UNIVERSITÀ DEGLI STUDI DI TRENTO
Department of Mathematics

Ph.D. in Mathematics
Ciclo XXV

Some Problems Concerning Polynomials over Finite Fields, or Algebraic Divertissements

Marco Pizzato

Supervisor: Prof. Sandro Mattarei

Head of PhD School: Prof. Francesco Serra Cassano

UNIVERSITÀ DEGLI STUDI DI TRENTO
Department of Mathematics

Ph.D. in Mathematics
Ciclo XXV

Some Problems Concerning Polynomials over Finite Fields, or Algebraic Divertissements

Candidate: Marco Pizzato

Supervisor: Sandro Mattarei

Head of PhD School: Francesco Serra Cassano

Mathematics, rightly viewed, possesses not only truth, but supreme beauty —a beauty cold and austere, like that of sculpture, without appeal to any part of our weaker nature, without the gorgeous trappings of painting or music, yet sublimely pure, and capable of a stern perfection such as only the greatest art can show.

Bertrand Russell, Mysticism and Logic: And Other Essays

Prefazione

Perché fare matematica al giorno d'oggi? Perché fare poesia, letteratura, arte? La domanda è, in fondo, la stessa. Vale ancora la pena di ricercare la bellezza in un mondo che sempre più sembra esserle indifferente e voltarle le spalle? Perché non possiamo negare che la spinta produttivistica e tecnologica che pervade i giorni nostri viene esaltata ed apprezzata con una certa aria di superiorità nei confronti di un atteggiamento più rilassato e romantico nei confronti dell'esistenza.

Sarà forse pigrizia, sarà forse una forma di presuntuoso distacco dalla realtà, ma sono convinto che valga ancora la pena di riaffermare a piena voce l'importanza di questi giochi del pensiero, di questa musica per l'anima, di questo sedersi su di un prato lungo il corso del fiume della storia e lasciarsi trasportare verso luoghi di bellezza assoluta.

Impossibile non citare le deliziose parole di Newton, quando raccontava la sua esperienza nella scienza: "I do not know what I may appear to the world, but to myself I seem to have been only like a boy playing on the sea-shore, and diverting myself in now and then finding a smoother pebble or a prettier shell than ordinary, whilst the great ocean of truth lay all undiscovered before me." [1] Ed è questo che, a parer mio, dovrebbe essere l'atteggiamento di una persona che vuole, ingenuamente e senz'altra meta che il divertimento, provare a scoprire qualche nuovo teorema, qualche nesso nascosto in qualche piega del tessuto che forma l'abito della matematica. Un bambino che, con i suoi primi giocattoli, scopre l'emozione creatrice della fantasia.

A malincuore non è però possibile negare che, in fondo, anche nella scienza si è purtroppo perso questo spirito romantico. Impossibile poter fare matematica al giorno d'oggi senza essere specializzati in una qualche branca, impossibile essere buoni allievi di geometria, algebra ed analisi. Il dilettantismo, massima forma di vita, non è più possibile in questa scienza. Viene da augurarsi che non perda completamente la sua anima diventando

[1] Memoirs of the Life, Writings, and Discoveries of Sir Isaac Newton (1855) by Sir David Brewster (Volume II. Ch. 27).

un'ulteriore strumento al servizio di un volgare produttivismo, terribile orrore.

Sarò solo un patetico sognatore, ma lasciatemi la forza di sperare che nel mondo moderno non venga mai a mancare la forza dei dilettanti, dei testardi, dei folli, degli illusi, degli sconfitti, e che la parte più infantile e giocosa della matematica e delle altre scienze, quella parte il cui nome non è altro che bellezza, possa ancora cantare la sua musica e portare un po' di lievità nel mondo.

Ancora una volta lanciamo quindi il nostro grido disperato, affinché qualcuno, anche fosse solo una persona su un milione, possa ascoltarlo: non prendiamo la vita troppo seriamente! Non prendiamo la matematica seriamente, non consideriamola più di quello che dovrebbe essere. Tanti, ormai spinti dall'inerzia di questa società hanno finito per dimenticare che la scienza non è altro che un modo, forse più divertente di altri, forse un poco più adulto, di giocare. Rimaniamo dilettanti in tutto quello che facciamo nella vita, evitiamo la complessità delle specializzazioni, che tutto assorbono, e manteniamo la mente aperta, cercando di espandere la nostra conoscenza in tutte le direzioni.

Preface

Why study Mathematics nowadays? Why do poetry, literature, art? All these questions are, deep inside, the same. Is it still worth looking for beauty in a world that, every day, every hour, every minute, is more and more indifferent to it, that turns its back on it? In fact, we cannot deny that the productivist and technological drive pervading our days is appreciated and celebrated with a sort of superiority in confront of a more relaxed, more romantic attitude toward life.

It is probably laziness, maybe a sort of presumptuous aloofness from reality, but I am convinced that it is still worth reaffirming the importance of these mind games, of this soul's music, of this sitting on a meadow along the stream of history's river and let be carried unto places of magnificent beauty.

It is impossible not to quote the delightful words of Newton, when he was recalling his science experience: "I do not know what I may appear to the world, but to myself I seem to have been only like a boy playing on the sea-shore, and diverting myself in now and then finding a smoother pebble or a prettier shell than ordinary, whilst the great ocean of truth lay all undiscovered before me." [2]

And this, in my opinion, should be the attitude of a person wanting, naively and without other aim but enjoyment, to try to find some new theorem, some connection hidden in some fold of the tissue forming mathematic's dress. A child that, with his first toys, discovers fantasy's creative emotion.

Is it impossible to deny, reluctantly, that, deep down, also science lost this romantic spirit. It is impossible to do mathematics nowadays without being specialized in some branch, being at the same time good students of geometry, algebra and analysis. Amateurism, highest form of life, is no more possible in this science. It is desirable that mathematics will not lose completely its soul and become another tool at the service of a vulgar pro-

[2] Memoirs of the Life, Writings, and Discoveries of Sir Isaac Newton (1855) by Sir David Brewster (Volume II. Ch. 27).

ductivism, terrible horror.

I am probably just a pathetic dreamer, but allow me to hope that in our modern world the power of amateurs, of stubborns, of fools, of deceived, of defeated could not go missing. Let me dream that mathematics' and other sciences' more infantile, more playful part, the one whose name is no other than beauty, can still sing its song and carry a bit of levity in this world.

Once again, let us throw our desperate cry, so that someone, even if one in a million, could listen to it: do not take life too seriously! Do not take mathematics too seriously, do not consider it more than it should be. Many, carried by this society's inertia, forget that science is just another, maybe funnier, maybe more adult, way to play. Let us stay amateurs in everything we do in our lives, let us avoid specializations' complexities and keep our mind open, trying to expand our knowledge in every possible direction.

Contents

Introduction

This thesis consists of four chapters. The first chapter, *Preliminaries*, is divided in two sections. In the first one, we introduce an action of the projective linear group of dimension two over (irreducible) polynomials over finite fields. We present also some properties of this action.

The second section introduces the concept of self-reciprocal polynomials. We state Carlitz's theorem on the number of these polynomials (over a finite field), appeared in [Car67]. We also prove a slight generalization of this theorem, which we will need in the second and third chapter of the thesis.

The second chapter, *Möbius Group and Polynomials*, is devoted to the study of the action, described in the first chapter, on polynomials over finite fields. In [MR10], the two authors studied the action of $\mathrm{PGL}_2(\mathbb{F}_2)$ over irreducible polynomials in $\mathbb{F}_2[x]$. We generalize their results considering also odd characteristics and studying also other groups. We consider $\mathcal{S}_3, \mathcal{D}_r$(for r prime), $\mathcal{S}_4, \mathcal{A}_4$ and $\mathcal{A}_5$ (each of which has its own section), seen as groups of matrices, and study their action over irreducible polynomials. More in detail, if an element g of the group is represented by the matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $f \in \mathbb{F}_q[x]$ of degree n is a polynomial, we define the action in the following way:

$$f \circ A = (cx + d)^n f\left(\frac{ax + b}{cx + d}\right).$$

The rest of the chapter is then devoted to the study of the orbits and stabilizers of these actions, of which we are able to compute the orders and describe their elements. In the last section of the chapter we present some general results, appeared in [ST12].

In the third chapter, *Generalizing self-reciprocal polynomials*, we present a joint work with Sandro Mattarei. We study *self-reciprocal* polynomials, i.e. polynomials satisfying the functional equation $f(x) = (-x)^n f(1/x)$. Starting from [Ahm11], we try to generalize the results presented in that work. The author considered transformations of the form $f^*(x) = h^n f(g(x)/h(x))$, where n is the degree of the irreducible polynomial f and g, h are coprime

polynomials with $\max\{\deg g, \deg h\} = 2$, and studied the number of f such that f^* is still irreducible. Since this number, except for some particular cases, is the same of the number of self-reciprocal irreducible polynomial, we try to view these concepts in a more general context. Using the action of $\mathrm{PGL}_2(\mathbb{F}_q) \times \mathrm{PGL}_2(\mathbb{F}_q)$ on the quadratic function g/h, we see that we need to consider only representatives of orbits instead of all the possible quadratic functions in order to recover Ahmadi's results. Using this ideas and some algebraic geometry tools, we manage to obtain some results when $\max\{\deg g, \deg h\} = 3$. Using Hurwitz's ramification formula, we are able to count the number of irreducible f^*, transformed by a cubic map. When possible (i.e. when the map associated to g and h has less than four ramification points) we give exact results, otherwise some bound, using Hasse-Weil's one, on the number of points of hyperelliptic curves over finite fields. Essentially, the main results could be summarized in the following way:

The number of f such that f^* is still irreducible is of the order of $q^n/2n$ in the quadratic case (Ahmadi) and of the order of $q^n/3n$ in the cubic case.

In the fourth chapter, *PN functions*, we introduce and give a generalization of this kind of functions. A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is called PN if the *derived* function $f(x+a)-f(x)$ is a permutation polynomial of $\mathbb{F}_q$, for every possible non-zero direction a. We concentrate primarily on PN monomials, i.e. functions of the form x^n. It is known, ([RS89], [Joh87], [Hir89], [Glu90], [Cou06] and [CL12]) that over $\mathbb{F}_p, \mathbb{F}_{p^2}$ and $\mathbb{F}_{p^4}$ the only PN monomial is essentially the trivial one, namely x^2, whose *derivative* is linear, hence bijective. Another class of PN monomials is given by x^{p^k+1}, where k must satisfy a condition depending on the base field. The main conjecture is now the following:

Conjecture. Suppose $f = x^n$ is a PN monomial over $K = \mathbb{F}_q$ with $\mathrm{char}(K) \geq 5$ and suppose $n \leq q-1$. Then we have $n = p^i + p^j$, for some integers i, j.

A recent result [Zie13], due to Michael Zieve, shows that, once we fix n, the conjecture holds for large q.

In the last section of the chapter we introduce the concept of k-PN functions, where we require the k-th *derivative* of a function f in every possible direction to be a permutation polynomials. We prove some results about these functions over $\mathbb{F}_p, \mathbb{F}_{p^2}$ and $\mathbb{F}_{p^4}$. Over the prime fields we see that we have only the trivial monomial, namely x^{k+1}, which k-th *derivative* is linear. We prove some general results for k-PN monomial over $\mathbb{F}_{p^2}$, and give a complete classification when $k \in \{2, 3\}$. In the first case, we note that the results depend on the value of p modulo 3. If $p \equiv -1 \pmod 3$, we show that x^3 and x^{3p} are the only 2-PN monomials. If $p \equiv 1 \pmod 3$, we also have x^{2+p} and x^{1+2p}. In the 3-PN case, we see that we have only the

monomials x^4 and x^{4p}. For the same values of k, we obtain results for k-PN monomials over $\mathbb{F}_{p^4}$. In this case we do not have a condition depending on congruences modulo 3, and we see that the 2-PN monomials are x^n, with $n \in \{3, 3p, 3p^2, 3p^3, 2+p^2, 2p+p^3, 1+2p^2, p+2p^3\}$, while the 3-PN monomials are x^n, with $n \in \{4, 4p, 4p^2, 4p^3\}$. We conclude the chapter with some result concerning k-PN monomials over $\mathbb{F}_{p^3}$.

