \leq 2^t \cdot 1$, we get $r = t$. Now $U_{-1} = \{0\}$ and

$$U_k = W_1^{(2^k)} = \ker(G_1^{2^k}) = \ker(X^{4^k} + X) = \mathbb{F}_{4^{2^k}} \text{ for } 0 \leq k \leq t.$$

Consequently $d_{-1} = \dim(\{0\}) = 0$ and $d_k = \dim(\mathbb{F}_{4^{2^k}}) = 2^k$, for $0 \leq k \leq t$. Now by Theorem 2.7 the cycle structure of L is

$$\begin{aligned}\mathrm{CS}(L) &= \mathrm{CS}_{W_1^{(2^t)}}(L) \\ &= 1^1 3^{(4^1 - 4^0)/3} (2 \cdot 3)^{(4^2 - 4^1)/(2 \cdot 3)} (4 \cdot 3)^{(4^4 - 4^2)/(4 \cdot 3)} \dots (2^t \cdot 3)^{(4^{2^t} - 4^{2^{t-1}})/(2^t \cdot 3)}.\end{aligned}$$

□

Example 2.3. Let a be a primitive element of $\mathbb{F}_4$ and $L(X) = X + aX^4 \in \mathbb{F}_{4^5}[X]$. Then the cycle structure of L is $\mathrm{CS}(L) = 1^1 3^1 5^3 15^{67}$.

Proof. With the notations of Theorem 2.7 we have $p = 2$, $n = 5$, so $n_1 = 5$ and $\Lambda(X) = aX + 1$. Further $X^5 + 1 = (X + 1)(X^2 + aX + 1)(X^2 + a^2X + 1)$, so

$$\Gamma_1(X) = X + 1 \qquad \Gamma_2(X) = X^2 + aX + 1 \qquad \Gamma_2(X) = X^2 + a^2X + 1.$$

Since $t = 0$, we get p^t=1 and are always in case (a) of part 2 of Theorem 2.7. This means we only need to determine the respective splitting field of Γ_i to determine the cycle structure on $W_i^{(2^t)} = W_i$.

The splitting field of $\Gamma_1(X) = X + 1$ is $\mathbb{F}_{4^1}$, a root of $\Gamma_i(X)$ is 1, so the number $j = \mathrm{ord}(\Lambda(1)) = \mathrm{ord}(a + 1) = 3$ and

$$\mathrm{CS}_{W_1}(L) = 1^1 3^{(4-1)/3} = 1^1 3^1.$$

The splitting field of $\Gamma_2(X) = X^2 + aX + 1$ is $\mathbb{F}_{4^2}$, let ω be a root of $\Gamma_2(X)$, then $j = \mathrm{ord}(a\omega + 1) = 5$ and

$$\mathrm{CS}_{W_2}(L) = 1^1 5^{(4^2-1)/5} = 1^1 5^3.$$

The splitting field of $\Gamma_3(X) = X^2 + a^2X + 1$ is $\mathbb{F}_{4^2}$, let ω be a root of $\Gamma_3(X)$, then $j = \mathrm{ord}(a\omega + 1) = 15$ and

$$\mathrm{CS}_{W_3}(L) = 1^1 15^{(4^2 1)/15} = 1^1 15^1.$$

Now we need to use part 1 of Theorem 2.7 to compute the cycle structure of L on the whole field $\mathbb{F}_{4^5}$. $K = \{1,2\} \times \{1,2\} \times \{1,2\}$,

$$s_{11} = s_{21} = s_{31} = 1, s_{12} = 3, s_{22} = 5, s_{23} = 15,$$
$$m_{11} = m_{21} = m_{21} = m_{31} = m_{32} = 1 \text{ and } m_{22} = 3.$$

So

$$\begin{aligned}
S_{(111)} &= \mathrm{lcm}(1,1,1) = 1, & M_{(111)} &= (1\cdot 1)(1\cdot 1)(1\cdot 1)/1 = 1,\\
S_{(112)} &= \mathrm{lcm}(1,1,15) = 15, & M_{(112)} &= (1\cdot 1)(1\cdot 1)(1\cdot 15)/15 = 1,\\
S_{(121)} &= \mathrm{lcm}(1,5,1) = 5, & M_{(121)} &= (1\cdot 1)(3\cdot 5)(1\cdot 1)/5 = 3,\\
S_{(122)} &= \mathrm{lcm}(1,5,15) = 15, & M_{(122)} &= (1\cdot 1)(3\cdot 5)(1\cdot 15)/15 = 15,\\
S_{(211)} &= \mathrm{lcm}(3,1,1) = 3, & M_{(211)} &= (1\cdot 3)(1\cdot 1)(1\cdot 1)/3 = 1,\\
S_{(212)} &= \mathrm{lcm}(3,1,15) = 15, & M_{(212)} &= (1\cdot 3)(1\cdot 1)(1\cdot 15)/15 = 3,\\
S_{(221)} &= \mathrm{lcm}(3,5,1) = 15, & M_{(221)} &= (1\cdot 3)(3\cdot 5)(1\cdot 1)/15 = 3,\\
S_{(222)} &= \mathrm{lcm}(3,5,15) = 15, & M_{(222)} &= (1\cdot 3)(3\cdot 5)(1\cdot 15)/15 = 45.
\end{aligned}$$

Thus

$$\mathrm{CS}(L) = 1^1 + 15^1 + 5^3 + 15^{15} + 3^1 + 15^3 + 15^3 + 15^{45} = 1^1 3^1 5^3 15^{67}.$$

□

Table 2.1 contains the cycle structures of specific linearized permutation polynomials. These were computed in MAGMA using the method from Theorem 2.7.

In [20] Panario and Reis studied the functional graph of linearized polynomials. For linearized permutation polynomials this is the same as determining the cycle structure. To state their result we need to define an analogue of Euler's totient function for polynomials.

Table 2.1: The cycle structure of $X + aX^4 \in \mathbb{F}_{4^n}[X]$.

n	**cycle structure**
7	$1^1\ 3^1\ 63^{260}$
11	$1^1\ 3^1\ 1023^{4100}$
14	$1^1\ 3^1\ 6^2\ 63^{260}\ 126^{2130310}$
19	$1^1\ 3^1\ 29127^{9437220}$
22	$1^1\ 3^1\ 6^2\ 1023^{4100}\ 2046^{8598329350}$
23	$1^1\ 3^1\ 1398101^3\ 4194303^{16777219}$
28	$1^1\ 3^1\ 6^2\ 12^{20}\ 63^{260}\ 126^{2130310}\ 252^{285942832418620}$
31	$1^1\ 3^1\ 341^{3075}\ 1023^{4508001973046275}$
34	$1^1\ 3^1\ 6^2\ 85^{771}\ 170^{25264128}\ 255^{67371779}\ 510^{578721382662505990}$
35	$1^1\ 3^1\ 5^3\ 15^{67}\ 63^{260}\ 315^{13260}\ 819^{81920}\ 4095^{288300762079936512}$
38	$1^1\ 3^1\ 6^2\ 29127^{9437220}\ 58254^{1297041640499183670}$
40	$1^1\ 3^1\ 5^3\ 6^2\ 10^{24}\ 12^{20}\ 15^{67}\ 20^{3264}\ 24^{2720}\ 30^{34910}\ 40^{107372544}\ 60^{18325175228}\ 120^{10074381830112711400928}$
44	$1^1\ 3^1\ 6^2\ 12^{20}\ 1023^{4100}\ 2046^{8598329350}\ 4092^{756317228302364312167 00}$
46	$1^1\ 3^1\ 6^2\ 1398101^3\ 2796202^{6291456}\ 4194303^{16777219}\ 8388606^{5902959510962170757 18}$
49	$1^1\ 3^1\ 63^{260}\ 4398046511103^{72057594037944320}$
52	$1^1\ 3^1\ 6^2\ 12^{20}\ 455^9\ 910^{18432}\ 1365^{49161}\ 1820^{154656571392}\ 2730^{1649670162450}\ 5460^{37147270336358361975957260 04}$
56	$1^1\ 3^1\ 6^2\ 12^{20}\ 24^{2720}\ 63^{260}\ 126^{2130310}\ 252^{285942832418620}\ 504^{10302176306616721342208139466720}$
58	$1^1\ 3^1\ 6^2\ 89478485^3\ 178956970^{402653184}\ 268435455^{1073741827}\ 536870910^{15474250548713328814220 9030}$
61	$1^1\ 3^1\ 54901024028897475^{96845406386975146068}$
65	$1^1\ 3^1\ 5^3\ 15^{67}\ 455^{589968}\ 585^{29367296}\ 819^{81940}\ 1365^{211157784529872}\ 4095^{33238814839652108763204156271884 5948}$
68	$1^1\ 3^1\ 6^2\ 12^{20}\ 85^{771}\ 170^{25264128}\ 255^{67371779}\ 340^{54255129615925248}\ 510^{578721382662505990}\ 1020^{85404201893882594751284612601258720316}$
70	$1^1\ 3^1\ 5^3\ 6^2\ 10^{24}\ 15^{67}\ 30^{34910}\ 63^{260}\ 126^{2130310}\ 315^{13260}\ 630^{27923670450}\ 819^{81920}\ 1638^{2749450117120}\ 4095^{288300762079936512}\ 8190^{17018273197901879686749716677638751 0272}$
73	$1^1\ 3^1\ 13797^{19923020}\ 87381^{3145740}\ 262143^{34028366500010487621696125050294 2654460}$

Definition 2.7. Let $F(X) \in \mathbb{F}_q[X]$ be monic. Then Euler's totient function for polynomials is defined as

$$\Phi(F) = \left| \left(\frac{\mathbb{F}_q[X]}{\langle F \rangle} \right)^* \right|,$$

where $\langle F \rangle$ is the ideal generated by $F(X)$ in $\mathbb{F}_q[X]$. Equivalently $\Phi(F)$ is the number of $G(X) \in \mathbb{F}_q[X]$, with $\deg(G(X)) < \deg(F(X))$ and $\gcd(G(X), F(X)) = 1$.

The following theorem gives a formula for the cycle structure of q-linearized permutation polynomials with coefficients in $\mathbb{F}_q$.

Theorem 2.8. *Let $\Lambda(X) \in \mathbb{F}_q[X]$ be a polynomial with $\gcd(\Lambda(X), X^n - 1) = 1$ and $L(X) \in \mathbb{F}_{q^n}[X]$ be its linearized q-associate. Let $\mathrm{ord}_\Gamma(\Lambda)$ denote the multiplicative order of $\Lambda(X)$ modulo $\Gamma(X)$ and Φ be Euler's totient function for polynomials. Then the cycle structure of L is*

$$CS(L) = \sum_{\Gamma(X) | X^n - 1} \mathrm{ord}_\Gamma(\Lambda)^{\frac{\Phi(\Gamma)}{\mathrm{ord}_\Gamma(\Lambda)}}.$$

Remark 2.4. Let L, Λ, Γ as before. The number of cycles of length $\mathrm{ord}_\Gamma(\Lambda)$ in the cycle decomposition of L is

$$\frac{\sum_{H \in \mathcal{H}} \Phi(H)}{\mathrm{ord}_\Gamma(\Lambda)},$$

where $\mathcal{H} = \{H \in \mathbb{F}_q[X] : H \mid X^n - 1, \mathrm{ord}_H(\Lambda) = \mathrm{ord}_\Gamma(\Lambda)\}$.

For an application of Theorem 2.8 see Theorem 5.10.

For a survey of further results on functional graphs of permutation polynomials see Martins, Panario, and Qureshi [17].

2.4 Rational Functions and Carlitz

Carlitz showed the following in [2].

Theorem 2.9. *Every permutation polynomial of a finite field $\mathbb{F}_q$ can be written as a composition of permutation polynomials $\alpha X + \beta, X^{q-2} \in \mathbb{F}_q[X]$, where the coefficients $\alpha \in \mathbb{F}_q^*, \beta \in \mathbb{F}_q$.*

He did this by first showing that the transposition $(0\ a)$, where $a \in \mathbb{F}_q$, is the associated map of the polynomial

$$-a^2 \left(\left((X - a)^{q-2} + a^{-1} \right)^{q-2} - a \right)^{q-2} \in \mathbb{F}_q[X].$$

Remark 2.5. This means every permutation polynomial over $\mathbb{F}_q$ can be written as a

$$\mathcal{P}_n(X) = (\ldots((a_0 X + a_1)^{q-2} + a_2)^{q-2} + \cdots + a_n)^{q-2} + a_{n+1}, \tag{2.1}$$

where $n \geq 1, a_i \neq 0$ for $i \in \{0, 2, 3, \ldots, n\}$.

Çeşmelioğlu, Meidl, and Topuzoğlu determined the cycle structure of polynomials $\mathcal{P}_2$ and $\mathcal{P}_3$ in [4] using the following generalisation of Chou's result from [6], for which they gave a new proof.

Definition 2.8. Let

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

be a nonconstant rational transformation. Its *associated permutation* of $\mathbb{F}_q$ is

$$E(x) = \begin{cases} R(x), & x \neq \frac{-d}{c}, \\ \frac{a}{c}, & x = \frac{-d}{c} \end{cases}.$$

The *associated matrix* of $R(X)$ and E is

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

The following theorem gives the cycle structure of the associated permutations of rational transformations.

Theorem 2.10. *Let $q = p^s$, $R(X) \in \mathbb{F}_q(X)$, E be its associated permutation and $\chi(X) \in \mathbb{F}_q[X]$ be the characteristic polynomial of the associated matrix A of $R(X)$ and E. Let $\alpha, \beta \in \mathbb{F}_{q^2}$ be the roots of $\chi(X)$ in its splitting field and $k = \mathrm{ord}(\alpha/\beta)$. Then the cycle structure of E satisfies the following.*

1. *If $\chi(X)$ is irreducible then $2 < k$ and $k \mid q+1$. Let $tk = q+1$. Then*

$$\mathrm{CS}(E) = (k-1)^1 k^{t-1}.$$

2. *If $\alpha, \beta \in \mathbb{F}_q$ and $\alpha \neq \beta$ then $k \mid q-1$. Let $tk = q-1$. Then*

$$\mathrm{CS}(E) = 1^2 (k-1)^1 k^{t-1}.$$

3. *If $\alpha = \beta \in \mathbb{F}_q^*$ then*

$$\mathrm{CS}(E) = 1^1 (p-1)^1 p^{p^{s-1}-1}$$

By replacing the exponent $q-2$ by -1 and using continued fractions Çeşmelioğlu, Meidl, and Topuzoğlu showed the following.

Definition 2.9. Let $\mathcal{P}_n$ be as in (2.1). Then

$$\mathcal{R}_n(X) = \frac{\alpha_{n-1}X + \beta_{n-1}}{\alpha_n X + \beta_n},$$

where $\alpha_k = a_k\alpha_{k-1} + \alpha_{k-2}$ and $\beta_k = a_k\beta_{k-1} + \beta_{k-2}$ for $k \geq 2$ and $\alpha_0 = 0, \alpha_1 = a_0, \beta_0 = 1, \beta_1 = a_1$ is its *corresponding rational function* and

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

is its *set of poles.*

Lemma 2.11. *Let $\mathcal{P}_n$ be as in (2.1), $\mathcal{R}_n(X)$ be its corresponding rational function, $\mathcal{E}_n$ the associated permutation of $\mathcal{R}_n(X)$ and $\mathbf{O}_n$ the set of poles. If $\infty \notin \mathbf{O}_n$ and $|\mathbf{O}_n| = n$ then*

$$\mathcal{P}_n(x_i) = \begin{cases} \mathcal{E}_n(x_{i-1}), & 2 \le i \le n, \\ \mathcal{E}_n(x_n), & i = 1. \end{cases}$$

So the permutation can be written as the composition

$$\mathcal{P}_n(x) = (\mathcal{E}_n(x_{n-1}) \ \dots \ \mathcal{E}_n(x_1) \ \mathcal{E}_n(x_n)) \circ \mathcal{E}_n(x).$$

By determining how composition with a cycle of length two or three changes the cycle structure of the associated permutation of a rational transformation, they were then able to determine the cycle structure of $\mathcal{P}_2$ and $\mathcal{P}_3$. Sometimes the order of the cycle structure will depend on the parameters. An unordered cycle structure will be denoted by CS^*.

Cycle structure of $\mathcal{P}_2$

Recall that

$$\mathcal{P}_2(X) = ((a_0X + a_1)^{q-2} + a_2)^{q-2} + a_3, \quad a_0a_2 \neq 0.$$

Its corresponding rational function is

$$\mathcal{R}_2(X) = \frac{a_0(a_2a_3 + 1)X + a_1(a_2a_3 + 1) + a_3}{a_0a_2X + a_1a_2 + 1}.$$

The poles are

$$x_1 = -\frac{a_1}{a_0}, \qquad x_2 = -\frac{a_1a_2 + 1}{a_0a_2}.$$

The characteristic polynomial of the associated matrix is

$$\chi(X) = X^2 - (a_0(a_2a_3 + 1) + a_1a_2 + 1)X + a_0.$$

In the following we state Theorem 6 and 7 of [4].

Theorem 2.12. *Suppose $\chi(X)$ has two distinct roots $\alpha, \beta \in \mathbb{F}_{q^2}$. Let $k = \mathrm{ord}(\alpha/\beta)$, $k > 2$ and*

$$kt = \begin{cases} q + 1, & \alpha, \beta \notin \mathbb{F}_q, \text{ i. e. } \chi(X) \text{ irreducible}, \\ q - 1, & \alpha, \beta \in \mathbb{F}_q, \text{ i. e. } \chi(X) \text{ reducible}. \end{cases}$$

Let $\delta = (\beta - 1)/(\alpha - 1) \in \mathbb{P}^1(\mathbb{F}_q)$. Then the following holds.

1. *If $\delta^k \neq 1$ and $\chi(X)$ is irreducible, then*

$$\mathrm{CS}(\mathcal{P}_2) = k^{t-2}(2k - 1)^1.$$

In particular $\mathcal{P}_2$ is a full cycle if $k = (q + 1)/2$.

2. *If $\delta^k \neq 1$ and $\chi(X)$ is reducible, then*

$$\mathrm{CS}(\mathcal{P}_2) = \begin{cases} 1^2 k^{t-2}(2k-1)^1, & a_3 \neq -a_1/a_0, \\ 1^1 k^t, & a_3 = -a_1/a_0. \end{cases}$$

3. *If $\delta^k = 1$ and $\chi(X)$ is irreducible, then*

$$\mathrm{CS}^*(\mathcal{P}_2) = (k-n-1)^1 n^1 k^{t-1},$$

where n is the smallest integer s. t. $(\alpha/\beta)^n = \delta$.

4. *If $\delta^k = 1$ and $\chi(X)$ is reducible, then*

$$\mathrm{CS}^*(\mathcal{P}_2) = 1^2 (k-n-1)^1 n^1 k^{t-1},$$

where n is the smallest integer s. t. $(\alpha/\beta)^n = \delta$.

Theorem 2.13. *Let $q = p^s$. Suppose $\chi(X)$ has a double root $\alpha \neq 0$. Then the following holds.*

1. *If $\alpha = 1$, then $a_0 = 1, a_3 = -a_1/a_0$ and*

$$\mathrm{CS}(\mathcal{P}_2) = p^{p^{s-1}}.$$

In particular if $s = 1$, then $\mathcal{P}_2$ is a full cycle of length $q = p$.

2. *If $\alpha \in \mathbb{F}_p \setminus \{1\}$, then*

$$\mathrm{CS}^*(\mathcal{P}_2) = 1^1 (p-n-1)^1 n^1 p^{p^{s-1}-1},$$

where $n \equiv \alpha/(1-\alpha) \pmod p$.

3. *If $s > 1$ and $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$, then*

$$\mathrm{CS}(\mathcal{P}_2) = 1^1 p^{p^{s-1}-2} (2p-1)^1.$$

Cycle structure of $\mathcal{P}_3$

The possible cycle structures of $\mathcal{P}_3$ do not change if we only consider those $\mathcal{P}_3$, where $a_4 = 0$, therefore and for simplicity Çeşmelioğlu, Meidl, and Topuzoğlu restrict themselves to analysis of permutation polynomials of the form

$$P_3(X) = \Big(\big((a_0X + a_1)^{q-2} + a_2\big)^{q-2} + a_3\Big)^{q-2}, \quad a_0a_2a_3 \neq 0.$$

The corresponding rational function is

$$R_3(X) = \frac{a_0a_2X + a_1a_2 + 1}{a_0(a_2a_3+1)X + a_1(a_2a_3+1) + a_3}.$$

The poles are

$$x_1 = -\frac{a_1}{a_0}, \qquad x_2 = -\frac{a_1a_2+1}{a_0a_2}, \qquad x_3 = -\frac{a_1(a_2a_3+1)+a_3}{a_0(a_2a_3+1)}.$$

The characteristic polynomial of the associated matrix is

$$\chi(X) = X^2 - (a_0a_2 + a_1(a_2a_3+1) + a_3)\,X - a_0.$$

In the following we state Theorems 11, 13 and 15 of [4], with added specification of the parameters n and m based on the lemmas and remarks in Section 4 of the same paper and necessary modifications based on this.

Remark 2.6. Here δ_1 and δ_2 correspond to γ_1 and γ_2 in [4], but δ_3 corresponds to ${}^1\!/_{\gamma_3}$.

Theorem 2.14. *Suppose $\chi(X)$ is irreducible with roots $\alpha, \beta \in \mathbb{F}_{q^2}$. Let $k = \operatorname{ord}({}^{\alpha}\!/_{\beta})$, $k > 2$ and $kt = q+1$. Let*

$$\delta_1 = \frac{\beta - a_3}{\alpha - a_3}, \qquad \delta_2 = \frac{a_2\beta + 1}{a_2\alpha + 1}, \qquad \delta_3 = \frac{\alpha - a_1}{\beta - a_1}, \qquad \delta_1, \delta_2, \delta_3 \in \mathbb{P}^1(\mathbb{F}_q)$$

and n_i be the smallest integers s. t. $({}^{\alpha}\!/_{\beta})^{n_i} = \delta_i$ for $i = 1, 2, 3$. Then the following holds.

1. *If $\delta_1^k = \delta_2^k = 1$ then*

$$\mathrm{CS}^*(P_3) = \begin{cases} (k-1)^1 k^{t-1}, & n_1 > n_2, \\ (n_2 - n_1)^1 (k - n_2 - 1)^1 n_1^1 k^{t-1}, & n_1 < n_2. \end{cases}$$

   In particular P_3 is a full cycle if $n_1 > n_2$ and $k = q+1$.

2. *If $\delta_1^k \neq 1$ and $\delta_2^k = 1$ then*

$$\mathrm{CS}(P_3) = (k - n_2 - 1)^1 k^{t-2} (k + n_2)^1.$$

3. *If $\delta_1^k, \delta_2^k, \delta_3^k \neq 1$ then*

$$\mathrm{CS}(P_3) = k^{t-3}(3k-1)^1.$$

   In particular P_3 is a full cycle if $k = (q+1)/3$.

4. *If $\delta_1^k, \delta_2^k \neq 1$ and $\delta_3^k = 1$ then*

$$\mathrm{CS}(P_3) = (k - n_3)^1 k^{t-2} (k + n_3 - 1)^1.$$

5. *If $\delta_1^k = 1$ and $\delta_2^k \neq 1$ then*

$$\mathrm{CS}(P_3) = n_1^1 k^{t-2} (2k - n_1 - 1)^1.$$

Theorem 2.15. *Suppose $\chi(X)$ has two distinct roots $\alpha, \beta \in \mathbb{F}_q$. Let $k = \mathrm{ord}(\alpha/\beta)$, $k \geq 2$ and $kt = q-1$. Let*

$$\delta_1 = \frac{\beta - a_3}{\alpha - a_3}, \qquad \delta_2 = \frac{a_2\beta + 1}{a_2\alpha + 1}, \qquad \delta_3 = \frac{\alpha - a_1}{\beta - a_1}, \qquad \delta_1, \delta_2, \delta_3 \in \mathbb{P}^1(\mathbb{F}_q)$$

and n_i be the smallest integers s. t. $(\alpha/\beta)^{n_i} = \delta_i$ for $i = 1, 2, 3$. Then the following holds.

1. *If $a_3 \neq -a_0/a_1$, $a_2 \neq -1/a_1$ and $\delta_1^k = \delta_2^k = 1$ then*

$$\mathrm{CS}^*(P_3) = \begin{cases} 1^2(k-1)^1 k^{t-1}, & n_1 > n_2, \\ 1^2(n_2 - n_1)^1 (k - n_2 - 1)^1 n_1^1 k^{t-1}, & n_1 < n_2. \end{cases}$$

2. *If $a_3 \neq -a_0/a_1$, $a_2 \neq -1/a_1$, $\delta_1^k \neq 1$ and $\delta_2^k = 1$ then*

$$\mathrm{CS}(P_3) = 1^2(k - n_2 - 1)^1 k^{t-2}(k + n_2)^1.$$

3. *If $a_3 \neq -a_0/a_1$, $a_2 \neq -1/a_1$ and $\delta_1^k, \delta_2^k, \delta_3^k \neq 1$ then*

$$\mathrm{CS}(P_3) = 1^2 k^{t-3}(3k-1)^1.$$

4. *If $a_3 \neq -a_0/a_1$, $a_2 \neq -1/a_1$, $\delta_1^k, \delta_2^k \neq 1$ and $\delta_3^k = 1$ then*

$$\mathrm{CS}(P_3) = 1^2(k - n_3)^1 k^{t-2}(k + n_3 - 1)^1.$$

5. *If $a_3 \neq -a_0/a_1$, $a_2 \neq -1/a_1$, $\delta_1^k = 1$ and $\delta_2^k \neq 1$ then*

$$\mathrm{CS}(P_3) = 1^2 n_1^1 k^{t-2}(2k - n_1 - 1)^1.$$

6. *If $a_3 = -a_0/a_1$ and $a_2 = -1/a_1$, then*

$$\mathrm{CS}(P_3) = k^{t-1}(k+1)^1.$$

   In particular P_3 is a full cycle if $k = q-1$.

7. *If $a_3 = -a_0/a_1$ and $\delta_2^k = 1$ then*

$$\mathrm{CS}^*(P_3) = 1^1(k - n_2)^1 n_2^1 k^{t-1}.$$

8. *If $a_2 = -1/a_1$ and $\delta_1^k = 1$ then*

$$\mathrm{CS}^*(P_3) = 1^1(k - n_1)^1 n_1^1 k^{t-1}.$$

9. *If $a_3 = -a_0/a_1$, $a_2 \neq -1/a_1$ and $\delta_2^k \neq 1$ or $a_3 \neq -a_0/a_1$, $a_2 = -1/a_1$ and $\delta_1^k \neq 1$ then*

$$CS(P_3) = 1^1 k^{t-2}(2k)^1.$$

Theorem 2.16. *Suppose $\chi(X)$ has a double root $\alpha \in \mathbb{F}_q^* = \mathbb{F}_{p^s}^*$. Define*

$$n_1 := \frac{\alpha}{a_3 - \alpha}, \qquad n_2 := -\frac{a_2\alpha}{a_2\alpha + 1}, \qquad n_3 := \frac{\alpha}{\alpha - a_1}.$$

If $n_1, n_2, n_3 \in \mathbb{F}_p$, we consider them as integers $0 \leq n_1, n_2, n_3 \leq p-1$. Then the following holds.

1. *If ${}^{\alpha}/_{a_3} \in \mathbb{F}_p \setminus \{1\}$ and $-a_2\alpha \in \mathbb{F}_p \setminus \{1\}$ then*

$$\mathrm{CS}^*(P_3) = \begin{cases} 1^1(p-1)^1 p^{p^{s-1}-1}, & n_1 > n_2, \\ 1^1(n_2-n_1)^1(p-n_2-1)^1 n_1^1 p^{p^{s-1}-1}, & n_1 < n_2. \end{cases}$$

2. *If $\alpha = -{}^{1}/_{a_2}$ and ${}^{\alpha}/_{a_3} \in \mathbb{F}_p \setminus \{1\}$ then*

$$\mathrm{CS}(P_3) = (p-n_1)^1 n_1^1 p^{p^{s-1}-1}.$$

3. *If $\alpha = a_3$ and $-a_2\alpha \in \mathbb{F}_p \setminus \{1\}$ then*

$$\mathrm{CS}(P_3) = (p-n_2)^1 n_2^1 p^{p^{s-1}-1}.$$

4. *If $s \geq 2$, ${}^{\alpha}/_{a_3} \in \mathbb{F}_p \setminus \{1\}$ and $-a_2\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$, then*

$$\mathrm{CS}(P_3) = 1^1 n_1^1 p^{p^{s-1}-2}(2p-n_1-1)^1.$$

5. *If $s \geq 2$, ${}^{\alpha}/_{a_3} \in \mathbb{F}_q \setminus \mathbb{F}_p$ and $-a_2\alpha \in \mathbb{F}_p \setminus \{1\}$, then*

$$\mathrm{CS}(P_3) = 1^1(p-n_2-1)^1 p^{p^{s-1}-2}(p+n_2)^1$$

6. *If $s \geq 2$, 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*

$$\mathrm{CS}(P_3) = p^{p^{s-1}-2}(2p)^1.$$

7. *If $s \geq 2$, $-a_2\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$ and ${}^{\alpha}/_{a_1} \in \mathbb{F}_p \setminus \{1\}$ or $a_1 = 0$, then*

$$\mathrm{CS}^*(P_3) = 1^1(p-n_3)^1(p+n_3-1)^1 p^{p^{s-1}-2}.$$

8. *If $s \geq 2$, ${}^{\alpha}/_{a_3} \in \mathbb{F}_q \setminus \mathbb{F}_p$, $-a_2\alpha \in \mathbb{F}_q \setminus \mathbb{F}_p$, ${}^{\alpha}/_{a_1} \in \mathbb{F}_q \setminus \mathbb{F}_p$ and $a_1 \neq 0$, then*

$$\mathrm{CS}(P_3) = 1^1 p^{p^{s-1}-3}(3p-1)^1.$$

The special case $x_3 = \infty$

Finally we need to consider the special case $a_2a_3 + 1 = 0$. In this case $x_3 = \infty$ and

$$P_3(X) = \left(\left((a_0X + a_1)^{q-2} + a_2\right)^{q-2} - \frac{1}{a_2}\right)^{q-2}. \tag{2.2}$$

Then R_3 reduces to the linear polynomial

$$R_3(X) = -a_0a_2^2X - (a_1a_2^2 + a_2),$$

$E_3(x) = R_3(x)$, $x \in \mathbb{F}_q$ and $P_3 = (-a_2\ 0) \circ E_3$.

This case was not explicitly computed in [4]. We derive it in Theorem 2.18 based on Lemma 2.17, which is Lemma 4 in [4].

Notation 2.10. Let E be a permutation of $\mathbb{F}_q$ and $x \in \mathbb{F}_q$. By $\mathcal{C}(E, x)$ denote the cycle of E containing x and by $\ell(E, x)$ the length of that cycle.

Lemma 2.17 describes the behaviour of the cycle structure of the composition of a transposition with an arbitrary permutation.

Lemma 2.17. *Let E be a permutation of $\mathbb{F}_q$, $u, v \in \mathbb{F}_q$ and $P = (u\ v) \circ E$.*

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

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

Theorem 2.18. *Let $q = p^s$, P_3 be as in (2.2), $k = \operatorname{ord}(-a_0a_2^2)$, $kt = q - 1$ and $\delta := \frac{a_1a_2 - a_0a_2^2}{a_1a_2 + 1}$. Then the following holds.*

1. *If $-a_0a_2^2 = 1$ and $a_1a_2^2 + a_2 = 0$, then*

$$\mathrm{CS}(P_3) = 1^{q-2}2^1.$$

2. *If $-a_0a_2^2 = 1$ and $a_1a_2^2 + a_2 \neq 0$, then*

   a) for $a_1a_2 \in \mathbb{F}_p \setminus \{-1\}$, we have

$$\mathrm{CS}^*(P_3) = (p - n)^1 n^1 p^{p^{s-1}-1},$$

   where $n \equiv 1/(a_1a_2 + 1) \pmod p$, and

   b) for $a_1a_2 \in \mathbb{F}_q \setminus \mathbb{F}_p$, we have

$$\mathrm{CS}(P_3) = p^{p^{s-1}-2}(2p)^1.$$

3. *If $-a_0a_2^2 \neq 1$ and $a_1 = -1/a_2$ or $a_1 = a_0a_2$, then*

$$\mathrm{CS}(P_3) = k^{t-1}(k + 1)^1.$$

   In particular P_3 is a full cycle if $k = q - 1$.