Chapter 1

Preliminaries

In this chapter we present some preliminary results. In the first section we give the definition of the action that we are going to study in the second chapter. It can be found for example in [ST12] or in [Gar11].

In the second section we will introduce self-reciprocal polynomials. The first important result can be found in [Car67], where the author counts the number of monic self-reciprocal irreducible polynomials of a fixed degree. A more elementary proof of this fact is in [Mey90].

1.1 The action of $\mathrm{PGL}_2(\mathbb{F}_q)$

We start considering the group $\mathrm{GL}_2(\mathbb{F}_q)$ of invertible square matrices of rank 2 over the finite field $\mathbb{F}_q$. We want to introduce an action of this set over (irreducible) polynomials over that field. We define the set

$$\mathcal{M} = \{P \in \mathbb{F}_q[x] : P \text{ has no roots in } \mathbb{F}_q\}.$$

Definition 1.1.1. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$ and $f \in \mathbb{F}_q[x]$ of degree n. We define

$$f \circ A = (cx+d)^n f\left(\frac{ax+b}{cx+d}\right).$$

The effect of this action is just to apply a precomposition to our polynomial. We will now present some known results, in order to understand better the consequences of this action.

Lemma 1.1.2 ([ST12])**.** *Let $A, B \in \mathrm{GL}_2(\mathbb{F}_q)$, E be the identity matrix and $f, g \in \mathcal{M}$. Then we have the following:*

1. *$f \circ A \in \mathcal{M}$ and $\deg(f \circ A) = \deg f$.*

2. $f \circ E = f$.

3. $f \circ (BA) = (f \circ B) \circ A$.

4. $(fg) \circ A = (f \circ A)(g \circ A)$.

5. *f is irreducible if and only if $f \circ A$ is irreducible.*

Proof. 1. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$ and $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathcal{M}$, where $a_n \neq 0$. Clearly $(f \circ A)(x)$ is a polynomial, and

$$\begin{aligned}(f \circ A)(x) & \\ &= a_n(ax+b)^n + a_{n-1}(ax+b)^{n-1}(cx+d) + \cdots + a_0(cx+d)^n \\ &= (a_n a^n + a_{n-1}a^{n-1}c + \cdots + a_1 a c^{n-1} + a_0 c^n)x^n + \ldots .\end{aligned}$$

If $c \neq 0$, the coefficient of x^n is $c^n(a_n(a/c)^n + a_{n-1}(a/c)^{n-1} + \cdots + a_0) = c^n f(a/c) \neq 0$, since f has no roots in $\mathbb{F}_q$. If $c = 0$, then $a \neq 0$ and the coefficient of x^n is $a_n a^n \neq 0$. We have thus shown that $\deg(f \circ A) = \deg f$, and it remains to to show that $f \circ A$ has no roots in $\mathbb{F}_q$.
Let $\gamma \in \mathbb{F}_q$. If $c\gamma + d \neq 0$, then $(f \circ A)(\gamma) = (c\gamma + d)^n f((a\gamma + b)/(c\gamma + d)) \neq 0$, since $f((a\gamma + b)/(c\gamma + d)) \neq 0$. If $c\gamma + d = 0$, then $(f \circ A)(\gamma) = a_n(a\gamma + b)^n$ by the previous equation. Assume that $a\gamma + b = 0$. This gives a non-trivial linear combination

$$\gamma(a, c) + (b, d) = (0, 0)$$

over $\mathbb{F}_q$, a contradiction since the columns of the matrix A are linearly independent. So we have also in this case that $(f \circ A)(\gamma) \neq 0$. This finishes the proof of 1.

5. Let $f \in \mathcal{M}$ and $\deg f = n$,

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} t & u \\ v & w \end{pmatrix}.$$

Then

$$(f \circ B)(x) = (vx + w)^n f\left(\frac{tx + u}{vx + w}\right),$$

hence

$$\begin{aligned}((f\circ B)\circ A)(x) &= (cx+d)^n\left(v\left(\frac{ax+b}{cx+d}\right)+w\right)^n f\left(\frac{t\frac{ax+b}{cx+d}+u}{v\frac{ax+b}{cx+d}+w}\right)\\ &= ((av+cw)x+(bv+dw))^n f\left(\frac{(at+cu)x+bt+du}{(av+cw)x+bv+dw}\right)\\ &= (f\circ BA)(x).\end{aligned}$$

Parts 2 and 4 are trivial, and part 5 follows from 4. □

Lemma 1.1.2 shows that we have a (right) action of $\mathrm{GL}_2(\mathbb{F}_q)$ on $\mathcal{M}$ and on

$$\mathcal{M}_n = \{P \in \mathbb{F}_q[x] : P \text{ irreducible, } \deg P = n\}.$$

We note that the actual action studied by the two authors in [ST12], is the *dual* of the one we have considered. In fact they define

$$A \circ f = (bx+d)^n f\left(\frac{ax+c}{bx+d}\right).$$

We introduce now two equivalence relations on $\mathrm{GL}_2(\mathbb{F}_q)$ and on $\mathcal{M}$, namely

$$A \sim B \Leftrightarrow A = \lambda B \text{ for some } \lambda \in \mathbb{F}_q^*,$$

and

$$f \sim g \Leftrightarrow f = \lambda g \text{ for some } \lambda \in \mathbb{F}_q^*.$$

We have the following result.

Lemma 1.1.3 ([ST12]). *For $A, B \in \mathrm{GL}_2(\mathbb{F}_q)$ and $f, g \in \mathcal{M}$ we have*

1. $A \sim B \Rightarrow f \circ A \sim f \circ B$.

2. $f \sim g \Rightarrow f \circ A \sim g \circ A$.

We will denote classes of matrices and polynomials with the same name, since we will consider only elements up to some scalar multiple.

Using the lemma we obtain an action of $\mathrm{PGL}_2(\mathbb{F}_q)$ on the sets

$$\mathcal{I} = \{P \in \mathbb{F}_q[x] : P \text{ monic irreducible, } \deg P \geq 2\},$$

and

$$\mathcal{I}_n = \{P \in \mathbb{F}_q[x] : P \text{ monic irreducible, } \deg P = n\},$$

given by

$$f \circ A = \text{ the unique monic polynomial } g \sim f \circ A.$$

We define now another (right) action of $\mathrm{PGL}_2(\mathbb{F}_q)$ on $\overline{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$.

Definition 1.1.4. Let $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$ and $A \in \mathrm{PGL}_2(\mathbb{F}_q)$ represented by the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We define

$$\alpha \circ A = \frac{d\alpha - b}{-c\alpha + a}.$$

We have the following results.

Lemma 1.1.5 ([ST12])**.** *Let $f \in \mathcal{M}$ and $A \in \mathrm{GL}_2(\mathbb{F}_q)$. Then, if $\alpha \in \overline{\mathbb{F}}_q$ we have*

$$f(\alpha) = 0 \Leftrightarrow (f \circ A)(\alpha \circ A) = 0.$$

Lemma 1.1.6 ([ST12])**.** *Let $A \in \mathrm{PGL}_2(\mathbb{F}_q)$ and let $\alpha \in \overline{\mathbb{F}}_q$ be a root of $f \in \mathcal{I}_n$. Then $f \circ A$ is the minimal polynomial of $\alpha \circ A$ over $\mathbb{F}_q$. We also have*

$$f \circ A = f \Leftrightarrow f(\alpha \circ A) = 0.$$

1.2 Self-reciprocal polynomials

We will now introduce self-reciprocal polynomials and present some known results.

Definition 1.2.1. Suppose $f \in K[x]$ is an irreducible non-linear polynomial of degree n. We say that f is self-reciprocal irreducible monic (srim) if $f(x) = x^n f(1/x)$.

Remark 1.2.2. We could have defined self-reciprocal polynomials in terms of their roots: a polynomial is self-reciprocal when the inverse of one of its root is still a root. We note that the two definitions agree for non-linear polynomials. They are the same definition if we had required $f(x) = (-x)^{\deg f} f(1/x)$. The only two linear self-reciprocal polynomials are $x + 1$ and $x - 1$.

Our main interest is this chapter is to count irreducible polynomials of certain forms, therefore our first task will be to count the number of self-reciprocal polynomials over $\mathbb{F}_q[x]$. A first theorem is due to Carlitz, [Car67]. In the following we will present an alternative proof, due to Meyn, given in [Mey90]. It is more elementary with respect of Carlitz's one and we will generalize it in the following.

We state the first result.

Theorem 1.2.3 ([Mey90])**.** *1. Each srim polynomial of degree $2n$ over $\mathbb{F}_q$ is an irreducible factor of the polynomial*

$$H_{q,n}(x) = x^{q^n+1} - 1.$$

2. *Each irreducible factor of degree* ≥ 2 *of* $H_{q,n}(x)$ *is a srim polynomial of degree* $2d$*, where* d *divides* n *and* n/d *is odd.*

We do not present a proof of this theorem because we will prove a more general result later.

It is now possible to count srim polynomials. Let $R_{q,n}(x)$ denote the product of all srim polynomials of degree $2n$ over $\mathbb{F}_q$. Then, using Theorem 1.2.3, we have

$$H_{q,n}(x) = (x^{1+e_q} - 1) \prod_{\substack{d|n, \\ n/d \text{ odd}}} R_{q,d}(x),$$

where $e_q = 0$ if q is even and $e_q = 1$ if q is odd. We then consider $H^0_{q,n}(x) = H_{q,n}(x)/(x^{1+e_q} - 1)$. We now use Möbius inversion formula to obtain the desired result.

Lemma 1.2.4 ([Mey90])**.** *The product* $R_{q,n}(x)$ *of all srim polynomials of degree* $2n$ *satisfies*

$$R_{q,n}(x) = \prod_{\substack{d|n, \\ d \text{ odd}}} H^0_{q,n}(x)^{\mu(d)}.$$

Finally we obtain the following result.

Theorem 1.2.5 ([Car67], [Mey90])**.** *Let* $S_q(n)$ *denote the number of srim polynomials of degree* $2n$ *over* $\mathbb{F}_q$*. Then*

$$S_q(2n) = \begin{cases} \frac{1}{2n}(q^n - 1) & \text{if } q \text{ is odd and } n = 2^s, \\ \frac{1}{2n} \sum_{d|n,\, d \text{ odd}} \mu(d) q^{n/d} & \text{otherwise.} \end{cases}$$

We will now present a first generalization of self-reciprocal polynomials, namely we are interested in polynomials fixed by the action of the rational map $x \mapsto \sigma/x$, where $\sigma \in \mathbb{F}_q$. We start with a generalization of Theorem 1.2.3. In the following let $\mathcal{I}_\sigma$ be the set of all irreducible monic polynomials $g \in \mathbb{F}_q[x]$ of even degree $2n$ which satisfy $x^{2n} \cdot g(\sigma x^{-1}) = \sigma^n g(x)$.

Lemma 1.2.6. *Let* $\sigma \in \mathbb{F}_q^*$*, and let* $\mathcal{I}_\sigma$ *be the set of all irreducible monic polynomials* $g \in \mathbb{F}_q[x]$ *of even degree* $2n$ *which satisfy* $x^{2n} \cdot g(\sigma x^{-1}) = \sigma^n g(x)$*. Then the polynomial*

$$\frac{x^{q^n+1} - \sigma}{(x^2 - \sigma, x^{q^n+1} - \sigma)}$$

equals the product of all $g \in \mathcal{I}_\sigma$ *of degree a divisor* $2d$ *of* $2n$ *such that* n/d *is odd.*

Proof. When q is odd the polynomial under consideration equals $(x^{q^n+1} - \sigma)/(x^2-\sigma)$ unless n is odd and σ is not a square in $\mathbb{F}_q$, in which case it equals $x^{q^n+1} - \sigma$. When q is even the polynomial equals $(x^{q^n+1} - \sigma)/(x - \sigma^{q/2})$. The field $\mathbb{F}_{q^{2n}}$ contains a splitting field for the polynomial. Its roots are all distinct, and are the elements of $\mathbb{F}_{q^{2n}}$ such that $\xi^{q^n} = \sigma\xi^{-1} \neq \xi$. Therefore, its roots are exactly all elements of $\mathbb{F}_{q^{2n}}$ whose orbit under the Frobenius automorphism $\alpha \mapsto \alpha^q$ has length an even divisor $2d$ of $2n$ such that $2d$ does not divide n. □

We can now present a slight generalization of Theorem 1.2.3.

Theorem 1.2.7. *The number of irreducible monic polynomials of degree* $2n$ *in* $\mathcal{I}_\sigma$ *is*

$$\tilde{S}_q(2n) = \begin{cases} \dfrac{1}{2n}(q^n - \delta_n) & \text{if } q \text{ is odd and } n = 2^s, s \geq 0, \\ \dfrac{1}{2n} \displaystyle\sum_{d|n, d \text{ odd}} \mu(d) q^{\frac{n}{d}} & \text{otherwise} \end{cases}$$

where δ_n *equals* $\sigma^{n(q-1)/2} \in \{\pm 1\}$ *for* q *odd and* 0 *for* q *even.*

Proof. Let $\tilde{S}_q(2n)$ be the number of irreducible monic polynomials of degree $2n$ in $\mathcal{I}_\sigma$. Taking degrees in Lemma 1.2.6 we find

$$q^n - \delta_n = \sum_{d|n,\ 2d\nmid n} 2d\tilde{S}_q(2d).$$

Möbius inversion then yields

$$2n\tilde{S}_q(2n) = \sum_{d|n,\ d \text{ odd}} \mu(d) q^{n/d} - \sum_{d|n,\ d \text{ odd}} \delta_{n/d}.$$

Because the sum $\displaystyle\sum_{d|n,\ d \text{ odd}} \delta_{n/d}$ is nonzero only when n is a power of 2, we reach the desired conclusion. □

Chapter 2

Möbius Group and Polynomials

In this chapter we study the action of some rational linear transformations on the set of irreducible polynomials. In [MR10], the two authors studied the action of $\mathrm{PGL}_2(\mathbb{F}_2)$ on irreducible polynomials over the finite field with two elements. We generalize their results considering certain subgroups of the projective linear group of dimension two and devote a section to each one of them. In each section we present counting results on the number of orbits of a prescribed length and the corresponding stabilizers. In the final section we present some general results that can be found in [ST12]. Another interesting paper dealing with these arguments is [Gar11].

In [MR10], Michon and Ravache studied the action of $\mathrm{PGL}_2(\mathbb{F}_2)$, generated by the two rational maps

$$x \mapsto 1/x \quad \text{and} \quad x \mapsto 1 + x$$

on irreducible nonlinear polynomials over $\mathbb{F}_2$. The authors studied orbits and stabilizers of this action. We will generalize their result in two directions, namely using other groups and considering also odd characteristics.

We introduce now the notation we will use. Let $G \leq \mathrm{PGL}_2(\mathbb{F}_q)$ be the group of rational transformations we want to study. Then we define

$$GP = \{P^\gamma, \gamma \in G\},$$

the orbit of the polynomial P under the action of the group G. For the sake of brevity we denote $P \circ A$ with P^γ, where γ is the element of the group G represented by the matrix A. Now, let $G(n)$ (resp. $G_i(n)$) be the number of all orbits (resp. orbits of size i) of irreducible polynomials of degree n. Then we have

$$G(n) = \sum_{i \in \mathcal{J}} G_i(n),$$

where $\mathcal{J}$ is the set of integers occurring as indices of subgroups of G.

We make now some general considerations about stabilizers. Let g be a root of an irreducible polynomial P of degree n and suppose α, β are elements of the stabilizer S of P, which we will assume to be cyclic. Since the set of roots is closed under the action of α we have that

$$g^\alpha = g^{q^{i_\alpha}},$$

for some integer i_α, and where g^α is the action of the element of the group. It follows almost immediately that $(g^\alpha)^q = (g^q)^\alpha$. Hence we have

$$g^{\alpha\beta} = g^{q^{i_\alpha + i_\beta}}$$

and the map $\alpha \mapsto i_\alpha$ is a morphism $S \to \mathbb{Z}/n\mathbb{Z}$, where $n = \deg P$. We distinguish two main cases: whether the morphism is injective or not. Suppose we are in former case. We obtain that the order of S has to divide the degree of the polynomial, as S is a subgroup of $\mathbb{Z}/n\mathbb{Z}$. This means that if a polynomial has a cyclic stabilizer of order r its degree would be rm for some m and an element of the stabilizer has the following action on a root: $g \mapsto g^{q^m}$. If now the morphism is not injective we have that there is some element $\alpha \in S, \alpha \neq 1$ such that $g^\alpha = g$. This implies that

$$g = \frac{dg - b}{-cg + a}$$

and therefore g is a root of a polynomial of degree 2.
Suppose now that if a subgroup of G is not cyclic then it contains at least two involutions. Hence there will be a non-trivial kernel in the morphism $S \to \mathbb{Z}/n\mathbb{Z}$ and n should be equal to 2. We have three cases. Both involutions have trivial effect on the roots of the polynomial, just one has a trivial action and the other permutes the two roots of the polynomial or both involutions permute the roots. We exclude the first case because g should be a root of two distinct polynomials of degree 2 and this is not possible. In the last case the composition of the two involutions will have trivial action and we obtain the polynomial of degree 2 we are looking for. If these polynomials of degree 2 are fixed by every element of the stabilizer (the two involutions do not necessarily generate it), are irreducible and are not fixed by another subgroup S' such that $S' \supset S$, we have found all irreducible polynomials that have S as stabilizer.

2.1 The action of $\mathcal{S}_3$

The group considered by Michon and Revache is isomorphic to the symmetric group on three objects. Now, we generalize the previous action for odd

characteristics.
We start considering the action of the group $\mathcal{S}_3$ over $\mathbb{F}_q[x]$, where $q = p^l$ is a power of a prime. We consider the representation of this group in $\mathrm{GL}_2(\mathbb{F}_q)$ given by:

$$(12) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } (13) \mapsto \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}.$$

This representation is just a real (or complex) irreducible representation of degree 2 considered in characteristic p.
We define now an action of $\mathcal{S}_3$ on the set

$$\mathcal{I} = \{P \in \mathbb{F}_q[x] : P \text{ irreducible }, \deg P \geq 2\}/\sim,$$

where $P \sim Q$ if and only if $P = \lambda Q$, with $\lambda \in \mathbb{F}_q^*$, in the following way:

$$P^*(x) = x^{\deg P} P\left(\frac{1}{x}\right) \text{ and } P^-(x) = P(1-x).$$

We call $P \in \mathcal{I}$ anti-invariant if $P^* = P^-$ and self-reciprocal if $P = P^*$.
Now we want to study

$$GP = \{P^\sigma, \sigma \in \mathcal{S}_3\},$$

the orbit of a polynomial under the action of the group.

Lemma 2.1.1. *The polynomial $P = x^2 - x + 1$ is irreducible (over $\mathbb{F}_p$) if and only if $p = 2$ or $p \equiv -1 \pmod 6$, and it has a root of multiplicity 2 if and only if $p = 3$.*

Proof. We have that $P = (x^3+1)/(x+1)$. Thus a root of P is just a primitive sixth root of unity σ in $\mathbb{F}_p$ and $\sigma \in \mathbb{F}_p$ if and only if $6 \mid p-1$. The polynomial $x^3 - 1$ is separable over $\mathbb{F}_p$ if and only if $p \neq 3$ and this proves the second part. □

2.1.1 Orbits of size one

Theorem 2.1.2. *$G_1(n) = 1$ if and only if $n = 2$ and $x^2 - x + 1$ is irreducible. In that case $G(x^2 - x + 1)$ is the only orbit with one element.*

Proof. The orbit consists of just one element if and only if P is fixed by every element of the group. In particular, that implies $P^*(x) = P^-(x) = P$. If g is a root of P we have

$$g^{q^k} = 1 - g \quad \text{and} \quad g^{q^l} = \frac{1}{g},$$

with $0 \leq k, l \leq n-1$.
This implies

$$g = g^{q^{2k}} = q^{q^{2l}},$$

hence $2k \equiv 2l \equiv 0 \pmod{n}$. Since n is even we have $k \equiv l \equiv 0 \pmod{n/2}$. The cases $k = 0$ or $l = 0$ are impossible and thus $k = l = n/2$. Finally this implies

$$1 - g = \frac{1}{g}$$

and g is a root of $x^2 - x + 1$. □

2.1.2 Orbits of size two

The orbits with two elements are the orbits of an anti-invariant polynomial. We have the following result.

Theorem 2.1.3. *The anti-invariant polynomials are the irreducible factors of*

$$B_{q,k}(x) = x^{q^k+1} - x + 1$$

for $k \in \mathbb{N}$. *If* P *is anti-invariant,* $\deg P \geq 2$ *(if an element of* $\mathbb{F}_q$ *is a root of* $B_{q,k}(x)$ *then it is a root of* $x^2 - x + 1$*), then* $\deg P \equiv 0 \pmod{3}$ *or* $P = x^2 - x + 1$ *(if irreducible). If* $\deg P = 3m$ *then* $P | B_{q,m}$ *or* $P | B_{q,2m}$.

Proof. If g is a root of P then $1 - 1/g$ is a root of P^{-*}. Let P be an irreducible factor of $B_{q,k}$. Then a root g of P is a root of $B_{q,k}$, hence

$$g^{q^k} = 1 - \frac{1}{g}$$

This implies that the set of roots of P is invariant under the map

$$T : g \mapsto 1 - \frac{1}{g}$$

and P is anti-invariant. Conversely, let P be anti-invariant and g one of his roots. Then

$$g^{q^k} = 1 - \frac{1}{g},$$

with $0 \leq k < n = \deg P$. Hence P divides $B_{q,k}$. The map T has order 3 and permutes the roots of P. Consequently we have $\deg P \equiv 0 \pmod{3}$. Since T has order 3 we have that

$$g^{q^{3k}} = g,$$

hence $g \in \mathbb{F}_{q^{3k}}$. From the fact that $\deg P = n$ we have that

$$\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^{3k}},$$

hence $3k \equiv 0 \pmod{n}$, and that implies $k = \frac{in}{3}, 1 \leq i \leq 2$. □

Suppose now that P is irreducible and anti-invariant of degree $3m$. If P divides $B_{q,m}$ we say that P is of type 1. Otherwise, if P divides $B_{q,2m}$, we say that P is of type 2.