4. If If $-a_0a_2^2 \neq 1$ *and* $a_1 \neq -1/a_2$ *and* $a_1 \neq a_0a_2$*, then*

a) for $\delta^k = 1$*, we have*

$$\mathrm{CS}^*(P_3) = 1^1(k-n)^1n^1k^{t-1},$$

where n *is the smallest positive integer s. t.* $(-a_0a_2^2)^n = \delta$*, and*

b) for $\delta^k \neq 1$*, we have*

$$\mathrm{CS}(P_3) = 1^1k^{t-2}(2k)^1.$$

Proof. Recall that for $x \in \mathbb{F}_q$ the permutation satisfies $P_3(x) = ((-a_2\ 0) \circ E_3)(x)$, where $E_3(x) = -a_0a_2^2x - (a_1a_2^2 + a_2)$.

Consider *Case 1*, $-a_0a_2^2 = 1$ and $a_1a_2^2 + a_2 = 0$. In this case $E_3(x) = x$ and thus $P_3(x) = (-a_2\ 0)(x)$ and

$$\mathrm{CS}(P_3) = 1^{q-2}2^1.$$

Consider *Case 2*, $-a_0a_2^2 = 1$ and $a_1a_2^2 + a_2 \neq 0$. In this case

$$\mathrm{CS}(E_3) = p^{p^{s-1}}.$$

Now we have to determine if 0 and $-a_2$ are contained in the same cycle of E_3, i. e. if there exists an integer n with $E_3^n(0) = -a_2$. We have

$$\begin{aligned} E_3^n(0) &= -n(a_1a_2^2 + a_2), \text{ so} \\ -a_2 &= E_3^n(0), \text{ if and only if} \\ -a_2 &= -n(a_1a_2^2 + a_2), \text{ i. e.} \\ n &= \frac{a_2}{a_1a_2^2 + a_2} = \frac{1}{a_1a_2 + 1}. \end{aligned}$$

An n with this property exists if and only if $a_1a_2 + 1 \in \mathbb{F}_p \setminus \{0\}$, or equivalently $a_1a_2 \in \mathbb{F}_p \setminus \{-1\}$.

Therefore if $a_1a_2 \in \mathbb{F}_p \setminus \{-1\}$, consider $n = \frac{1}{a_1a_2+1} \in \mathbb{F}_p$ as an integer with $0 < n < p$. Then $-a_2 = E_3^n(0)$, $\ell(E_3, 0) = p$ and using Lemma 2.17 we see $-a_2 \notin \mathcal{C}(P_3, 0)$, $\ell(P_3, 0) = n$ and $\ell(P_3, -a_2) = p - n$. The cycle structure of P_3 is then

$$\mathrm{CS}^*(P_3) = (p-n)^1n^1p^{p^{s-1}-1}.$$

If otherwise $a_1a_2 \in \mathbb{F}_q \setminus \mathbb{F}_p$, then $-a_2 \notin \mathcal{C}(E_3, 0)$, $\ell(E_3, 0) = \ell(E_3, -a_2) = p$. Using Lemma 2.17 we see $-a_2 \in \mathcal{C}(P_3, 0)$ and $\ell(P_3, 0) = 2p$. The cycle structure of P_3 is then

$$\mathrm{CS}(P_3) = p^{p^{s-1}-2}(2p)^1.$$

Consider *Case 3* and *Case 4*, $-a_0a_2^2 \neq 1$. In these cases

$$\mathrm{CS}(E_3) = 1^1k^t,$$

where $-(a_1a_2^2 + a_2)/(1 + a_0a_2^2)$ is the fixed point.

We are in Case 3 if this fixed point is $-a_2$ or 0, i. e. $a_1 = -1/a_2$ or $a_1 = a_0 a_2$. In this case $-a_2 \notin \mathcal{C}(E_3, 0)$ and $\ell(E_3, 0) + \ell(E_3, -a_2) = k + 1$, so Lemma 2.17 shows that $-a_2 \in \mathcal{C}(P_3, 0)$ and $\ell(P_3, 0) = k + 1$. The cycle structure is

$$\mathrm{CS}(P_3) = k^{t-1}(k+1)^1.$$

If this is not the case, we get Case 4 and have to determine if 0 and $-a_2$ are contained in the same cycle of E_3, i. e. if there exists an integer n with $E_3^n(0) = -a_2$. We have

$$\begin{aligned}
E_3^n(0) &= \frac{(-a_0a_2^2)^n - 1}{-a_0a_2^2 - 1}(-(a_1a_2^2 + a_2)), \text{ so} \\
-a_2 &= E_3^n(0), \text{ if and only if} \\
-a_2 &= \frac{(-a_0a_2^2)^n - 1}{-a_0a_2^2 - 1}(-(a_1a_2^2 + a_2)), \text{ i. e.} \\
1 &= \frac{(-a_0a_2^2)^n - 1}{-a_0a_2^2 - 1}(a_1a_2 + 1), \text{ or} \\
-(a_0a_2^2)^n &= \frac{a_1a_2 - a_0a_2^2}{a_1a_2 + 1} = \delta.
\end{aligned}$$

This is exactly the case if $\delta \in \langle -a_0a_2^2 \rangle$, i. e. if $\delta^k = 1$.

Therefore if $\delta^k = 1$, let n be the smallest positive integer s. t. $(-a_0a_2^2)^n = \delta$. Then $-a_2 = E_3^n(0)$, $\ell(E_3, 0) = k$ and using Lemma 2.17 we see $-a_2 \notin \mathcal{C}(P_3, 0)$, $\ell(P_3, 0) = n$ and $\ell(P_3, -a_2) = k - n$. The cycle structure of P_3 is then

$$\mathrm{CS}^*(P_3) = 1^1(k-n)^1 n^1 k^{t-1}.$$

If otherwise $\delta^k \neq 1$, then $-a_2 \notin \mathcal{C}(E_3, 0)$, $\ell(E_3, 0) = \ell(E_3, -a_2) = k$. By Lemma 2.17 we see $-a_2 \in \mathcal{C}(P_3, 0)$ and $\ell(P_3, 0) = 2k$. The cycle structure of P_3 is then

$$\mathrm{CS}(P_3) = 1^1 k^{t-2}(2k)^1.$$

□

Chapter 3

Polynomials of Shape $X^t + \gamma f(X)$

In this chapter we consider polynomials of shape $F(X) = X^t + \gamma f(X)$, where the map $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$. The next section gives a necessary condition for F to be a permutation. We see that this can be extended to a more general class of polynomials without having to significantly alter the proof. After that we give an overview of the currently known infinite families of permutation polynomials of shape $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$. The section after that contains results on linear translators and algebraic curves that will be crucial to determine the cycle structure of some of those infinite families. In the special case $q = 2$ all permutation polynomials of shape $X + \gamma \operatorname{Tr}_{2^n/2}(X^k)$ are known. In Section 3.4 the cycle structures of these permutations are determined. Finally we see, that the number of fixed points can be determined for all permutation polynomials of shape $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$, that belong to one of the known infinite families.

3.1 A Necessary Condition

This section is based on work published in [10].

Theorem 3.1. *Let $n \geq 1$, $1 \leq t \leq q^n - 1$, $\gamma \in \mathbb{F}_{q^n}$ and $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ be an arbitrary map. If the map $F(x) = x^t + \gamma f(x)$ is a permutation of $\mathbb{F}_{q^n}$, then $\gcd(t, q^n - 1) = 1$.*

Proof. Let α be a fixed nonzero element in $\mathbb{F}_{q^n}$ with $\operatorname{Tr}_{q^n/q}(\alpha\gamma) = 0$. Consider the map $g : \mathbb{F}_{q^n} \to \mathbb{F}_q$ defined by

$$g(x) = \operatorname{Tr}_{q^n/q}(\alpha F(x)) = \operatorname{Tr}_{q^n/q}(\alpha(x^t + \gamma f(x)))$$

Since F is a permutation of $\mathbb{F}_{q^n}$, every $y \in \mathbb{F}_q$ has q^{n-1} preimages in $\mathbb{F}_{q^n}$ under g, i. e. $\left|g^{-1}(y)\right| = q^{n-1}$. Further observe that

$$g(x) = \operatorname{Tr}_{q^n/q}(\alpha(x^t + \gamma f(x))) = \operatorname{Tr}_{q^n/q}(\alpha x^t) + f(x) \operatorname{Tr}_{q^n/q}(\alpha\gamma) = \operatorname{Tr}_{q^n/q}(\alpha x^t),$$

due to the choice of α. Let $d = \gcd(t, q^n - 1)$. Then the power map $x \mapsto x^t$ is d-to-1 on $\mathbb{F}_{q^n}^*$. This shows that d must divide $\left|g^{-1}(y)\right| = q^{n-1}$ if $y \neq 0$, completing the proof. □

The above proof works for a larger class of maps on $\mathbb{F}_{q^n}$. Recall that $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is called balanced if for every $y \in \mathbb{F}_q$, the cardinality of $\{x \in \mathbb{F}_{q^n} : f(x) = y\}$ is q^{n-1}.

Theorem 3.2. *Let $G, H : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$. Suppose there exists an element $\alpha \in \mathbb{F}_{q^n}^*$ such that the map $h(x) = \mathrm{Tr}_{q^n/q}(\alpha H(x))$ is constant on $\mathbb{F}_{q^n}$ and the map $g(x) = \mathrm{Tr}_{q^n/q}(\alpha G(x))$ is not balanced. Then the sum $G + H$ is not a permutation of $\mathbb{F}_{q^n}$.*

Proof. The proof follows from the observation, that if $G + H$ is a permutation of $\mathbb{F}_{q^n}$, then necessarily the map $\mathrm{Tr}_{q^n/q}(\alpha(G(x)+H(x))) = g(x)+h(x)$ is balanced. □

Observe that $\mathrm{Tr}_{q^n/q}(\alpha H(x))$ is constant on $\mathbb{F}_{q^n}$ if and only if the image set of H is contained in a coset of the hyperplane $\mathcal{H}_\alpha = \{x \in \mathbb{F}_{q^n} : \mathrm{Tr}_{q^n/q}(\alpha x) = 0\}$. In particular such an α exists if $H(X)$ is an affine q-polynomial with a nontrivial kernel.

The next result demonstrates a specific application of Theorem 3.2.

Corollary 3.3. *Let $L : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be a q-linear map with an image set contained in $\mathcal{H}_\alpha$ for some $\alpha \in \mathbb{F}_{q^n}^*$. Furthermore, let t be a positive integer with $\gcd(t, q^n-1) > 1$, $P : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ a permutation and $K : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ arbitrary. Then $P(x)^t + L(K(x))$ is not a permutation on $\mathbb{F}_{q^n}$.*

Remark 3.1. Arguments similar to ours in the proofs of Theorem 3.1 and Theorem 3.2 are used in [21], where permutation polynomials $X^t + L(X)$ are studied, where $L(X)$ is a linearized polynomial.

3.2 Known Permutation Polynomials of Shape $X^t + \gamma\,\mathrm{Tr}(X^k)$

By Theorem 3.1, any permutation polynomial $F(X) = X^t + \gamma\,\mathrm{Tr}_{q^n/q}(X^k)$ satisfies $\gcd(t, q^n - 1) = 1$. Let t^{-1} be the inverse of t modulo $q^n - 1$. Then $F(X^{t^{-1}}) = X + \gamma\,\mathrm{Tr}_{q^n/q}(X^{kt^{-1}})$ is a permutation polynomial as well. Hence to characterize all permutation polynomials of shape $X^t+\gamma\,\mathrm{Tr}_{q^n/q}(X^k)$ it suffices to consider those with $t = 1$. Note that the polynomials $X + \gamma\,\mathrm{Tr}_{q^n/q}(X^k)$ and $X + \gamma\,\mathrm{Tr}_{q^n/q}(X^{qk})$ have the same associated map, because $\mathrm{Tr}_{q^n/q}(x^k) = \mathrm{Tr}_{q^n/q}(x^{qk})$, for $x \in \mathbb{F}_{q^n}$. Consequently if one of them is a permutation polynomial so is the other. The next theorem lists the currently known permutation polynomials of type $X + \gamma\,\mathrm{Tr}_{q^n/q}(X^k)$. Case (F_{24}) can be obtained by using results on permutations constructed via linear translators from [12]. Cases (F_1) to (F_5) for odd q, case (F_6) and cases (F_{16}) to (F_{18}) are from [11]. Cases (F_1) to (F_5) for even q, cases (F_7) to (F_{14}) and cases (F_{19}) to (F_{23}) are from [13]. Case (F_{15}) is from [16].

Theorem 3.4. *Let $q = p^s$, where p is prime and $s \geq 1$. Then*

$$F(X) = X + \gamma\,\mathrm{Tr}_{q^n/q}(X^k) \in \mathbb{F}_{q^n}[X]$$

is a permutation polynomial in each of the following cases.

(F_1) $n = 2$, $q \equiv 1 \pmod 3$, $\gamma = -1/3$, $k = 2q - 1$,

(F_2) $n = 2$, $q \equiv -1 \pmod 3$, $\gamma^3 = -1/27$, $k = 2q - 1$,

(F_3) $n = 2$, $q \equiv 1 \pmod 3$, $\gamma = 1$, $k = (q^2 + q + 1)/3$,

(F_4) $n = 2$, $q = Q^2$, $\gamma = -1$, $k = Q^3 - Q + 1$,

(F_5) $n = 2$, $q = Q^2$, $\gamma = -1$, $k = Q^3 + Q^2 - Q$,

(F_6) $n = 2$, $q \equiv 1 \pmod 4$, $(2\gamma)^{(q+1)/2} = 1$, $k = (q + 1)^2/4$,

(F_7) $n = 2$, $q = 2^s$, s *even*, $\gamma^3 = 1$, $k = (3q - 2)(q^2 + q + 1)/3$,

(F_8) $n = 2$, $q = 2^s$, s *odd*, $\gamma^3 = 1$, $k = (3q^2 - 2)(q + 4)/5$,

(F_9) $n = 2$, $q = 2^s$, $\gamma \in \mathbb{F}_q$, *s. t.* $X^3 + X + \gamma^{-1}$ *has no root in* $\mathbb{F}_q$, $k = 2^{2s-2} + 3 \cdot 2^{s-2}$,

(F_{10}) $n = 2$, $q = 2^s$, $s \equiv 1 \pmod 3$, $\gamma = 1$, $k = (2q^2 - 1)(q + 6)/7$,

(F_{11}) $n = 2$, $q = 2^s$, $s \equiv 2 \pmod 3$, $\gamma = 1$, $k = -(q^2 - 2)(q + 6)/7$,

(F_{12}) $n = 2$, $q = 2^s$, s *odd*, $\gamma^{(q+1)/3} = 1$, $k = (2^{2s-1} + 3 \cdot 2^{s-1} + 1)/3$,

(F_{13}) $n = 2$, $q = 2^s$, s *even*, $\gamma = 1$, $k = (q^2 - 2q + 4)/3$,

(F_{14}) $n = 2$, $q = 2^s$, $s = 2t$, $\gamma \in \mathbb{F}_{2^t}^*$, $k = 2^{4t-1} - 2^{3t-1} + 2^{2t-1} + 2^{t-1}$,

(F_{15}) $n = 2$, $q = 3^s$, $s \geq 2$, $\gamma^{(q-1)/2} = (\gamma - 1)^{(q-1)/2}$, $k = 3^{2s-1} + 3^s - 3^{s-1}$,

(F_{16}) $n = 3$, q *odd*, $\gamma = 1$, $k = (q^2 + 1)/2$,

(F_{17}) $n = 3$, q *odd*, $\gamma = -1/2$, $k = q^2 - q + 1$,

(F_{18}) $n = 2lr$, q *arbitrary*, $\gamma^{q^{2l}-1} = -1$, $k = q^l + 1$, *where* l, r *are positive integers,*

(F_{19}) $n = 2m$, $q = 2^s$, $\gamma \in \mathbb{F}_{q^2}^*$, $k = 2^i(q + 1)$, *where* m, i *are positive integers,*

(F_{20}) $n = 2m$, $q = 2^s$, $\gamma \in \mathbb{F}_q^*$, $k = q^2 + 1$, *where* m *is a positive integer,*

(F_{21}) $n = 2m$, $q = 2^s$, $\gamma \in \mathbb{F}_{q^2}^*$, $k = 2^i(q^2+1)$, *where* m, i *are positive integers and either* m *is even or* m *is odd and* $(\gamma^{2^{i+1}} + \gamma^{2^{i+1}q})^{(q-1)/\gcd(2^{i+1}-1, 2^s-1)} \neq 1$,

(F_{22}) $n = 2m + 1$, $q = 2^s$, $s \equiv \pm 2 \pmod 6$, $\gamma \in \mathbb{F}_q^*$, $\gamma^{(q-1)/3} \neq 1$, $k = 2q^i + 2q^j$, *where* m, i, j *are positive integers and* $i \neq j$,

(F_{23}) $n = 2m + 1$, $q = 2^s$, $\gamma \in \mathbb{F}_q \setminus \{0, 1\}$, $k = (q^2 + q)/2$, *where* m *is a positive integer,*

(F_{24}) $n \geq 2$, $q = p^s$, $(-\operatorname{Tr}_{q^n/q}(\gamma))^{(q-1)/(p^d-1)} \neq 1$, $k = p^i$, *where* $1 \leq i \leq s$ *and* $d = \gcd(i, s)$.

Proof of case (F_{24}). By Theorem 6 of [12], the mapping $F_0(x) = x + \gamma \operatorname{Tr}_{q^n/q}(x^{p^i})$ permutes $\mathbb{F}_{q^n}$ if and only if $g(u) = u + \operatorname{Tr}_{q^n/q}(\gamma)u^{p^i}$ permutes $\mathbb{F}_q$. By Theorem 7.9 of [15] this is the case precisely if $g(u) = 0$ has no solution $u \in \mathbb{F}_q^*$. Let $u \neq 0$, then

$$\begin{aligned} u + \operatorname{Tr}_{q^n/q}(\gamma) = 0 \text{ is equivalent to} \\ -\operatorname{Tr}_{q^n/q}(\gamma) = v^{p^d-1}, \text{ where } v = (1/u)^{p^{i/d}-1} \end{aligned}$$

This equation has no solution in $\mathbb{F}_q^*$ if and only if $(-\operatorname{Tr}_{q^n/q}(\gamma))^{(q-1)/(p^d-1)} \neq 1$. □

Remark 3.2. (a) In Case (F_{18}) if q is odd, then in particular $\gamma \in \mathbb{F}_{q^{4l}}$, so $4l \mid n$.

(b) It can be easily checked that $k = 2q - 1$ satisfies $\gcd(k, q^2 - 1) = 1$ if $q \equiv 1 \pmod 3$ and $\gcd(k, q^2-1) = 3$ if $q \equiv -1 \pmod 3$. This observation concerning (F_1) shows that in contrast to t the exponent k need not be coprime with q^n-1 if $X^t + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ is a permutation polynomial.

3.3 Tools to Help Determine Cycle Structures

This section collects two results, which we use as tools to determine the cycle structure of some of the infinite families listed in Theorem 3.4.

Linear translators

These are results from [12] by Kyureghyan.

Definition 3.1. Let $\alpha \in \mathbb{F}_{q^n}$ and $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$. If there exists an $a \in \mathbb{F}_q$, s. t. $f(x + u\alpha) - f(x) = ua$ for any $x \in \mathbb{F}_{q^n}, u \in \mathbb{F}_q$, then we call α an *a-linear translator* for f.

The following is based on Theorem 9 from [12]. Recall that by $\mathcal{C}(E, x)$ we denote the cycle of E containing x.

Theorem 3.5. *Let $q = p^s$, $\gamma \in \mathbb{F}_{q^n}$ be a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $b \neq -1$. Consider the permutation polynomial $F(X) = X + \gamma f(X)$. Let N_0 be the number of fixed points of F, i. e. the number of roots of $f(X)$. Then the following holds.*

1. *If $b = 0$, then*
$$\mathrm{CS}(F) = 1^{N_0} p^{\frac{q^n - N_0}{p}}.$$
Moreover for any $u \in \mathbb{F}_{q^n}, f(u) \neq 0$ the cycle $\mathcal{C}(F, u) = (u_0\ u_1\ \ldots\ u_{p-1})$, where $u_j = u + j\gamma f(u)$.

2. *If $b \neq 0$, then*
$$\mathrm{CS}(F) = 1^{N_0} \ell^{\frac{q^n - N_0}{\ell}},$$
where ℓ is the order of $(b + 1)$ in $\mathbb{F}_q^*$. Moreover for any $u \in \mathbb{F}_{q^n}, f(u) \neq 0$ the cycle $\mathcal{C}(F, u) = (u_0\ u_1\ \ldots\ u_{\ell-1})$, where $u_j = u + \frac{(b+1)^j - 1}{b}\gamma f(u)$.

A useful result on algebraic curves

The following two theorems are special cases of Theorems 2, 5 and 6 by Coşgun, Özbudak, and Saygı in [7]. Theorems 5 and 6 were originally published in [19] by Özbudak and Saygı.

Theorem 3.6. *Let $q = 2^s$, $n = 2^u w n_1$, $h = 2^v w h_1$, where $\gcd(n_1, h_1) = 1$ and $\gcd(2, w n_1 h_1) = 1$, and $\kappa = 2^{v+1} w$. Then the number of solutions N of the equation $y^q - y = x^{q^h+1}$, where $x, y \in \mathbb{F}_{q^n}$, satisfies the following.*

$$N = \begin{cases} q^n, & u < v+1, \\ q^n + q^{\frac{n+\kappa}{2}}(q-1), & u = v+1, \\ q^n - q^{\frac{n+\kappa}{2}}(q-1), & u > v+1. \end{cases}$$

Theorem 3.7. *Let $p \neq 2$ be a prime, $q = p^s$, $n = 2^u w n_1$, $h = 2^v w h_1$, where $\gcd(n_1, h_1) = \gcd(2, w n_1 h_1) = 1$, and $\kappa = 2^{v+1} w$. Then the number of solutions N of the equation $y^q - y = x^{q^h+1}$, where $x, y \in \mathbb{F}_{q^n}$, satisfies the following.*

$$N = \begin{cases} q^n, & u < v+1,\ n \text{ odd}, \\ q^n + (q-1)q^{n/2}, & u < v+1,\ q \equiv 3 \pmod 4 \text{ and } 4 \mid n, \\ q^n - (q-1)q^{\frac{n+\kappa}{2}}, & u > v+1, \\ q^n - (q-1)q^{n/2}, & \text{else}. \end{cases}$$

These theorems allow us to determine the number of roots of $\mathrm{Tr}_{q^n/q}(X^{q^h+1})$ by the following theorem from [15, p. 56]. The second part follows from the proof given there.

Theorem 3.8. *Let $\alpha \in \mathbb{F}_{q^n}$, then $\mathrm{Tr}_{q^n/q}(\alpha) = 0$ if and only if $\alpha = \beta^q - \beta$ for some $\beta \in \mathbb{F}_{q^n}$. Furthermore, for any $\alpha \in \mathbb{F}_{q^n}$ with $\mathrm{Tr}_{q^n/q}(\alpha) = 0$ the equation $\alpha = \beta^q - \beta$ has exactly q solutions $\beta \in \mathbb{F}_{q^n}$.*

Corollary 3.9. *Let $g(X) \in \mathbb{F}_{q^n}[X]$ and denote by N the number of solutions of the equation $g(x) = y^q - y$. Then $\mathrm{Tr}_{q^n/q}(g(X))$ has $N_0 = {}^N\!/_q$ roots.*

Using Corollary 3.9 we can translate Theorem 3.6 and Theorem 3.7 into the following two theorems.

Theorem 3.10. *Let $q = 2^s$, $n = 2^u w n_1$, $h = 2^v w h_1$, where $\gcd(n_1, h_1) = 1$ and $\gcd(2, w n_1 h_1) = 1$, and $\kappa = 2^{v+1} w$. Then the number of roots N_0 of the polynomial $\mathrm{Tr}_{q^n/q}(X^{q^h+1}) \in \mathbb{F}_{q^n}[X]$ satisfies the following.*

$$N_0 = \begin{cases} q^{n-1}, & u < v+1, \\ q^{n-1} + q^{\frac{n+\kappa-2}{2}}(q-1), & u = v+1, \\ q^{n-1} - q^{\frac{n+\kappa-2}{2}}(q-1), & u > v+1. \end{cases}$$

Theorem 3.11. *Let p be an odd prime $q = p^s$, $n = 2^u w n_1$, $h = 2^v w h_1$, where $\gcd(n_1, h_1) = \gcd(2, w n_1 h_1) = 1$, and $\kappa = 2^{v+1} w$. Then the number of roots N_0 of $\mathrm{Tr}_{q^n/q}(X^{q^h+1}) \in \mathbb{F}_{q^n}[X]$ satisfies the following.*

$$N_0 = \begin{cases} q^{n-1}, & u < v+1,\ n \text{ odd}, \\ q^{n-1} + (q-1)q^{\frac{n-2}{2}}, & u < v+1,\ q \equiv 3 \pmod 4 \text{ and } 4 \mid n, \\ q^{n-1} - (q-1)q^{\frac{n+\kappa-2}{2}}, & u > v+1, \\ q^{n-1} - (q-1)q^{\frac{n-2}{2}}, & else. \end{cases}$$

3.4 The Special Case $q = 2$

Charpin and Kyureghyan give a complete characterization of permutation polynomials of shape $X + \gamma \,\mathrm{Tr}_{2^n/2}(X^k)$, i. e. for $q = 2$, in [5]. The following two theorems summarize their findings in this special case.

Theorem 3.12. *Let $\gamma \in \mathbb{F}_{2^n}$. The polynomial $X + \gamma \,\mathrm{Tr}_{2^n/2}(X^{2^i}) \in \mathbb{F}_{2^n}[X]$, $i \in \mathbb{N}$, is a permutation polynomial if and only if $\mathrm{Tr}_{2^n/2}(\gamma) = 0$. Its associated mapping is $x \mapsto x + \gamma \,\mathrm{Tr}_{2^n/2}(x)$.*

Theorem 3.13. *Let $\gamma \in \mathbb{F}_{2^n}^*$ and $3 \le k \le 2^n - 2$ be no power of 2, with the property, that $x \mapsto \mathrm{Tr}_{2^n/2}(x^k)$ is not the zero function. Then $X + \gamma \,\mathrm{Tr}_{2^n/2}(X^k) \in \mathbb{F}_{2^n}[X]$ is a permutation polynomial precisely if n is even, $k = 2^i + 2^j$, $\mathrm{Tr}_{2^n/2}(\gamma^{2^h+1}) = 0$ and $\gamma^{2^{2h}-1} = 1$, where $h = |j - i|$. Its associated mapping is $x \mapsto x + \gamma \,\mathrm{Tr}_{2^n/2}(x^{2^h+1})$.*

Using the results of the previous section the cycle structure of these permutation polynomials can be determined.

Theorem 3.14. *Let $\gamma \neq 0$ and $F(X) = X + \gamma \,\mathrm{Tr}_{2^n/2}(X^{2^i}) \in \mathbb{F}_{2^n}[X]$, where $\gamma \in \mathbb{F}_{2^n}, \mathrm{Tr}_{2^n/2}(\gamma) = 0$ and $i \in \mathbb{N}$. Then its cycle structure is*

$$\mathrm{CS}(F) = 1^{2^{n-1}} 2^{2^{n-2}}.$$

Proof. Let $x \in \mathbb{F}_{2^n}, u \in \mathbb{F}_2$, then

$$\mathrm{Tr}_{2^n/2}(x + u\gamma) - \mathrm{Tr}_{2^n/2}(x) = u \,\mathrm{Tr}_{2^n/2}(\gamma) = 0,$$

i. e. γ is a 0-linear translator for $\mathrm{Tr}_{2^n/2}(x)$. Additionally $\mathrm{Tr}_{2^n/2}(X)$ has 2^{n-1} roots. The theorem now follows from Theorem 3.5, 1. □

Theorem 3.15. *Let $F(X) = X + \gamma \,\mathrm{Tr}_{2^n/2}(X^{2^i+2^j}) \in \mathbb{F}_{2^n}[X]$, where $n = 2m$ is even, $\mathrm{Tr}_{2^n/2}(\gamma^{2^h+1}) = 0$, $\gamma^{2^{2h}-1} = 1$ and $h = |j - i|$. Let $n = 2^u w n_1$, $h = 2^v w h_1$, where $\gcd(n_1, h_1) = \gcd(2, w n_1 h_1) = 1$. Let $\lambda = m + \gcd(h, m)$. Then the following holds.*

$$\mathrm{CS}(F) = \begin{cases} 1^{2^{n-1}} 2^{2^{n-2}}, & u < v+1, \\ 1^{2^{n-1}+2^{\lambda-1}} 2^{2^{n-2}-2^{\lambda-2}}, & u = v+1, \\ 1^{2^{n-1}-2^{\lambda-1}} 2^{2^{n-2}+2^{\lambda-2}}, & u > v+1. \end{cases}$$

Proof. According to [5] γ is a 0-linear translator for $\mathrm{Tr}_{2^n/2}(x^{2^i+2^j})$. The associated map of $F(X)$ is given by $F(x) = x + \gamma\,\mathrm{Tr}_{2^n/2}(x^{2^h+1})$. Let N_0 be the number of fixed points of F, i. e. the number of roots of $\mathrm{Tr}_{2^n/2}(X^{2^h+1})$. Then by Theorem 3.5 the cycle structure of F is

$$\mathrm{CS}(F) = 1^{N_0} 2^{\frac{2^n - N_0}{2}}.$$

To determine N_0 we need Theorem 3.10. Let now $\kappa = 2^{v+1}w$, then $\kappa = 2\gcd(h, m)$ if $u \geq v + 1$.

Let $u < v + 1$, then

$$N_0 = 2^{n-1} \text{ and } \frac{2^n - N_0}{2} = \frac{2^n - 2^{n-1}}{2} = 2^{n-2}.$$

Let $u = v + 1$, then

$$N_0 = 2^{n-1} + 2^{\frac{n+\kappa-2}{2}}(2-1) = 2^{n-1} + 2^{\frac{2m+2\gcd(h,m)-2}{2}} = 2^{n-1} + 2^{\lambda-1} \text{ and}$$
$$\frac{2^n - N_0}{2} = \frac{2^n - (2^{n-1} + 2^{\lambda-1})}{2} = 2^{n-2} - 2^{\lambda-2}.$$

Let $u > v + 1$, then

$$N_0 = 2^{n-1} - 2^{\frac{n+\kappa-2}{2}}(2-1) = 2^{n-1} - 2^{\frac{2m+2\gcd(h,m)-2}{2}} = 2^{n-1} - 2^{\lambda-1} \text{ and}$$
$$\frac{2^n - N_0}{2} = \frac{2^n - (2^{n-1} - 2^{\lambda-1})}{2} = 2^{n-2} + 2^{\lambda-2}.$$

□

3.5 Counting Fixed Points

The number of fixed points can be determined for any case of Theorem 3.4. For some cases we will need the following lemmas.

Lemma 3.16. *Let q be a prime power and $k < q$. If q is odd let k be odd. If $q \equiv -1 \pmod{k}$, then $\mathrm{Tr}_{q^2/q}(X^k) \in \mathbb{F}_{q^2}[X]$ has exactly $N_0 = k(q-1)+1$ roots.*

Proof. Let x be a root:

$$0 = \mathrm{Tr}_{q^2/q}(x^k) = x^k + x^{qk} = x^k(1 + x^{k(q-1)}).$$

So we know that 0 is a root, let $x \neq 0$, then

$$-1 = x^{k(q-1)}.$$

Now we need to consider two cases.

Case 1, q even: In this case $-1 = 1$ and $x \neq 0$ is a root of $\mathrm{Tr}_{q^2/q}(X^k)$ if and only if $x^{k(q-1)} = 1$. Since $k \mid (q+1)$, we know $k(q-1) \mid (q^2-1)$, so the subgroup $U_k = \{x \in \mathbb{F}_{q^2}^* : x^{k(q-1)} = 1\}$ of $\mathbb{F}_{q^2}^*$ exists, and $|U_k| = k(q-1)$. Therefore $N_0 = |U_k| + 1 = k(q-1) + 1$.