Proposition 2.1.4. *P and P^* have different types.*

Proof. Let P irreducible anti-invariant of type 1. If $\deg P = 3m$ and g is one of its roots we have

$$g^{q^m} = 1 - \frac{1}{g}.$$

Let $h = g^{-1}$ be a root of P^*. Then

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

Hence h is a root of $B_{q,2m}$. If P has type 2 we have similar calculations. □

Corollary 2.1.5. *Among anti-invariant polynomials of degree $3m$, half divides $B_{q,m}$ and the other half $B_{q,2m}$.*

Proposition 2.1.6. *$B_{q,k}$ has no multiple roots.*

Proof. We have

$$B'_{q,k} = x^{q^k} - 1 = (x-1)^{q^k}.$$

Since 1 is not a root of $B_{q,k}$ the result follows immediately. □

Proposition 2.1.7. *If $p = 3$ we have $x^2 - x + 1 = (x+1)^2$ and $x + 1 | B_{q,k}$ for every k.*
If $p \neq 3$ and $P = x^2 - x + 1$ is reducible over $\mathbb{F}_q$ then $x^2 - x + 1 | B_{q,k}$ for every k.
If $p \neq 3$ and $P = x^2 - x + 1$ is irreducible over $\mathbb{F}_q$ then $x^2 - x + 1 | B_{q,k}$ if and only if k is even.

Proof. The first statement is trivial.
Let α be a root of P. Then $\alpha^{q^2} = \alpha$. If k is even then $\alpha^{q^k+1} = \alpha^2$ and $B_{q,k}(\alpha) = 0$.
If k is odd then $\alpha^{q^k+1} = \alpha^{q+1}$. Now $\alpha^{q+1} = \alpha^2$ if and only if $\alpha^{q-1} = 1$, if and only if P is reducible. □

Theorem 2.1.8. *Let P be an irreducible polynomial of degree $3m$. Then $P | B_{q,k}$ if and only if P is anti-invariant, m divides k and the type of P is congruent to k/m modulo 3.*

Proof. Let P be irreducible of degree $3m$ and suppose $P | B_{q,k}$. We know from Theorem 2.1.3 that P is anti-invariant and using the same reasoning used in its proof we know that all the roots of $B_{q,k}$ are in $\mathbb{F}_{q^{3k}}$. The smallest

field containing the roots of P is $\mathbb{F}_{q^{3m}}$. Hence m divides k. Now, if $k = ml$ and P is of type z we have

$$g^{q^{zm}} = 1 - \frac{1}{g} = g^{q^k} = g^{q^{ml}}.$$

Hence $zm \equiv ml \pmod 3 m$ and we have

$$z \equiv l \pmod 3,$$

as was to be shown. Conversely, suppose P is anti-invariant, let $k = ml$, where $l \equiv t \pmod 3$ is the type of P. Then

$$g^{q^k} = g^{q^{ml}} = g^{q^{mt}} = 1 - \frac{1}{g}.$$

Hence P divides $B_{q,k}$ and the theorem is proved. □

Theorem 2.1.9. *Consider $G_2(3m)$, $m \geq 1$. For every $k \geq 1$ we have*

$$q^k - (-1)^k = \sum_{d|k,\ \frac{k}{d} \not\equiv 0 \pmod 3} 3dG_2(3d)$$

if $x^2 - x + 1$ is irreducible,

$$q^k - 1 = \sum_{d|k,\ \frac{k}{d} \not\equiv 0 \pmod 3} 3dG_2(3d)$$

if $x^2 - x + 1$ is reducible and $p \neq 3$ and

$$q^k = \sum_{d|k,\ \frac{k}{d} \not\equiv 0 \pmod 3} 3dG_2(3d)$$

if $p = 3$.

Proof. Let EB_k be the set of all irreducible polynomials of degree greater than 2 dividing $B_{q,k}$. From Theorem 2.1.8 we have

$$EB_k = \bigcup_{d|k,\ \frac{k}{d} \equiv 1 \pmod 3} ES_1(3d) \cup \bigcup_{d|k,\ \frac{k}{d} \equiv 2 \pmod 3} ES_2(3d)$$

where $ES_i(3d)$ is the set of all irreducible anti-invariant polynomials of degree $3d$ and type i dividing $B_{q,k}$. This implies

$$\sum_{Q \in EB_k} \deg Q = \sum_{d|k,\ \frac{k}{d} \equiv 1 \pmod 3} 3d|ES_1(3d)| + \sum_{d|k,\ \frac{k}{d} \equiv 2 \pmod 3} 3d|ES_2(3d)|$$

According to Corollary 2.1.5 we have

$$\sum_{Q\in EB_k} \deg Q = \sum_{d|k,\ \frac{k}{d}\equiv 1 \pmod 3} 3dG_2(3d) + \sum_{d|k,\ \frac{k}{d}\equiv 2 \pmod 3} 3dG_2(3d),$$

and finally

$$\sum_{Q\in EB_k} \deg Q = \sum_{d|k,\ \frac{k}{d}\not\equiv 0 \pmod 3} 3dG_2(3d).$$

According to Proposition 2.1.7 we have

$$\sum_{Q\in EB_k} \deg Q = \begin{cases} q^k - (-1)^k & \text{if } x^2 - x + 1 \text{ is irreducible} \\ q^k - 1 & \text{if } x^2 - x + 1 \text{ is reducible and } p \neq 3 \\ q^k & \text{if } p = 3 \end{cases}$$

and we reach the desired result. □

Using Möbius inversion we obtain the following result.

Theorem 2.1.10. *$G_2(n) = 0$ if $n \not\equiv 0 \pmod 3$. Moreover, we have*

$$G_2(3m) = \frac{1}{3m} \sum_{d|m,\ d\not\equiv 0 \pmod 3} \mu(d)(q^{\frac{m}{d}} - (-1)^{\frac{m}{d}})$$

if $q \not\equiv 1 \pmod 6$ and $p \neq 3$ or $q = 2^{2l+1}$,

$$G_2(3m) = \frac{1}{3m} \sum_{d|m,\ d\not\equiv 0 \pmod 3} \mu(d)(q^{\frac{m}{d}} - 1)$$

if $q \equiv 1 \pmod 6$ or $q = 2^{2l}$ and

$$G_2(3m) = \frac{1}{3m} \sum_{d|m,\ d\not\equiv 0 \pmod 3} \mu(d) q^{\frac{m}{d}}$$

if $p = 3$.

2.1.3 Orbits of size three

Orbits consisting of 3 elements are of the form

$$GP = \{P, P^-, P^{-*}\},$$

where P is self-reciprocal.
Using the same notations as in Theorem 1.2.5, we have $G_3(2n) = S_q(2n)$ and $G_3(n) = 0$ if n is odd.

2.1.4 Orbits of size six

The remaining polynomials form orbits with 6 elements.

Theorem 2.1.11. *If $n \geq 2$ we have*

$$G_6(n) = \frac{1}{6}\left(I(n) - G_1(n) - 2G_2(n) - 3G_3(n)\right),$$

where

$$I(n) = \frac{1}{n}\sum_{d|n} \mu(d) q^{\frac{n}{d}}$$

is the number of total irreducible monic polynomials of degree n.

2.1.5 Not necessarily monic polynomials

We can do a similar count without imposing the condition that the polynomials have to be monic. First of all we need to modify the action in the following way:

$$P^*(x) = (-x)^{\deg P} P\left(\frac{1}{x}\right) \text{ and } P^-(x) = P(1-x)$$

Otherwise the action will not be well defined. We have the following result.

Proposition 2.1.12. *Let $P \in \mathbb{F}_q[x]$ be an irreducible non-linear polynomial of degree $m+1$. Then we have:*

1. *If P is irreducible and the set of roots is closed under inversion, then $P^*(x) = P(x)$;*

2. *If P is irreducible and the set of roots is closed under the map $g \mapsto 1 - 1/g$, then $P^{-*}(x) = P(x)$;*

3. *If P is irreducible and the set of roots is closed under the map $g \mapsto 1-g$, then $P^-(x) = P(x)$.*

Proof. Let

$$P(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^m}),$$

with $\deg P = m+1$.
We have

$$P^*(x) = x^{m+1}\left(\frac{1}{x} - \alpha\right)\left(\frac{1}{x} - \alpha^q\right)\cdots\left(\frac{1}{x} - \alpha^{q^m}\right).$$

Extracting the q-th powers of α we obtain

$$P^*(x) = \alpha\alpha^q\cdots\alpha^{q^m}\left(x - \frac{1}{\alpha}\right)\left(x - \frac{1}{\alpha^q}\right)\cdots\left(x - \frac{1}{\alpha^{q^m}}\right).$$

We know that $\alpha^{q^k} = 1/\alpha$, for some $1 \leq k \leq m$. Noting that $\alpha^{q^i}\alpha^{q^{k+i}} = 1$ for every integer i, we have that $\alpha\alpha^q \cdots \alpha^{q^m} = 1$ and thus we have proved 1.

We have now

$$P^{-*}(x) = (-x)^{m+1}\left(1 - \frac{1}{x} - \alpha\right)\left(1 - \frac{1}{x} - \alpha^q\right)\cdots\left(1 - \frac{1}{x} - \alpha^{q^m}\right).$$

Extracting $-1/x$ and $(\alpha - 1)^{p^i}$ we have

$$P^{-*}(x) = (\alpha - 1)(\alpha^q - 1)\cdots(\alpha^{q^m} - 1)\left(x - \frac{1}{1-\alpha}\right)\cdots\left(x - \frac{1}{1-\alpha^{q^m}}\right).$$

We know that $\alpha^{q^k} = 1 - 1/\alpha, 1 \leq k \leq m$. This implies that

$$\alpha^i\alpha^{q^{i+k}}\alpha^{q^{i+2k}} = 1$$

for every integer i, hence $(\alpha-1)(\alpha^q-1)\cdots(\alpha^{q^m}-1) = 1$ and we have proved the second point.

As for the last point we have

$$P^-(x) = (x - (1-\alpha))(x - (1-\alpha^q))\cdots(x - (1-\alpha^{q^m})).$$

Since $\alpha^{q^k} = 1 - \alpha, 1 \leq k \leq m$, we have that $P^-(x) = P(x)$. □

Consider now orbits of size two,

$$G_2(P) = \{P, P^*\}.$$

From what we said before the two polynomials have distinct roots, hence they are distinct in the quotient set. If we consider 3-elements orbits,

$$G_3(P) = \{P, P^-, P^{-*}\},$$

we note that the same thing happens. Summarizing, if the orbit of a monic polynomial is

$$\{P, P^*, P^-, P^{*-}, P^{-*}, P^{-*-}\},$$

with no polynomial multiple of another, then the orbit of $\lambda P, \lambda \in \mathbb{F}_q^*$ is

$$\{\lambda P, \lambda P^\star, \lambda P^-, \lambda P^{\star+}, \lambda P^{+\star}, \lambda P^{+\star+}\}$$

and therefore the number of the orbits of a fixed length is just $q - 1$ times the number of the orbits of that length, considering only monic polynomials.