Case 2, q odd: In this case k is odd and $x \neq 0$ is a root of $\mathrm{Tr}_{q^2/q}(X^k)$ if and only if $x^{k(q-1)} = -1$. Since $k \mid (q+1)$ and q and k are odd, we know $2k \mid (q+1)$ and $2k(q-1) \mid (q^2-1)$, so the subgroup $U_{2k} = \{x \in \mathbb{F}_{q^2}^* : x^{2k(q-1)} = 1\}$ of $\mathbb{F}_{q^2}^*$ exists, and $|U_{2k}| = 2k(q-1)$. Now consider the nonsquares $\hat{S}_{2k}$ of U_{2k}. We know

$$\begin{aligned}\hat{S}_{2k} &= \{u \in U_{2k} : \nexists v \in U_{2k}, \text{ s. t. } v^2 = u\} = \{u \in U_{2k} : u^{k(q-1)} = -1\} \\ &= \{x \in \mathbb{F}_{q^2}^* : x^{k(q-1)} = -1\}\end{aligned}$$

and $|\hat{S}_{2k}| = |U_{2k}|/2 = k(q-1)$. Therefore $N_0 = |\hat{S}_{2k}| + 1 = k(q-1) + 1$.

□

Lemma 3.17. *Let q be a prime power, k a positive integer and $d = \gcd(k, q^n - 1)$. The polynomials $\mathrm{Tr}_{q^n/q}(X^k)$ and $\mathrm{Tr}_{q^n/q}(X^d)$ have the same number of roots in $\mathbb{F}_{q^n}$.*

Proof. Let $e = k/d$, then $\gcd(e, q^n - 1) = 1$, so $x \mapsto x^e$ is a permutation of $\mathbb{F}_{q^n}$. Therefore

$$\begin{aligned}\left|\{x \in \mathbb{F}_{q^n} : \mathrm{Tr}_{q^n/q}(x^d) = 0\}\right| &= \left|\{x \in \mathbb{F}_{q^n} : \mathrm{Tr}_{q^n/q}((x^e)^d) = 0\}\right| \\ &= \left|\{x \in \mathbb{F}_{q^n} : \mathrm{Tr}_{q^n/q}(x^k) = 0\}\right|\end{aligned}$$

□

Theorem 3.18. *Let $q = p^s$, where p is prime and $s \geq 1$. Let N_0 be the number of fixed points of*

$$F(X) = X + \gamma \,\mathrm{Tr}_{q^n/q}(X^k) \in \mathbb{F}_{q^n}[X].$$

Then the following holds.

(F_1), (F_3), (F_9), (F_{13}), (F_{14}) and (F_{15}) *If $n = 2$ and*

(F_1) $q \equiv 1 \pmod 3$, $\gamma = -1/3$, $k = 2q - 1$,

(F_3) $q \equiv 1 \pmod 3$, $\gamma = 1$, $k = (q^2 + q + 1)/3$,

(F_9) $q = 2^s$, $\gamma \in \mathbb{F}_q$, *s. t.* $X^3 + X + \gamma^{-1}$ *has no root in* $\mathbb{F}_q$, $k = 2^{2s-2} + 3 \cdot 2^{s-2}$,

(F_{13}) $q = 2^s$, s *even*, $\gamma = 1$, $k = (q^2 - 2q + 4)/3$,

(F_{14}) $q = 2^s$, $s = 2t$, $\gamma \in \mathbb{F}_{2^t}^*$, $k = 2^{4t-1} - 2^{3t-1} + 2^{2t-1} + 2^{t-1}$ *or*

(F_{15}) $q = 3^s$, $s \geq 2$, $\gamma^{(q-1)/2} = (\gamma - 1)^{(q-1)/2}$, $k = 3^{2s-1} + 3^s - 3^{s-1}$,

then

$$N_0 = q.$$

(F_2) and (F_8) *If $n = 2$ and*

(F_2) $q \equiv -1 \pmod 3$, $\gamma^3 = -1/27$, $k = 2q - 1$ *or*

(F_8) $q = 2^s$, s *odd*, $\gamma^3 = 1$, $k = (3q^2 - 2)(q + 4)/5$,

then

$$N_0 = 3(q - 1) + 1.$$

(F_4) *If $n = 2$, $q = Q^2$, $\gamma = -1$, $k = Q^3 - Q + 1$, then*

$$N_0 = \begin{cases} 5(q-1)+1, & Q \equiv -2 \pmod 5, \\ q, & \text{else.} \end{cases}$$

(F_5) *If $n = 2$, $q = Q^2$, $\gamma = -1$, $k = Q^3 + Q^2 - Q$, then*

$$N_0 = \begin{cases} 5(q-1)+1, & Q \equiv 2 \pmod 5, \\ q, & \text{else.} \end{cases}$$

(F_6) *If $n = 2$, $q \equiv 1 \pmod 4$, $(2\gamma)^{(q+1)/2} = 1$, $k = (q + 1)^2/4$, then*

$$N_0 = \frac{q^2 + 1}{2}.$$

(F_7), (F_{10}) and (F_{11}) *If $n = 2$, $q = 2^s$ and*

(F_7) s *even*, $\gamma^3 = 1$, $k = (3q - 2)(q^2 + q + 1)/3$,

(F_{10}) $s \equiv 1 \pmod 3$, $\gamma = 1$, $k = (2q^2 - 1)(q + 6)/7$ *or*

(F_{11}) $s \equiv 2 \pmod 3$, $\gamma = 1$, $k = -(q^2 - 2)(q + 6)/7$,

then

$$N_0 = \begin{cases} 5(q-1)+1, & q \equiv -1 \pmod 5, \\ q, & \text{else.} \end{cases}$$

(F_{12}) *If $n = 2$, $q = 2^s$, s odd, $\gamma^{(q+1)/3} = 1$, $k = (2^{2s-1} + 3 \cdot 2^{s-1} + 1)/3$, then*

$$N_0 = \frac{q^2 + 2}{3}.$$

(F_{16}) and (F_{17}) *If $n = 3$, q odd and*

(F_{16}) $\gamma = 1$, $k = (q^2 + 1)/2$ *or*

(F_{17}) $\gamma = -1/2$, $k = q^2 - q + 1$,

then

$$N_0 = q^2.$$

(F_{18}) *If $n = 2lr$, q arbitrary, $\gamma^{q^{2l}-1} = -1$, $k = q^l + 1$, where l, r are positive integers, then*

$$N_0 = q^{l(r+1)-1}(q^{l(r-1)} - (-1)^r(q-1)).$$

(F_{19}) *If $n = 2m$, $q = 2^s$, $\gamma \in \mathbb{F}_{q^2}^*$, $k = 2^i(q+1)$, where m, i are positive integers, then*

$$N_0 = q^m(q^{m-1} - (-1)^m(q-1)).$$

(F_{20}) and (F_{21}) *If $n = 2m$, $q = 2^s$, where m is a positive integer, and*

(F_{20}) *$\gamma \in \mathbb{F}_q^*$, $k = q^2 + 1$ or*

(F_{21}) *$\gamma \in \mathbb{F}_{q^2}^*$, $k = 2^i(q^2+1)$, where i is a positive integer and either m is even or m is odd and $(\gamma^{2^{i+1}} + \gamma^{2^{i+1}q})^{(q-1)/\gcd(2^{i+1}-1, 2^s-1)} \neq 1$,*

then

$$N_0 = \begin{cases} q^{2m-1}, & m \text{ odd}, \\ q^{m+1}(q^{m-2} - (-1)^{m/2}(q-1)), & m \text{ even}. \end{cases}$$

(F_{22}) and (F_{23}) *If $n = 2m+1$, where m is a positive integer, and*

(F_{22}) *$n = 2m+1$, $q = 2^s$, $s \equiv \pm 2 \pmod 6$, $\gamma \in \mathbb{F}_q^*$, $\gamma^{(q-1)/3} \neq 1$, $k = 2q^i + 2q^j$, where i, j are positive integers with $i \neq j$ or*

(F_{23}) *$n = 2m+1$, $q = 2^s$, $\gamma \in \mathbb{F}_q \setminus \{0, 1\}$, $k = (q^2+q)/2$,*

then

$$N_0 = q^{2m}.$$

(F_{24}) *If $n \geq 2$, $q = p^s$, $(-\operatorname{Tr}_{q^n/q}(\gamma))^{(q-1)/(p^d-1)} \neq 1$, $k = p^i$, where $1 \leq i \leq s$ and $d = \gcd(i, s)$, then*

$$N_0 = q^{n-1}.$$

Proof. Since $x + \gamma \operatorname{Tr}_{q^n/q}(x^k) = x$ if and only if $\operatorname{Tr}_{q^n/q}(x^k) = 0$, the number of roots of $\operatorname{Tr}_{q^n/q}(X^k)$ is N_0. In particular we do not have to care about γ. We will go through all of the cases of Theorem 3.4 in order.

Case (F_1) $n = 2$, $q \equiv 1 \pmod 3$, $k = 2q - 1$.
Let $d = \gcd(k, q^2 - 1)$, then

$$\begin{aligned} d &= \gcd(2q-1, q^2-1) = \gcd(2(q-1)+1, (q-1)(q+1)) \\ &= \gcd(2(q-1)+1, q+1) = \gcd(2(q+1)-3, q+1) = \gcd(3, q+1). \end{aligned}$$

Since $q \equiv 1 \pmod 3$, we get $d = 1$ and Lemma 3.17 shows, that N_0 is the number of roots of $\operatorname{Tr}_{q^2/q}(X)$, which is q.

Case (F_2) $n = 2$, $q \equiv -1 \pmod 3$, $k = 2q - 1$.
Let $d = \gcd(k, q^2 - 1)$, then

$$\begin{aligned} d &= \gcd(2q-1, q^2-1) = \gcd(2(q-1)+1, (q-1)(q+1)) \\ &= \gcd(2(q-1)+1, q+1) = \gcd(2(q+1)-3, q+1) = \gcd(3, q+1). \end{aligned}$$

Since $q \equiv -1 \pmod 3$, we get $d = 3$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X^3)$, which is $3(q-1)+1$, by Lemma 3.16.

Case (F_3) $n = 2$, $q \equiv 1 \pmod 3$, $k = (q^2 + q + 1)/3$.
Let $d = \gcd(k, q^2 - 1)$, then

$$\begin{aligned} 3d &= \gcd(q^2+q+1, 3(q^2-1)) = \gcd(q^2+q+1, 3(q+2)) \\ &= \gcd\left(q^2+q+1 - \frac{q-1}{3}\cdot 3(q+2), 3(q+2)\right) = \gcd(3, 3(q+2)) = 3. \end{aligned}$$

So $d = 1$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q.

Case (F_4) $n = 2$, $q = Q^2$, $k = Q^3 - Q + 1$.
Let $d = \gcd(k, q^2 - 1)$, then

$$\begin{aligned} d &= \gcd(Q^3-Q+1, Q^4-1) = \gcd(Q^3-Q+1, Q^2-Q-1) \\ &= \gcd(Q^2+1, Q^2-Q-1) = \gcd(Q^2+1, Q+2) = \gcd(2Q-1, Q+2) \\ &= \gcd(5, Q+2). \end{aligned}$$

So if $Q \equiv -2 \pmod 5$, then $d = 5$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X^5)$, which is $5(q-1)+1$, by Lemma 3.16.

Otherwise $d = 1$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q.

Case (F_5) $n = 2$, $q = Q^2$, $k = Q^3 + Q^2 - Q$.
Since

$$\mathrm{Tr}_{q^2/q}(x^{Q^3+Q^2-Q}) = \mathrm{Tr}_{q^2/q}(x^{Q^5+Q^4-Q^3}) = \mathrm{Tr}_{q^2/q}(x^{Q^4-Q^3+Q})$$

for any $x \in \mathbb{F}_{q^2}$, the number of roots of $\mathrm{Tr}_{q^2/q}(X^{k_1})$, where $k_1 = Q^4 - Q^3 + Q$ is also N_0. Let $d = \gcd(k_1, q^2 - 1)$, then

$$\begin{aligned} d &= \gcd(Q^4-Q^3+Q, Q^4-1) = \gcd(Q^3-Q-1, Q^4-1) \\ &= \gcd(Q^3-Q-1, Q^2+Q-1) = \gcd(Q^2+1, Q^2+Q-1) = \gcd(Q^2+1, Q-2) \\ &= \gcd(2Q+1, Q-2) = \gcd(5, Q-2). \end{aligned}$$

So if $Q \equiv 2 \pmod 5$, then $d = 5$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X^5)$, which is $5(q-1)+1$, by Lemma 3.16.

Otherwise $d = 1$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q.

Case (F_6) $n = 2$, $q \equiv 1 \pmod 4$, $k = (q+1)^2/4$.

This was already determined by Kyureghyan and Zieve in Remark 5.2 of [11]. The following is a slight modification of their proof. Consider

$$k = \frac{(q+1)^2}{4} = \frac{q^2+2q+1}{4} = \frac{q^2-1}{4} \cdot \frac{q+1}{2}.$$

Also for any $x \in \mathbb{F}_{q^2}$, we know $x^{\frac{q^2-1}{4}} \in \mathbb{F}_q$, because

$$\left(x^{\frac{q^2-1}{4}}\right)^{q-1} = \left(x^{\frac{q-1}{4}}\right)^{q^2-1} = 1.$$

So any $x \in \mathbb{F}_{q^2}$ is a root of $\mathrm{Tr}_{q^2/q}(X^k)$ if and only if it is a root of $\mathrm{Tr}_{q^2/q}(X^{k_1})$, where $k_1 = \frac{q+1}{2}$. Since $q \equiv 1 \pmod 4$, we know k_1 is odd and $q \equiv -1 \pmod{k_1}$. By Lemma 3.16 the number $N_0 = k_1(q-1)+1 = \frac{q+1}{2}(q-1)+1 = \frac{q^2+1}{2}$.

Case (F_7) $n = 2$, $q = 2^s$, s even, $\gamma^3 = 1$, $k = (3q-2)(q^2+q+1)/3$.

Since s is even, let $s = 2t$, then $q = 4^t$. Let $d = \gcd(k, q^2-1)$, then

$$\begin{aligned} 3d &= \gcd((3\cdot 4^t - 2)(4^{2t} + 4^t + 1), 4^{2t} - 1) = \gcd((3\cdot 4^t - 2)(4^t + 2), 4^{2t} - 1) \\ &= \gcd(3\cdot 4^{2t} + 4^{t+1} - 4, 4^{2t} - 1) = \gcd(4^{t+1} - 1, 4^{2t} - 1) = 4^{\gcd(t+1,2t)} - 1 \\ &= 4^{\gcd(t+1,2)} - 1 \end{aligned}$$

So if t is even, i. e. $q = 4^t \equiv 1 \pmod 5$, then $3d = 4 - 1$, so $d = 1$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q.

Otherwise, if t is odd, i. e. $q = 4^t \equiv -1 \pmod 5$, then $3d = 4^2 - 1$, so $d = 5$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X^5)$, which is $5(q-1)+1$, by Lemma 3.16.

Case (F_8) $n = 2$, $q = 2^s$, s odd, $k = (3q^2-2)(q+4)/5$.

Since s is odd, let $s = 2t+1$. Because $\gcd(5, q^2-1) = 1$, the map $x \mapsto x^5$ permutes $\mathbb{F}_{q^2}$, so $f : \mathbb{F}_{q^2} \to \mathbb{F}_q, x \mapsto \mathrm{Tr}_{q^2/q}(x^k)$ has the same number of roots as $x \mapsto f(x^5) = \mathrm{Tr}_{q^2/q}(x^{q+4})$. Let $d = \gcd(q+4, q^2-1)$, then

$$d = \gcd(q+4, q+1)\gcd(q+4, q-1) = \gcd(3, q+1)\gcd(5, q-1) = 3,$$

because

$$\begin{aligned} &q + 1 = 2^s + 1 \equiv (-1)^s + 1 \equiv -1 + 1 \equiv 0 \pmod 3 \text{ and} \\ &\gcd(5, q-1) \mid \gcd(5, q^2-1) = 1. \end{aligned}$$

Now Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X^3)$, which is $3(q-1)+1$, by Lemma 3.16.

Case (F_9) $n = 2$, $q = 2^s$, $k = 2^{2s-2} + 3 \cdot 2^{s-2}$.

Because $\gcd(4, q^2 - 1) = 1$, the map $x \mapsto x^4$ permutes $\mathbb{F}_{q^2}$, therefore $f : \mathbb{F}_{q^2} \to \mathbb{F}_q, x \mapsto \mathrm{Tr}_{q^2/q}(x^k)$ has the same number of roots as $x \mapsto f(x^4) = \mathrm{Tr}_{q^2/q}(x^{3q+1})$. Let $d = \gcd(3q + 1, q^2 - 1)$, then

$$d = \gcd(3q + 1, q + 1) \gcd(3q + 1, q - 1) = \gcd(2, q + 1) \gcd(4, q - 1) = 1$$

Now Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q.

Case (F_{10}) $n = 2$, $q = 2^s$, $s \equiv 1 \pmod 3$, $k = (2q^2 - 1)(q + 6)/7$.

Since $s \equiv 1 \pmod 3$, let $s = 3t + 1$. Because

$$q^2 - 1 = 4^{3t+1} - 1 \equiv 4(4^3)^t - 1 \equiv 4 - 1 \equiv 3 \pmod 7,$$

we know $\gcd(7, q^2-1) = 1$ and $x \mapsto x^7$ permutes $\mathbb{F}_{q^2}$, so $f : \mathbb{F}_{q^2} \to \mathbb{F}_q, x \mapsto \mathrm{Tr}_{q^2/q}(x^k)$ has the same number of roots as $x \mapsto f(x^7) = \mathrm{Tr}_{q^2/q}(x^{q+6})$. Let $d = \gcd(q+6, q^2-1)$, then

$$d = \gcd(q + 6, q + 1) \gcd(q + 6, q - 1) = \gcd(5, q + 1) \gcd(7, q - 1) = \gcd(5, q + 1).$$

So if $q \equiv -1 \pmod 5$, then $d = 5$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X^5)$, which is $5(q - 1) + 1$, by Lemma 3.16.

Otherwise $d = 1$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q.

Case (F_{11}) $n = 2$, $q = 2^s$, $s \equiv 2 \pmod 3$, $k = -(q^2 - 2)(q + 6)/7$.

Because $2s \equiv 1 \pmod 3$, we know

$$\gcd(7, q^2 - 1) = \gcd(2^3 - 1, 2^{2s} - 1) = 2^{\gcd(3,2s)} - 1 = 2 - 1 = 1$$

and $x \mapsto x^7$ permutes $\mathbb{F}_{q^2}$, so $f : \mathbb{F}_{q^2} \to \mathbb{F}_q, x \mapsto \mathrm{Tr}_{q^2/q}(x^k)$ has the same number of roots as $x \mapsto f(x^7) = \mathrm{Tr}_{q^2/q}(x^{q+6})$. Let $d = \gcd(q + 6, q^2 - 1)$, then

$$d = \gcd(q + 6, q + 1) \gcd(q + 6, q - 1) = \gcd(5, q + 1) \gcd(7, q - 1) = \gcd(5, q + 1).$$

So if $q \equiv -1 \pmod 5$, then $d = 5$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X^5)$, which is $5(q - 1) + 1$, by Lemma 3.16.

Otherwise $d = 1$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q.

Case (F_{12}) $n = 2$, $q = 2^s$, s odd, $k = (2^{2s-1} + 3 \cdot 2^{s-1} + 1)/3$.

Let $d = \gcd(k, q^2 - 1)$, then

$$d = \gcd\left(\frac{2^{2s-1} + 3 \cdot 2^{s-1} + 1}{3}, 2^s + 1\right) \gcd\left(\frac{2^{2s-1} + 3 \cdot 2^{s-1} + 1}{3}, 2^s - 1\right) = \frac{2^s + 1}{3}$$

because

$$\begin{aligned} 3\gcd\left(\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}, 2^s+1\right) &= \gcd(2^{2s-1}+3\cdot 2^{s-1}+1, 3(2^s+1)) \\ &= \gcd((2^{s-1}+1)(2^s+1), 3(2^s+1)) \\ &= (2^s+1)\gcd(2^{s-1}+1, 3) = 2^s+1 \end{aligned}$$

and

$$\begin{aligned} \gcd\left(\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}, 2^s-1\right) &= \gcd\left(\frac{2^{s-1}+2}{3}(2^s-1)+1, 2^s-1\right) \\ &= \gcd(1, 2^s-1) = 1. \end{aligned}$$

So Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X^{(q+1)/3})$, which is $(q+1)(q-1)/3+1 = (q^2+2)/3$, by Lemma 3.16.

Case (F_{13}) $n = 2$, $q = 2^s$, s even, $k = (q^2-2q+4)/3$.

Since s is even, let $s = 2t$. Let $d = \gcd(k, q^2-1)$, then

$$d = \gcd\left(\frac{q^2-2q+4}{3}, q+1\right)\gcd\left(\frac{q^2-2q+4}{3}, q-1\right) = 1$$

because

$$\begin{aligned} 3\gcd\left(\frac{q^2-2q+4}{3}, q+1\right) &= \gcd(q^2-2q+4, 3(q+1)) \\ &= \gcd(q^2-2q+4, 3)\gcd(q^2-2q+4, q+1) \\ &= \gcd(q^2-2q+4, 3)\gcd(7, q+1) = 3, \text{ because} \\ q^2-2q+4 = (q-1)^2+3 &= (4^t-1)^2 \equiv 0 \pmod 3 \text{ and} \\ q+1 = 4^t+1 &\not\equiv 0 \pmod 7 \end{aligned}$$

and

$$\gcd\left(\frac{q^2-2q+4}{3}, q-1\right) = \gcd\left(\frac{q-1}{3}(q-1)+1, q-1\right) = \gcd(1, q-1) = 1.$$

So Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q.

Case (F_{14}) $n = 2$, $q = 2^s$, $s = 2t$, $k = 2^{4t-1} - 2^{3t-1} + 2^{2t-1} + 2^{t-1}$.

Let $d = \gcd(k, q^2-1)$, then $d = d_1 d_2 = 1$, where

$$\begin{aligned} d_1 &= \gcd(2^{4t-1} - 2^{3t-1} + 2^{2t-1} + 2^{t-1}, 1^{2t}+1) \\ &= \gcd((2^{2t}+1)(2^{2t-1}-2^{t-1}) + 2^t, 2^{2t+1}) \\ &= \gcd(2^t, 2^{2t}+1) = 1 \text{ and} \\ d_2 &= \gcd(2^{4t-1} - 2^{3t-1} + 2^{2t-1} + 2^{t-1}, 1^{2t}-1) \\ &= \gcd((2^{2t}-1)(2^{2t-1}-2^{t-1}+1)+1, 2^{2t+1}) \\ &= \gcd(1, 2^{2t}+1) = 1 \end{aligned}$$

So Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q.

Case (F_{15}) $n = 2$, $q = 3^s$, $s \geq 2$, $k = 3^{2s-1} + 3^s - 3^{s-1}$.
Let $d = \gcd(k, q^2 - 1)$, then

$$\begin{aligned} d &= \gcd(3^{2s-1} + 3^s - 3^{s-1}, 3^{s+1} - 3^s + 1) \\ &= \gcd\left(\frac{3^{s-1}+1}{2}(3^{s+1} - 3^s + 1) - \frac{3^s+1}{2}, 3^{s+1} - 3^s + 1\right) \\ &= \gcd\left(\frac{3^s+1}{2}, 2 \cdot 3^s + 1\right) = \gcd\left(\frac{3^s+1}{2}, 4 \cdot \frac{3^s+1}{2} - 1\right) = \gcd\left(\frac{3^s+1}{2}, 1\right) = 1 \end{aligned}$$

So Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q.

Case (F_{16}) $n = 3$, q odd, $k = (q^2 + 1)/2$.
Let $d = \gcd(k, q^3 - 1)$, then

$$\begin{aligned} 2d &= \gcd(q^2 + 1, 2(q^3 - 1)) = \gcd(q^2 + 1, 2(q + 1)) \\ &= \gcd\left(q^2 + 1 - \frac{q-1}{2} \cdot 2(q+1), 2(q+1)\right) = \gcd(2, 2(q+1)) = 2 \end{aligned}$$

So $d = 1$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q^2.

Case (F_{17}) $n = 3$, q odd, $k = q^2 - q + 1$.
Let $d = \gcd(k, q^3 - 1)$, then

$$d = \gcd(q^2 - q + 1, q^2 - q - 1) = \gcd(2, q^2 - q - 1) = 1$$

So $d = 1$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^2/q}(X)$, which is q^2.

Case (F_{18}) $n = 2lr$, q arbitrary, $k = q^l + 1$, where l, r are positive integers.
Let $2lr = n = 2^u w n_1$, $l = h = 2^v w h_1$, where $\gcd(n_1, h_1) = \gcd(2, w n_1 h_1) = 1$, and $\kappa = 2^{v+1} w$.

We need to consider two cases.

Case 1: q is odd. In this case $4l \mid n$ by Remark 3.2(a). Further $u > v + 1$ and $h_1 = n_1 = 1$, because $4h \mid n$. Consequently $\kappa = 2l$ and $(-1)^r = 1$. By Theorem 3.11 we get

$$N_0 = q^{n-1} - (q-1)q^{\frac{n+\kappa-2}{2}} = q^{2lr-1} - (-1)^r(q-1)q^{l(r+1)-1}.$$

Case 2: q is even. In this case $u \geq v + 1$ and $h_1 = n_1 = 1$, because $2h \mid n$. Consequently $\kappa = 2l$ and

$$(-1)^r = \begin{cases} -1, & u = v + 1, \\ 1, & u > v + 1. \end{cases}$$

By Theorem 3.10 we get

$$N_0 = q^{n-1} - (-1)^r(q-1)q^{\frac{n+\kappa-2}{2}} = q^{2lr-1} - (-1)^r(q-1)q^{l(r+1)-1}.$$

In both cases we have

$$N_0 = q^{2lr-1} - (-1)^r(q-1)q^{l(r+1)-1} = q^{l(r+1)-1}(q^{l(r-1)} - (-1)^r(q-1)).$$

Case (F_{19}) $n = 2m$, $q = 2^s$, $k = 2^i(q+1)$, where m, i are positive integers.

Note that $\mathrm{Tr}_{q^n/q}(x^{2^i(q+1)}) = \mathrm{Tr}_{q^n/q}(x^{q+1})^{2^i}$. Consequently $\mathrm{Tr}_{q^n/q}(x^{2^i(q+1)}) = 0$ if and only if $\mathrm{Tr}_{q^n/q}(x^{q+1}) = 0$ and thus it suffices to determine the number of roots of $\mathrm{Tr}_{q^n/q}(X^{q+1})$. Let $2m = n = 2^u w n_1$, $1 = h = 2^v w h_1$, where $\gcd(n_1, h_1) = 1$ and $\gcd(2, wn_1h_1) = 1$, and $\kappa = 2^{v+1}w$. Then $u > 0$, $v = 0$, $w = 1$ and $\kappa = 2$, because $2 \mid n$ and $h = 1$. Further note, that $u = v + 1 = 1$, if and only if m is odd, and $u > v + 1 = 1$, if and only if m is even. Consequently

$$(-1)^m = \begin{cases} -1, & u = v+1, \\ 1, & u > v+1. \end{cases}$$

By Theorem 3.10 we get

$$\begin{aligned} N_0 &= q^{n-1} - (-1)^m(q-1)q^{\frac{n+\kappa-2}{2}} = q^{2m-1} - (-1)^m(q-1)q^m \\ &= q^m(q^{m-1} - (-1)^m(q-1)). \end{aligned}$$

Case (F_{20}) $n = 2m$, $q = 2^s$, $k = q^2 + 1$, where m is a positive integer.

Let $2m = n = 2^u w n_1$, $2 = h = 2^v w h_1$, where $\gcd(n_1, h_1) = \gcd(2, wn_1h_1) = 1$, and $\kappa = 2^{v+1}w$. Then $v = 1$, $w = 1$ and $\kappa = 4$, because $h = 2$.

If m *is odd*, then $u = 1 < 2 = v + 1$ and by Theorem 3.10 the number of roots

$$N_0 = q^{n-1} = q^{2m-1}.$$

If m *is even*, then note that $m/2$ is odd if and only if $u = 2 = v + 1$ and even if and only if $u > 2 = v + 1$. Consequently

$$(-1)^{m/2} = \begin{cases} -1, & u = v+1, \\ 1, & u > v+1. \end{cases}$$

By Theorem 3.10 we get

$$\begin{aligned} N_0 &= q^{n-1} - (-1)^{m/2}(q-1)q^{\frac{n+\kappa-2}{2}} = q^{2m-1} - (-1)^{m/2}(q-1)q^{m+1} \\ &= q^{m+1}(q^{m-2} - (-1)^{m/2}(q-1)). \end{aligned}$$

Case (F_{21}) $n = 2m$, $q = 2^s$, $k = 2^i(q^2+1)$, where m and i are positive integers.

Note that $\mathrm{Tr}_{q^n/q}(x^{2^i(q^2+1)}) = \mathrm{Tr}_{q^n/q}(x^{q^2+1})^{2^i}$. Consequently $\mathrm{Tr}_{q^n/q}(x^{2^i(q^2+1)}) = 0$ if and only if $\mathrm{Tr}_{q^n/q}(x^{q^2+1}) = 0$ and N_0 in this case behaves exactly like N_0 in Case (F_{20}).

Case (F_{22}) $n = 2m+1$, $q = 2^s$, $s \equiv \pm 2 \pmod 6$, $k = 2q^i + 2q^j$, where m, i, j are positive integers and $i \neq j$.

Note that $\mathrm{Tr}_{q^n/q}(x^k) = 0$ if and only if $\mathrm{Tr}_{q^n/q}(x^{q^h+1}) = 0$, where $h = |i-j|$. Let $2m = n = 2^u w n_1$, $2 = h = 2^v w h_1$, where $\gcd(n_1, h_1) = \gcd(2, w n_1 h_1) = 1$. Then $u = 0 < v+1$, because n is odd. Consequently, by Theorem 3.10, we get

$$N_0 = q^{n-1} = q^{2m}.$$

Case (F_{23}) $n = 2m+1$, $q = 2^s$, $k = (q^2+q)/2$, where m is a positive integer.

Let $d = \gcd(k, q^3-1)$, then

$$\begin{aligned} d &= \gcd\left(\frac{q^2+q}{2}, q^{2m+1}-1\right) = \gcd\left(\frac{q}{2}(q+1), 2^{2m+1}-1\right) \\ &= \gcd\left(\frac{q}{2}(q+1), \frac{q}{2}(q+1)2\frac{q^{2m}-1}{q+1} + q - 1\right) \\ &= \gcd\left(\frac{q}{2}(q+1), q-1\right) = \gcd(q, q-1) = 1. \end{aligned}$$

So $d = 1$ and Lemma 3.17 shows, that N_0 is the number of roots of $\mathrm{Tr}_{q^n/q}(X)$, which is $q^{n-1} = q^{2m}$.

Case (F_{24}) $n \geq 2$, $q = p^s$, $k = p^i$, where $1 \leq i \leq s$.

Note that $\mathrm{Tr}_{q^n/q}(x^{p^i}) = \mathrm{Tr}_{q^n/q}(x)^{p^i}$. Therefore $\mathrm{Tr}_{q^n/q}(x^{p^i}) = 0$ if and only if $\mathrm{Tr}_{q^n/q}(x) = 0$, so $N_0 = q^{n-1}$. □

Chapter 4

Invariant Cycle Structure on Lines

This chapter (excluding Section 4.5) is based on work published in [9]. First we take a look at polynomials of shape $F(X) = X + \gamma f(X)$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$, and see, that certain lines of the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$ are invariant under F. A consequence of this is, that permutation polynomials of this shape are always also permutations of these lines. We further see, that, if f is 1-homogeneous, then the induced permutations on affine lines, i. e. lines not containing the origin, contained in certain 2-dimensional subspaces have the same cycle structure. This result is especially useful if $n = 2$, because in this case $F_{q^n} = \mathbb{F}_{q^2}$ is already 2-dimensional. This allows us to determine the cycle structure of cases (F_2) and (F_{12}) completely and of case (F_9) in a special case.

4.1 Induced Permutations on Lines and Subspaces

We consider $\mathbb{F}_{q^n}$ as an $\mathbb{F}_q$-vector space.

Notation 4.1. Let M and L be subspaces of $\mathbb{F}_{q^n}$. If L is a subspace of M we write $L \leq M$. If additionally $M \neq L$ we write $L < M$.

The following result is straightforward:

Lemma 4.1. *Let $F(x) = x + \gamma f(x)$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^n}$. Then F maps every line $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^n}$ into itself.*

Proof. Let $\alpha + \gamma u \in \alpha + \gamma\mathbb{F}_q$, then

$$F(\alpha + \gamma u) = \alpha + \gamma u + \gamma f(\alpha + \gamma u) = \alpha + \gamma(u + f(\alpha + \gamma u)) \in \alpha + \gamma\mathbb{F}_q.$$

So F maps $\alpha + \gamma\mathbb{F}_q$ into itself. □

The next lemma shows that the converse of the above lemma is also true.

Lemma 4.2. *Let $\gamma \in \mathbb{F}_{q^n}^*$. If $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ maps every line $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^n}$ into itself, then $F(x) = x + \gamma f(x)$ for an appropriate mapping $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$.*

Proof. By assumption, for any $\alpha \in \mathbb{F}_{q^n}$ there exists a mapping $f_\alpha : \mathbb{F}_q \to \mathbb{F}_q$ such that

$$F(\alpha + \gamma u) = \alpha + \gamma(u + f_\alpha(u)) = \alpha + \gamma u + \gamma f_\alpha(u)$$

for $u \in \mathbb{F}_q$. Let now A be a system of representatives for the cosets of the line $\gamma\mathbb{F}_q$ in $\mathbb{F}_{q^n}$. Then every $x \in \mathbb{F}_{q^n}$ can be uniquely written as $\alpha + \gamma u$ with $\alpha \in A, u \in \mathbb{F}_q$. For $x = \alpha + \gamma u$ with $\alpha \in A$ and $u \in \mathbb{F}_q$ we define $f(x) = u + f_\alpha(u)$. Then clearly

$$F(x) = F(\alpha + \gamma u) = \alpha + \gamma u + \gamma f_\alpha(u) = x + \gamma f(x),$$

where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$, with $f(x) = u + f_\alpha(u)$. □

Remark 4.1. Let $F(x) = x + \gamma f(x)$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^n}^*$. Further let L be a subspace of $\mathbb{F}_{q^n}$ containing γ. Then $\gamma\mathbb{F}_q \leq L$ and $L = \bigcup_{\alpha \in L} \alpha + \gamma\mathbb{F}_q$. So any of its cosets $\beta + L = \bigcup_{\alpha \in L}(\alpha + \beta) + \gamma\mathbb{F}_q$. Since F maps any of those lines into themselves it also maps any coset of L into itself.

As an immediate corollary of Lemma 4.1 we get the following result.

Theorem 4.3. *Let $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, $F(x) = x + \gamma f(x)$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^n}^*$. Then F permutes $\mathbb{F}_{q^n}$ if and only if it permutes every line $\alpha + \gamma\mathbb{F}_q$ with $\alpha \in \mathbb{F}_{q^n}$.*

The next observation follows directly from Theorem 4.3.

Proposition 4.4. *Let $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^n}^*$. If $F(x) = x + \gamma f(x)$ is a permutation of $\mathbb{F}_{q^n}$, then every cycle in its cycle decomposition has a length not exceeding q.*

Definition 4.2. A mapping $g : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is called *homogeneous* of degree 1 or 1-*homogeneous* if $g(ux) = ug(x)$ for any $u \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^n}$.

Next we consider a special class of permutations $F(x) = x + \gamma f(x)$, where f is homogeneous of degree 1. The following theorem shows that the cycle structure of such permutations has an interesting regularity.

Theorem 4.5. *Let $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ be 1-homogeneous and $\gamma \in \mathbb{F}_{q^n}^*$. Further let L and M be subspaces of $\mathbb{F}_{q^n}$ such that $\gamma \in L$, $L < M$ and $\dim(L) = \dim(M) - 1$. If $F(x) = x + \gamma f(x)$ permutes $\mathbb{F}_{q^n}$, then F has the same cycle structure on all cosets $m + L \neq L$ of L in M.*

Proof. Let $\alpha \in M \setminus L$ be fixed. Then for any $m \in M \setminus L$, the coset $m + L$ can be represented as $\alpha t + L$ with $t \in \mathbb{F}_q^*$. By Remark 4.1, the mapping F is a permutation on the coset $t\alpha + L$. Let now $l \in L$. Then for a fixed t, we get

$$F(t\alpha + l) = t\alpha + l + \gamma f(t\alpha + l) = t\alpha + G_t(l)$$

with $G_t : L \to L$, $G_t(l) = l + \gamma f(t\alpha + l)$. Since $G_t(l) = F(t\alpha + l) - t\alpha = \tau^{-1} \circ F \circ \tau$, where $\tau : L \to t\alpha + L$, with $\tau(l) = l + t\alpha$, Proposition 1.1 shows that $G_t(l)$ is a permutation of L that has the same cycle structure as F on $t\alpha + L$. To complete the

proof, it remains to show, that the cycle structure of G_t is independent of t. Since f is homogeneous of degree 1, we have

$$\begin{aligned} t^{-1}G_t(tl) &= t^{-1}(tl + \gamma f(t\alpha + tl)) = t^{-1}(tl + \gamma f(t(\alpha + l)) \\ &= t^{-1}(tl + t\gamma f(\alpha + l)) = l + \gamma f(\alpha + l) = G_1(l). \end{aligned}$$

This shows that G_t and G_1 are conjugate permutations in the symmetric group S_L and consequently have the same cycle structure. □

For the choice $L = \gamma\mathbb{F}_q$ and M any two dimensional subspace of $\mathbb{F}_{q^n}$ containing γ, Theorem 4.5 implies that the cycle structure of the permutation $F(x) = x+\gamma f(x)$ is the same on all parallel lines $m+\gamma\mathbb{F}_q \neq \gamma\mathbb{F}_q$ contained in M. This is a key observation for understanding the cycle structure of permutations of shape $x + \gamma f(x)$ which we summarize in the following theorem.

Theorem 4.6. *Let $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ be 1-homogeneous and $\gamma \in \mathbb{F}_{q^n}^*$. Suppose the map $F(x) = x + \gamma f(x)$ is a permutation on $\mathbb{F}_{q^n}$. Then the following properties hold:*

(a) *If M is a two dimensional subspace of $\mathbb{F}_{q^n}$ containing γ, then the cycle structure of F is the same on every line $m + \gamma\mathbb{F}_q \neq \gamma\mathbb{F}_q$ lying in M.*

(b) *There are at most $1+(q^{n-1}-1)/(q-1)$ lines in $\mathbb{F}_{q^n}$ such that the cycle structure of F is pairwise different on them.*

Proof. The statement follows from Theorem 4.5 with M of dimension 2 and the observation that $(q^{n-1}-1)/(q-1)$ is the number of pairwise different two dimensional subspaces containing γ. We need to consider the cycle structure of F on the line $\gamma\mathbb{F}_q$ separately. □

Remark 4.2. Example 4.1 shows that there are permutations $x + \gamma \operatorname{Tr}_{q^n/q}(x^k)$, for which there exist two dimensional subspaces M of $\mathbb{F}_{q^n}$, such that the cycle structure of F is not the same on every line $m + \gamma\mathbb{F}_q \neq \gamma\mathbb{F}_q$ lying in M.

The following permutations are from [11], they do not belong to a known infinite family.

Example 4.1. Let $q = 9$, $n = 3$, $k \in \{11, 19\}$ and $\gamma \in \mathbb{F}_q$, where $\gamma^4 = -1$. Let $F(x) = x + \gamma \operatorname{Tr}_{q^3/q}(x^k)$. Then the cycle structure of F on $\gamma\mathbb{F}_q$ is 1^9. And for the 80 lines $l \parallel \gamma\mathbb{F}_q$, $l \neq \gamma\mathbb{F}_q$, it holds, that

on 8 the cycle structure of F is 3^3,

on 36 the cycle structure of F is $1^1 4^2$,

on 36 the cycle structure of F is $1^1 8^1$.

Since a two dimensional subspace of $\mathbb{F}_{9^3}$, containing $\gamma\mathbb{F}_9$, contains 8 further lines and $8 \nmid 36$, there exists a two dimensional subspace of $\mathbb{F}_{9^3}$, containing $\gamma\mathbb{F}_9$, that contains at least two lines with different cycle structures.

4.2 Consequences for the Cycle Structure of $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$

In this section we consider Cases (F_1) to (F_{17}) of Theorem 3.4. That is $f(x) = \operatorname{Tr}_{q^n/q}(x^k)$, where $n \in \{2, 3\}$. We repeat these cases here for convenience.

Theorem 4.7 (Theorem 3.4, Cases (F_1) to (F_{17}))**.** *Let $q = p^s$, where p is prime and $s \geq 1$. Then*

$$F(X) = X + \gamma \operatorname{Tr}_{q^n/q}(X^k) \in \mathbb{F}_{q^n}[X]$$

is a permutation polynomial in each of the following cases.

(F_1) $n = 2$, $q \equiv 1 \pmod 3$, $\gamma = -1/3$, $k = 2q - 1$,

(F_2) $n = 2$, $q \equiv -1 \pmod 3$, $\gamma^3 = -1/27$, $k = 2q - 1$,

(F_3) $n = 2$, $q \equiv 1 \pmod 3$, $\gamma = 1$, $k = (q^2 + q + 1)/3$,

(F_4) $n = 2$, $q = Q^2$, $\gamma = -1$, $k = Q^3 - Q + 1$,

(F_5) $n = 2$, $q = Q^2$, $\gamma = -1$, $k = Q^3 + Q^2 - Q$,

(F_6) $n = 2$, $q \equiv 1 \pmod 4$, $(2\gamma)^{(q+1)/2} = 1$, $k = (q + 1)^2/4$,

(F_7) $n = 2$, $q = 2^s$, s *even*, $\gamma^3 = 1$, $k = (3q - 2)(q^2 + q + 1)/3$,

(F_8) $n = 2$, $q = 2^s$, s *odd*, $\gamma^3 = 1$, $k = (3q^2 - 2)(q + 4)/5$,

(F_9) $n = 2$, $q = 2^s$, $\gamma \in \mathbb{F}_q$, *s. t.* $X^3 + X + \gamma^{-1}$ *has no root in* $\mathbb{F}_q$, $k = 2^{2s-2} + 3 \cdot 2^{s-2}$,

(F_{10}) $n = 2$, $q = 2^s$, $s \equiv 1 \pmod 3$, $\gamma = 1$, $k = (2q^2 - 1)(q + 6)/7$,

(F_{11}) $n = 2$, $q = 2^s$, $s \equiv 2 \pmod 3$, $\gamma = 1$, $k = -(q^2 - 2)(q + 6)/7$,

(F_{12}) $n = 2$, $q = 2^s$, s *odd*, $\gamma^{(q+1)/3} = 1$, $k = (2^{2s-1} + 3 \cdot 2^{s-1} + 1)/3$,

(F_{13}) $n = 2$, $q = 2^s$, s *even*, $\gamma = 1$, $k = (q^2 - 2q + 4)/3$,

(F_{14}) $n = 2$, $q = 2^s$, $s = 2t$, $\gamma \in \mathbb{F}_{2^t}^*$, $k = 2^{4t-1} - 2^{3t-1} + 2^{2t-1} + 2^{t-1}$,

(F_{15}) $n = 2$, $q = 3^s$, $s \geq 2$, $\gamma^{(q-1)/2} = (\gamma - 1)^{(q-1)/2}$, $k = 3^{2s-1} + 3^s - 3^{s-1}$,

(F_{16}) $n = 3$, q *odd*, $\gamma = 1$, $k = (q^2 + 1)/2$,

(F_{17}) $n = 3$, q *odd*, $\gamma = -1/2$, $k = q^2 - q + 1$.

It can be easily seen that in all cases of Theorem 4.7 the integer k satisfies $k \equiv 1 \pmod{q - 1}$, implying the following.

Proposition 4.8. *If q and k appear in one of the cases of Theorem 4.7, then $x^k = x$ for any $x \in \mathbb{F}_q$, and hence the function $\operatorname{Tr}_{q^n/q}(x^k)$ is homogeneous of degree 1.*

Consequently every permutation listed in Theorem 4.7 fulfils the conditions of Theorem 4.6. Thus to determine the cycle structure of these permutations, it is enough to find the cycle structure of the induced permutations on lines parallel to $\gamma\mathbb{F}_q$. By Theorem 4.6(b), for $n = 2$ there are at most two lines with different cycle structure, and for $n = 3$ there are at most $q + 2$ such lines. One of the lines for which we need to compute the cycle structure is $\gamma\mathbb{F}_q$.

Remark 4.3. Let $F(X) = X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ be one of the cases appearing in Theorem 4.7. Then the cycle structure of F on $\gamma\mathbb{F}_q$ is easy to determine. Indeed, for any $\gamma u \in \gamma\mathbb{F}_q$ it holds $F(\gamma u) = \gamma(1 + \operatorname{Tr}_{q^n/q}(\gamma^k))u$, and hence the cycle containing γu has length equal to the multiplicative order of $(1 + \operatorname{Tr}_{q^n/q}(\gamma^k))$ in $\mathbb{F}_q$.

Note that in several of the cases listed in Theorem 4.7 there are multiple choices for γ defining permutations. However in some of these cases the choice of γ does not impact the cycle structure of the permutations.

Proposition 4.9. *Let $i \in \{2, 6, 8, 12\}$ be fixed and $F_{i,\gamma}$ be a permutation of $\mathbb{F}_{q^2}$ described in case (F_i) of Theorem 4.7. Further let $\gamma_1, \gamma_2 \in \mathbb{F}_{q^2}$ be such, that F_{i,γ_1} and $\mathbb{F}_{i,\gamma_2}$ are permutations. Then F_{i,γ_1} and $\mathbb{F}_{i,\gamma_2}$ are conjugate in the symmetric group over $\mathbb{F}_{q^2}$ and hence they have the same cycle structure. Further the cycle structure of F_{i,γ_1} on $\gamma_1\mathbb{F}_q$ is the same as the cycle structure of F_{i,γ_2} on $\gamma_2\mathbb{F}_q$ and for any $\alpha_1 \in \mathbb{F}_{q^2} \setminus \gamma_1\mathbb{F}_q$, $\alpha_2 \in \mathbb{F}_{q^2} \setminus \gamma_2\mathbb{F}_q$, the cycle structure of F_{i,γ_1} on $\alpha_1 + \gamma_1\mathbb{F}_q$ is the same as the cycle structure of F_{i,γ_2} on $\alpha_2 + \gamma_2\mathbb{F}_q$.*

Proof.

Case (F_2) $F_{2,\gamma}(x) = x + \gamma \operatorname{Tr}_{q^2/q}(x^{2q-1})$, where $\gamma^3 = -\frac{1}{27}$. One possible choice for γ is $-1/3$. Set

$$F_2^*(x) = x - 1/3 \operatorname{Tr}_{q^2/q}(x^{2q-1}).$$

In the following we proceed similar to the proof of Theorem 3.2 from [11]: Let $\omega_2 := -3\gamma$, then $\omega_2^3 = 1$ and consequently $\omega_2^{2q-1} = 1$. Then

$$\begin{aligned} F_{2,\gamma}(\omega_2 x) &= \omega_2 x - \frac{1}{3}\omega_2 \operatorname{Tr}_{q^2/q}(\omega_2^{2q-1} x^{2q-1}) = \omega_2(x - \frac{1}{3}\operatorname{Tr}_{q^2/q}(x^{2q-1})) \\ &= \omega_2 F_2^*(x). \end{aligned} \tag{4.1}$$

This shows that $F_{2,\gamma}$ is a conjugate of F_2^* for any γ with $\gamma^3 = -\frac{1}{27}$, that is the cycle structure of $F_{2,\gamma}$ is the same for every γ, such that $F_{2,\gamma}$ is a permutation.

Case (F_6) $F_{6,\gamma}(x) = x + \gamma \operatorname{Tr}_{q^2/q}(x^{(q+1)^2/4})$, where $(2\gamma)^{(q+1)/2} = 1$. One possible choice for γ is $1/2$. Set

$$F_6^*(x) = x + 1/2 \operatorname{Tr}_{q^2/q}(x^{(q+1)^2/4}).$$

Let $\omega_6 := 2\gamma$, then $\omega_6^{(q+1)/2} = 1$ and consequently $\omega_6^{(q+1)^2/4} = 1$. Then

$$\begin{aligned} F_{6,\gamma}(\omega_6 x) &= \omega_2 x + \frac{1}{2}\omega_6 \operatorname{Tr}_{q^2/q}(\omega_6^{(q+1)^2/4} x^{(q+1)^2/4}) = \omega_6(x + \frac{1}{2}\operatorname{Tr}_{q^2/q}(x^{(q+1)^2/4})) \\ &= \omega_6 F_6^*(x). \end{aligned} \tag{4.2}$$

This shows that $F_{6,\gamma}$ is a conjugate of F_6^* for any γ with $(2\gamma)^{(q+1)/2} = 1$, that is the cycle structure of $F_{6,\gamma}$ is the same for every γ, such that $F_{6,\gamma}$ is a permutation.

Case (F_8) $F_{8,\gamma}(x) = x + \gamma \operatorname{Tr}_{q^2/q}(x^{k_8})$, where $\gamma^3 = 1$ and $k_8 = (3q^2 - 2)(q + 4)/5$. One possible choice for γ is 1. Set

$$F_8^*(x) = x + \operatorname{Tr}_{q^2/q}(x^{k_8}).$$

Let $\omega_8 := \gamma$, then $\omega_8^3 = 1$ and consequently $\omega_8^{k_8} = 1$, because $3 \mid k_8$. Then

$$\begin{aligned} F_{8,\gamma}(\omega_8 x) &= \omega_8 x + \omega_8 \operatorname{Tr}_{q^2/q}(\omega_8^{k_8} x^{k_8}) = \omega_8(x + \operatorname{Tr}_{q^2/q}(x^{k_8})) \\ &= \omega_8 F_8^*(x). \end{aligned} \tag{4.3}$$

This shows that $F_{8,\gamma}$ is a conjugate of F_8^* for any γ with $\gamma^3 = 1$, that is the cycle structure of $F_{8,\gamma}$ is the same for every γ, such that $F_{8,\gamma}$ is a permutation.

Case (F_{12}) $F_{12,\gamma}(x) = x + \gamma \operatorname{Tr}_{q^2/q}(x^{k_{12}})$, where $q = 2^s$, s odd, $\gamma^{(q+1)/3} = 1$ and $k_{12} = (2^{2s-1} + 3 \cdot 2^{s-1} + 1)/3$. One possible choice for γ is 1. Set

$$F_{12}^*(x) = x + \operatorname{Tr}_{q^2/q}(x^{k_{12}}).$$

Let $\omega_{12} := \gamma$, then $\omega_{12}^{(q+1)/3} = 1$ and consequently $\omega_{12}^{k_{12}} = 1$, because $(q + 1)/3$ is a divisor of k_{12}. Then

$$\begin{aligned} F_{12,\gamma}(\omega_{12} x) &= \omega_{12} x + \omega_{12} \operatorname{Tr}_{q^2/q}(\omega_{12}^{k_{12}} x^{k_{12}}) = \omega_{12}(x + \operatorname{Tr}_{q^2/q}(x^{k_{12}})) \\ &= \omega_{12} F_{12}^*(x). \end{aligned} \tag{4.4}$$

This shows that $F_{12,\gamma}$ is a conjugate of F_{12}^* for any γ with $\gamma^{(q+1)/3} = 1$, that is the cycle structure of $F_{12,\gamma}$ is the same for every γ, such that $F_{12,\gamma}$ is a permutation.

Since for any $i \in \{2, 6, 8, 12\}$, the mapping $\varphi_i : \mathbb{F}_q \to \gamma\mathbb{F}_q, \varphi_i(x) = \omega_i x$ is a bijection, (4.1), (4.2), (4.3) and (4.4) also show, that the cycle structure of $F_{i,\gamma}$ on $\gamma\mathbb{F}_q$ is the same as the cycle structure of F_i^* on $\mathbb{F}_q$.

Let $\beta_0 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be fixed and for any $i \in \{2, 6, 8, 12\}$ let $\beta_i = \omega_i \beta_0 \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$. Then $\varphi_i' : \beta_0 + \mathbb{F}_q \to \beta_i + \gamma\mathbb{F}_q, \varphi_i'(x) = \omega_i x$ is a bijection. Consequently (4.1), (4.2), (4.3) and (4.4) also show, that the cycle structure of $\mathbb{F}_{i,\gamma}$ on $\beta_i + \gamma\mathbb{F}_q$ is the same as the cycle structure of F_i^* on $\beta_0 + \mathbb{F}_q$. By Theorem 4.6 for any $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$, the cycle structure of $F_{i,\gamma}$ on $\alpha + \gamma\mathbb{F}_q$ is the same as the cycle structure of $F_{i,\gamma}$ on $\beta_i + \gamma\mathbb{F}_q$.

These two facts together show that for any $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$, the cycle structure of $F_{i,\gamma}$ on $\alpha + \gamma\mathbb{F}_q$ is the same as the cycle structure of F_i^* on $\beta_0 + \mathbb{F}_q$. □

Table 4.1: Examples of cycle structure on lines for $n = 2$.

case	q	γ	cycle structure on any line $l \parallel \gamma\mathbb{F}_q, l \neq \gamma\mathbb{F}_q$
(F_1)	289		$1^1 4^2 28^{10}$
	1024		$4^1 8^{25} 20^1 40^{20}$
(F_2)*	125		$1^3 2^1 30^4$
	1103		$1^3 18^2 28^2 252^4$
(F_3)	289		$1^1 4^2 28^{10}$
	1024		$4^1 8^{25} 20^1 40^{20}$
(F_4)	289		$1^1 4^1 12^2 14^2 28^1 62^2 80^1$
	1024		$4^1 140^1 880^1$
(F_5)	289		$1^5 8^1 19^4 52^1 148^1$
	1024		$1^4 140^2 240^1 500^1$
(F_6)	289		$1^{145} 4^1 28^5$
	2197		$1^{1099} 3^2 52^3 156^6$
(F_7)	1024	1	$1^4 11^{20} 19^{20} 42^{10}$
		$\neq 1$	$1^4 30^2 70^2 80^2 260^1 400^1$
	4096	1	$8^2 72^6 120^6 144^2 440^6$
		$\neq 1$	$4^1 6^1 212^2 30^2 252^1 360^4 561^4$
(F_8)	2048		$1^2 20^{11} 22^1 44^1 66^5 88^5 110^1 132^2 176^1 198^1 242^1$
	8192		$1^2 7^{78} 26^6 39^{10} 52^5 65^4 91^{16} 104^{14} 117^4 130^4 143^2 156^6 208^4 260^1 364^1$
(F_9)	1024	1	$4^1 60^{17}$
		a	$2^1 6^5 62^1 186^5$
		a^{99}	16^{64} **
(F_{10})	1024		$1^4 10^2 20^5 35^4 60^6 400^1$
	8192		$2^1 26^2 52^2 390^2$ $1014^1 2574^1 3666^1$
(F_{11})	2048		$2^1 22^4 55^2 138^{11} 165^2$
	16384		$1^4 28^3 40^7 42^2 553^4 1141^4 4572^2$
(F_{12})*	2048		$1^{682} 2^1 22^{62}$
	32768		$1^{10922} 6^1 30^{728}$
(F_{13})	1024		$2^2 4^5 30^2 80^1 320^1 540^1$
	16384		$2^2 14^2 56^1 170^{14} 308^1 3402^4$
(F_{14})	1024	1	$4^1 12^5 20^6 36^5 60^5 180^2$
		b	256^4 **
(F_{15})	243	c	$1^1 242^1$ **
		c^4	$1^1 2^1 6^1 13^2 26^2 78^2$

Here a is a root of $X^{10} + X^6 + X^5 + X^3 + X^2 + X + 1$ in $\mathbb{F}_{1024}$, b is a root of $X^5 + X^2 + 1$ in $\mathbb{F}_{32}$ and c is a root of $X^5 - X + 1$ in $\mathbb{F}_{243}$.
* We determine the cs for these cases completely in Theorem 4.14 and Theorem 4.20.

Table 4.2: Examples of cycle structure on lines for $n = 3$. Here column A contains the cycle structure on lines $l \parallel \gamma\mathbb{F}_q$, $l \neq \gamma\mathbb{F}_q$ and B the number of planes $P > \gamma\mathbb{F}_q$ with such lines.

case (F_{16})		
q	A	B
23	$1^2 2^1 4^1 5^3$	3
	$4^2 5^3$	3
	$9^1 14^1$	3
	$2^1 10^1 11^1$	6
	$1^2 3^2 6^1 9^1$	9
81	$3^1 6^1 9^4 12^3$	1
	$1^1 2^6 4^6 11^4$	3
	$1^1 2^1 3^1 5^3 6^5 15^2$	6
	$1^1 2^1 4^1 10^1 11^4 20^1$	12
	$1^1 2^1 9^1 11^1 22^1 36^1$	12
	$1^1 3^1 9^1 27^1 41^1$	12
	$1^1 5^3 9^1 10^3 35^1$	12
	$1^1 3^1 5^1 14^1 28^1 30^1$	24
125	$1^2 2^1 3^2 4^1 6^2 12^3 21^1 42^1$	9
	$2^1 7^9 10^1 50^1$	9
	$2^1 11^1 34^2 44^1$	9
	$2^1 14^5 53^1$	9
	$5^1 6^1 18^3 60^1$	9
	$14^4 69^1$	9
	$3^2 4^2 9^1 18^3 24^2$	18
	$1^2 2^1 3^2 4^1 6^1 9^1 12^5 36^1$	27
	$1^2 7^9 10^2 20^2$	27

case (F_{17})		
q	A	B
23	$1^2 2^3 5^1 10^1$	3
	$1^1 5^1 8^1 9^1$	3
	$1^2 6^1 15^1$	3
	$1^1 8^1 14^1$	3
	$1^2 9^1 12^1$	3
	$1^1 22^1$	3
	$2^1 6^1 15^1$	3
	$4^1 8^1 11^1$	3
81	$3^1 6^1 9^4 12^3$	1
	$1^3 2^3 6^6 12^3$	3
	$4^2 9^1 32^2$	6
	$1^3 3^1 4^1 7^1 9^1 22^1 33^1$	12
	$1^3 3^1 6^1 7^1 27^1 35^1$	12
	$2^1 3^1 7^1 10^1 14^1 45^1$	12
	$2^1 36^1 43^1$	12
	$18^1 63^1$	12
	$19^1 62^1$	12
125	$1^1 2^2 3^1 4^2 8^1 15^1 86^1$	9
	$1^1 2^2 3^1 7^1 9^1 13^1 15^1 20^1 53^1$	9
	$1^4 2^2 5^1 12^1 29^1 71^1$	9
	$1^1 2^2 7^1 8^1 9^1 96^1$	9
	$1^1 3^1 4^1 7^1 18^1 39^1 53^1$	9
	$1^2 5^1 9^1 46^1 63^1$	9
	$1^2 8^1 115^1$	9
	$1^2 11^1 16^1 30^1 66^1$	9
	$2^2 3^2 8^1 26^1 81^1$	9
	$2^2 3^1 8^1 48^1 62^1$	9
	$2^2 5^1 33^1 83^1$	9
	$6^1 8^1 44^1 67^1$	9
	$8^1 41^1 76^1$	9
	$25^1 26^1 74^1$	9

Table 4.1 and Table 4.2 contain numerical results on the cycle structure on affine lines l parallel to $\gamma\mathbb{F}_q$ and $l \neq \gamma\mathbb{F}_q$ for permutations obtained by Theorem 4.7. Recall that $m_1^{r_1} m_2^{r_2} \dots m_i^{r_i}$ denotes the cycle structure of a permutation with r_1 cycles of length m_1, r_2 cycles of length m_2, ...and r_i cycles of length m_i, where $m_1 < m_2 < \cdots < m_i$.

We computed the cycle structure for all cases with $n = 2$ in all finite fields with $q < 10^7$. Unfortunately, in many of the cases we found no apparent pattern to these cycle structures. A particularly strong example for this is (F_8), see Table 4.3.

Table 4.3: Cycle Structures in case (F_8)

q	cycle structure on any line $l \parallel \gamma\mathbb{F}_q$,$l \neq \gamma\mathbb{F}_q$
2	1^2
2^3	$1^2\ 6^1$
2^5	$1^2\ 5^2\ 20^1$
2^7	$1^2\ 14^2\ 28^2\ 42^1$
2^9	$1^2\ 6^1\ 9^2\ 12^3\ 18^2\ 27^6\ 45^4\ 72^1$
2^{11}	$1^2\ 20^{11}\ 22^1\ 44^1\ 66^5\ 88^5\ 110^1\ 132^2\ 176^1\ 198^1\ 242^1$
2^{13}	$1^2\ 7^{78}\ 26^6\ 39^{10}\ 52^5\ 65^4\ 91^{16}\ 104^{14}\ 117^4\ 130^4\ 143^2\ 156^6\ 208^4\ 260^1\ 364^1$
2^{15}	$1^2\ 5^8\ 6^1\ 10^3\ 12^40\ 15^2\ 20^{13}\ 24^{35}\ 28^{15}\ 30^{58}\ 40^9\ 42^5\ 46^{15}\ 50^{12}\ 60^{36}\ 66^{10}\ 70^{21}$ $72^5\ 80^9\ 90^{20}\ 110^6\ 114^{10}\ 120^8\ 140^3\ 150^6\ 180^8\ 204^5\ 210^2\ 240^3\ 250^3\ 260^3\ 300^3$ $330^2\ 350^3\ 360^3\ 390^3\ 450^1\ 480^2\ 570^1\ 600^1\ 660^1\ 720^1\ 750^1\ 1110^1$
2^{17}	$1^2\ 9^{68}\ 32^{17}\ 34^1\ 36^{17}\ 44^{17}\ 51^{12}\ 68^{35}\ 85^{22}\ 102^{55}\ 119^{14}\ 136^{13}\ 153^{16}\ 170^1\ 187^{10}$ $204^{34}\ 221^{12}\ 238^8\ 255^8\ 272^{21}\ 289^{12}\ 323^{16}\ 340^9\ 357^2\ 374^8\ 391^{10}\ 408^{11}\ 425^6$ $442^4\ 459^2\ 476^6\ 493^2\ 527^2\ 544^2\ 561^2\ 595^6\ 612^1\ 663^2\ 680^6\ 697^6\ 731^2\ 748^7\ 799^2$ $816^3\ 884^1\ 1003^2\ 1020^1\ 1088^2\ 1156^1\ 1292^4\ 1564^2\ 1632^1\ 1700^1\ 1768^3\ 1972^1$ 2040^2
2^{19}	$1^2\ 14^{76}\ 19^4\ 20^{76}\ 36^{19}\ 56^{19}\ 57^2\ 70^{38}\ 76^1\ 80^{19}\ 86^{38}\ 92^{38}\ 95^4\ 114^{83}\ 130^{19}$ $133^2\ 144^{19}\ 152^{29}\ 171^4\ 190^{81}\ 228^{41}\ 266^{77}\ 304^{40}\ 342^{23}\ 380^{37}\ 418^{21}\ 456^{34}\ 494^{18}$ $532^{15}\ 570^{17}\ 608^{13}\ 646^7\ 684^8\ 722^6\ 760^7\ 798^1\ 836^5\ 874^{13}\ 912^8\ 950^2\ 988^5\ 1026^{10}$ $1064^{21}\ 1102^6\ 1140^7\ 1178^5\ 1216^9\ 1254^2\ 1292^7\ 1330^4\ 1368^6\ 1406^5\ 1444^5\ 1482^5$ $1520^4\ 1558^3\ 1596^3\ 1634^2\ 1672^2\ 1710^3\ 1748^9\ 1786^3\ 1862^2\ 1900^4\ 1938^1\ 1976^3$ $2014^2\ 2052^1\ 2090^1\ 2128^1\ 2166^3\ 2242^1\ 2280^1\ 2318^1\ 2394^3\ 2432^1\ 2546^1\ 2622^1$ $2660^2\ 2774^2\ 2888^1\ 3002^2\ 3078^1\ 3154^1\ 3192^1\ 3230^1\ 3268^2\ 3306^2\ 3648^1\ 3686^1$ $3724^1\ 4066^2\ 4256^1\ 4408^1\ 4522^1\ 5244^1$

In contrast, the cycle structures marked with $**$ in Table 4.1 look particularly simple and we believe that the following statements hold.

Conjecture 4.4. Permutations listed in Theorem 4.7 fulfill:

1. For fixed q, then the cycle structures of the permutations in case (F_1) are the same as the cycle structures of the permutations in case (F_3).

2. Let F_γ be as described in case (F_9) and t be the largest integer, s. t. $2^t \leq s$. Then there exists an elment γ, such that F_γ has $2^{s-(t+1)}$ cycles of length 2^{t+1} on any line $\alpha + \gamma\mathbb{F}_q$, where $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$.

   If $2^t = s$, then this is the case for $\gamma = 1$. For this case there is a proof in Section 4.5.

3. Let F_γ be as described in case (F_{14}). If $4 \nmid s$, then there exists an element γ, such that F_γ has 4 cycles of length 2^{s-2} on any line $\alpha+\gamma\mathbb{F}_q$, where $\alpha \in \mathbb{F}_{q^2}\setminus\gamma\mathbb{F}_q$.