2.2 The action of $\mathcal{D}_r$

Now we consider the action of Dihedral groups $\mathcal{D}_r$, where r is prime, on univariate polynomial rings over finite fields. In order to describe the action we need to construct a faithful representation of the group of degree 2. For the rest of the section we suppose that $q \equiv 1 \pmod{r}$. Let β be a primitive r-th root of unity in $\mathbb{F}_q$. We consider the two following matrices representing, respectively, σ, a rotation of order r and τ, an involution:

$$\sigma \sim \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} \qquad \tau \sim \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

For the rest of the section let $\omega = \beta^2$.
We can now define the action of the group over the set $\mathcal{I}$ of monic irreducible non-linear polynomials over $\mathbb{F}_q$ in the following way:

$$P^\sigma(x) = P(\omega x) \qquad P^\tau(x) = x^{\deg P} P\left(\frac{1}{x}\right).$$

As always we will study

$$GP = \{P^\gamma, \gamma \in \mathcal{D}_r\},$$

the orbit of the polynomial under the action of the group.

2.2.1 Orbits of size one

The orbit consists of just one element if and only if P is fixed by every element of the group. In particular this implies $P^{\tau\sigma}(x) = P^\tau(x) = P$.
Let g be a root of P. Then we have

$$g^{q^k} = g^{-1} \text{ and } g^{q^l} = \omega g^{-1},$$

with $0 \leq k, l \leq n-1$.
This implies

$$g^{q^{2k}} = g \text{ and } g^{q^{2l}} = g.$$

We cannot have $k = 0$ or $l = 0$, since $x^2 - 1$ and $x^2 - \omega$ are not irreducible, hence we have $k = l = \frac{n}{2}$ and $g = \omega g$. Clearly this is impossible.

Theorem 2.2.1. *$G_1(n) = 0$ for every $n \geq 2$ and for every $r \geq 3$.*

2.2.2 Orbits of size two

An orbit has 2 elements if and only if P is fixed by the cyclic group of order r generated by σ.

Lemma 2.2.2. *The polynomials fixed by σ are the irreducible factors of*

$$S_{q,k}(x) = x^{q^k-1} - \omega^{-1},$$

with k a positive integer. Moreover, if $P = P^\sigma$, we have $\deg P \equiv 0 \pmod r$ and, if $\deg P = rm$, then P divides one of $S_{q,im}, 1 \leq i \leq r-1$.

Proof. If g is a root of P then $\omega^{-1}g$ is a root of P^σ. Let P be an irreducible factor of $S_{q,k}$. Then a root g of P is a root of $S_{q,k}$, hence

$$g^{q^k} = \omega^{-1}g.$$

This implies that the set of roots of P is invariant under the map

$$T : g \mapsto \omega^{-1}g$$

and $P = P^\sigma$.
Conversely, suppose $P = P^\sigma$ and let g be one of its roots. Then

$$g^{q^k} = \omega^{-1}g,$$

with $0 \leq k < n = \deg P$. Hence P divides $S_{q,k}$. The map T has order r and permutes the roots of P. Consequently we have $\deg P \equiv 0 \pmod r$. Since T has order r we have that

$$g^{q^{rk}} = g,$$

hence $g \in \mathbb{F}_{q^{rk}}$. From the fact that $\deg P = n$ we have that

$$\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^{rk}}$$

and thus $rk \equiv 0 \pmod n$, and that implies $k = in/r, 1 \leq i \leq r-1$. □

We note that $S_{q,k}$ has no multiple roots since its derivative is $-x^{q^k-2}$.

Suppose now that P is irreducible, $P = P^\sigma$ and that it has degree rm. If P divides $S_{q,ik}$ we say that P is of type i.

We argue in the same way considering σ^k instead of σ and we obtain that the other polynomials fixed by σ are irreducible factors of

$$x^{q^k-1} - \omega^{-k},$$

with $1 \leq k \leq r-1$.
Now, if g is a root of $x^{q^k-1} - \omega^{-1}$ and β is a (q^k-1)-root of ω^{-1}, we have that $\beta^z g$ is a root of

$$x^{q^k-1} - \omega^{-z-1},$$

$1 \leq z \leq r-2$.
We also have that $x^{q^k-1} - \omega^{-k}$ and $x^{q^k-1} - \omega^{-l}$ are coprime if $l \not\equiv k \pmod r$. Finally we note that

$$x^{q^k-1} - \omega^{-k} | x^{q^{zk}-1} - \omega^{-1}$$

if and only if $zk \equiv 1 \pmod r$.

Proposition 2.2.3. *The number of polynomials of degree rm fixed by σ is the same for every type.*

Theorem 2.2.4. *Let P be an irreducible polynomial of degree rm. Then $P|S_{q,k}$ if and only if $P = P^\sigma$, m divides k and the type of P is congruent to k/m modulo 3.*

Proof. Let P be irreducible of degree rm and suppose $P|S_{q,k}$. We know that $P = P^\sigma$ and that all the roots of P are in $\mathbb{F}_{q^{rk}}$. The smallest field containing the roots of P is $\mathbb{F}_{q^{rm}}$. This implies that m divides k. Now, if $k = ml$ and P is of type z we have

$$g^{q^{zm}} = \omega^{-1} g = g^{q^k} = g^{q^{ml}}.$$

Hence $zm \equiv ml \pmod{rm}$ and

$$z \equiv l \pmod{r},$$

as was to be shown. Conversely, suppose $P = P^\sigma$ and let $k = ml$, where $l \equiv t \pmod{r}$ is the type of P. Then

$$g^{q^k} = g^{q^{ml}} = g^{q^{mt}} = \omega^{-1} g.$$

Hence P divides $S_{q,k}$, and the theorem is proved. □

Theorem 2.2.5. *For any $k \geq 1$ we have*

$$q^k - 1 = \sum_{d|k,\ \frac{k}{d} \not\equiv 0 \pmod{r}} \frac{2rd}{r-1} G_2(rd).$$

Proof. Let ES_k be the set of all irreducible polynomials of degree greater than 2 dividing $S_{q,k}$. From Theorem 2.2.4 we have

$$ES_k = \bigcup_{d|k,\ \frac{k}{d} \equiv 1 \pmod{r}} ES_1(rd) \cup \cdots \cup \bigcup_{d|k,\ \frac{k}{d} \equiv r-1 \pmod{r}} ES_{r-1}(rd),$$

where $ES_i(rd)$ is the set of all irreducible polynomials of degree rd and type i dividing $S_{q,k}$. This implies

$$\sum_{Q \in ES_k} \deg Q = \sum_{d|k, \frac{k}{d} \equiv 1 \pmod{r}} rd|ES_1(rd)| + \cdots + \sum_{d|k, \frac{k}{d} \equiv r-1 \pmod{r}} rd|ES_{r-1}(rd)|.$$

According to Proposition 2.2.3 we have

$$\sum_{Q \in ES_k} \deg Q = \sum_{d|k, \frac{k}{d} \equiv 1 \pmod{r}} rd \frac{2}{r-1} G_2(rd) + \cdots + \sum_{d|k, \frac{k}{d} \equiv r-1 \pmod{r}} rd \frac{2}{r-1} G_2(rd).$$

Finally

$$\sum_{Q\in ES_k} \deg Q = \sum_{d|k,\ \frac{k}{d}\not\equiv 0 \pmod r} \frac{2rd}{r-1} G_2(rd).$$

Since

$$\sum_{Q\in ES_k} \deg Q = q^k - 1,$$

we have the thesis. □

Using Möbius inversion we obtain the following result.

Theorem 2.2.6. *$G_2(n) = 0$ if $n \not\equiv 0 \pmod r$. Otherwise, if $n = rm$, we have*

$$G_2(rm) = \frac{r-1}{2rm} \sum_{d|m,\ d\not\equiv 0 \pmod r} \mu(d)(q^{\frac{m}{d}} - 1).$$

2.2.3 Orbits of size r

The results of this subsection are substantially the same of the corresponding ones in the $\mathcal{S}_3$ case, but we rewrite them for sake of clarity.
Orbits consisting of r elements are of the form

$$GP = \{P, P^\tau, \dots, P^{\tau^{r-1}}\},$$

where P is self-reciprocal. As before, using Theorem 1.2.5, we obtain $G_r(n) = S_q(n)$ (because all subgroups of order r are conjugate) if n is even and $G_r(n) = 0$ otherwise.

2.2.4 Orbits of size $2r$

The remaining polynomials form orbits with $2r$ elements.

Theorem 2.2.7. *If $n \geq 2$ we have*

$$G_{2r}(n) = \frac{1}{2r}\left(I(n) - G_1(n) - 2G_2(n) - rG_r(n)\right),$$

where

$$I(n) = \frac{1}{n}\sum_{d|n} \mu(d) q^{\frac{n}{d}}$$

is the number of total irreducible monic polynomials of degree n.

2.2.5 Not necessarily monic polynomials

As we did in the previous section we may consider the action of $\mathcal{D}_r$ over the set of all irreducible polynomials, without the equivalence relation given by scalar multiplication.
First of all we have to modify the action, otherwise it is not well defined. We adjust it in the following way:

$$P^\sigma(x) = (\omega^{\frac{r-1}{2}})^{\deg P} P(\omega x) \qquad P^\tau(x) = x^{\deg P} P\left(\frac{1}{x}\right).$$

We note these two facts.

1. If P is irreducible and the set of roots is closed under the map $T : g \mapsto \omega/g$ then $P^\gamma = P$, where γ is the involution associated to T.

2. If P is irreducible and the set of roots is closed under the map $g \mapsto \omega^{-1}g$ then $P^\sigma = P$.

Now, if P is self reciprocal, its orbit will still have r elements

$$GP = \{P, P^\sigma, \ldots, P^{\sigma^{r-1}}\}.$$

All the polynomials in this orbit are fixed by the r different involutions, hence none is multiple of another.
If the polynomial is fixed under $g \mapsto \omega^{-1}g$ its orbit is

$$GP = \{P, P^\tau\}.$$

The two polynomials are different and fixed by the elements of order r.
Summarizing, the number of orbits of a certain length is just $q - 1$ times that number in the monic case.

2.2.6 Some comments

We note that we have obtained results using the action of $\mathcal{S}_3 \cong \mathcal{D}_3$ in two different ways. But when they can be compared we observe that they are the same. Why does this happen?
We know that $\mathcal{D}_3$ is the group of the symmetries of the regular triangle. In the first case we took the basis $\mathcal{B}$ of the plane, respect to which the rotation σ of 120° has matrix

$$M = \mathcal{M}_{\mathcal{B}}^{\mathcal{B}}(\sigma) \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

If we consider now another basis $\mathcal{B}'$ such that

$$N = \mathcal{M}_{\mathcal{B}'}^{\mathcal{B}}(Id) = \begin{pmatrix} 1 & \beta \\ 1 & \beta^{-1} \end{pmatrix},$$

we obtain

$$\mathcal{M}_{\mathcal{B}'}^{\mathcal{B}'}(\sigma) = NMN^{-1} = \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}.$$

The same thing happens when we consider the matrices of the involutions. Hence the two representation are similar (since this group has only one irreducible representation of degree two, this was in fact trivial) and the results should clearly be the same.

2.3 The action of $\mathcal{S}_4$

Now we consider the Octahedral group which is isomorphic to $\mathcal{S}_4$. From [Tot02] we know that the corresponding Möbius transformations are

$$x \mapsto i^k x, \qquad x \mapsto \frac{i^k}{x}, \qquad x \mapsto i^k \frac{x+1}{x-1},$$

$$x \mapsto i^k \frac{x-1}{x+1}, \qquad x \mapsto i^k \frac{x+i}{x-i}, \qquad x \mapsto i^k \frac{x-i}{x+i},$$

where i is a primitive 4-th root of unity. Hence in the following we will assume $q \equiv 1 \pmod 4$.

Remark. We note that we could have used a rational representation of $\mathcal{S}_4$, without imposing the condition $q \equiv 1 \pmod 4$. We made this choice since we were more interested in the geometric aspects of these groups, seen as groups of symmetries of platonic solids.