4. Let F_γ be as described in case (F_{15}). Then there exists an element γ, such that F_γ has 1 fixed point and 1 cycle of length $q-1$ on any line $\alpha+\gamma\mathbb{F}_q$, where $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$.

For the permutations considered in the previous conjecture, it is easy to describe their cycle structure on the line $\gamma\mathbb{F}_q$. We state this in the next proposition. Note that in cases (F_9), (F_{14}) and (F_{15}), $\gamma \in \mathbb{F}_q$ and thus $\gamma\mathbb{F}_q = \mathbb{F}_q$.

Proposition 4.10. *Let* $\mathrm{ord}(x)$ *be the multiplicative order of* x *in* $\mathbb{F}_q$.

(a) *In cases* (F_1) *and* (F_3) *the permutations have* q *fixed points on* $\gamma\mathbb{F}_q$*, if* q *is even, and 1 fixed point and* $(q-1)/\mathrm{ord}(3)$ *cycles of length* $\mathrm{ord}(3)$ *on* $\gamma\mathbb{F}_q$*, if* q *is odd.*

(b) *In cases* (F_9) *and* (F_{14}) *the permutation* F_γ *reduces to the identity mapping on* $\gamma\mathbb{F}_q$ *and consequently has* q *fixed points on* $\gamma\mathbb{F}_q$.

(c) *In case* (F_{15}) *the permutation* F_γ *reduces to* $F(u) = (2\gamma+1)u$ *on* $\gamma\mathbb{F}_q$ *and consequently has one fixed point and* $(q-1)/\mathrm{ord}(2\gamma+1)$ *cycles of length* $\mathrm{ord}(2\gamma+1)$ *on* $\gamma\mathbb{F}_q$.

Recall that Theorem 4.6 shows that for $n = 3$, there are at most $q+2$ different kinds of lines, where "different" means, that on those lines the considered permutation has different cycle structures. One of those lines is $\gamma\mathbb{F}_q$, which we do not consider in the table. So the upper bound for different lines in the table is $q + 1$. Observe that Table 4.2 shows in particular that in cases (F_{16}) and (F_{17}) this upper bound $q+1$ is not achieved. Instead for $q = 81$ there are only 8 different lines in case (F_{16}), and 9 different lines in case (F_{17}); and for $q = 125$ there are 9 different lines in case (F_{16}), and 14 different lines in case (F_{17}).

Remark 4.5. At present we have no explanation for the cycle structure of case (F_{16}). In Chapter 6 we describe it explicitly for the composition of this mapping with x^{q^2+q-1}, that is for $x^{q^2+q-1} + \mathrm{Tr}_{q^3/q}(x)$. The possible cycle lengths are only 1, the multiplicative order of 4 modulo p and twice the multiplicative order of 4 modulo p, where p is the characteristic of $\mathbb{F}_q$.

Table 4.4: The cycle structure of F in case (F_2) for different q.

q	$q-1$	cycle structure of F on any line $\alpha + \mathbb{F}_q \neq \mathbb{F}_q$
2^5	31	$1^2 30^1$
2^9	$7 \cdot 73$	$1^2 6^1 12^{42}$
2^{11}	$23 \cdot 89$	$1^2 11^2 88^{23}$
2^{15}	$7 \cdot 31 \cdot 151$	$1^2 6^1 30^7 50^3 150^{216}$
2^{19}	524287	$1^2 524286^1$
5^3	$2^2 \cdot 31$	$1^3 2^1 30^4$
5^5	$2^2 \cdot 11 \cdot 71$	$1^3 2^1 5^4 10^2 35^{44} 70^{22}$
11	$2 \cdot 5$	$1^3 4^2$
11^3	$2 \cdot 5 \cdot 7 \cdot 19$	$1^3 4^2 6^2 12^4 18^4 36^{28}$
17	2^4	$1^3 2^3 4^2$
17^3	$2^4 \cdot 307$	$1^3 2^3 4^2 34^{72} 68^{36}$
257	2^8	$1^3 2^3 4^2 8^2 16^2 32^2 64^2$
491	$2 \cdot 5 \cdot 7^2$	$1^3 4^2 6^2 12^4 42^2 84^4$
821	$2^2 \cdot 5 \cdot 41$	$1^3 2^1 4^4 8^{100}$
1409	$2^7 \cdot 11$	$1^3 2^3 4^2 5^4 8^2 10^6 16^2 20^4 32^2 40^4 80^4 160^4$
1613	$2^2 \cdot 13 \cdot 31$	$1^3 2^1 3^8 6^4 30^{52}$
2351	$2 \cdot 5^2 \cdot 47$	$1^3 4^2 20^2 23^4 92^4 460^4$
2939	$2 \cdot 13 \cdot 113$	$1^3 3^8 112^2 336^8$
3257	$2^3 \cdot 11 \cdot 37$	$1^3 2^3 5^4 10^6 18^1 690^{32}$
4637	$2^2 \cdot 19 \cdot 61$	$1^3 2^1 10^{24} 18^4 90^{48}$
5171	$2 \cdot 5 \cdot 11 \cdot 47$	$1^3 4^2 5^4 20^4 23^4 92^4 115^8 460^8$
5711	$2 \cdot 5 \cdot 571$	$1^3 4^2 570^2 1140^4$
6359	$2 \cdot 11 \cdot 17^2$	$1^3 5^4 16^2 80^4 272^2 1360^4$
7547	$2 \cdot 7^3 \cdot 11$	$1^3 5^4 6^2 30^4 42^2 210^4 294^2 1470^4$
8513	$2^6 \cdot 7 \cdot 13$	$1^3 2^3 4^2 6^8 8^2 12^4 16^2 18^{56} 24^4 36^{28} 48^4 72^{28} 144^{28}$
8543	$2 \cdot 4271$	$1^3 2135^4$
9941	$2^2 \cdot 5 \cdot 7 \cdot 71$	$1^3 2^2 4^4 6^4 12^8 35^4 70^2 140^8 210^8 420^{16}$

4.3 Determining the Cycle Structure in Case (F_2)

Numerical results (Table 4.4) for case (F_2) show that the cycle structure of these permutations on lines $l \parallel \gamma\mathbb{F}_q$, $l \neq \gamma\mathbb{F}_q$ is always the same as the cycle structure of X^3 on $\mathbb{F}_q$. The cycle structure of X^3 on $\mathbb{F}_q$ is known by Theorem 2.2.

Let $\mathrm{Tr}(x) = \mathrm{Tr}_{q^2/q}(x) = x + x^q$ be the trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. We use this notation for the remainder of the chapter. In this section we determine the cycle structure of case (F_2), which is $F(x) = x + \gamma\,\mathrm{Tr}(x^{2q-1})$ on $\mathbb{F}_{q^2}$, where $q \equiv -1 \pmod 3$ and $\gamma^3 = -\frac{1}{27}$. We do this by showing, that indeed the cycle structure of $F(x) = x + \gamma\,\mathrm{Tr}(x^{2q-1})$ on lines $l \parallel \gamma\mathbb{F}_q$, $l \neq \gamma\mathbb{F}_q$ is the same as the cycle structure of x^3 on $\mathbb{F}_q$.

By Proposition 4.9 for all admissible choices of γ the cycle structure of F as well as its cycle structure on the lines parallel to $\gamma\mathbb{F}_q$ is the same. Hence we consider the case $\gamma = -\frac{1}{3}$, for which $\gamma\mathbb{F}_q = \mathbb{F}_q$ holds, because in this case $\gamma \in \mathbb{F}_q$.

First we determine the cycle structure of F on $\mathbb{F}_q$.

Lemma 4.11. *Let $q \equiv -1 \pmod 3$ and p be the characteristic of $\mathbb{F}_q$. Then*

(a) *If q is even, the permutation $F(x) = x - 1/3\,\mathrm{Tr}(x^{2q-1})$ reduces to $F(x) = x$ on the line $\mathbb{F}_q$. Consequently it has q fixed points on $\mathbb{F}_q$.*

(b) *If q is odd, the permutation $F(x) = x - 1/3\,\mathrm{Tr}(x^{2q-1})$ reduces to $F(x) = 1/3 \cdot x$ on the line $\mathbb{F}_q$. Consequently, it has one fixed point and $(q-1)/\operatorname{ord}_p(3)$ cycles of length $\operatorname{ord}_p(3)$ on $\mathbb{F}_q$.*

Proof. If q is even and $x \in \mathbb{F}_q$, then clearly $F(x) = x$. If otherwise q is odd and $x \in \mathbb{F}_q$, then

$$F(x) = x - \frac{1}{3}\,\mathrm{Tr}(x^{2q-1}) = x - \frac{1}{3}\,\mathrm{Tr}(x) = x - \frac{2}{3}x = \frac{1}{3}x.$$

So $x = 0$ is a fixed point and the n-th iterate of F is $(1/3)^n x$. Therefore if $x \neq 0$ it is contained in the cycle $\left(x, 1/3 \cdot x, \ldots, (1/3)^{k-1}x\right)$ where $k = \operatorname{ord}_p(1/3) = \operatorname{ord}_p(3)$. □

To determine the cycle structure of F on the other lines parallel to $\mathbb{F}_q$, by Theorem 4.6, we only need to pick one of them and find the cycle structure on it. The following claim will be used for a suitable choice of this line.

Claim 4.12. If $q \equiv 5 \pmod 6$, then $-1/3$ is a nonsquare of $\mathbb{F}_q$.

Proof. Let $q = p^s$ with p prime. then $p \equiv 5 \pmod 6$ and s is odd. $-1/3$ is a nonsquare of $\mathbb{F}_q$ if and only if $X^2 + 1/3$ is irreducible in $\mathbb{F}_q[x]$. Since $q = p^s$ with odd s, $X^2 + 1/3$ is irreducible in $\mathbb{F}_q[X]$ if and only if it is irreducible in $\mathbb{F}_p[X]$. $X^2 + 1/3$ is irreducible in $\mathbb{F}_p[X]$ if and only if $-1/3$ is a nonsquare in $\mathbb{F}_p$. Consequently it suffices to show that $-1/3$ is a nonsquare of the prime field $\mathbb{F}_p$, where $p \equiv 5 \pmod 6$. Obviously $-1/3$ is nonsquare if and only if -3 is nonsquare. So our goal is to show

that the Legendre symbol $\left(\frac{-3}{p}\right) = -1$. This follows easily from the law of quadratic reciprocity, stating that

$$\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$$

for any two distinct odd primes a and b.

$$\text{Clearly, } \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right).$$

For $p \equiv 1 \pmod 4$, we have

$$\left(\frac{-1}{p}\right) = 1, \quad \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1, \text{ and thus } \left(\frac{-3}{p}\right) = 1 \cdot (-1) = -1.$$

For $p \equiv 3 \pmod 4$, we have

$$\left(\frac{-1}{p}\right) = -1, \ \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{2}{3}\right) = 1 \text{ and thus } \left(\frac{-3}{p}\right) = (-1) \cdot 1 = -1.$$

□

Now we are ready to determine the rest of the cycle structure of F.

Theorem 4.13. *Let $q \equiv -1 \pmod 3$ and $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then the permutation $F(x) = x - 1/3 \operatorname{Tr}(x^{2q-1})$ has the same cycle structure on $\alpha + \mathbb{F}_q$ as the permutation x^3 on $\mathbb{F}_q$.*

Proof. According to Theorem 4.6 the cycle structure of F on the line $\alpha + \mathbb{F}_q$ does not depend on the choice of $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. As in the proof of Theorem 4.5 for any α and $l \in \mathbb{F}_q$ the following holds: $F(\alpha + l) = \alpha + G_\alpha(l)$ and $G_\alpha(l) := l + \gamma \operatorname{Tr}((\alpha + l)^{2q-1})$ permutes $\mathbb{F}_q$ and has the same cycle structure as F on $\alpha + \mathbb{F}_q$. Next we show that for a particular choice of α, and thus for any choice of α by Theorem 4.6, the permutation G_α is a conjugate of $m(x) = x^3$ in $S_{\mathbb{F}_q}$.

If q is *even*, then $\gamma = -1/3 = 1 \in \mathbb{F}_2$. Let $\alpha \in \mathbb{F}_4 \leq \mathbb{F}_{q^2}$, $\alpha \notin \mathbb{F}_2$. Since $q = 2^s$, with s odd, $\alpha \notin \mathbb{F}_{2^s}$. This α satisfies

$$\alpha^2 = \alpha + 1, \quad \alpha^3 = 1, \qquad \operatorname{Tr}(\alpha) = \alpha^q + \alpha = \alpha^2 + \alpha = 1,$$
$$\operatorname{Tr}(\alpha^2) = \operatorname{Tr}(\alpha + 1) = \operatorname{Tr}(\alpha) = 1, \qquad \operatorname{Tr}(\alpha^3) = \operatorname{Tr}(1) = 0$$

and

$$(\alpha+l)^{q+1} = (\alpha+l)(\alpha^q+l) = (\alpha+l)(\alpha+1+l) = \alpha^2+\alpha+\alpha l+\alpha l+l+l^2 = l^2+l+1.$$

Using the above equations we get

$$\begin{aligned}
G_\alpha(l) &= l + \operatorname{Tr}((\alpha+l)^{2q-1}) = l + \operatorname{Tr}\left(\frac{(\alpha^q+l)^2}{\alpha+l}\right) \\
&= l + \frac{(\alpha^q+l)^2}{\alpha+l} + \frac{(\alpha+l)^2}{\alpha^q+l} = l + \frac{(\alpha^q+l)^3+(\alpha+l)^3}{(\alpha+l)(\alpha^q+l)} \\
&= l + \frac{\operatorname{Tr}((\alpha+l)^3)}{(\alpha+l)^{q+1}} = l + \frac{2l^3+3l^2\operatorname{Tr}(\alpha)+3l\operatorname{Tr}(\alpha^2)+\operatorname{Tr}(\alpha^3)}{l^2+l+1} \\
&= l + \frac{l^2+l}{l^2+l+1} = \frac{l^3+l^2+l+l^2+l}{l^2+l+1} = \frac{l^3}{l^2+l+1}.
\end{aligned}$$

Now we can show that $G_\alpha = \varphi^{-1} \circ m \circ \varphi$, or equivalently $\varphi \circ G_\alpha = m \circ \varphi$ for the permutation

$$\varphi(l) := l^{q-2} + 1 = \begin{cases} \frac{1}{l} + 1, & l \neq 0, \\ 1, & l = 0. \end{cases}$$

We have

$$(\varphi \circ G_\alpha)(0) = f(0) = 1 = m(1) = (m \circ \varphi)(0).$$

If $l \neq 0$ then

$$(\varphi \circ G_\alpha)(l) = \frac{l^2+l+1}{l^3} + 1 = \frac{1}{l^3} + \frac{1}{l^2} + \frac{1}{l} + 1 = \left(\frac{1}{l}+1\right)^3 = (m \circ \varphi)(l).$$

This proves the theorem for even q.

If q is *odd*, then by Claim 4.12, $-\frac{1}{3}$ is a nonsquare of $\mathbb{F}_q$, so there is $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^2 = -\frac{1}{3}$. This α satisfies $(\alpha^q)^2 = (\alpha^2)^q = \alpha^2$ and thus

$$\alpha^q = -\alpha, \quad \operatorname{Tr}(\alpha) = \operatorname{Tr}(-\alpha) = 0, \quad \operatorname{Tr}(\alpha^2) = 2\alpha^2, \quad \operatorname{Tr}(\alpha^3) = \alpha^2 \operatorname{Tr}(\alpha) = 0.$$

Using these equations we obtain

$$\begin{aligned}
G_\alpha(l) &= l - \frac{1}{3}\operatorname{Tr}((\alpha+l)^{2q-1}) = l - \frac{1}{3}(\alpha+l)^{2(q+1)} \operatorname{Tr}\left(\frac{1}{(\alpha+l)^3}\right) \\
&= l - \frac{1}{3}\left[(\alpha^q+l)(\alpha+l)\right]^2 \left(\frac{1}{(\alpha+l)^3} + \frac{1}{(\alpha^q+l)^3}\right) \\
&= l - \frac{1}{3}(l^2-\alpha^2)^2 \cdot \frac{(\alpha+l)^3+(\alpha^q+l)^3}{(l^2-\alpha^2)^3} = l - \frac{1}{3}\cdot\frac{\operatorname{Tr}((l+\alpha)^3)}{l^2-\alpha^2} \\
&= l - \frac{1}{3}\cdot\frac{2l^3+3l^2\operatorname{Tr}(\alpha)+3l\operatorname{Tr}(\alpha^2)+\operatorname{Tr}(\alpha^3)}{l^2-\alpha^2} \\
&\overset{*}{=} l - \frac{1}{3}\cdot\frac{2l^3+6l\alpha^2}{l^2-\alpha^2} = l - \frac{1}{3}\cdot\frac{2l^3-2l}{l^2+1/3} \\
&= l - \frac{l(2l^2-2)}{3l^2+1} = \frac{l(3l^2+1)-l(2l^2-2)}{3l^2+1} = \frac{l(l^2+3)}{3l^2+1},
\end{aligned}$$

where * follows from $\alpha^2 = -1/3$. Next we show that $G_\alpha = \varphi^{-1} \circ m \circ \varphi$, or equivalently $\varphi \circ G_\alpha = m \circ \varphi$ for the permutation

$$\varphi(l) := \left(\frac{1}{2}l + \frac{1}{2}\right)^{q-2} - 1 = \begin{cases} \frac{1-l}{1+l}, & l \neq -1, \\ -1, & l = -1. \end{cases}$$

We have

$$(\varphi \circ G_\alpha)(-1) = \varphi\left(\frac{-1(1+3)}{3+1}\right) = \varphi(-1) = -1 = m(-1) = (m \circ \varphi)(-1).$$

If $l \neq -1$ then

$$(\varphi \circ G_\alpha)(l) = \frac{1 - \frac{l(l^2+3)}{3l^2+1}}{1 + \frac{l(l^2+3)}{3l^2+1}} = \frac{1 - 3l + 3l^2 - l^3}{1 + 3l + 3l^2 + l^3} = \left(\frac{1-l}{1+l}\right)^3 = (m \circ \varphi)(l)$$

Consequently F has the same cycle structure on $\alpha + \mathbb{F}_q$ as x^3 on $\mathbb{F}_q$. □

We summarize the results of this section by describing explicitly the cycle structure of F in the general case.

Theorem 4.14. *Let $q \equiv -1 \pmod 3$, p be the characteristic of $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^2}$ with $\gamma^3 = -\frac{1}{27}$. Let N_t be defined by the following recursion.*

$$N_1 = \gcd(2, q-1) = \begin{cases} 1, & q \text{ even} \\ 2, & q \text{ odd} \end{cases}$$

and

$$t \cdot N_t = \gcd(3^t - 1, q - 1) - \sum_{i \mid t, i \neq t} i \cdot N_i.$$

1. *Let q be even. Then the permutation $F(x) = x + \gamma \operatorname{Tr}(x^{2q-1})$ of $\mathbb{F}_{q^2}$ has q fixed points on $\gamma\mathbb{F}_q$. Further, on any affine line $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$, the permutation $F(x)$ has $N_1 + 1 = 2$ fixed points and N_t cycles of length t for every $t > 1$, such that $t = \operatorname{ord}_m(3)$ for a divisor m of $q - 1$.*

2. *Let q be odd. Then the permutation $F(x) = x + \gamma \operatorname{Tr}(x^{2q-1})$ of $\mathbb{F}_{q^2}$ has one fixed point and $\frac{q-1}{\operatorname{ord}_p(3)}$ cycles of length $\operatorname{ord}_p(3)$ on $\gamma\mathbb{F}_q$. Further, on any affine line $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$, the permutation $F(x)$ has $N_1 + 1 = 3$ fixed points and N_t cycles of length t for every $t > 1$, such that $t = \operatorname{ord}_m(3)$ for a divisor m of $q - 1$.*

Proof. The theorem follows from Lemma 4.11, Theorem 4.13 and Theorem 2.2. □

4.4 Determining the Cycle Structure in Case (F_{12})

In this section we determine the cycle structure of case (F_{12}), which is $F(x) = x + \gamma \operatorname{Tr}(x^{(2^{2s-1}+3\cdot 2^{s-1}+1)/3})$ on $\mathbb{F}_{q^2}$, where $q = 2^s$, s odd and $\gamma^{(q+1)/3} = 1$. Recall, that by $\operatorname{Tr}(x)$, we denote $\operatorname{Tr}_{q^2/q}(x) = x^q + x$. By Proposition 4.9 for all admissible choices of γ the cycle structure of F as well as its cycle structure on the lines parallel to $\gamma\mathbb{F}_q$ is the same. Hence it is enough to consider $\gamma = 1$, for which $\gamma\mathbb{F}_q = \mathbb{F}_q$ holds.

The next Lemma describes the cycle structure of F on the line $\mathbb{F}_q$.

Lemma 4.15. *Let $q = 2^s$ and s be odd. Then the permutation*

$$F(x) = x + \operatorname{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$$

reduces to the identity on the line $\mathbb{F}_q$. Consequently it has q fixed points on $\mathbb{F}_q$.

Proof. Clearly $F(x) = x$ for $x \in \mathbb{F}_q$. □

Lemma 4.16. *Let $q = 2^s$ and s be odd. Let $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then the permutation $F(x) = x + \operatorname{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$ has $\frac{2^s-2}{3}$ fixed points on the line $\alpha + \mathbb{F}_q$.*

Proof. By Theorem 3.18, the permutation F has $\frac{q^2+2}{3}$ fixed points and by Lemma 4.15 we know that q of them are on the line $\mathbb{F}_q$. By Theorem 4.6, the permutation F has the same number of fixed points on every line $\alpha + \mathbb{F}_q$, where $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. So on any of those lines the number of fixed points is

$$\left(\frac{2^{2s}+2}{3} - 2^s\right)/(2^s - 1) = \frac{2^s - 2}{3}.$$

□

To determine the cycle structure of F on the lines parallel but not equal to $\mathbb{F}_q$, by Theorem 4.6 it suffices to pick one of them and find the cycle structure on it.

Theorem 4.17. *Let $q = 2^s$ and s be odd. Let $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $\beta \in (\mathbb{F}_4 \setminus \mathbb{F}_2) \subseteq (\mathbb{F}_{q^2} \setminus \mathbb{F}_q)$. Then the permutation $F(x) = x + \operatorname{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$ has the same cycle structure on $\alpha + \mathbb{F}_q$ as the permutation $G_\beta(x) = x + P_s(x)(x^{2^{s-1}} + x + 1)$ on $\mathbb{F}_q$, where $P_s(x) = \operatorname{Tr}\left(\prod_{k=0}^{s-1}(x^{2^k} + \beta)\right)$. In particular $G_\beta(x)$ has $\frac{2^s-2}{3}$ fixed points.*

Proof. By Theorem 4.6 the cycle structure of F on the line $\alpha + \mathbb{F}_q$ does not depend on the choice of $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Here we choose $\alpha = \beta$ and as in Theorem 4.13 conclude, that the considered cycle structure is the same as that of

$$G_\beta : \mathbb{F}_q \to \mathbb{F}_q, \quad G_\beta(x) = x + \operatorname{Tr}\left((x+\beta)^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right).$$

Since $\beta \in \mathbb{F}_4 \setminus \mathbb{F}_2$, we have that

$$\beta^2 = \beta + 1, \qquad \beta^3 = 1, \qquad \beta^4 = \beta, \qquad \beta^q = \beta^2.$$

Note that

$$\frac{2^{2s-1} + 3 \cdot 2^{s-1} + 1}{3} = 2^{s-1} + 4^{s-1} - \frac{4^{s-1} - 1}{3} = 2^{s-1} + 4^{s-1} - \sum_{k=0}^{s-2} 4^k,$$

and therefore

$$G_\beta(x) = x + \mathrm{Tr}\left(\frac{(x+\beta)^{2^{s-1}} (x+\beta)^{4^{s-1}}}{\prod_{k=0}^{s-2} (x^{4^k} + \beta)} \right).$$

Since for $x \in \mathbb{F}_q$

$$\begin{aligned} \prod_{k=0}^{s-1} (x^{4^k} + \beta) &= \prod_{k=0}^{(s-1)/2} (x^{2^{2k}} + \beta) \prod_{k=(s-1)/2+1}^{s-1} (x^{2^{2k}} + \beta) \\ &= \prod_{k=0}^{(s-1)/2} (x^{2^{2k}} + \beta) \prod_{k=1}^{(s-1)/2} (x^{2^{2k-1}} + \beta) = \prod_{k=0}^{s-1} (x^{2^k} + \beta), \end{aligned}$$

we get

$$\prod_{k=0}^{s-2} (x^{4^k} + \beta) = \frac{\prod_{k=0}^{s-1} (x^{2^k} + \beta)}{x^{4^{s-1}} + \beta}$$

and

$$\begin{aligned} G_\beta(x) &= x + \mathrm{Tr}\left(\frac{x^{2^{s-1}} + \beta^2}{\prod_{k=0}^{s-2} (x^{2^k} + \beta)} \right) = x + \frac{x^{2^{s-1}} + \beta}{\prod_{k=0}^{s-2} (x^{2^k} + \beta^2)} + \frac{x^{2^{s-1}} + \beta^2}{\prod_{k=0}^{s-2} (x^{2^k} + \beta)} \\ &= x + \frac{\prod_{k=0}^{s-1} (x^{2^k} + \beta) + \prod_{k=0}^{s-1} (x^{2^k} + \beta^2)}{\prod_{k=0}^{s-2} (x^{2^k} + \beta^2)(x^{2^k} + \beta)} = x + \frac{\mathrm{Tr}\left(\prod_{k=0}^{s-1} (x^{2^k} + \beta) \right)}{\prod_{k=0}^{s-2} ((x^2 + x)^{2^k} + 1)}. \end{aligned}$$

Further, note that

$$\prod_{k=0}^{s-2} ((x^2 + x)^{2^k} + 1) = \sum_{j=0}^{2^{s-1}-1} (x^2 + x)^j = \frac{(x^2 + x)^{2^{s-1}} + 1}{x^2 + x + 1} = \frac{x^{2^{s-1}} + x + 1}{x^2 + x + 1}$$

and hence

$$G_\beta(x) = x + \frac{(x^2 + x + 1) P_s(x)}{x^{2^{s-1}} + x + 1} = x + P_s(x)(x^{2^{s-1}} + x + 1),$$

where $P_s(x) = \mathrm{Tr}\left(\prod_{k=0}^{s-1} (x^{2^k} + \beta) \right)$. □

The following properties of $P_s(x)$ will allow us to determine the cycle structure of G_β explicitly. Recall that for $s = 3^m \cdot l$, where $3 \nmid l$, we write $\nu_3(s) = m$.

Lemma 4.18. *Let $\beta \in \mathbb{F}_4 \setminus \mathbb{F}_2$, $x \in \mathbb{F}_{2^s}$ and s be odd. Let $t \mid s$, $u \in \mathbb{F}_{2^t}$ and $G_\beta(x) = x + P_s(x)(x^{2^{s-1}} + x + 1)$, where $P_s(x) = \mathrm{Tr}\left(\prod_{k=0}^{s-1}(x^{2^k} + \beta)\right)$. Then*

(a) $P_s(x) \in \mathbb{F}_2$,

(b) $P_s(u) = \begin{cases} 0, & 3 \mid (s/t) \\ P_t(u), & 3 \nmid (s/t) \end{cases}$

(c) $G_\beta(x) = x$ *if and only if* $P_s(x) = 0$,

(d) $|\{x \in \mathbb{F}_{2^s} \mid P_s(x) = 0\}| = \frac{2^s-2}{3}$,

(e) $|\{x \in \mathbb{F}_{2^s} \mid P_s(x) = 1\}| = \frac{2^{s+1}+2}{3}$,

(f) $|\{u \in \mathbb{F}_{2^t} | P_s(u) = 1\}| = \begin{cases} 0, & \nu_3(t) < \nu_3(s), \\ \frac{2^{t+1}+2}{3}, & \nu_3(t) = \nu_3(s). \end{cases}$

Proof. The fact that

$$\left(\prod_{k=0}^{s-1}(x^{2^k} + \beta)\right)^4 = \prod_{k=0}^{s-1}(x^{4\cdot 2^k} + \beta) = \prod_{k=0}^{s-1}(x^{2^k} + \beta), \text{ shows that } \prod_{k=0}^{s-1}(x^{2^k} + \beta) \in \mathbb{F}_4.$$

Thus

$$P_s(x) = \mathrm{Tr}_{2^{2s}/2^s}\left(\prod_{k=0}^{s-1}(x^{2^k} + \beta)\right) = \mathrm{Tr}_{4/2}\left(\prod_{k=0}^{s-1}(x^{2^k} + \beta)\right) \in \mathbb{F}_2,$$

which is (a). Further note that $u^{2^k} + \beta \neq 0$ and

$$\prod_{k=0}^{s-1}(u^{2^k} + \beta) = \left(\prod_{k=0}^{t-1}(u^{2^k} + \beta)\right)^{s/t} = \begin{cases} 1, & s/t \equiv 0 \pmod 3 \\ \prod_{k=0}^{t-1}(u^{2^k} + \beta), & s/t \equiv 1 \pmod 3 \\ \prod_{k=0}^{t-1}(u^{2^k} + \beta^2), & s/t \equiv 2 \pmod 3 \end{cases}$$

and, because $\beta^q = \beta^2$,

$$\mathrm{Tr}_{q^2/q}\left(\prod_{k=0}^{t-1}(u^{2^k} + \beta^2)\right) = \mathrm{Tr}_{q^2/q}\left(\prod_{k=0}^{t-1}(u^{2^k} + \beta)\right) = P_t(u).$$

This shows (b). Since s is odd, $X^{2^{s-1}} + X + 1$ has no root in $\mathbb{F}_{2^s}$, which implies (c). By Theorem 4.17, G_β has $\frac{2^s-2}{3}$ fixed points. With (c), we see that $|\{x \in \mathbb{F}_{2^s} \mid P_s(x) = 0\}| = \frac{2^s-2}{3}$, which is (d). By (a), we know that $P_s(x) \in \mathbb{F}_2$, so

$$|\{x \in \mathbb{F}_{2^s} \mid P_s(x) = 1\}| = 2^s - |\{x \in \mathbb{F}_{2^s} \mid P_s(x) = 0\}| = 2^s - \frac{2^s - 2}{3} = \frac{2^{s+1} + 2}{3}.$$

This is (e). With (b) we obtain

$$|\{u \in \mathbb{F}_{2^t} | P_s(u) = 1\}| = \begin{cases} 0, & 3 \mid (s/t) \\ |\{u \in \mathbb{F}_{2^t} | P_t(u) = 1\}|, & 3 \nmid (s/t) \end{cases}$$
$$= \begin{cases} 0, & 3 \mid (s/t) \\ \frac{2^{t+1}+2}{3}, & 3 \nmid (s/t) \end{cases}.$$

Since $3 \nmid (s/t)$ if and only if $\nu_3(t) = \nu_3(s)$, (f) follows. □

Now we are ready to determine the cycle structure of G_β.

Theorem 4.19. *Let $q = 2^s$ and s be odd. Let $\beta \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Then the permutation $G_\beta(x) = x + P_s(x)(x^{2^{s-1}} + x + 1)$ of $\mathbb{F}_q$, where $P_s(x) = \mathrm{Tr}\left(\prod_{k=0}^{s-1}(x^{2^k} + \beta)\right)$, has $\frac{q-2}{3}$ fixed points and N_t cycles of length $2t$ for every $t \mid s$, with $\nu_3(t) = \nu_3(s)$. The Numbers N_t are positive and satisfy*

$$2tN_t = \frac{2^{t+1}+2}{3} - \sum_{\substack{d|t, d<t, \\ \nu_3(d)=\nu_3(s)}} 2dN_d \text{ and } 2 \cdot 3^m N_{3^m} = \frac{2^{3^m+1}+2}{3}, \text{ where } m = \nu_3(s).$$

Proof. By Lemma 4.18(c), $x \in \mathbb{F}_q$ is a fixed point of G_β if and only if $P_s(x) = 0$ and then Lemma 4.18(d) shows that G_β has $\frac{q-2}{3}$ fixed points. Let $G_\beta^n = \underbrace{G \circ \cdots \circ G}_{n}$ denote the n-th iterate of G_β.

Consider now an $x_0 \in \mathbb{F}_q$ that is not fixed by G_β, i. e. an $x_0 \in \mathbb{F}_q$ with $P_s(x_0) \neq 0$. Then $P_s(x_0) = 1$ by Lemma 4.18(a). Consequently on the cycle containing x_0 the permutation G_β reduces to

$$G_\beta(x) = x + x^{2^{s-1}} + x + 1 = x^{2^{s-1}} + 1$$

and thus has its inverse given by

$$G_\beta^{-1}(x) = x^2 + 1.$$

As a result an even number of iterations of G_β^{-1} yields

$$G_\beta^{-2t}(x) = x^{2^{2t}},$$

while an odd number of iterations gives

$$G_\beta^{-(2t+1)}(x) = x^{2^{2t+1}} + 1.$$

Since s is odd, $X^{2^{2t+1}} + X + 1$ has no roots in $\mathbb{F}_q$, so

$$x_0 \neq x_0^{2^{2t+1}} + 1 = G_\beta^{-(2t+1)}(x_0), \quad \text{and thus} \quad G_\beta^{2t+1}(x_0) \neq x_0.$$

Hence the cycle length is even, say $2t$. Since t is minimal with $x_0 = G_\beta^{-2t}(x_0) = (x_0^{2t})^{2t}$, it must hold that $x_0 \in \mathbb{F}_{2^t}$. This forces $t \mid s$.

Suppose now $t \mid s$ and G_β has N_t cycles of length $2t$. Then it must hold that

$$\begin{aligned} 2tN_t &= |\{u \in \mathbb{F}_{2^t} \mid P_s(u) = 1 \text{ and } u \text{ is not in a subfield of } \mathbb{F}_{2^t}\}| \\ &= |\{u \in \mathbb{F}_{2^t} \mid P_s(u) = 1\}| - \sum_{\substack{d \mid t \\ d<t}} \left| \left\{ u \in \mathbb{F}_{2^d} \;\middle|\; \begin{array}{c} P_s(u) = 1 \text{ and } u \text{ is not} \\ \text{in a subfield of } \mathbb{F}_{2^d} \end{array} \right\} \right|. \end{aligned}$$

Combining this with Lemma 4.18(f), we get

$$2tN_t = \begin{cases} 0, & \nu_3(t) < \nu_3(s) \\ \frac{2^{t+1}+2}{3} - \sum\limits_{\substack{d \mid t \\ d<t}} 2dN_d, & \nu_3(t) = \nu_3(s) \end{cases}$$

Note that $2dN_d = 0$ if $d \mid s$ with $\nu_3(d) < \nu_3(s)$. Finally observe that for any $t \mid s$ with $\nu_3(t) = \nu_3(s)$, the number N_t is positive. Indeed by Lemma 4.18(e) there are proper elements u of $\mathbb{F}_{2^t}$ with $P_s(u) = 1$. These numbers satisfy then

$$2tN_t = \frac{2^{t+1}+2}{3} - \sum_{\substack{d \mid t, d<t, \\ \nu_3(d)=\nu_3(s)}} 2dN_d.$$

For $t = 3^m$ with $m = \nu_3(s)$, the sum is empty and thus $2 \cdot 3^m N_{3^m} = \frac{2^{3^m+1}+2}{3}$. □

We summarize the results of this section by describing explicitly the cycle structure of F in the general case.

Theorem 4.20. *Let $q = 2^s$ and s be odd. Let $\gamma \in \mathbb{F}_{q^2}$ with $\gamma^{(q+1)/3} = 1$. For $t \mid s$, with $\nu_3(t) = \nu_3(s)$, let N_t be defined by the following recursion:*

$$N_{3^m} = \frac{2^{3^m+1}+2}{2 \cdot 3^{m+1}}, \text{ for } m = \nu_3(s)$$

and

$$2tN_t = \frac{2^{t+1}+2}{3} - \sum_{\substack{d \mid t, d<t, \\ \nu_3(d)=\nu_3(s)}} 2dN_d.$$

Then the permutation $F(x) = x + \gamma \operatorname{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$ of F_{q^2} has

1. *q fixed points on $\gamma\mathbb{F}_q$ and*
2. *$\frac{q-2}{3}$ fixed points and N_t cycles of length $2t$ on every affine line $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$, where t is an arbitrary divisor of s satisfying $\nu_3(t) = \nu_3(s)$.*

Proof. Part 1 follows from Lemma 4.15 and part 2 follows from Theorem 4.17 and Theorem 4.19. □

4.5 Properties of the Cycle Structure in Case (F_9)

In this section we study the cycle structure of $F_\gamma(x) = x + \gamma \operatorname{Tr}_{q^2/q}(x^{2^{2s-2}+3\cdot 2^{s-2}})$, where $q = 2^s$ and $\gamma \in \mathbb{F}_q$, s. t. $X^3 + X + \gamma^{-1}$ has no root in $\mathbb{F}_q$. Note $\gamma\mathbb{F}_q = \mathbb{F}_q$, because $\gamma \in \mathbb{F}_q$.

We can easily determine the cycle structure of F on the line $\mathbb{F}_q$.

Lemma 4.21. *Let $q = 2^s$ and $\gamma \in \mathbb{F}_q$ be s. t. $X^3 + X + \gamma^{-1}$ has no root in $\mathbb{F}_q$. Then the permutation $F_\gamma(x) = x + \gamma \operatorname{Tr}_{q^2/q}(x^{2^{2s-2}+3\cdot 2^{s-2}})$ reduces to the identity on the line $\mathbb{F}_q$. Consequently it has q fixed points on $\mathbb{F}_q$.*

Proof. Clearly $F(x) = x$ for $x \in \mathbb{F}_q$. □

Theorem 4.22. *Let $\delta = \beta^2 + \beta$, where $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, with $\operatorname{Tr}_{q^2/q}(\beta) = 1$. Then the cycle structure of F_γ on any line $\alpha + \mathbb{F}_q$, where $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is the same as that of the permutation $G_{\gamma,\delta}(x) = x + \gamma^2 x^{2^{s-1}} + \gamma x^{2^{s-2}} + \delta$ on $\mathbb{F}_q$.*

Proof. By Theorem 4.6 the cycle structure of F_γ on the line $\alpha + \mathbb{F}_q$ does not depend on the choice of $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Here we choose $\alpha = \beta$ and as in Theorem 4.13 conclude, that this cycle structure is the same as that of

$$G'_{\gamma,\beta}(x) = x + \gamma \operatorname{Tr}_{q^2/q}\left((x+\beta)^{2^{2s-2}+3\cdot 2^{s-2}}\right)$$

on $\mathbb{F}_q$.

Consider

$$\begin{aligned}(x+\beta)^{2^{2s-2}+3\cdot 2^{s-2}} &= \left((x+\beta)^{2^s+3}\right)^{2^{s-2}} = \left((x+\beta^{2^s})(x+\beta)^3\right)^{2^{s-2}} \\ &= \left((x+\beta^{2^s})(x^3+x^2\beta+x\beta^2+\beta^3)\right) \\ &= \left(x^4+(\beta^{2^s}+\beta)x^3+\beta(\beta^{2^s}+\beta)x^2+\beta^2(\beta^{2^s}+\beta)x+\beta^{2^s+3}\right)^{2^{s-2}}.\end{aligned}$$

Recall that $\operatorname{Tr}_{q^2/q}(\beta) = \beta^{2^s} + \beta = 1$ and thus

$$\operatorname{Tr}_{q^2/q}(\beta^2) = \left(\operatorname{Tr}_{q^2/q}(\beta)\right)^2 = 1, \qquad \delta^{2^s} = (\beta^2+\beta)^{2^s} = \beta^2+\beta = \delta, \text{ i. e. } \delta \in \mathbb{F}_q.$$

Consequently

$$\operatorname{Tr}_{q^2/q}(\beta^{2^s+3}) = \operatorname{Tr}_{q^2/q}(\beta^2(\beta^2+\beta)) = \beta^2+\beta.$$

We get

$$\operatorname{Tr}_{q^2/q}\left((x+\beta)^{2^{2s-2}+3\cdot 2^{s-2}}\right) = (0+0+x^2+x+\beta^2+\beta)^{2^{s-2}}$$

So $G'_{\gamma,\beta}(x) = x + \gamma x^{2^{s-1}} + \gamma x^{2^{s-2}} + \gamma(\beta^2+\beta)^{2^{s-2}}$. Now by Proposition 1.1 the cycle structure of $G'_{\gamma,\beta}$ on $\mathbb{F}_q$ is the same as of

$$G_{\gamma,\delta}(x) = \left(\frac{G'_{\gamma,\beta}\left(\gamma x^{2^{s-2}}\right)}{\gamma}\right)^{2^2} = x + \gamma^2 x^{2^{s-1}} + \gamma x^{2^{s-2}} + \delta.$$

□

We can determine the cycle structure in the special case, where $\gamma = 1$ and s is a power of 2.

Lemma 4.23. *Let $q = 2^s$, where $s = 2^t$ and $t > 0$. Let $\delta = \beta^2 + \beta$, where $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, with $\mathrm{Tr}_{q^2/q}(\beta) = 1$ and $G_\delta(x) = x + x^{2^{2^t-1}} + x^{2^{2^t-2}} + \delta$. Then, for $m < t$, the 2^m-th iterate of G_δ is*

$$G_\delta^{2^m} = x + x^{2^{2^t-2^m}} + x^{2^{2^t-2^{m+1}}} + \sum_{j=2^m-2}^{2(2^m-1)} \delta^{2^{2^t-j}}.$$

Proof. This lemma can be shown by induction.

Let $m = 0 < t$, then

$$G_\delta^{2^0}(x) = G_{1,\delta}(x) = x + x^{2^{2^t-2^0}} + x^{2^{2^t-2^{0+1}}} + \sum_{j=2^0-1}^{2(2^0-1)} \delta^{2^{2^t-j}}$$

Let $m + 1 < t$ and

$$G_\delta^{2^m} = x + x^{2^{2^t-2^m}} + x^{2^{2^t-2^{m+1}}} + \sum_{j=2^m-2}^{2(2^m-1)} \delta^{2^{2^t-j}},$$

then

$$\begin{aligned}
&G_\delta^{2^{m+1}}(x) = G_\delta^{2^m}(G_\delta^{2^m}(x)) \\
&= \quad x \quad + x^{2^{2^t-2^m}} \quad + x^{2^{2^t-2^{m+1}}} \quad + \sum_{j=2^m-2}^{2(2^m-1)} \delta^{2^{2^t-j}} \\
&\quad + x^{2^{2^t-2^m}} \quad + x^{2^{2^t-2^{m+1}}} \quad + x^{2^{2^t-2^{m+1}-2^m}} \quad + \sum_{j=2^m-1}^{2(2^m-1)} \delta^{2^{2^t-(j+2^m)}} \\
&\quad + x^{2^{2^t-2^{m+1}}} \quad + x^{2^{2^t-2^{m+1}-2^m}} \quad + x^{2^{2^t-2^{m+2}}} \quad + \sum_{j=2^m-1}^{2(2^m-1)} \delta^{2^{2^t-(j+2^{m+1})}} \\
&\quad + \sum_{j=2^m-2}^{2(2^m-1)} \delta^{2^{2^t-j}}
\end{aligned}$$

and thus

$$\begin{aligned}
G_\delta^{2^{m+1}}(x) &= x + x^{2^{2^t-2^{m+1}}} + x^{2^{2^t-2^{m+2}}} + \sum_{j=2^m-1}^{2(2^m-1)} \delta^{2^{2^t-(j+2^m)}} + \sum_{j=2^m-1}^{2(2^m-1)} \delta^{2^{2^t-(j+2^{m+1})}} \\
&= x + x^{2^{2^t-2^{m+1}}} + x^{2^{2^t-2^{m+2}}} + \sum_{j=2^m-1+2^m}^{2(2^m-1)+2^m} \delta^{2^{2^t-j}} + \sum_{j=2^m-1+2^{m+1}}^{2(2^m-1)+2^{m+1}} \delta^{2^{2^t-j}} \\
&= x + x^{2^{2^t-2^{m+1}}} + x^{2^{2^t-2^{m+2}}} + \sum_{j=2^{m+1}-1}^{2^{m+1}+2^m-1} \delta^{2^{2^t-j}} + \sum_{j=2^{m+1}+2^m-1}^{2(2^{m+1}-1)} \delta^{2^{2^t-j}} \\
&= x + x^{2^{2^t-2^{m+1}}} + x^{2^{2^t-2^{m+2}}} + \sum_{j=2^{m+1}-1}^{2(2^{m+1}-1)} \delta^{2^{2^t-j}}.
\end{aligned}$$

□

Theorem 4.24. *Let $q = 2^s$, where $s = 2^t$. Then for $\delta = \beta^2 + \beta$, where $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, with $\mathrm{Tr}_{q^2/q}(\beta) = 1$ the permutation $G_\delta(x) = x + x^{2^{2^t-1}} + x^{2^{2^t-2}} + \delta$ has 2^{s-t-1} cycles of length $2s = 2^{t+1}$.*

Proof. By Lemma 4.23 in particular

$$G_\delta^{2^{t-1}} = x + x^{2^{2^t-2^{t-1}}} + x^{2^{2^t-2^t}} + \sum_{j=2^{t-1}-1}^{2^t-2} \delta^{2^{2^t-j}} = x^{2^{2^t-1}} + \sum_{j=2^{t-1}-1}^{2^t-2} \delta^{2^{2^t-j}},$$

so

$$\begin{aligned}
G_\delta^{2^t}(x) &= \left(x^{2^{2^t-1}}\right)^{2^{2^t-1}} + \left(\sum_{j=2^{t-1}-1}^{2^t-2} \delta^{2^{2^t-j}}\right)^{2^{2^t-1}} + \sum_{j=2^{t-1}-1}^{2^t-2} \delta^{2^{2^t-j}} \\
&= x + \sum_{j=2^{t-1}-1}^{2^t-2} \delta^{2^{2^t-(j-2^{t+1})}} + \sum_{j=2^{t-1}-1}^{2^t-2} \delta^{2^{2^t-j}} \\
&= x + \sum_{j=-1}^{2^{t-1}-2} \delta^{2^{2^t-j}} + \sum_{j=2^{t-1}-1}^{2^t-2} \delta^{2^{2^t-j}} \\
&= x + \sum_{j=-1}^{2^t-2} \delta^{2^{2^t-j}} = x + \mathrm{Tr}_{2^{2^t}/2}(\delta) \overset{*}{=} x + 1,
\end{aligned} \tag{4.5}$$

where * follows from

$$\begin{aligned}
\mathrm{Tr}_{2^{2^t}/2}(\delta) &= \mathrm{Tr}_{2^s/2}(\beta^2+\beta) = \sum_{i=0}^{s-1} (\beta^2+\beta)^{2^i} = \sum_{i=0}^{s-1} (\beta^{2^{i+1}} + \beta^{2^i}) = \beta + \beta^{2^s} \\
&= \mathrm{Tr}_{q^2/q}(\beta) = 1.
\end{aligned}$$

Further

$$G_\delta^{2^{t+1}}(x) = x + 1 + 1 = x. \tag{4.6}$$

For an arbitrary $x \in \mathbb{F}_q$, let $\mathcal{C}(G_\delta, x)$ be the cycle of G_δ containing x and $\ell(G_\delta, x)$ be its length, then (4.5) shows that $\ell(G_\delta, x)$ does not divide 2^t and (4.6) shows that $\ell(G_\delta, x)$ divides 2^{t+1}, so $\ell(G_\delta, x) = 2^{t+1} = 2s$. Since this holds for any x, the permutation G_δ has only cycles of length $2s$. □

Now we can determine the cycle structure of F_γ for $\gamma = 1$ and s a power of 2.

Theorem 4.25. *Let $q = 2^s$ and $s = 2^t$.*
Then the permutation $F(x) = x + \mathrm{Tr}\left(x^{2^{2s-2}+3\cdot 2^{s-2}}\right)$ of F_{q^2} has

1. *q fixed points on $\mathbb{F}_q$ and*
2. *2^{s-t-1} cycles of length $2s = 2^{t+1}$ on every affine line $\alpha + \mathbb{F}_q$.*

Proof. Part 1 follows from Lemma 4.21 and part 2 follows from Theorem 4.22 and Theorem 4.24. □

Chapter 5

Linear Structure and High Extension Degree

All cases of Theorem 3.4, where the extension degree n is arbitrary, exhibit one of two special properties. For convenience these cases are repeated in the next theorem.

Theorem 5.1 (Theorem 3.4, Cases $(\boldsymbol{F_{18}})$ to $(\boldsymbol{F_{24}})$)**.** *Let $q = p^s$, where p is prime and $s \geq 1$. Then*

$$F(X) = X + \gamma \operatorname{Tr}_{q^n/q}(X^k) \in \mathbb{F}_{q^n}[X]$$

is a permutation polynomial in each of the following cases.

- (F_{18}) *$n = 2lr$, q arbitrary, $\gamma^{q^{2l}-1} = -1$, $k = q^l+1$, where l, r are positive integers,*
- (F_{19}) *$n = 2m$, $q = 2^s$, $\gamma \in \mathbb{F}_{q^2}^*$, $k = 2^i(q+1)$, where m, i are positive integers,*
- (F_{20}) *$n = 2m$, $q = 2^s$, $\gamma \in \mathbb{F}_q^*$, $k = q^2 + 1$, where m is a positive integer,*
- (F_{21}) *$n = 2m$, $q = 2^s$, $\gamma \in \mathbb{F}_{q^2}^*$, $k = 2^i(q^2+1)$, where m, i are positive integers and either m is even or m is odd and $(\gamma^{2^{i+1}} + \gamma^{2^{i+1}q})^{(q-1)/\gcd(2^{i+1}-1, 2^s-1)} \neq 1$,*
- (F_{22}) *$n = 2m + 1$, $q = 2^s$, $s \equiv \pm 2 \pmod 6$, $\gamma \in \mathbb{F}_q^*$, $\gamma^{(q-1)/3} \neq 1$, $k = 2q^i + 2q^j$, where m, i, j are positive integers and $i \neq j$,*
- (F_{23}) *$n = 2m + 1$, $q = 2^s$, $\gamma \in \mathbb{F}_q \setminus \{0, 1\}$, $k = (q^2 + q)/2$, where m is a positive integer,*
- (F_{24}) *$n \geq 2$, $q = p^s$, $(-\operatorname{Tr}_{q^n/q}(\gamma))^{(q-1)/(p^d-1)} \neq 1$, $k = p^i$, where $1 \leq i \leq s$ and $d = \gcd(i, s)$.*

Let $F(X)$ be a permutation polynomial described in any one of these cases, then it satisfies one of the following two properties

1. γ is a 0-linear translator for $\operatorname{Tr}_{q^n/q}(x^k)$, in which case we can use Theorem 3.5 to determine the cycle structure of F.
2. The cycle structure of F is the same on any line parallel to $\gamma\mathbb{F}_q$ and equal to the cycle structure of a linearized permutation of $\mathbb{F}_q$. In some of these cases we can use Theorem 2.8 and Remark 2.4 to determine the cycle structure of F.

We will see, that in cases (F_{18}), (F_{19}) and (F_{20}) the permutation F always satisfies 1, in cases (F_{22}) and (F_{23}) the permutation F always satisfies 2 and that in cases (F_{21}) and (F_{24}) this depends on the parameters γ and m.

5.1 Determining the Cycle Structure in Case (F_{18})

In this section we determine the cycle structure of $F(X) = X + \gamma \operatorname{Tr}_{q^{2lr}/q}(X^{q^l+1}) \in \mathbb{F}_{q^{2lr}}[X]$, where q is arbitrary, $\gamma^{q^{2l}-1} = -1$ and l and r are positive integers.

Theorem 5.2. *Let $F(X) = X + \gamma \operatorname{Tr}_{q^{2lr}/q}(X^{q^l+1}) \in \mathbb{F}_{q^{2lr}}[X]$, where q is arbitrary, $\gamma^{q^{2l}-1} = -1$ and l and r are positive integers. Then γ is a 0-linear translator for $\operatorname{Tr}_{q^{2lr}/q}(x^{q^l+1})$.*

Proof. Remark 10.2 in [11] states, that this follows from the proof of Theorem 10.1 in [11]. We repeat the relevant parts of this proof here.

We want to show that for any $x \in \mathbb{F}_{q^{2lr}}$ and $u \in \mathbb{F}_q$:

$$\operatorname{Tr}_{q^{2lr}/q}((x+u\gamma)^{q^l+1}) - \operatorname{Tr}_{q^{2lr}/q}(x^{q^l+1}) = 0. \tag{5.1}$$

Let $x \in \mathbb{F}_{q^{2lr}}$ and $u \in \mathbb{F}_q$, then

$$(x+u\gamma)^{q^l+1} = (x^{q^l} + u\gamma^{q^l})(x+u\gamma) = \gamma^{q^l+1}u^2 + x\gamma^{q^l}u + x^{q^l}\gamma u + x^{q^l+1},$$

so

$$\operatorname{Tr}_{q^{2lr}/q}((x+u\gamma)^{q^l+1}) = \operatorname{Tr}_{q^{2lr}/q}(\gamma^{q^l+1})u^2 + \operatorname{Tr}_{q^{2lr}/q}(x\gamma^{q^l} + x^{q^l}\gamma)u + \operatorname{Tr}_{q^{2lr}/q}(x^{q^l+1}).$$

Recall that $\gamma^{q^{2l}-1} = -1$, or equivalently $\gamma^{q^{2l}} + \gamma = 0$. We get

$$\begin{aligned}
\operatorname{Tr}_{q^{2lr}/q}(\gamma^{q^l+1}) &= \operatorname{Tr}_{q^l/q}\Big(\operatorname{Tr}_{q^{2l}/q^l}\big(\operatorname{Tr}_{q^{2lr}/q^{2l}}(\gamma^{q^l+1})\big)\Big) \\
&= \operatorname{Tr}_{q^l/q}\Big(\operatorname{Tr}_{q^{2lr}/q^{2l}}(\gamma^{q^l}\gamma) + \operatorname{Tr}_{q^{2lr}/q^{2l}}(\gamma^{q^l}\gamma)^{q^l}\Big) \\
&= \operatorname{Tr}_{q^l/q}\Big(\operatorname{Tr}_{q^{2lr}/q^{2l}}(\gamma^{q^{2l}}\gamma^{q^l} + \gamma^{q^l}\gamma)\Big) \\
&= \operatorname{Tr}_{q^l/q}\Big(\operatorname{Tr}_{q^{2lr}/q^{2l}}\big(\gamma^{q^l}(\gamma^{q^{2l}} + \gamma)\big)\Big) \\
&= \operatorname{Tr}_{q^l/q}(\operatorname{Tr}_{q^{2lr}/q^{2l}}(0)) = 0
\end{aligned}$$

and

$$\begin{aligned}
\operatorname{Tr}_{q^{2lr}/q}(x\gamma^{q^l} + x^{q^l}\gamma) &= Tr_{q^{2lr}/q}(x\gamma^{q^l}) + Tr_{q^{2lr}/q}(x^{q^l}\gamma) \\
&= Tr_{q^{2lr}/q}(x^{q^l}\gamma^{q^{2l}}) + Tr_{q^{2lr}/q}(x^{q^l}\gamma) = \operatorname{Tr}_{q^{2lr}/q}(x^{q^l}\gamma^{q^{2l}} + x^{q^l}\gamma) \\
&= \operatorname{Tr}_{q^{2lr}/q}\big(x^{q^l}(\gamma^{q^{2l}} + \gamma)\big) = \operatorname{Tr}_{q^{2lr}/q}(0) = 0.
\end{aligned}$$

Therefore $\operatorname{Tr}_{q^{2lr}/q}((x+u\gamma)^{q^l+1}) = \operatorname{Tr}_{q^{2lr}/q}(x^{q^l+1})$, which is (5.1). □

Knowing this, one can determine the cycle structure of F using Theorem 3.5.

Theorem 5.3. *Let $F(X) = X + \gamma \operatorname{Tr}_{q^{2lr}/q}(X^{q^l+1}) \in \mathbb{F}_{q^{2lr}}[X]$, where $q = p^s$ for an arbitrary prime p, $\gamma^{q^{2l}-1} = -1$ and l and r are positive integers. Then the cycle structure of F is*

$$\mathrm{CS}(F) = 1^{N_0} p^{N_1},$$

where

$$N_0 = q^{l(r+1)-1}\left(q^{l(r-1)} - (-1)^r(q-1)\right)$$

and

$$N_1 = p^{s-1} q^{l(r+1)-2}\left(q^{l(r-1)} + (-1)^r\right)(q-1).$$

Moreover for any $x \in \mathbb{F}_{q^{2lr}}, \operatorname{Tr}_{q^{2lr}/q}(X^{q^l+1}) \neq 0$ the cycle $\mathcal{C}(F,x) = (x_0\ x_1\ \ldots\ x_{p-1})$, where $x_j = x + j\gamma \operatorname{Tr}_{q^{2lr}/q}(x^{q^l+1})$.

Proof. By Theorem 5.2 the permutation F satisfies the conditions of Theorem 3.5. Theorem 3.18 then gives us the expression for N_0 and thus also for the number $N_1 = (q^{2lr} - N_0)/p$. □

5.2 Determining the Cycle Structure in Case (F_{19})

In this section we determine the cycle structure of the permutation polynomial $F(X) = X + \gamma \operatorname{Tr}_{q^{2m}/q}(X^{2^i(q+1)}) \in \mathbb{F}_{q^{2m}}[X]$, where $q = 2^s$, $\gamma \in \mathbb{F}_{q^2}^*$ and m and i are positive integers.

Theorem 5.4. *Let $F(X) = X + \gamma \operatorname{Tr}_{q^{2m}/q}(X^{2^i(q+1)}) \in \mathbb{F}_{q^{2m}}[X]$, where $q = 2^s$, $\gamma \in \mathbb{F}_{q^2}^*$ and m and i are positive integers. Then γ is a 0-linear translator for $\operatorname{Tr}_{q^{2m}/q}(x^{2^i(q+1)})$.*

Proof. We want to show that for any $x \in \mathbb{F}_{q^{2m}}$ and $u \in \mathbb{F}_q$:

$$\operatorname{Tr}_{q^{2m}/q}((x+u\gamma)^{2^i(q+1)}) - \operatorname{Tr}_{q^{2m}/q}(x^{2^i(q+1)}) = 0. \tag{5.2}$$

Let $x \in \mathbb{F}_{q^{2m}}$ and $u \in \mathbb{F}_q$, then

$$(x+u\gamma)^{q+1} = (x^q + u\gamma^q)(x+u\gamma) = \gamma^{q+1}u^2 + \gamma x^q u + \gamma^q x u + x^{q+1}$$

so

$$\operatorname{Tr}_{q^{2m}/q}((x+u\gamma)^{q+1}) = \operatorname{Tr}_{q^{2m}/q}(\gamma^{q+1})u^2 + \operatorname{Tr}_{q^{2m}/q}(x\gamma^q + x^q\gamma)u + \operatorname{Tr}_{q^{2m}/q}(x^{q+1}).$$

Recall that $\gamma \in \mathbb{F}_{q^2}^*$ or equivalently $\gamma^{q^2} = \gamma$. We get

$$\begin{aligned}\operatorname{Tr}_{q^{2m}/q}(\gamma^{q+1}) &= \operatorname{Tr}_{q^2/q}\left(\operatorname{Tr}_{q^{2m}/q^2}(\gamma^{q+1})\right) = m \operatorname{Tr}_{q^2/q}(\gamma^{q+1}) = m(\gamma^{q+1} + \gamma^{q^2+q}) \\ &= m(\gamma^{q+1} + \gamma^{q+1}) = 0\end{aligned}$$

and

$$\begin{aligned}\mathrm{Tr}_{q^{2m}/q}(\gamma^q x + \gamma x^q) &= \mathrm{Tr}_{q^{2m}/q}(\gamma^q x) + \mathrm{Tr}_{q^{2m}/q}(\gamma x^q) = \mathrm{Tr}_{q^{2m}/q}(\gamma^{q^2} x^q) + \mathrm{Tr}_{q^{2m}/q}(\gamma x^q) \\ &= \mathrm{Tr}_{q^{2m}/q}(\gamma x^q) + \mathrm{Tr}_{q^{2m}/q}(\gamma x^q) = 0.\end{aligned}$$

Therefore

$$\begin{aligned}\mathrm{Tr}_{q^{2m}/q}((x+u\gamma)^{2^i(q+1)}) &= \mathrm{Tr}_{q^{2m}/q}((x+u\gamma)^{q+1})^{2^i} = \mathrm{Tr}_{q^{2m}/q}(x^{q+1})^{2^i} \\ &= \mathrm{Tr}_{q^{2m}/q}(x^{2^i(q+1)}),\end{aligned}$$

which is (5.2). □

Knowing this, one can determine the cycle structure of F using Theorem 3.5.

Theorem 5.5. *Let $F(X) = X + \gamma \,\mathrm{Tr}_{q^{2m}/q}(X^{2^i(q+1)}) \in \mathbb{F}_{q^{2m}}[X]$, where $q = 2^s$, $\gamma \in \mathbb{F}_{q^2}^*$ and m and i are positive integers. Then the cycle structure of F is*

$$\mathrm{CS}(F) = 1^{N_0} 2^{N_1},$$

where

$$N_0 = q^m \left(q^{m-1} - (-1)^m (q-1)\right)$$

and

$$N_1 = 2^{s-1} q^{m-1} \left(q^{m-1} + (-1)^m\right)(q-1).$$

Proof. By Theorem 5.4 the permutation F satisfies the conditions of Theorem 3.5. Theorem 3.18 then gives us the expression for N_0 and thus also for the number $N_1 = (q^{2m} - N_0)/2$. □

Remark 5.1. Since F only has cycles of length 2 it is an involution.

5.3 Determining the Cycle Structure in Case (F_{20})

In this section we determine the cycle structure of the permutation polynomial $F(X) = X + \gamma \,\mathrm{Tr}_{q^{2m}/q}(X^{q^2+1}) \in \mathbb{F}_{q^{2m}}[X]$, where $q = 2^s$, $\gamma \in \mathbb{F}_q^*$ and m is a positive integer.

Theorem 5.6. *Let $F(X) = X + \gamma \,\mathrm{Tr}_{q^{2m}/q}(X^{q^2+1}) \in \mathbb{F}_{q^{2m}}[X]$, where $q = 2^s$, $\gamma \in \mathbb{F}_q^*$ and m is a positive integer. Then γ is a 0-linear translator for $\mathrm{Tr}_{q^{2m}/q}(x^{q^2+1})$.*

Proof. We want to show that for any $x \in \mathbb{F}_{q^{2m}}$ and $u \in \mathbb{F}_q$:

$$\mathrm{Tr}_{q^{2m}/q}((x+u\gamma)^{q^2+1}) - \mathrm{Tr}_{q^{2m}/q}(x^{q^2+1}) = 0. \tag{5.3}$$

Let $x \in \mathbb{F}_{q^{2m}}$ and $u \in \mathbb{F}_q$, then

$$(x+u\gamma)^{q^2+1} = (x^{q^2}+u\gamma)(x+u\gamma) = \gamma^2u^2 + \gamma x^{q^2}u + \gamma xu + x^{q^2+1}$$

so

$$\mathrm{Tr}_{q^{2m}/q}((x+u\gamma)^{q^2+1}) = \mathrm{Tr}_{q^{2m}/q}(\gamma^2)u^2 + \mathrm{Tr}_{q^{2m}/q}(x\gamma + x^{q^2}\gamma)u + \mathrm{Tr}_{q^{2m}/q}(x^{q^2+1}).$$

Now

$$\mathrm{Tr}_{q^{2m}/q}(\gamma^2) = 2m\gamma^2 = 0$$

and

$$\begin{aligned}\mathrm{Tr}_{q^{2m}/q}(x\gamma + x^{q^2}\gamma) &= \gamma\,\mathrm{Tr}_{q^{2m}/q}(x + x^{q^2}) = \gamma\big(\mathrm{Tr}_{q^{2m}/q}(x) + \mathrm{Tr}_{q^{2m}/q}(x^{q^2})\big)\\ &= \gamma\big(\mathrm{Tr}_{q^{2m}/q}(x) + \mathrm{Tr}_{q^{2m}/q}(x)\big) = 0.\end{aligned}$$

Therefore

$$\mathrm{Tr}_{q^{2m}/q}((x+u\gamma)^{q^2+1}) = \mathrm{Tr}_{q^{2m}/q}(x^{q^2+1}),$$

which is (5.3). □

Knowing this, one can determine the cycle structure of F using Theorem 3.5.