A particular isomorphism of $\mathcal{S}_4$ with this group is determined by

$$(1,2,3,4) \mapsto (x \mapsto ix) \text{ and } (1,2,4,3) \mapsto \left(x \mapsto -i\frac{x+i}{x-i}\right).$$

We now define an action of $\mathcal{S}_4$ in the following way:

$$P^{(1,2,4,3)}(x) = (-x+i)^{\deg P} P\left(\frac{ix-1}{-x+i}\right) \text{ and } P^{(1,2,3,4)}(x) = P(ix).$$

This suffices, since $\mathcal{S}_4$ is generated by these two 4-cycles.
We note that the two involutions $(1,4)(2,3)$ and $(1,2)(3,4)$ correspond, under the previous isomorphism, respectively to pre-compositions with the rational functions $x \mapsto 1/x$ and $x \mapsto -1/x$. We call V the subgroup they generate, which is isomorphic to the Klein group.
We will frequently use the following:

Lemma 2.3.1. *There is no polynomial fixed by the subgroup V.*

Proof. Suppose P is fixed by $x \mapsto \frac{1}{x}$ and $x \mapsto -\frac{1}{x}$. If g is a root of P we have

$$g^{q^l} = \frac{1}{g} \text{ and } g^{q^k} = -\frac{1}{g},$$

with $0 \leq k, l < n = \deg P$. Hence

$$g^{q^{2l}} = g^{q^{2k}} = g$$

and this implies

$$2l \equiv 2k \equiv 0 \pmod{n}.$$

We cannot have $k = 0$ or $l = 0$, since $x^2 + 1$ and $x^2 - 1$ are not irreducible. Thus $k = l = n/2$ and

$$\frac{1}{x} = -\frac{1}{x}.$$

This is clearly impossible. □

2.3.1 Orbits of size one, two and three

If H is a subgroup of $\mathcal{S}_4$ of order $24, 12$ or 8 we have that $V \leq G$.

Proposition 2.3.2. *There are no polynomials having orbits of length* $1, 2$ *or* 3.

2.3.2 Orbits of size four

Let H the subgroup of $\mathcal{S}_4$ generated by:

$$(1, 3) \text{ and } (1, 2, 3).$$

H is isomorphic to $\mathcal{S}_3$ and every subgroup of order 6 is conjugate to this one.

Theorem 2.3.3. *$G_4(n) = 1$ if and only $n = 2$ and $x^2 + (i - 1)x + i$ is irreducible.*

Proof. Let P be fixed by H. In particular it is fixed by

$$(1, 3) = x \mapsto \frac{i}{x} \text{ and } (1, 2) = x \mapsto \frac{-x + 1}{x + 1}.$$

If g is a root of P we have

$$g^{q^l} = \frac{i}{g} \text{ and } g^{q^l} = \frac{-g + 1}{g + 1},$$

with $0 \leq k, l < n = \deg P$. Hence

$$g^{q^{2l}} = g^{q^{2k}} = g$$

and this implies

$$2l \equiv 2k \equiv 0 \pmod{n}.$$

If $l = 0$ we obtain the polynomial $x^2 - i$, which is not fixed by $(1, 2)$. If $k = 0$ we obtain $x^2 + 2x - 1$ which is not fixed by $(1, 3)$, thus we have $k = l = n/2$ and

$$\frac{i}{g} = \frac{-g+1}{g+1}.$$

Therefore g is a root of

$$x^2 + (i-1)x + i.$$

□

2.3.3 Orbits of size six

The orbit of P has length 6 if the stabilizer of the polynomial has length 4. We have three conjugacy classes of such subgroups, namely $H_1 =< (1, 2, 3, 4) >$, $H_2 =< (1, 3), (2, 4) >$ and $H_3 = V =< (1, 2)(3, 4), (1, 3)(2, 4) >$.

We will denote by $G_{6,i}(n)$ the orbits of length 6 of polynomials of degree n corresponding to H_i. We note that $H_3 = V$, therefore there is no orbit of length 6, with stabilizer H_3. We will consider the other two subgroups in order.

Subgroup H_1

Proposition 2.3.4. *If P is fixed by $\sigma = (1, 2, 3, 4)$, which corresponds to pre-composition with the rational function $x \mapsto ix$, then P is an irreducible factor of*

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

If P is fixed by σ then $\deg P \equiv 0 \pmod 4$, and if $\deg P = 4m$ then $P|Z_m$ or $P|Z_{3m}$.

Proof. If g is a root of P then $-ig$ is a root of P^σ. If P is an irreducible factor of Z_k, then we clearly have

$$g^{q^k-1} = -i.$$

Hence the set of the roots of P is invariant under

$$T : g \mapsto -ig$$

and $P^\sigma = P$. Suppose now that $P^\sigma = P$. Then we have

$$g^{q^k} = -ig,$$

with $0 \leq k < n = \deg P$, hence $P|Z_k$. T has order 4 and permutes the roots of P. Thus $\deg P \equiv 0 \pmod 4$. Since

$$g^{q^{4k}} = g,$$

we have that $g \in \mathbb{F}_{q^{4k}}$ and

$$\mathbb{F}_{q^n} \subset \mathbb{F}_{q^{4k}}.$$

Hence $4k \equiv 0 \pmod n$ and $k = n/4$ or $k = 3n/4$. We cannot have $k = n/2$. In fact, if P has degree $4m$ and divides Z_{2m}, then we have

$$g^{q^{2m}} = -ig.$$

This implies

$$g^{q^{4m}} = -ig^{q^{2m}} = -g$$

and this is impossible. □

Suppose now that $P^{(1,2,3,4)} = P$ and that $\deg P = 4m$. If P divides Z_k, we say that P has type 1. Otherwise, if P divides Z_{3k}, we say that has type 3.

Proposition 2.3.5. *P and $P^{(1,3)}$ have different types.*

Proof. Suppose P has type 1 and let g be one of its roots. We have

$$g^{q^m} = -ig.$$

Then $h = ig^{-1}$ is a root of $P^{(1,3)}$ and

$$h^{-q^m} = -ih^{-1}.$$

Therefore

$$h^{q^m} = ih$$

and

$$h^{q^{3m}} = -ih.$$

Hence $P^{(1,3)}|Z_{3k}$ and $P^{(1,3)}$ has type 3. If P has type 3 we have similar computations. □

Corollary 2.3.6. *Among all polynomials fixed by $(1, 2, 3, 4)$ half divides Z_m and half divides Z_{3m}.*

We also note that Z_k has not multiple roots since is derivative has only 0 as root.

Theorem 2.3.7. *Let P be an irreducible polynomial of degree $4m$. Then $P|Z_k$ if and only if $P = P^{(1,2,3,4)}$, m divides k and the type of P is congruent to k/m modulo 4.*

Proof. We know that if $P|Z_k$, then $P = P^{(1,2,3,4)}$. Since $g^{q^{4k}} = g$ and the degree of P is $4m$ we have

$$\mathbb{F}_{q^{4m}} \subset \mathbb{F}_{q^{4k}}$$

and $m|k$. Write $k = ml$ and suppose P is of type t. Then

$$g^{q^{tm}} = -ig = g^{q^k} = g^{q^{ml}}.$$

Therefore

$$mt \equiv ml \pmod{4m}$$

and

$$t \equiv l \pmod{4}.$$

Conversely, suppose $P = P^{(1,2,3,4)}, \deg P = 4m$ and P has type t. Write $k = ml$ with $l \equiv t \pmod 4$. Hence, if g is a root of P

$$g^{q^k} = g^{q^{ml}} = g^{q^{mt}} = -ig$$

and therefore $P|Z_k$. □

Now we can count orbits of such polynomials.

Theorem 2.3.8. *We have*

$$q^k - 1 = \sum_{d|k,\ \frac{k}{d} \not\equiv 0,2 \pmod 4} 4dG_6(4d).$$

Proof. Let EZ_k be the set of all irreducible polynomials of degree greater than 2 dividing Z_k. From Theorem 2.3.7 we have

$$EZ_k = \bigcup_{d|k,\ \frac{k}{d} \equiv 1 \pmod 4} EZ_1(4d) \cup \bigcup_{d|k,\ \frac{k}{d} \equiv 3 \pmod 4} EZ_3(4d),$$

where $EZ_i(4d)$ is the set of all irreducible polynomials of degree $4d$ and type i dividing Z_k. This implies

$$\sum_{Q \in EZ_k} \deg Q = \sum_{d|k,\ \frac{k}{d} \equiv 1 \pmod 4} 4d|EZ_1(4d)| + \sum_{d|k,\ \frac{k}{d} \equiv 3 \pmod 4} 4d|EZ_3(4d)|.$$

According to Corollary 2.3.6 we have

$$\sum_{Q \in EZ_k} \deg Q = \sum_{d|k,\ \frac{k}{d} \equiv 1 \pmod 4} 4dG_{6,1}(4d) + \sum_{d|k,\ \frac{k}{d} \equiv 3 \pmod 4} 4dG_{6,1}(4d).$$

Finally

$$\sum_{Q \in EZ_k} \deg Q = \sum_{d|k,\ \frac{k}{d} \not\equiv 0,2 \pmod 4} 4dG_{6,1}(4d).$$

Since

$$\sum_{Q \in EZ_k} \deg Q = q^k - 1 = \deg Z_k,$$

the proof is complete. □

Using Möbius inversion we obtain the following result.

Theorem 2.3.9. *$G_{6,1}(n) = 0$ if $n \not\equiv 0 \pmod 4$. Otherwise, if $n = 4m$, we have*

$$G_{6,1}(4m) = \frac{1}{4m} \sum_{d|m,\ d \not\equiv 0,2 \pmod 4} \mu(d)(q^{\frac{m}{d}} - 1).$$

Subgroup H_2

We have that P is fixed by $(1,3) = x \mapsto i/x$ and $(2,4) = x \mapsto -i/x$.
If g is a root of P we have

$$g^{q^l} = \frac{i}{g} \text{ and } g^{q^k} = -\frac{i}{g},$$

with $0 \leq k, l < n = \deg P$. Hence

$$g^{q^{2l}} = g^{q^{2k}} = g$$

and this implies

$$2l \equiv 2k \equiv 0 \pmod n.$$

If $k = 0$ or $l = 0$ we have that g is a root of $x^2 + i$ or $x^2 - i$. If $k = l = n/2$ we have

$$\frac{i}{g} = -\frac{i}{g}$$

and that is not possible. We note that $x^2 - i$ and $x^2 + i$ are in the same orbit, hence we obtain the following result.

Theorem 2.3.10. *$G_{6,2}(n) = 1$ if and only if $n = 2$ and both $x^2 - i$ and $x^2 + i$ are irreducible, i.e. when $q \equiv 5 \pmod 8$. Otherwise $G_{6,2}(n) = 0$.*

2.3.4 Orbits of size eight

There is only one conjugacy class of subgroups of order 3, i.e. $(1,2,3)$. Thus, for the rest of the section P would be an irreducible polynomial fixed by this permutation.

Proposition 2.3.11. *If P is fixed by $\tau = (1,2,3)$, which corresponds to pre-composition with the rational function $x \mapsto (-x+i)/(-x-i)$, then P is an irreducible factor of*

$$L_k(x) = x^{q^k}(-ix + i) + x + 1.$$

If P is fixed by σ, then $P = x^2 + x(i-1) + i$ or $\deg P \equiv 0 \pmod 3$ and, if $\deg P = 3m$, then $P|L_m$ or $P|L_{2m}$.