Theorem 5.7. *Let $F(X) = X + \gamma\,\mathrm{Tr}_{q^{2m}/q}(X^{q^2+1}) \in \mathbb{F}_{q^{2m}}[X]$, where $q = 2^s$, $\gamma \in \mathbb{F}_q^*$ and m is a positive integer. Then the cycle structure of F is*

$$\mathrm{CS}(F) = 1^{N_0}2^{N_1},$$

where the following holds:

1. *If m is odd, then*
$$N_0 = q^{2m-1}$$
and
$$N_1 = 2^{s-1}q^{2m-2}(q-1).$$
2. *If m is even, then*
$$N_0 = q^{m+1}\left(q^{m-2} - (-1)^{m/2}(q-1)\right)$$
and
$$N_1 = 2^{s-1}q^m\left(q^{m-2} + (-1)^{m/2}\right)(q-1).$$

Proof. By Theorem 5.6 the permutation F satisfies the conditions of Theorem 3.5. Theorem 3.18 then gives us the expression for N_0 and thus also for the number $N_1 = (q^{2m} - N_0)/2$. □

Remark 5.2. Since F only has cycles of length 2 it is an involution.

5.4 Determining the Cycle Structure in Case (F_{22})

In this section we determine the cycle structure of the permutation polynomial $F(X) = X + \gamma \operatorname{Tr}_{q^{2m+1}/q}(X^{2q^i+2q^j}) \in \mathbb{F}_{q^{2m+1}}[X]$, where $q = 2^s$, $s \equiv \pm 2 \pmod 6$, $\gamma \in \mathbb{F}_q^*$, with $\gamma^{(q-1)/3} \neq 1$, and m, i, j are positive integers with $i \neq j$. Note that $\gamma \mathbb{F}_q = \mathbb{F}_q$.

Theorem 5.8. *Let $q = 2^s$, where $s \equiv \pm 2 \pmod 6$ and $\alpha \in \mathbb{F}_{q^{2m+1}}$. Then the permutation $F(x) = x + \gamma \operatorname{Tr}_{q^{2m+1}/q}(x^{2q^i+2q^j})$, where $\gamma \in \mathbb{F}_q^*$, with $\gamma^{(q-1)/3} \neq 1$, and m, i, j are positive integers with $i \neq j$, has the same cycle structure on $\alpha + \mathbb{F}_q$ as the permutation $L(x) = x + \gamma x^4$ on $\mathbb{F}_q$.*

Proof. We abbreviate $\operatorname{Tr}(x) = \operatorname{Tr}_{q^{2m+1}/q}(x)$. As in the proof of Theorem 4.5, we see that the cycle structure of F on $\alpha + \mathbb{F}_q$ is the same as the cycle structure of

$$L_\alpha : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x + \gamma \operatorname{Tr}((\alpha + x)^{2q^i+2q^j})$$

on $\mathbb{F}_q$. Now for $x \in \mathbb{F}_q$, we get

$$(\alpha + x)^{2q^i+2q^j} = (\alpha^{2q^i} + x^2)(\alpha^{2q^j} + x^2) = x^4 + \alpha^{2q^i} x^2 + \alpha^{2q^j} x^2 + \alpha^{2q^i+2q^j}$$

so

$$\operatorname{Tr}((\alpha + x)^{2q^i+2q^j}) = x^4 + \left(\operatorname{Tr}(\alpha^{2q^i}) + \operatorname{Tr}(\alpha^{2q^j})\right) x^2 + \operatorname{Tr}(\alpha^{2q^i+2q^j})$$

and

$$L_\alpha(x) = x + \gamma \left(x^4 + \operatorname{Tr}(\alpha^{2q^i+2q^j})\right).$$

Note that $L(x) := L_0(x) = x + \gamma x^4$ and it therefore suffices to show that for any $\alpha \in \mathbb{F}_{q^{2m+1}}$, the permutation L_α has the same cycle structure as L_0.

Let $\alpha \in \mathbb{F}_{q^{2m+1}}$. Since $x \mapsto x^4$ is a permutation of $\mathbb{F}_q$, there exists a $u_\alpha \in \mathbb{F}_q$ with $u_\alpha^4 = \operatorname{Tr}(\alpha^{2q^i+2q^j})$. By Proposition 1.1, the permutation L_α has the same cycle structure as

$$\begin{aligned} L_\alpha(x - u_\alpha) + u_\alpha &= x - u_\alpha + \gamma \left((x - u_\alpha)^4 + \operatorname{Tr}(\alpha^{2q^i+2q^j})\right) + u_\alpha \\ &= x + \gamma \left(x^4 + \operatorname{Tr}(\alpha^{2q^i+2q^j}) - u_\alpha^4\right) = x + \gamma x^4 = L_0(x). \end{aligned}$$

□

The permutation L is a 4-linearized polynomial. For $\gamma \in \mathbb{F}_4$, we can determine the cycle structure of L using Theorem 2.8. The next theorem shows, that the cycle structure of L is the same for any choice of γ. Since we can always choose a $\gamma \in \mathbb{F}_4$ this means, we can always determine the cycle structure of L.

Theorem 5.9. *Let $q = 2^s$, where $s \equiv \pm 2 \pmod 6$ and $\gamma_1, \gamma_2 \in \mathbb{F}_q^*$ with $\gamma_1^{(q-1)/3} \neq 1, \gamma_2^{(q-1)/3} \neq 1$. Then the permutations $L_{\gamma_1}(x) = x + \gamma_1 x^4$ and $L_{\gamma_2}(x) = x + \gamma_2 x^4$ have the same cycle structure on $\mathbb{F}_q$.*

Proof. Let $L_\gamma = x + \gamma x^4$, where $\gamma \in \mathbb{F}_q^*$ with $\gamma^{(q-1)/3} \neq 1$. First we will show that L_γ has the same cycle structure as L_δ for a $\delta \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Note that $\gamma^{(q-1)/3} \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Since $q = 2^s$ with s even and not divisible by 3, we can write $q = 4^t$, where $2t = s$ and t is not divisible by 3.

If $t \equiv 1 \pmod 3$, then $t = 3r + 1$ for some $r \in \mathbb{N}$ and

$$q - 4 \equiv 4(4^3)^r - 4 \equiv 4(1)^r - 4 \equiv 0 \pmod 9, \text{ so } \frac{q-4}{9} \in \mathbb{Z}.$$

Now we see

$$\frac{L_\gamma\left(x\gamma^{(q-4)/9}\right)}{\gamma^{(q-4)/9}} = x + \gamma\left(\gamma^{(q-4)/9}\right)^3 x^4 = x + \gamma^{\frac{q-1}{3}} x^4 = x + \delta x^4 = L_\delta(x)$$

for some $\delta \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Proposition 1.1 shows, that L_γ has the same cycle structure as L_δ.

If $t \equiv -1 \pmod 3$, then $t = 3r + 2$ for some $r \in \mathbb{N}$ and

$$q + 2 \equiv 16(4^3)^r + 2 \equiv 7(1)^r + 2 \equiv 0 \pmod 9, \text{ so } -\frac{q+2}{9} \in \mathbb{Z}.$$

Now we see

$$\frac{L_\gamma\left(x\gamma^{-(q+2)/9}\right)}{\gamma^{-(q+2)/9}} = x + \gamma\left(\gamma^{-(q+2)/9}\right)^3 x^4 = x + \gamma^{-\frac{q-1}{3}} x^4 = x + \delta x^4 = L_\delta(x)$$

for some $\delta \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Proposition 1.1 shows, that L_γ has the same cycle structure as L_δ.

Let a be a primitive element of $\mathbb{F}_4$, then $\mathbb{F}_4 \setminus \mathbb{F}_2 = \{a, a^2\}$. It remains to show, that L_a has the same cycle structure as L_{a^2}. For that consider

$$L_{a^2}(x^{2^{s-1}})^2 = \left(x^{2^{s-1}} + a^2(x^4)^{2^{s-1}}\right)^2 = x + a^4x^4 = x + ax^4 = L_a(x).$$

Proposition 1.1 shows, that L_{a^2} has the same cycle structure as L_a. □

Now the cycle structure of L can be determined. Note that by Theorem 5.9 it is the same as that of the linearized polynomial L_a considered in the example (Example 2.1, Example 2.2, Example 2.3 and Table 2.1) used in Section 2.3 of Chapter 2.

Theorem 5.10. *Let $q = 2^s$, where $s \equiv \pm 2 \pmod 6$ and $\gamma \in \mathbb{F}_q^*$ with $\gamma^{(q-1)/3} \neq 1$. Let a be a primitive element of $\mathbb{F}_4$ and $s = 2t$. Let $\mathrm{ord}_\Gamma(\Lambda)$ denote the multiplicative order of $\Lambda(X)$ modulo $\Gamma(X)$ and Φ denote Euler's totient function for polynomials.*

Then the cycle structure of the permutation polynomial $L(X) = X + \gamma X^4 \in \mathbb{F}_q[X]$ *is*

$$\mathrm{CS}(L) = \sum_{\Gamma(X)|X^t-1} \mathrm{ord}_\Gamma(1+aX)^{\frac{\Phi(\Gamma)}{\mathrm{ord}_\Gamma(1+aX)}},$$

where $\Gamma(X), 1+aX \in \mathbb{F}_4[X]$. *Further the number of cycles of length* $\mathrm{ord}_\Gamma(1+aX)$ *in the cycle structure of* L *is*

$$\frac{\sum_{H\in\mathcal{H}} \Phi(H)}{\mathrm{ord}_\Gamma(1+aX)},$$

where $\mathcal{H} = \{H \in \mathbb{F}_4[X] : H \mid X^t - 1, \mathrm{ord}_H(1+aX) = \mathrm{ord}_\Gamma(1+aX)\}$.

Proof. By Theorem 5.9 the cycle structure of L does not depend on γ, so we can choose $\gamma = a$. The theorem then follows by Theorem 2.8 and Remark 2.4. □

The next theorem summarizes the results of this section by stating the cycle structure of F.

Theorem 5.11. *Let* $q = 2^s$, *where* $s \equiv \pm 2 \pmod 6$ *and* $\gamma \in \mathbb{F}_q^*$ *with* $\gamma^{(q-1)/3} \neq 1$. *Let* a *be a primitive element of* $\mathbb{F}_4$ *and* $s = 2t$. *Let* $\mathrm{ord}_\Gamma(\Lambda)$ *denote the multiplicative order of* $\Lambda(X)$ *modulo* $\Gamma(X)$ *and* Φ *denote Euler's totient function for polynomials. The cycle structure of the permutation* $F(x) = x + \gamma \,\mathrm{Tr}_{q^{2m+1}/q}(x^{2q^i+2q^j})$, *where* m, i *and* j *are positive integers with* $i \neq j$, *on any line* $\alpha + \mathbb{F}_q$ *is*

$$\mathrm{CS}_{\alpha+\mathbb{F}_q}(F) = \sum_{\Gamma(X)|X^t-1} \mathrm{ord}_\Gamma(1+aX)^{\frac{\Phi(\Gamma)}{\mathrm{ord}_\Gamma(1+aX)}},$$

where $\Gamma(X), 1+aX \in \mathbb{F}_4[X]$. *Further the number of cycles of length* $\mathrm{ord}_\Gamma(1+aX)$ *in the cycle decomposition of* F *on* $\alpha + \mathbb{F}_q$ *is*

$$\frac{\sum_{H\in\mathcal{H}} \Phi(H)}{\mathrm{ord}_\Gamma(1+aX)},$$

where $\mathcal{H} = \{H \in \mathbb{F}_4[X] : H \mid X^t - 1, \mathrm{ord}_H(1+aX) = \mathrm{ord}_\Gamma(1+aX)\}$.

Proof. The theorem follows from Theorem 5.8 and Theorem 5.10. □

Remark 5.3. Example 2.2 shows the following. If $t = 2^r$ then the cycle structure $\mathrm{CS}_{\alpha+\mathbb{F}_q}(F) = CS(L) = 1^1 3^1 6^2 12^{20} \ldots (2^r \cdot 3)^{(4^{2^r} - 4^{2^{r-1}})/(2^r \cdot 3)}$.

5.5 Determining the Cycle Structure in Case (F_{23})

In this section we determine the cycle structure of the permutation polynomial $F(X) = X + \gamma \,\mathrm{Tr}_{q^{2m+1}/q}(X^{(q^2+q)/2}) \in \mathbb{F}_{q^{2m+1}}[X]$, where $q = 2^s$, $\gamma \in \mathbb{F}_q \setminus \{0, 1\}$ and m and s are positive integers. Note that $\gamma\mathbb{F}_q = \mathbb{F}_q$.

Theorem 5.12. *Let $q = 2^s$, where s is a positive integer and $\alpha \in \mathbb{F}_{q^{2m+1}}$. Then the permutation $F(x) = x + \gamma \operatorname{Tr}_{q^{2m+1}/q}(x^{(q^2+q)/2})$, where $\gamma \in \mathbb{F}_q \setminus \{0,1\}$ and m is a positive integer, has the same cycle structure on $\alpha + \mathbb{F}_q$ as the permutation $L(x) = (\gamma+1)x$ on $\mathbb{F}_q$.*

Proof. We abbreviate $\operatorname{Tr}(x) = \operatorname{Tr}_{q^{2m+1}/q}(x)$. Note that $(q^2+q)/2 = 2^{2s-1} + 2^{s-1}$. As in the proof of Theorem 4.5, we see that the cycle structure of F on $\alpha + \mathbb{F}_q$ is the same as the cycle structure of $L_\alpha : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x + \gamma \operatorname{Tr}((\alpha+x)^{2^{2s-1}+2^{s-1}})$ on $\mathbb{F}_q$. Now for $x \in \mathbb{F}_q$, we get

$$\begin{aligned}(\alpha+x)^{2^{2s-1}+2^{s-1}} &= (\alpha^{2^{2s-1}} + x^{2^{s-1}})(\alpha^{2^{s-1}} + x^{2^{s-1}}) \\ &= x + (\alpha^{2^{2s-1}} + \alpha^{2^{s-1}})x^{2^{s-1}} + \alpha^{2^{2s-1}+2^{s-1}}\end{aligned}$$

so

$$\begin{aligned}\operatorname{Tr}((\alpha+x)^{2^{2s-1}+2^{s-1}}) &= x + \left(\operatorname{Tr}(\alpha^{2^{2s-1}}) + \operatorname{Tr}(\alpha^{2^{s-1}})\right) x^{2^{s-1}} + \operatorname{Tr}(\alpha^{2^{2s-1}+2^{s-1}}) \\ &= x + \operatorname{Tr}(\alpha^{2^{2s-1}+2^{s-1}})\end{aligned}$$

and

$$L_\alpha(x) = x + \gamma\left(x + \operatorname{Tr}(\alpha^{2^{2s-1}+2^{s-1}})\right).$$

Note that $L(x) = L_0(x) = x + \gamma x$ and it therefore suffices to show that for any $\alpha \in \mathbb{F}_{q^{2m+1}}$, the permutation L_α has the same cycle structure as L_0.

Let $\alpha \in \mathbb{F}_{q^{2m+1}}$ and $u_\alpha = \operatorname{Tr}(\alpha^{2^{2s-1}+2^{s-1}})$. By Proposition 1.1, the permutation L_α has the same cycle structure as

$$L_\alpha(x - u_\alpha) + u_\alpha = x - u_\alpha + \gamma(x - u_\alpha + \operatorname{Tr}(\alpha^{2^{2s-1}+2^{s-1}}) + u_\alpha = x + \gamma x = L_0(x).$$

□

Since the cycle structure of L is easy to determine, we can now immediately also determine the cycle structure of F.

Theorem 5.13. *Let $q = 2^s$, where s is a positive integer and $\alpha \in \mathbb{F}_{q^{2m+1}}$. The cycle structure of the permutation $F(x) = x + \gamma \operatorname{Tr}_{q^{2m+1}/q}(x^{(q^2+q)/2})$, where $\gamma \in \mathbb{F}_q \setminus \{0,1\}$ and m is a positive integer, on any line $\alpha + \gamma\mathbb{F}_q$ is*

$$\mathrm{CS}_{\alpha+\gamma\mathbb{F}_q}(F) = 1^1 \operatorname{ord}(\gamma+1)^{q/\operatorname{ord}(\gamma+1)}.$$

5.6 Properties of the Cycle Structure in Case (F_{21})

In this section we study the cycle structure of $F(X) = X + \gamma \operatorname{Tr}_{q^{2m}/q}(X^{2^i(q^2+1)}) \in \mathbb{F}_{q^{2m}}[X]$, where $q = 2^s$, $\gamma \in \mathbb{F}_{q^2}^*$, m, s and i are positive integers, and either m is even, or m is odd and $(\gamma^{2^{i+1}} + \gamma^{2^{i+1}q})^{(q-1)/\gcd(2^{i+1}-1, 2^s-1)} \neq 1$. For m even or $\gamma \in \mathbb{F}_q$ the cycle structure can be determined explicitly.

Theorem 5.14. *Let $F(X) = X + \gamma \operatorname{Tr}_{q^{2m}/q}(X^{2^i(q^2+1)}) \in \mathbb{F}_{q^{2m}}[X]$, where $q = 2^s$ and $\gamma \in \mathbb{F}_{q^2}^*$ and m, s and i are positive integers, and either m is even, or m is odd and $(\gamma^{2^{i+1}} + \gamma^{2^{i+1}q})^{(q-1)/\gcd(2^{i+1}-1, 2^s-1)} \neq 1$. If m is even or $\gamma \in \mathbb{F}_q$, then γ is a 0-linear translator for $\operatorname{Tr}_{q^{2m}/q}(x^{2^i(q^2+1)})$.*

Proof. Let m be even or $\gamma \in \mathbb{F}_q$. We want to show that for any $x \in \mathbb{F}_{q^{2m}}$ and $u \in \mathbb{F}_q$:

$$\operatorname{Tr}_{q^{2m}/q}((x+u\gamma)^{2^i(q^2+1)}) - \operatorname{Tr}_{q^{2m}/q}(x^{2^i(q^2+1)}) = 0. \tag{5.4}$$

Let $x \in \mathbb{F}_{q^{2m}}$ and $u \in \mathbb{F}_q$, then

$$\begin{aligned}(x+u\gamma)^{q^2+1} &= (x+u\gamma)^{q^2+1} = (x^{q^2}+u\gamma)(x+u\gamma)\\ &= \gamma^2u^2 + \gamma x^{q^2}u + \gamma x u + x^{q^2+1}\end{aligned}$$

so

$$\operatorname{Tr}_{q^{2m}/q}((x+u\gamma)^{q^2+1}) = \operatorname{Tr}_{q^{2m}/q}(\gamma^2)u^2 + \operatorname{Tr}_{q^{2m}/q}(x\gamma + x^{q^2}\gamma)u + \operatorname{Tr}_{q^{2m}/q}(x^{q^2+1}).$$

Now

$$\operatorname{Tr}_{q^{2m}/q}(x\gamma + x^{q^2}\gamma) = \operatorname{Tr}_{q^{2m}/q}(x\gamma) + \operatorname{Tr}_{q^{2m}/q}(x^{q^2}\gamma) = 0$$

and if m is even, then

$$\operatorname{Tr}_{q^{2m}/q}(\gamma^2) = \operatorname{Tr}_{q^2/q}\left(\operatorname{Tr}_{q^{2m}/q^2}(\gamma^2)\right) = m \operatorname{Tr}_{q^2/q}(\gamma^2) = 0,$$

if $\gamma \in \mathbb{F}_q$, then

$$\operatorname{Tr}_{q^{2m}/q}(\gamma^2) = 2m\gamma^2 = 0.$$

Therefore

$$\begin{aligned}\operatorname{Tr}_{q^{2m}/q}((x+u\gamma)^{2^i(q^2+1)}) &= \operatorname{Tr}_{q^{2m}/q}((x+u\gamma)^{q^2+1})^{2^i} = \operatorname{Tr}_{q^{2m}/q}(x^{q^2+1})^{2^i}\\ &= \operatorname{Tr}_{q^{2m}/q}(x^{2^i(q^2+1)}),\end{aligned}$$

which is (5.4). □

Knowing this, one can determine the cycle structure of F for m even or $\gamma \in \mathbb{F}_q$ using Theorem 3.5.

Theorem 5.15. *Let $F(X) = X + \gamma \operatorname{Tr}_{q^{2m}/q}(X^{2^i(q^2+1)}) \in \mathbb{F}_{q^{2m}}[X]$, where $q = 2^s$ and $\gamma \in \mathbb{F}_{q^2}^*$ and m, s and i are positive integers, and either m is even, or m is odd and $(\gamma^{2^{i+1}} + \gamma^{2^{i+1}q})^{(q-1)/\gcd(2^{i+1}-1, 2^s-1)} \neq 1$. If m is even or $\gamma \in \mathbb{F}_q$, then the cycle structure of F is*

$$\operatorname{CS}(F) = 1^{N_0}2^{N_1},$$

where the following holds:

1. *If m is odd, then*
$$N_0 = q^{2m-1}$$
and
$$N_1 = 2^{s-1}q^{2m-2}(q-1).$$

2. *If m is even, then*
$$N_0 = q^{m+1}\left(q^{m-2} - (-1)^{m/2}(q-1)\right)$$
and
$$N_1 = 2^{s-1}q^m\left(q^{m-2} + (-1)^{m/2}\right)(q-1).$$

Proof. By Theorem 5.14 the permutation F satisfies the conditions of Theorem 3.5. Theorem 3.18 then gives us the expression for N_0 and thus also for the number $N_1 = (q^{2m} - N_0)/2$. □

Remark 5.4. Since F only has cycles of length 2, if m is even or $\gamma \in \mathbb{F}_q$, it is an involution for this choice of parameters.

In the other case the following holds.

Theorem 5.16. *Let $F(X) = X + \gamma \operatorname{Tr}_{q^{2m}/q}(X^{2^i(q^2+1)}) \in \mathbb{F}_{q^{2m}}[X]$, where $q = 2^s$ and $\gamma \in \mathbb{F}_{q^2}^*$ and m, s and i are positive integers, and either m is even, or m is odd and $(\gamma^{2^{i+1}} + \gamma^{2^{i+1}q})^{(q-1)/\gcd(2^{i+1}-1,2^s-1)} \neq 1$. Let $\alpha \in \mathbb{F}_{q^{2m}}$. If m is odd and $\gamma \notin \mathbb{F}_q$, then F has the same cycle structure on $\alpha + \gamma\mathbb{F}_q$ as the permutation $L(x) = x + \operatorname{Tr}_{q^2/q}(\gamma^{2^i+1})x^{2^{i+1}}$ on $\mathbb{F}_q$.*

Proof. We abbreviate $\operatorname{Tr}(x) = \operatorname{Tr}_{q^{2m+1}/q}(x)$. Let m be odd and $\gamma \notin \mathbb{F}_q$. By Remark 4.1, the mapping F is a permutation of the coset $\alpha + \gamma\mathbb{F}_q$. Let $x \in \mathbb{F}_q$. Then for a fixed α, we get
$$F(\alpha + \gamma x) = \alpha + \gamma x + \gamma \operatorname{Tr}\left((\alpha + \gamma x)^{2^i(q^2+1)}\right) = \alpha + \gamma L_\alpha(x)$$
with $L_\alpha : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x + \operatorname{Tr}\left((\alpha + \gamma x)^{2^i(q^2+1)}\right)$. Since
$$L_\alpha(x) = (F(\alpha + \gamma x) - \alpha)/\gamma = \tau^{-1} \circ F \circ \tau,$$
where $\tau : \mathbb{F}_q \to \alpha + \gamma\mathbb{F}_q$, with $\tau(x) = \alpha + \gamma x$, Proposition 1.1 shows that L_α is a permutation of $\mathbb{F}_q$ that has the same cycle structure as F on $\alpha + \gamma\mathbb{F}_q$.

Now we see
$$(\alpha + \gamma x)^{q^2+1} = (\alpha^{q^2} + \gamma x)(\alpha + \gamma x) = \gamma^2 x^2 + (\alpha + \alpha^{q^2})\gamma x + \alpha^{q^2+1}$$
so
$$\begin{aligned}\operatorname{Tr}((\alpha + \gamma x)^{q^2+1}) &= \operatorname{Tr}(\gamma^2)x^2 + \left(\operatorname{Tr}(\alpha\gamma) + \operatorname{Tr}(\alpha^{q^2}\gamma)\right)x + \operatorname{Tr}(\alpha^{q^2+1}) \\ &= \operatorname{Tr}(\gamma^2)x^2 + \operatorname{Tr}(\alpha^{q^2+1})\end{aligned}$$

and

$$L_\alpha = x + \left[\mathrm{Tr}(\gamma^2)x^2 + \mathrm{Tr}(\alpha^{q^2+1})\right]^{2^i}.$$

Note that $L(x) = L_0(x) = x + \mathrm{Tr}_{q^2/q}(\gamma^{2^i+1})x^{2^{i+1}}$ and it therefore suffices to show that for any $\alpha \in \mathbb{F}_{q^{2m}}$, the permutation L_α has the same cycle structure as L_0.

Let $\alpha \in \mathbb{F}_{q^{2m}}$. Since $x \mapsto x^2$ is a permutation of $\mathbb{F}_q$, there exists a $u_\alpha \in \mathbb{F}_q$ with $u_\alpha^2 = \mathrm{Tr}(\alpha^{q^2+1})/\mathrm{Tr}(\gamma^2)$. By Proposition 1.1, the permutation L_α has the same cycle structure as

$$\begin{aligned} L_\alpha(x-u_\alpha)+u_\alpha &= x - u_\alpha + \left[\mathrm{Tr}(\gamma^2)x^2 - \mathrm{Tr}(\gamma^2)\frac{\mathrm{Tr}(\alpha^{q^2+1})}{\mathrm{Tr}(\gamma^2)} + \mathrm{Tr}(\alpha^{q^2+1})\right]^{2^i} + u_\alpha \\ &= x + \left[\mathrm{Tr}_{q^2/q}(\gamma^2)x^2\right]^{2^i} = x + \mathrm{Tr}_{q^2/q}(\gamma^{2^{i+1}})x^{2^{i+1}} = L_0(x). \end{aligned}$$

□

Here L is a 2^{i+1}-linearized permutation polynomial, but since we cannot assume, that $\mathrm{Tr}_{q^2/q}(\gamma^{2^i+1}) \in \mathbb{F}_{2^{i+1}}$, we cannot use Theorem 2.8 to determine the cycle structure of L in this case completely.

5.7 Properties of the Cycle Structure in Case (F_{24})

In this section we study the cycle structure of $F(X) = X + \gamma\,\mathrm{Tr}_{q^n/q}(X^{p^i}) \in \mathbb{F}_{q^n}[X]$, where $q = p^s$, $\gamma \in \mathbb{F}_{q^n}^*$ with $(-\mathrm{Tr}_{q^n/q}(\gamma))^{(q-1)/(p^d-1)} \neq 1$ and n, s, d and i are positive integers with $1 \leq i \leq s$ and $d = \gcd(i,s)$. For $\mathrm{Tr}_{q^n/q}(\gamma) = 0$ the cycle structure can be determined explicitly.

Theorem 5.17. *Let $F(X) = X + \gamma\,\mathrm{Tr}_{q^n/q}(X^{p^i}) \in \mathbb{F}_{q^n}[X]$, where $q = p^s$, $\gamma \in \mathbb{F}_{q^n}^*$ with $(-\mathrm{Tr}_{q^n/q}(\gamma))^{(q-1)/(p^d-1)} \neq 1$ and n, s, d and i are positive integers with the properties $1 \leq i \leq s$ and $d = \gcd(i,s)$. If $\mathrm{Tr}_{q^n/q}(\gamma) = 0$, then γ is a 0-linear translator for $\mathrm{Tr}_{q^n/q}(x^{p^i})$.*

Proof. Let $\mathrm{Tr}_{q^n/q}(\gamma) = 0$. We want to show that for any $x \in \mathbb{F}_{q^n}$ and $u \in \mathbb{F}_q$:

$$\mathrm{Tr}_{q^n/q}((x+u\gamma)^{p^i}) - \mathrm{Tr}_{q^n/q}(x^{p^i}) = 0 \tag{5.5}$$

Let $x \in \mathbb{F}_{q^n}$ and $u \in \mathbb{F}_q$, then

$$\begin{aligned} \mathrm{Tr}_{q^n/q}((x+u\gamma)^{p^i}) - \mathrm{Tr}_{q^n/q}(x^{p^i}) &= \left[\mathrm{Tr}_{q^n/q}(x+u\gamma) - \mathrm{Tr}_{q^n/q}(x)\right]^{p^i} \\ &= \left[u\,\mathrm{Tr}_{q^n/q}(\gamma)\right]^{p^i} = 0. \end{aligned}$$

□

Knowing this, one can determine the cycle structure of F for $\mathrm{Tr}_{q^n/q}(\gamma) = 0$ using Theorem 3.5.

Theorem 5.18. *Let $F(X) = X + \gamma \mathrm{Tr}_{q^n/q}(X^{p^i}) \in \mathbb{F}_{q^n}[X]$, where $q = p^s$, $\gamma \in \mathbb{F}_{q^n}^*$ with $(-\mathrm{Tr}_{q^n/q}(\gamma))^{(q-1)/(p^d-1)} \neq 1$ and n, s, d and i are positive integers with the properties $1 \leq i \leq s$ and $d = \gcd(i, s)$. If $\mathrm{Tr}_{q^n/q}(\gamma) = 0$, then the cycle structure of F is*

$$\mathrm{CS}(F) = 1^{N_0} p^{N_1},$$

where

$$N_0 = q^{n-1}$$

and

$$N_1 = p^{s-1} q^{n-2}(q-1).$$

Moreover for any $x \in \mathbb{F}_{q^n}, \mathrm{Tr}_{q^n/q}(x^{p^i}) \neq 0$ the cycle $\mathcal{C}(F, x) = (x_0\ x_1\ \ldots\ x_{p-1})$, where $x_j = x + j\gamma \mathrm{Tr}_{q^n/q}(x^{p^i})$.

Proof. By Theorem 5.17 the permutation F satisfies the conditions of Theorem 3.5. Theorem 3.18 then gives us the expression for N_0 and thus also for the number $N_1 = (q^n - N_0)/p$. □

In the other case the following holds.

Theorem 5.19. *Let $F(X) = X + \gamma \mathrm{Tr}_{q^n/q}(X^{p^i}) \in \mathbb{F}_{q^n}[X]$, where $q = p^s$, $\gamma \in \mathbb{F}_{q^n}^*$ with $(-\mathrm{Tr}_{q^n/q}(\gamma))^{(q-1)/(p^d-1)} \neq 1$ and n, s, d and i are positive integers with the properties $1 \leq i \leq s$ and $d = \gcd(i, s)$. If $\mathrm{Tr}_{q^n/q}(\gamma) \neq 0$, then F has the same cycle structure on $\alpha + \gamma\mathbb{F}_q$ as the permutation $L(x) = x + \mathrm{Tr}_{q^n/q}(\gamma^{p^i})x^{p^i}$ on $\mathbb{F}_q$.*

Proof. We abbreviate $\mathrm{Tr}(x) = \mathrm{Tr}_{q^n/q}(x)$. Let $\mathrm{Tr}(\gamma) \neq 0$. As in the proof of Theorem 4.5, we see that the cycle structure of F on $\alpha + \mathbb{F}_q$ is the same as the cycle structure of $L_\alpha : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x + \mathrm{Tr}((\alpha + \gamma x)^{p^i})$ on $\mathbb{F}_q$. Now for $x \in \mathbb{F}_q$ we get

$$L_\alpha(x) = x + \mathrm{Tr}(\alpha + \gamma x)^{p^i} = x + \mathrm{Tr}(\gamma^{p^i})x^{p^i} + \mathrm{Tr}(\alpha^{p^i}).$$

Note that $L(x) = L_0(x) = x + \mathrm{Tr}(\gamma^{p^i})x^{p^i}$ and it therefore suffices to show that for any $\alpha \in \mathbb{F}_{q^n}$, the permutation L_α has the same cycle structure as L_0.

Let $\alpha \in \mathbb{F}_{q^n}$ and $u_\alpha = \mathrm{Tr}(\alpha)/\mathrm{Tr}(\gamma)$. By Proposition 1.1, the permutation L_α has the same cycle structure as

$$\begin{aligned} L_\alpha(x - u_\alpha) + u_\alpha &= x - u_\alpha + \mathrm{Tr}(\gamma^{p^i})x^{p^i} - \frac{\mathrm{Tr}(\alpha^{p^i})}{\mathrm{Tr}(\gamma^{p^i})}\mathrm{Tr}(\gamma^{p^i}) + \mathrm{Tr}(\alpha^{p^i}) + u_\alpha \\ &= x + \mathrm{Tr}(\gamma^{p^i})x^{p^i} = L_0(x). \end{aligned}$$

□

Here L is a p^i-linearized permutation polynomial, but since we cannot assume, that $\mathrm{Tr}_{q^n/q}(\gamma^{p^i}) \in \mathbb{F}_{p^i}$, we cannot use Theorem 2.8 to determine the cycle structure of L in this case completely.

Chapter 6

Shifting the Exponent

By composing one of the permutation polynomials in Theorem 3.4 with a suitable monomial permutation one can get a permutation polynomial, which has the shape $X^t + \gamma \operatorname{Tr}_{q^n/q}(X)$. In one of these cases the cycle structure of the resulting permutation can be determined explicitly by computing its iterates.

The next section is based on work published in [10].

6.1 The Permutation Polynomial $X^{q^2+q-1} + \operatorname{Tr}_{q^3/q}(X)$

In this section, we consider the reduced permutation polynomial $F(X)$ on $\mathbb{F}_{q^3}$ associated to the map given by

$$F(x) = (x + \operatorname{Tr}_{q^3/q}(x^{(q^2+1)/2})) \circ (x^{q^2+q-1}),$$

which is obtained by composing the permutation described in case (F_{16}) of Theorem 3.4 with the permutation $x \mapsto x^{q^2+q-1}$. We describe explicitly the iterates of F and then use this to determine its cycle structure and the polynomial representation of its inverse map.

It is easy to check that

$$(q^2+q-1) \cdot \frac{q^2+1}{2} = \frac{(q^3-1)(q+1)}{2} + q \equiv q \pmod{q^3-1}$$

and therefore

$$F(X) = X^{q^2+q-1} + \operatorname{Tr}_{q^3/q}(X).$$

Further, for $x \neq 0$, we have

$$F(x) = \frac{x^{q^2+q} + x(x + x^q + x^{q^2})}{x} = x + \frac{\operatorname{Tr}_{q^3/q}(x^{q+1})}{x},$$

and hence

$$F(x) = \begin{cases} x + \frac{\operatorname{Tr}_{q^3/q}(x^{q+1})}{x}, & x \in \mathbb{F}_{q^3}^* \\ 0, & x = 0. \end{cases}$$

In the remaining part of this section, we use the convention $0/0 = 0$ and write

$$F(x) = x + \frac{\operatorname{Tr}_{q^3/q}(x^{q+1})}{x} \text{ for all } x \in \mathbb{F}_{q^3}.$$

The following two lemmas describe computational connections in $\mathbb{F}_{q^3}$, which are fundamental for the results of this section.

Lemma 6.1. *Any $x \in \mathbb{F}_{q^3}$ satisfies*

$$x^3 - \mathrm{Tr}_{q^3/q}(x)x^2 + \mathrm{Tr}_{q^3/q}(x^{q+1})x - \mathrm{N}_{q^3/q}(x) = 0, \tag{6.1}$$

where $N_{q^3/q}(x) = x^{1+q+q^2}$ is the norm of x *over $\mathbb{F}_q$.*

Proof. Any $x \in \mathbb{F}_q$ clearly fulfils (6.1). Let hence $x \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and $m(X) \in \mathbb{F}_q[X]$ be the minimal polynomial of x over $\mathbb{F}_q$. Since $m(X) = (X-x)(X-x^q)(X-x^{q^2})$ in $\mathbb{F}_{q^3}[X]$, we get

$$m(X) = X^3 - \mathrm{Tr}_{q^3/q}(x)X^2 + \mathrm{Tr}_{q^3/q}(x^{q+1})X - \mathrm{N}_{q^3/q}(x),$$

implying the statement. □

Lemma 6.2. *Let $x \in \mathbb{F}_{q^3}^*$. Then we have*

(a) $\mathrm{Tr}_{q^3/q}\left(\frac{1}{x}\right) = \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{\mathrm{N}_{q^3/q}(x)}$;

(b) $\mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q+1}}\right) = \frac{\mathrm{Tr}_{q^3/q}(x)}{\mathrm{N}_{q^3/q}(x)}$;

(c) $\mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q-1}}\right) + \mathrm{Tr}_{q^3/q}(x^{q-1}) = \mathrm{Tr}_{q^3/q}(x^{q+1})\,\mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q+1}}\right) - 3.$

Proof. Property (a) follows from

$$\mathrm{Tr}_{q^3/q}\left(\frac{1}{x}\right) = \frac{1}{x} + \frac{1}{x^q} + \frac{1}{x^{q^2}} = \frac{x^{q^2+q} + x^{q^2+1} + x^{q+1}}{x^{1+q+q^2}} = \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{\mathrm{N}_{q^3/q}(x)}.$$

This also shows that

$$\mathrm{Tr}_{q^3/q}(x) = \frac{\mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q+1}}\right)}{\mathrm{N}_{q^3/q}\left(\frac{1}{x}\right)} = \mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q+1}}\right)\mathrm{N}_{q^3/q}(x),$$

from which (b) follows. For (c), note that

$$\begin{aligned}
\mathrm{Tr}_{q^3/q}(x^{q+1})\,\mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q+1}}\right) &= \mathrm{Tr}_{q^3/q}\left(\frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x^{q+1}}\right) \\
&= \mathrm{Tr}_{q^3/q}\left(\frac{x^{q+1} + x^{q^2+q} + x^{q^3+q^2}}{x^{q+1}}\right) \\
&= \mathrm{Tr}_{q^3/q}(1 + x^{q^2-1} + x^{q^2-q}) \\
&= 3 + \mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q-1}}\right) + \mathrm{Tr}_{q^3/q}(x^{q-1}).
\end{aligned}$$

□

Theorem 6.3. *Let*

$$\mathrm{Fix}(F) = \{x \in \mathbb{F}_{q^3} : F(x) = x\}$$

be the set of fixed points of $F(x) = x + (\mathrm{Tr}_{q^3/q}(x^{q+1}))/x$. *Then we have*

$$\mathrm{Fix}(F) = \{x \in \mathbb{F}_{q^3} : \mathrm{Tr}_{q^3/q}(x^{q+1}) = 0\} = \{0\} \cup \{x \in \mathbb{F}_{q^3}^* : \mathrm{Tr}_{q^3/q}(x^{-1}) = 0\}.$$

In particular, $|\mathrm{Fix}(F)| = q^2$.

Proof. By definition of F, it is straightforward, that

$$\mathrm{Fix}(F) = \{x \in \mathbb{F}_{q^3} : \mathrm{Tr}_{q^3/q}(x^{q+1}) = 0\}.$$

Lemma 6.2(a) completes the proof. □

Claim. For an integer $n \geq 0$, set

$$\begin{aligned} a_n &= \frac{4^n + (-2)^n - 2}{9}, \\ b_n &= \frac{(-2)^n - 1}{3}, \\ c_n &= a_{n+1} - a_n = \frac{4^n - (-2)^n}{3}, \\ d_n &= b_{n+1} - b_n = -(-2)^n. \end{aligned}$$

Then all these numbers are integers and they satisfy

$$b_n^2 + 2a_n - b_n = c_n \tag{6.2}$$

$$-(c_n b_n + d_n a_n) = c_n \tag{6.3}$$

$$d_n b_n = -c_n \tag{6.4}$$

Proof. Equations (6.2)–(6.4) can be easily checked by the following direct calculations:

$$\begin{aligned} b_n^2 + 2a_n - b_n &= \frac{((-2)^n - 1)^2}{9} + \frac{2 \cdot 4^n + 2 \cdot (-2)^n - 4}{9} - \frac{(-2)^n - 1}{3} \\ &= \frac{4^n - 2(-2)^n + 1 + 2 \cdot 4^n + 2(-2)^n - 4}{9} - \frac{(-2)^n - 1}{3} \\ &= \frac{4^n - 1 - ((-2)^n - 1)}{3} = \frac{4^n - (-2)^n}{3}; \\ -(c_n b_n + d_n a_n) &= -\left(\frac{4^n - (-2)^n}{3} \cdot \frac{(-2)^n - 1}{3} - (-2)^n \cdot \frac{4^n + (-2)^n - 2}{9}\right) \\ &= -\frac{(4^n - (-2)^n)((-2)^n - 1) - (-2)^n(4^n + (-2)^n - 2)}{9} \\ &= -\frac{4^n(-2)^n - 4^n - 4^n + (-2)^n - 4^n(-2)^n - 4^n + 2(-2)^n}{9} \\ &= -\frac{(-2)^n - 4^n}{3} = \frac{4^n - (-2)^n}{3}; \\ d_n b_n &= -(-2)^n \cdot \frac{(-2)^n - 1}{3} = -\frac{4^n - (-2)^n}{3}. \end{aligned}$$

Note that

$$b_n = \begin{cases} (2^n - 1)/3, & n \text{ even}, \\ -(2^n + 1)/3, & n \text{ odd}. \end{cases}$$

Recall that $3 = 2^2 - 1$ divides $2^n - 1$ if and only if n is even. Consequently, 3 divides $2^n + 1$ if and only if n is odd. These observations show, that b_n is an integer. Since $c_n = -d_n b_n$ and $2a_n = c_n - b_n^2 + b_n$, these numbers are also integers. □

Remark 6.1. By abuse of notation, we use the same symbol a for an integer number a and an element a mod p of a prime field $\mathbb{F}_p$. In the remainder of this chapter, we use $a/3$ to denote elements in $\mathbb{F}_p$ not only for $p \geq 5$ but also in $\mathbb{F}_3$. In the latter case, we assume that the integer a is divisible by 3 and the quotient $a/3$ is computed in the ring of integers.

For an integer $n \geq 0$, set

$$F^n(x) = (\underbrace{F \circ F \circ \cdots \circ F}_{n})(x)$$

to denote the nth iterate of F.

Theorem 6.4. *Let q be a power of an odd prime and*

$$F(x) = x + \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x}$$

on $\mathbb{F}_{q^3}$. Then for $n \geq 0$, we have

$$F^n(x) = a_n \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})^2}{\mathrm{N}_{q^3/q}(x)} - b_n \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} + x, \tag{6.5}$$

where $a_n = (4^n + (-2)^n - 2)/9$ and $b_n = ((-2)^n - 1)/3$.

Proof. For $n \geq 0$, we put

$$c_n = a_{n+1} - a_n = (4^n - (-2)^n)/3 \text{ and } d_n = b_{n+1} - b_n = -(-2)^n$$

and define

$$F_n(x) = a_n \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})^2}{\mathrm{N}_{q^3/q}(x)} - b_n \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} + x.$$

We aim to prove that $F^n(x) = F_n(x)$.

First, consider $x \in \mathbb{F}_q$. Then we have $\mathrm{Tr}_{q^3/q}(x^{q+1}) = 3x^2$ and $\mathrm{N}_{q^3/q}(x) = x^3$, implying

$$F(x) = x + \frac{3x^2}{x} = 4x,$$

and

$$\begin{aligned} F_n(x) &= a_n \frac{9x^4}{x^3} - b_n \frac{3x^2}{x} + x = (9a_n - 3b_n + 1)x \\ &= (4^n + (-2)^n - 2 - (-2)^n + 1 + 1)x = 4^n x = F^n(x). \end{aligned}$$

The statement is obviously true also for $x \in \mathrm{Fix}(F)$, since in this case we get $\mathrm{Tr}_{q^3/q}(x^{q+1}) = 0$. We apply induction on n to prove the identity for the remaining cases. Hence let $x \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and $\mathrm{Tr}_{q^3/q}(x^{q+1}) \neq 0$. The statement is true for $n = 0$ and $n = 1$. Our goal is to show that

$$F_{n+1}(x) = F^{n+1}(x) = F(F^n(x)) = F(F_n(x)) = F_n(x) + \frac{\mathrm{Tr}_{q^3/q}(F_n(x)^{q+1})}{F_n(x)},$$

or equivalently

$$(F_{n+1}(x) - F_n(x)) \cdot F_n(x) = \mathrm{Tr}_{q^3/q}(F_n(x)^{q+1}),$$

holds, if $F^n(x) = F_n(x)$. In the rest of the proof, we use the following abbreviations:

$$L(x) = (F_{n+1}(x) - F_n(x)) \cdot F_n(x)$$
$$R(x) = \mathrm{Tr}_{q^3/q}(F_n(x)^{q+1})$$

and $\mathrm{Tr} = \mathrm{Tr}_{q^3/q}$, $\mathrm{N} = \mathrm{N}_{q^3/q}$, $u(x) = \mathrm{Tr}_{q^3/q}(x^{q+1})$. Our goal is to show $L(x) = R(x)$ for all $x \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ with $u(x) \neq 0$. First, observe that $R(x)$ can be written as follows:

$$\begin{aligned}
R(x) &= \mathrm{Tr}\left[\left(a_n\frac{u(x)^2}{\mathrm{N}(x)} - b_n\frac{u(x)}{x} + x\right)^q \cdot \left(a_n\frac{u(x)^2}{\mathrm{N}(x)} - b_n\frac{u(x)}{x} + x\right)\right] \\
&= \mathrm{Tr}\left[\left(a_n\frac{u(x)^2}{\mathrm{N}(x)} - b_n\frac{u(x)}{x^q} + x^q\right) \cdot \left(a_n\frac{u(x)^2}{\mathrm{N}(x)} - b_n\frac{u(x)}{x} + x\right)\right] \\
&= \mathrm{Tr}\left[a_n^2\frac{u(x)^4}{\mathrm{N}(x)^2} + b_n^2\frac{u(x)^2}{x^{q+1}} - a_nb_n\frac{u(x)^3}{\mathrm{N}(x)}\left(\frac{1}{x} + \frac{1}{x^q}\right) + a_n\frac{u(x)^2}{\mathrm{N}(x)}(x + x^q)\right. \\
&\qquad \left. -b_nu(x)\left(x^{q-1} + \frac{1}{x^{q-1}}\right) + x^{q+1}\right] \\
&= 3a_n^2\frac{u(x)^4}{\mathrm{N}(x)^2} + b_n^2u(x)^2\,\mathrm{Tr}\left(\frac{1}{x^{q+1}}\right) - 2a_nb_n\frac{u(x)^3}{\mathrm{N}(x)}\,\mathrm{Tr}\left(\frac{1}{x}\right) + 2a_n\frac{u(x)^2}{\mathrm{N}(x)}\,\mathrm{Tr}(x) \\
&\quad - b_nu(x)\left(\mathrm{Tr}(x^{q-1}) + \mathrm{Tr}\left(\frac{1}{x^{q-1}}\right)\right) + u(x).
\end{aligned}$$

Applying Lemma 6.2(a), (b) and (c) to the last expression, we get

$$\begin{aligned}
R(x) &= 3a_n^2\frac{u(x)^4}{\mathrm{N}(x)^2} + b_n^2u(x)^2\frac{\mathrm{Tr}(x)}{\mathrm{N}(x)} - 2a_nb_n\frac{u(x)^3}{\mathrm{N}(x)} \cdot \frac{u(x)}{\mathrm{N}(x)} + 2a_n\frac{u(x)^2}{\mathrm{N}(x)}\,\mathrm{Tr}(x) \\
&\quad - b_nu(x)\left(u(x)\frac{\mathrm{Tr}(x)}{\mathrm{N}(x)} - 3\right) + u(x). \\
&= (3a_n^2 - 2a_nb_n)\frac{u(x)^4}{\mathrm{N}(x)^2} + (b_n^2 + 2a_n - b_n)\frac{u(x)^2}{\mathrm{N}(x)}\,\mathrm{Tr}(x) + (3b_n + 1)u(x),
\end{aligned}$$

and hence

$$\frac{R(x)}{u(x)} = (3a_n^2 - 2a_nb_n)\frac{u(x)^3}{\mathrm{N}(x)^2} + (b_n^2 + 2a_n - b_n)\frac{u(x)}{\mathrm{N}(x)}\,\mathrm{Tr}(x) + 3b_n + 1.$$

We compute now $L(x)/u(x)$:

$$\begin{aligned}\frac{L(x)}{u(x)} &= \left(c_n\frac{u(x)}{\mathrm{N}(x)} - d_n\frac{1}{x}\right)\left(a_n\frac{u(x)^2}{\mathrm{N}(x)} - b_n\frac{u(x)}{x} + x\right)\\ &= c_n a_n\frac{u(x)^3}{\mathrm{N}(x)^2} - (c_n b_n + d_n a_n)\frac{u(x)^2}{\mathrm{N}(x)x} + d_n b_n\frac{u(x)}{x^2} + c_n\frac{u(x)x}{\mathrm{N}(x)} - d_n.\end{aligned}$$

Because

$$3a_n^2 - 2a_n b_n = a_n(3a_n - 2b_n) = a_n\frac{4^n + (-2)^n - 2 - 2(-2)^n + 2}{3} = a_n c_n$$

and

$$3b_n + 1 = (-2)^n = -d_n,$$

to prove $R(x)/u(x) = L(x)/u(x)$ it is enough to show that

$$c_n\frac{u(x)x}{\mathrm{N}(x)} - (b_n^2 + 2a_n - b_n)\frac{u(x)}{\mathrm{N}(x)}\,\mathrm{Tr}(x) - (c_n b_n + d_n a_n)\frac{u(x)^2}{\mathrm{N}(x)x} + d_n b_n\frac{u(x)}{x^2} = 0$$

Or equivalently, by multiplying with $\mathrm{N}(x)x^2/u(x) \neq 0$,

$$c_n x^3 - (b_n^2 + 2a_n - b_n)\,\mathrm{Tr}(x)x^2 - (c_n b_n + d_n a_n)u(x)x + d_n b_n\,\mathrm{N}(x) = 0. \tag{6.6}$$

Using (6.2)–(6.4), we reduce (6.6) to

$$c_n x^3 - c_n\,\mathrm{Tr}(x)x^2 + c_n\,\mathrm{Tr}(x^{q+1})x - c_n\,\mathrm{N}(x) = 0,$$

for $n \geq 1$, also $c_n \geq 1$ and we can further reduce to

$$x^3 - \mathrm{Tr}(x)x + \mathrm{Tr}(x^{q+1})x - \mathrm{N}(x) = 0,$$

which is satisfied for any $x \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ by Lemma 6.1. □

Remark 6.2. The iterate $F^n(x)$ in (6.5) can be written in polynomial form

$$F^n(X) = a_n\,\mathrm{Tr}_{q^3/q}(X^{q^2+q-1}) + (2a_n - b_n)\,\mathrm{Tr}_{q^3/q}(X) - b_n X^{q^2+q-1} + (b_n + 1)X,$$

using the following identities in $\mathbb{F}_{q^3}$:

$$\begin{aligned}\frac{\mathrm{Tr}_{q^3/q}(x^{q+1})^2}{\mathrm{N}_{q^3/q}(x)} &= \mathrm{Tr}_{q^3/q}(x^{q+1})\,\mathrm{Tr}_{q^3/q}\left(\frac{1}{x}\right) = \mathrm{Tr}_{q^3/q}\left(\frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x}\right)\\ &= \mathrm{Tr}_{q^3/q}\left(\frac{x^{q+1} + x^{q^2+q} + x^{q^2+1}}{x}\right)\\ &= \mathrm{Tr}_{q^3/q}(x^q) + \mathrm{Tr}_{q^3/q}(x^{q^2+q-1}) + \mathrm{Tr}_{q^3/q}(x^{q^2})\\ &= \mathrm{Tr}_{q^3/q}(x^{q^2+q-1}) + 2\,\mathrm{Tr}_{q^3/q}(x)\end{aligned}$$

and

$$F(x) = \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} + x = x^{q^2+q-1} + \mathrm{Tr}_{q^3/q}(x).$$

Theorem 6.5. *Let $q = p^s$ where $p \geq 5$ and $m = \mathrm{ord}_p(4)$. Then the permutation F on $\mathbb{F}_{q^3}$ defined by $F(x) = x + (\mathrm{Tr}_{q^3/q}(x^{q+1}))/x$ satisfies the following properties:*

(a) *If $\mathrm{ord}_p(-2) = \mathrm{ord}_p(4)$, then the cycle structure of F is*

$$\mathrm{CS}(F) = 1^{q^2} m^{(q^3-q^2)/m}.$$

(b) *If $\mathrm{ord}_p(-2) = 2 \cdot \mathrm{ord}_p(4)$, then the cycle structure of F is*

$$\mathrm{CS}(F) = 1^{q^2} m^{(q-1)/m} (2m)^{(q^3-q^2-q+1)/(2m)}.$$

The cycles of length m partition the set of nonzero elements of the subfield $\mathbb{F}_q$, i. e.

$$\mathrm{CS}_{\mathbb{F}_q}(F) = 1^1 m^{(q-1)/m}.$$

(c) *The permutation F has order $\mathrm{ord}_p(-2)$ in the symmetric group of permutations on $\mathbb{F}_{q^3}$.*

Proof. Clearly, (c) is a direct consequence of (a) and (b). Let $y \in \mathbb{F}_{q^3}$ and $y \notin \mathrm{Fix}(F)$, i. e. $u(y) \neq 0$. Let $t \geq 2$ be the minimal integer with $F^t(y) = y$, i. e. $t = \ell(F, y)$, the length of the cycle containing y in the cycle decomposition of F. Recall the abbreviations $\mathrm{Tr} = \mathrm{Tr}_{q^3/q}$, $\mathrm{N} = \mathrm{N}_{q^3/q}$, $u(y) = \mathrm{Tr}_{q^3/q}(y^{q+1})$. Then

$$F^t(y) - y = a_t \frac{u(y)^2}{\mathrm{N}(y)} - b_t \frac{u(y)}{y} = 0,$$

implying

$$a_t \cdot u(y) = b_t \cdot \frac{\mathrm{N}(y)}{y} = b_t \cdot y^{q^2+q}. \tag{6.7}$$

Then necessarily it holds

$$\mathrm{Tr}(a_t \cdot u(y)) = \mathrm{Tr}(b_t \cdot y^{q^2+q}),$$

or equivalently

$$3 \cdot a_t \cdot u(y) = b_t \cdot u(y),$$

and hence

$$\frac{4^t + (-2)^t - 2}{3} = 3 \cdot a_t = b_t = \frac{(-2)^t - 1}{3},$$

which is equivalent to $4^t = 1$. This shows that t must be divisible by $\mathrm{ord}_p(4)$, and in particular

$$t \geq \mathrm{ord}_p(4). \tag{6.8}$$

Let $r = \mathrm{ord}_p(-2)$. Then $a_r = b_r = 0$ and, therefore

$$t \leq \mathrm{ord}_p(-2). \tag{6.9}$$

Hence if $\mathrm{ord}_p(4) = \mathrm{ord}_p(-2)$, the statement in (a) follows from (6.8) and (6.9). Suppose now $r = 2 \cdot \mathrm{ord}_p(4)$, then $t \in \{m, 2m\}$ and we have to determine for which y, the integer $t = m$. For $t = m$, the equation (6.7) reduces to

$$u(y) = 3 \cdot y^{q^2+q},$$

since in this case $a_t = -2/9$ and $b_t = -2/3$. In particular, y^{q^2+q} then belongs to the subfield $\mathbb{F}_q$, since $u(y)$ does. This yields

$$y^{q^2+1} = (y^{q^2+q})^q = y^{q^2+q},$$

which is equivalent to $y \in \mathbb{F}_q$. This proves (b). □

Theorem 6.6. *Let $q = p^s$, where $p \geq 5$. The inverse map of*

$$F(x) = x + \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} = x^{q^2+q-1} + \mathrm{Tr}_{q^3/q}(x)$$

on $\mathbb{F}_{q^3}$ is $F^k(x)$, where $k = \mathrm{ord}_p(-2) - 1$. More precisely, it holds

$$\begin{aligned} F^{-1}(x) &= -\frac{1}{4} \cdot \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})^2}{\mathrm{N}_{q^3/q}(x)} + \frac{1}{2} \cdot \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} + x \\ &= -\frac{1}{4} \cdot \mathrm{Tr}_{q^3/q}(x^{q^2+q-1}) + \frac{1}{2} \cdot x^{q^2+q-1} + \frac{1}{2}x. \end{aligned}$$

Proof. Theorem 6.5(c) yields $F^{-1}(x) = F^k(x)$, where $k = \mathrm{ord}_p(-2) - 1$. It remains to note that $a_k = -1/4$ and $b_k = -1/2$. The polynomial form is obtained using the identities from Remark 6.2. □

In [8] it is shown, that the inverse map of a permutation $x + \gamma \,\mathrm{Tr}_{q^n/q}(x^k)$ has the form $x + \gamma g(x)$, with $g : \mathbb{F}_{q^n} \to \mathbb{F}_q$. In general, an explicit description of g is a difficult problem. The inverse of the permutation $F_{16}(x) = x + \mathrm{Tr}_{q^3/q}(x^{(q^2+1)/2})$ can be determined using Theorem 6.6 and he fact that $F(x) = F_{16}(x^{q^2+q-1})$:

Corollary 6.7. *Let $q = p^s$, where $p \geq 5$. The inverse map of the permutation $F_{16}(x) = x + \mathrm{Tr}_{q^3/q}(x^{(q^2+1)/2}))$ on $\mathbb{F}_{q^3}$ is given by*

$$F_{16}^{-1}(x) = \left(-\frac{1}{4} \cdot \mathrm{Tr}_{q^3/q}(x^{q^2+q-1}) + \frac{1}{2} \cdot x^{q^2+q-1} + \frac{1}{2}x\right)^{q^2+q-1}.$$

The next theorem presents results on $F(x)$ in the case $p = 3$.

Theorem 6.8. *Let $q = 3^s$, with $s \geq 1$, and F be the permutation on $\mathbb{F}_{q^3}$ given by $F(x) = x + (\mathrm{Tr}_{q^3/q}(x^{q+1}))/x$. Then F has the following properties:*

(a) *The order of F is* 3.

(b) *The cycle structure of F is*

$$\mathrm{CS}(F) = 1^{q^2} 3^{(q^3-q^2)/3}.$$

(c) *The inverse map of F is given by*

$$\begin{aligned} F^{-1}(x) &= 2 \cdot \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})^2}{\mathrm{N}_{q^3/q}(x)} - \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} + x \\ &= -\mathrm{Tr}_{q^3/q}(x^{q^2+q-1}) - x^{q^2+q-1} - x. \end{aligned}$$

Proof. Recall the abbreviations $\mathrm{Tr} = \mathrm{Tr}_{q^3/q}$, $\mathrm{N} = \mathrm{N}_{q^3/q}$, $u(y) = \mathrm{Tr}_{q^3/q}(y^{q+1})$. Let id_{q^3} be the identity function on $\mathbb{F}_{q^3}$. Using formula (6.5) and computing $a_2 = 2$, $b_2 = 1$, $a_3 = 0$, $b_3 = 0$, it is easy to see that $F^2 \neq \mathrm{id}_{q^3}$, whereas $F^3 = \mathrm{id}_{q^3}$, proving (a). To verify (b), note that by (a) the cycles of F have length at most 3. To show that there are no cycles of length 2, we prove that if $F^3(y) = y$ for $y \in \mathbb{F}_{q^3}$, then $y \in \mathrm{Fix}(F)$. Indeed, if

$$F^2(y) = 2 \cdot \frac{u(y)^2}{\mathrm{N}(y)} - \frac{u(y)}{y} + y = y,$$

it follows that

$$2 \cdot u(y) = y^{q^2+q},$$

and then

$$0 = \mathrm{Tr}(2 \cdot u(y)) = \mathrm{Tr}(x^{q^2+q}) = u(y),$$

i. e. $y \in \mathrm{Fix}(F)$. Theorem 6.3 completes the proof. The statement in (c) follows from (a), which implies that $F^{-1}(x) = F^2(x)$. □

Bibliography

[1] Shair Ahmad. Cycle Structure of Automorphisms of Finite Cyclic Groups. In: *J. Comb. Theory* 6.4 (1969), pp. 370–374.

[2] Leonard Carlitz. Permutations in a finite field. In: *Proc. Amer. Math. Soc.* 4.4 (1953), p. 538.

[3] Leonard Carlitz. Permutations in finite fields. In: *Acta Sci. Math. Szeged* 24 (1963), pp. 196–203.

[4] Ayça Çeşmelioğlu, Wilfried Meidl, and Alev Topuzoğlu. On the cycle structure of permutation polynomials. In: *Finite Fields Appl.* 14.3 (2008), pp. 593–614.

[5] Pascale Charpin and Gohar M. Kyureghyan. On a Class of Permutation Polynomials over $\mathbb{F}_{2^n}$. In: *Sequences and Their Applications - SETA 2008*. Ed. by Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof. Lect. Notes Comput. Sci. 5203. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 368–376.

[6] Wun-Seng Chou. The Period Lengths of Inversive Pseudorandom Vector Generations. In: *Finite Fields Appl.* 1.1 (1995), pp. 126–132.

[7] Ayhan Coşgun, Ferruh Özbudak, and Zülfükar Saygı. Further results on rational points of the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over $\mathbb{F}_{q^m}$. In: *Des. Codes Cryptogr.* 79.3 (2016), pp. 423–441.

[8] Mikayel G. Evoyan, Gohar M. Kyureghyan, and Melsik K. Kyuregyan. On k-Switching of Mappings on Finite Fields. In: *Math. Probl. Comput. Sci.* 39 (2013), pp. 5–12.

[9] Daniel Gerike and Gohar M. Kyureghyan. Permutations on Finite Fields with invariant Cycle Structure on Lines. In: *Des. Codes Cryptogr.* (2020). DOI: 10.1007/s10623-020-00721-2.

[10] Daniel Gerike and Gohar M. Kyureghyan. Results on permutation polynomials of shape $x^t+\gamma \operatorname{Tr}_{q^n/q}(x^d)$. In: *Combinatorics and Finite Fields*. Ed. by Kai-Uwe Schmidt and Arne Winterhof. Radon Ser. Comput. Appl. Math. 23. Berlin, Boston: De Gruyter, 2019, pp. 67–78.

[11] Gohar Kyureghyan and Michael Zieve. Permutation polynomials of the form $X + \gamma \operatorname{Tr}(X^k)$. In: *Contemporary Developments in Finite Fields and Applications*. Ed. by Anne Canteaut, Gove Effinger, Sophie Huczynska, Daniel Panario, and Leo Storme. Singapore: World Scientific, 2016, pp. 178–194.

[12] Gohar M. Kyureghyan. Constructing permutations of finite fields via linear translators". In: *J. Comb. Theory*. Ser. A 118.3 (2011), pp. 105–1061.

[13] Kangquan Li, Longjiang Qu, Xi Chen, and Chao Li. Permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$ and permutation trinomials over finite fields with even characteristic. In: *Cryptogr. Commun.* 10.3 (2018), pp. 531–554.

[14] Rudolf Lidl and Gary L. Mullen. Cycle Structure of Dickson Permutation Polynomials. In: *Math. J. Okayama Univ.* 33 (1991), pp. 1–11.

[15] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. 2nd ed. Encyclopedia Math. Appl. 20. Cambridge: Cambridge University Press, 1996.

[16] Jingxue Ma and Gennian Ge. A note on permutation polynomials over finite fields. In: *Finite Fields Appl.* 48 (2017), pp. 261–270.

[17] Rodrigo Martins, Daniel Panario, and Claudio Qureshi. A survey on iterations of mappings over finite fields. In: *Combinatorics and Finite Fields*. Ed. by Kai-Uwe Schmidt and Arne Winterhof. Radon Ser. Comput. Appl. Math. 23. Berlin, Boston: De Gruyter, 2019, pp. 135–172.

[18] Gary L. Mullen and Theresa P. Vaughan. Cycles of Linear Permutations Over a Finite Field. In: *Linear Algebra Appl.* 108 (1988), pp. 63–82.

[19] Ferruh Özbudak and Zülfükar Saygı. Rational points of the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over $\mathbb{F}_{q^m}$. In: *Applied Algebra and Number Theory*. Ed. by Gerhard Larcher, Friedrich Pillichshammer, Arne Winterhof, and Chaoping Xing. Cambridge: Cambridge University Press, 2014, pp. 297–306.

[20] Daniel Panario and Lucas Reis. The functional graph of linear maps over finite fields and applications. In: *Des. Codes Cryptogr.* 87.2 (2019), pp. 437–453.

[21] Enes Pasalic and Pascale Charpin. Some results concerning cryptographically significant mappings over GF(2^n). In: *Des. Codes Cryptogr.* 57.3 (2010), pp. 257–269.

[22] Ivelisse M. Rubio, Gary L. Mullen, Carlos Corrada, and Francis N. Castro. Dickson permutation polynomials that decompose in cycles of the same length. In: *Finite Fields and Applications*. Ed. by Gary L. Mullen, Daniel Panario, and Igor E. Shparlinski. Contemp. Math. 461. Providence, RI: Amer. Math. Soc., 2008, pp. 229–239.

[23] Amin Sakzad, Mohammad-Reza Sadeghi, and Daniel Panario. Cycle structure of permutation functions over finite fields and their applications. In: *Adv. Math. Commun.* 6.3 (2012), pp. 347–361.