Proof. If g is a root of P, then $\frac{-g-1}{-ig+i}$ is a root of P^τ. If P is an irreducible factor of L_k, then we clearly have

$$g^{q^k} = \frac{-g-1}{-ig+i}.$$

Hence the set of the roots if P is invariant under

$$T : g \mapsto \frac{-g-1}{-ig+i}$$

and $P^\tau = P$. Suppose now that $P^\tau = P$. Then we have

$$g^{q^k} = \frac{-g-1}{-ig+i},$$

with $0 \leq k < n = \deg P$. Therefore $P|L_k$. T has order 3. If T fixes one root of P, then g is a root of $x^2 + x(i-1) + i$. Otherwise it permutes the roots of P and we have that $\deg P \equiv 0 \pmod 3$. Since

$$g^{q^{3k}} = g,$$

we have that $g \in \mathbb{F}_{q^{3k}}$ and

$$\mathbb{F}_{q^n} \subset \mathbb{F}_{q^{3k}}.$$

Hence $3k \equiv 0 \pmod n$ and $k = n/3$ or $k = 2n/3$. □

Suppose that $P^{(1,2,3)} = P$ and that $\deg P = 3m$. If P divides L_k we say that P has type 1. Otherwise, if P divides L_{2k}, we say that P has type 2.

Proposition 2.3.12. *P and $P^{(1,3)}$ have different types.*

Proof. Suppose P has type 1 and let g be one of its roots. We have

$$g^{q^m} = \frac{-g-1}{-ig+i}.$$

Then $h = ig^{-1}$ is a root of $P^{(1,3)}$ and

$$h^{-q^m} = \frac{-i-h}{i-h}.$$

Hence

$$h^{q^m} = \frac{i-h}{-i-h}$$

and

$$h^{q^{2m}} = \frac{-h-1}{-ih+i}.$$

Hence $P^{(1,3)}|L_{2k}$ and $P^{(1,3)}$ has type 2. If P has type 2 we have similar computations. □

Corollary 2.3.13. *Among all polynomials fixed by* $(1,2,3)$ *half divides* L_m *and half divides* L_{2m}.

We also note that L_k has not multiple roots since its derivative is $-ix^{q^k}+1$ and is coprime with L_k.

Proposition 2.3.14. *If* $P = x^2 + x(i-1) + i$ *is irreducible, then* $P|L_k$ *if and only if* k *is even. If it is reducible, then it divides* L_k *for every* k.

Proof. Suppose g is a root of P. Then we have $g^{q^2} = g$. If k is even we have that $g^{q^k} = g$. Substituting we obtain $L_k(g) = 0$ and therefore P always divides L_k when k is even. If k is odd we have $g^{q^k} = g^q$. Substituting in L_k we get $L_k(g) = 0$ if and only if $(g^2 - g)(g^{q-1} - 1) = 0$. Hence if and only if $g^{q-1} - 1$, if and only if $g \in \mathbb{F}_q$ and P is reducible. □

Theorem 2.3.15. *Let* P *be an irreducible polynomial of degree* $3m$. *Then* $P|L_k$ *if and only if* $P = P^{(1,2,3)}$, m *divides* k *and the type of* P *is congruent to* k/m *modulo* 3.

Proof. We know that if $P|L_k$, then $P = P^{(1,2,3)}$. Since $g^{q^{3k}} = g$ and the degree of P is $3m$, we have

$$\mathbb{F}_{q^{3m}} \subset \mathbb{F}_{q^{3k}}$$

and $m|k$. Write $k = ml$ and suppose P is of type t. Then

$$g^{q^{tm}} = \frac{-g-1}{-ig+i} = g^{q^k} = g^{q^{ml}}.$$

Thus

$$mt \equiv ml \pmod{3m}$$

and

$$t \equiv l \pmod{3}.$$

Conversely, suppose $P = P^{(1,2,3)}, \deg P = 3m$ and P has type t. Write $k = ml$ with $l \equiv t \pmod 3$. Hence, if g is a root of P we have

$$g^{q^k} = g^{q^{ml}} = g^{q^{mt}} = \frac{-g-1}{-ig+i}$$

and thus $P|L_k$. □

Now we can count orbits of such polynomials.

Theorem 2.3.16. *If* $x^2 + (i-1)x + i$ *is reducible, i.e. if* $-6i$ *is a square in* $\mathbb{F}_q$, *then*

$$q^k - 1 = \sum_{d|k,\ \frac{k}{d} \not\equiv 0 \pmod 3} 3dG_8(3d).$$

Otherwise, we have

$$q^k - (-1)^k = \sum_{d|k,\ \frac{k}{d} \not\equiv 0 \pmod 3} 3dG_8(3d).$$

Proof. Let EL_k be the set of all irreducible polynomials of degree greater than 2 dividing L_k. From Theorem 2.3.15 we have

$$EL_k = \bigcup_{d|k, \frac{k}{d}\equiv 1 \pmod 3} EL_1(3d) \cup \bigcup_{d|k, \frac{k}{d}\equiv 2 \pmod 3} EL_2(3d),$$

where $EL_i(3d)$ is the set of all irreducible polynomials of degree $3d$ and type i dividing L_k. This implies

$$\sum_{Q\in EL_k} \deg Q = \sum_{d|k,\ \frac{k}{d}\equiv 1 \pmod 3} 3d|EL_1(3d)| + \sum_{d|k,\ \frac{k}{d}\equiv 2 \pmod 3} 3d|EL_2(3d)|.$$

According to Corollary 2.3.13, we have

$$\sum_{Q\in EL_k} \deg Q = \sum_{d|k,\ \frac{k}{d}\equiv 1 \pmod 3} 3dG_8(3d) + \sum_{d|k,\ \frac{k}{d}\equiv 2 \pmod 3} 3dG_8(3d).$$

Finally

$$\sum_{Q\in EL_k} \deg Q = \sum_{d|k,\ \frac{k}{d}\not\equiv 0 \pmod 3} 3dG_8(3d).$$

Since

$$\sum_{Q\in EZ_k} \deg Q = \begin{cases} q^k - 1 & \text{if } x^2 + (i-1)x + i \text{ is reducible,} \\ q^k - (-1)^k & \text{otherwise,} \end{cases}$$

the proof is complete. □

Using Möbius inversion we obtain the following result.

Theorem 2.3.17. *$G_8(n) = 0$ if $n \not\equiv 0 \pmod 3$. Let $n = 3m$. Then we have*

$$G_8(3m) = \frac{1}{3m} \sum_{d|m,\ d\not\equiv 0 \pmod 3} \mu(d)(q^{\frac{m}{d}} - 1)$$

if $x^2 + (i-1)x + i$ is reducible and

$$G_8(3m) = \frac{1}{3m} \sum_{d|m,\ d\not\equiv 0 \pmod 3} \mu(d)(q^{\frac{m}{d}} - (-1)^{\frac{m}{d}})$$

otherwise.

2.3.5 Orbits of size twelve

We have 2 conjugacy classes of subgroups of order 2, namely $H_1 =< (1,4)(2,3) >$ and $H_2 =< (1,3) >$. We consider each one of them in order.

Subgroup H_1

A polynomial P is fixed by $(1,4)(2,3) = x \mapsto 1/x$ if and only if it is self-reciprocal. First of all, we note that there are 3 subgroups of $\mathcal{S}_4$ conjugate to H_1. Since the orbit will have length 12 it means that 4 polynomials fixed by $(1,4)(2,3)$ lie in the same orbit. Therefore if we consider the total number of self-reciprocal polynomials, the number of the orbits of length 12 would be that number divided by 4.
Let us start considering polynomials of degree 2. We know that the number of self-reciprocal polynomials of degree 2 is

$$\frac{q-1}{2}.$$

We know that the two polynomials $x^2 \pm i$ are fixed by $(1,3)(2,4)$, which corresponds to pre-composition with the rational function $x \mapsto -x$. Therefore there are two polynomials in their orbit that are fixed by H_1, but their orbit has length 6. Hence we do not consider these two polynomials if they are irreducible and we obtain the following result.

Theorem 2.3.18.

$$G_{12,1}(2) = \frac{1}{4}\left(\frac{q-1}{2} - 2\right) = \frac{q-5}{8}$$

if $x^2 \pm i$ are irreducible, i.e. if $q \equiv 5 \pmod 8$ and

$$G_{12,1}(2) = \frac{1}{4}\frac{q-1}{2} = \frac{q-1}{8}$$

if $q \equiv 1 \pmod 8$.

Now consider self-reciprocal polynomials of degree $2n$, with n odd. If they are fixed by some element of the group, then they are fixed by a subgroup of order at least 8, which, as we have seen, fixes no polynomials.

Theorem 2.3.19.

$$G_{12,1}(2n) = \frac{1}{8n} \sum_{d|n,\ d\equiv 1 \pmod 2} \mu(d) q^{\frac{n}{d}},$$

with $n \equiv 1 \pmod 2, n \geq 3$.

Suppose now that the degree of P is a multiple of 4. We know that some of the self-reciprocal polynomials of degree $4m$ are fixed by a permutation of order 4, hence their orbits will have length 6. To obtain the total number of orbits of length 12 we have to exclude these latter polynomials.

Theorem 2.3.20. *We have*

$$G_{12,1}(4n) = \frac{1}{4}\left(\frac{1}{4n}(q^{2n}-1) - \frac{1}{2n}\sum_{d|n,\ d\not\equiv 0,2 \pmod 4} \mu(d)(q^{\frac{m}{d}}-1)\right)$$

if $n = 2^s$ *and*

$$G_{12,1}(4n) = \frac{1}{4}\left(\frac{1}{4n}\sum_{d|2n,\ d\equiv 1 \pmod 2\mu(d)} q^{\frac{2n}{d}} - \frac{1}{2n}\sum_{d|n,\ d\not\equiv 0,2 \pmod 4} \mu(d)(q^{\frac{m}{d}}-1)\right)$$

otherwise.

Subgroup H_2

We have 6 subgroups conjugate to $(1,3)$. Hence in an orbit of length 12 there are 2 polynomials fixed by each subgroup. We consider the polynomials fixed by $(1,3)$, which corresponds to pre-composition with the rational function $x \mapsto i/x$.
In order to conclude we will use 1.2.7, the generalization of Carlitz's Theorem, which we proved in the previous chapter.
Suppose now that P has degree 2. We know that $P = x^2 + (i-1)x + i$ is fixed by $(1,3)$ and $(1,2,3)$ and its orbit will have length 4. If we consider $P^{(2,4)}$ we know that it is fixed by $(1,3)$ and $(1,4,3)$ and its orbit has length 4. Hence we discard these two polynomials. If $x^2 \pm i$ are irreducible, also these have orbits of length not equal to 12.

Theorem 2.3.21.

$$G_{12,2}(2) = \frac{q-5}{4}$$

if $x^2 + (i-1)x + i$ *is irreducible and*

$$G_{12,2}(2) = \frac{q-1}{4}$$

otherwise.

Proof. Suppose that $x^2 - i$ and $x^2 + i$ are irreducible. We know that $\tilde{S}_q(2) = (q+1)/2$. We know that $x^2 + i$ is $\mathcal{I}_\sigma$ and we have to discard it. Therefore we are left with $(q-1)/2$ polynomials fixed by $x \mapsto i/x$. As we said before, we have to discard $P = x^2 + (i-1)x + i$ and $P^{(2,4)}$ if and only if they are irreducible, and this concludes the proof when $x^2 - i$ is irreducible.
Suppose now $x^2 - i$ is reducible. We have $\tilde{S}_q(2) = (q-1)/2$. Considering $x^2 + (i-1)x + i$ we can conclude as before. □

Suppose now that the degree of P is $2n$, with $n \geq 2$. We have seen in the previous sections that there are no polynomials of degree greater than

2 fixed by $(1,3)$ and some other element of the group. Thus the number of orbits of these polynomials is just half of the number of the irreducible factor of $x^{q^k+1} - i$ of degree $2n$. From what we have said we have the following result.

Theorem 2.3.22.

$$G_{12,2}(2n) = \frac{1}{4n}(q^n - 1)$$

if $n = 2^s$ *and*

$$G_{12,2}(2n) = \frac{1}{4n}\left(\sum_{d|n,\ d\equiv 1 \pmod 2} \mu(d) q^{\frac{n}{d}}\right)$$

otherwise.

2.3.6 24 elements orbit

The remaining polynomials form orbits with 24 elements.

Theorem 2.3.23. *If* $n \geq 2$ *we have*

$$G_{24}(n) = \frac{1}{24}\left(I(n) - \sum_{d|24} d G_d(n)\right),$$

where

$$I(n) = \frac{1}{n}\sum_{d|n} \mu(d) q^{\frac{n}{d}}$$

is the number of total irreducible monic polynomials of degree n*.*

2.4 The action of $\mathcal{A}_4$

To obtain $\mathcal{A}_4$ we consider only the even permutations of the previous section. With the same proofs we obtain the following results:

Theorem 2.4.1. *Let* $P = x^2 + (i-1)x + i$*.*

1. *The number of orbits having length* 1 *or* 3 *is always zero.*
2. $$G_4(2) = 1 \text{ if and only if } n = 2 \text{ and } P \text{ is irreducible,}$$

$$G_4(3m) = \frac{2}{3m}\sum_{d|m,\ d\neq 0 \pmod 3} \mu(d)\left(q^{\frac{m}{d}} - 1\right) \text{ if } P \text{ is reducible,}$$

$$G_4(3m) = \frac{2}{3m} \sum_{d|m,\ d\not\equiv 0 \pmod 3} \mu(d)\left(q^{\frac{m}{d}} - (-1)^{\frac{m}{d}}\right) \text{ if } P \text{ is irreducible.}$$

3.

$$G_{12}(2m) = \frac{1}{4m}(q^m - 1)$$

if $m = 2^s$ and

$$G_{12}(2m) = \frac{1}{4m} \sum_{d|m,\ d\equiv 1 \pmod 2} \mu(d) q^{\frac{m}{d}}$$

otherwise.

2.5 The action of $\mathcal{A}_5$

We conclude considering the Icosahedral group (isomorphic to $\mathcal{A}_5$), which, as in [Tot02], consists of the following 60 elements:

$$x \mapsto \omega^i x, \qquad x \mapsto -\frac{1}{\omega^i x}, \qquad x \mapsto \omega^i \frac{-(\omega-\omega^4)\omega^k x + (\omega^2-\omega^3)}{(\omega^2-\omega^3)\omega^k x + (\omega-\omega^4)},$$

$$x \mapsto \omega^i \frac{(\omega^2-\omega^3)\omega^k x + (\omega-\omega^4)}{(\omega-\omega^4)\omega^k x - (\omega^2-\omega^3)},$$

with $i, j \in \{0, \dots, 4\}$ and where ω is a (primitive) fifth-root of unity. In the rest of the section we will assume $q \equiv 1 \pmod 5$.
A particular isomorphism of $\mathcal{A}_5$ with this group is determined by

$$(1,2,3,4,5) \mapsto (x \mapsto \omega x),$$

$$(1,5,4,2,3) \mapsto \left(x \mapsto \omega \frac{(\omega^2-\omega^3)x + (\omega-\omega^4)}{(\omega-\omega^4)x - (\omega^2-\omega^3)}\right).$$

We note that in $\mathcal{A}_5$ there is only one conjugacy class of subgroups of index $5, 6, 10, 12, 15, 20$ and 30.

Theorem 2.5.1. *There are no orbits of length* $1, 5$ *or* 6.

Proof. In the first and in the third case we consider the two involutions $x \mapsto -1/x$ and $x \mapsto -1/\omega x$ and we note that, as in the proof of 2.3.1, no polynomial can be fixed by both elements. Since the subgroup generated by

these two elements and $x \mapsto \omega x$ has order 10 we can conclude. Regarding orbits of length 5 we consider the two involutions $x \mapsto -1/\omega^2 x$ and

$$x \mapsto \omega^4 \frac{(\omega^2-\omega^3)\omega x + (\omega-\omega^4)}{(\omega-\omega^4)\omega x - (\omega^2-\omega^3)},$$

and conclude in the same way noting that $x^2+\omega^3$ is fixed by these two elements but not by

$$x \mapsto \omega^2 \frac{-(\omega-\omega^4)\omega^2 x + (\omega^2-\omega^3)}{(\omega^2-\omega^3)\omega^2 x + (\omega-\omega^4)},$$

which is another element of the subgroup of order 12 we are considering. □

Theorem 2.5.2. *$G_{10}(m) = 1$ if and only if $m = 2$ and $x^2 - (1+\omega)^2 x - \omega^2$ is irreducible.*

Proof. We consider the involutions $x \mapsto -1/\omega^3 x$ and $x \mapsto \omega^4 \frac{(\omega^2-\omega^3)\omega x+(\omega-\omega^4)}{(\omega-\omega^4)\omega x-(\omega^2-\omega^3)}$. They generate a subgroup of order 6. Suppose a polynomial P is fixed by the two involutions. If g is a root of P we must have

$$g^{q^l} = -\frac{1}{\omega^3 x} \quad \text{and} \quad g^{q^k} = -\frac{\omega^2 x + \omega^2 + \omega + 1}{(\omega+1)x + \omega^2},$$

with $0 \le k, l < n = \deg P$. Hence

$$g^{q^{2l}} = g^{q^{2k}} = g$$

and this implies

$$2l \equiv 2k \equiv 0 \pmod{n}.$$

If $l = 0$ or $k = 0$ we obtain two polynomials of degree 2, fixed by one involution, but not by the other one. Hence we must have $k = l = n/2$ and we obtain $x^2 - (\omega+1)^2 - \omega^2$. □

Theorem 2.5.3. *We have*

$$G_{12}(5m) = \frac{2}{5m} \sum_{d|m,\ d \not\equiv 0 \pmod 5} \mu(d) \left(q^{m/d} - 1\right).$$

Proof. This is Theorem 2.2.6 with $r = 5$ applied to the map $x \mapsto \omega x$. □

Theorem 2.5.4. *We have $G_{15}(m) = 1$ if and only if $m = 2$ and $x^2 + \omega^3$ is irreducible, i.e. $q \not\equiv 1 \pmod 4$.*

Proof. We consider the involutions $x \mapsto -1/\omega^2 x$ and

$$x \mapsto \omega^4 \frac{(\omega^2-\omega^3)\omega x + (\omega-\omega^4)}{(\omega-\omega^4)\omega x - (\omega^2-\omega^3)},$$

which generate a subgroup of order 4. Suppose a polynomial P is fixed by the two involutions. If g is a root of P we must have

$$g^{q^l} = -\frac{1}{\omega^2 x} \quad \text{and} \quad g^{q^k} = -\frac{\omega^2 x + \omega^2 + \omega + 1}{(\omega+1)x + \omega^2},$$

with $0 \leq k, l < n = \deg P$. Hence

$$g^{q^{2l}} = g^{q^{2k}} = g$$

and this implies

$$2l \equiv 2k \equiv 0 \pmod{n}.$$

If $l = 0$ we obtain the polynomial $x^2 + \omega^3$, which is fixed by the two involutions. If $k = 0$ we obtain another polynomial of degree 2 which is in the orbit of $x^2 + \omega^3$, thus one is irreducible if and only if the other one is. If $k = l = n/2$ we obtain another polynomial of degree 2, still in the same orbit, namely $x^2 - (\omega+1)^2 - \omega^2$. □

Now we study orbits of length 20. We consider the rational transformation τ of order 3 given by

$$x \mapsto \omega^2 \frac{-(\omega - \omega^4)\omega^2 x + (\omega^2 - \omega^3)}{(\omega^2 - \omega^3)\omega^2 x + (\omega - \omega^4)}.$$

Theorem 2.5.5. *The polynomials invariant under the previous transformation are the irreducible factors of*

$$B_{q,k}(x) = x^{q^k+1} - (\omega^4+1)x^{q^k} - \omega(\omega^4+1)x - 1$$

for $k \in \mathbb{N}$. If $P = P^\tau$, $\deg P \geq 2$, then $\deg P \equiv 0 \pmod 3$ or $P = x^2 - (\omega^4 + 1)(\omega+1)x - 1$ (if irreducible). If $\deg P = 3m$ then $P | B_{q,m}$ or $P | B_{q,2m}$.

Proof. If g is a root of P then $\dfrac{(\omega - \omega^4)g + 1 - \omega^4}{(1-\omega^4)g + \omega^3 - 1}$ is a root of P^τ. Let P be an irreducible factor of $B_{q,k}$. Then a root g of P is a root of $B_{q,k}$, hence

$$g^{q^k} = \frac{(\omega - \omega^4)g + 1 - \omega^4}{(1-\omega^4)g + \omega^3 - 1}.$$

This implies that the set of roots of P is invariant under the map

$$T : g \mapsto \frac{(\omega - \omega^4)g + 1 - \omega^4}{(1-\omega^4)g + \omega^3 - 1}$$

and $P = P^\tau$. Conversely, suppose $P = P^\tau$ and g one of his roots. Then

$$g^{q^k} = \frac{(\omega - \omega^4)g + 1 - \omega^4}{(1-\omega^4)g + \omega^3 - 1},$$

with $0 \leq k < n = \deg P$. Hence P divides $B_{q,k}$. If the map T let a root of P invariant we obtain the polynomial $x^2 - (\omega + 1)(\omega^1)x - 1$. Otherwise the map T has order 3 and permutes the roots of P. Consequently we have $\deg P \equiv 0 \pmod 3$. We have that

$$g^{q^{3k}} = g$$

and therefore $g \in \mathbb{F}_{q^{3k}}$. From the fact that $\deg P = n$ we have that

$$\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^{3k}}.$$

This implies $3k \equiv 0 \pmod n$ and finally $k = \frac{in}{3}, 1 \leq i \leq 2$. □

Suppose now that P is irreducible, that $P = P^\tau$ and that it has degree $3m$. If P divides $B_{q,m}$, we say that P is of type 1. Otherwise, if P divides $B_{q,2m}$, we say P is of type 2.

With a proof similar to Proposition 2.1.4 we obtain the following result.

Proposition 2.5.6. *Let σ be the transformation $x \mapsto -1/x$. Suppose $P = P^\tau$. Then P and P^σ have different types.*

Corollary 2.5.7. *Among polynomials of degree $3m$ such that $P = P^\tau$, half divides $B_{q,m}$ and the other half divides $B_{q,2m}$.*

We note that $B_{q,k}$ has no multiple roots.

Proposition 2.5.8. *Let $P = x^2 - (\omega^4 + 1)(\omega + 1)x - 1$. Then, if P is reducible over $\mathbb{F}_q$ we have $P|B_{q,k}$ for every k. If P is irreducible over $\mathbb{F}_q$, then $P|B_{q,k}$ if and only if k is even.*

Proof. Let α be a root of P. Then $\alpha^{q^2} = \alpha$. If k is even then $\alpha^{q^k+1} = \alpha^2$ and $B_{q,k}(\alpha) = 0$.
If k is odd then $\alpha^{q^k+1} = \alpha^{q+1}$. We have $B_{q,k}(\alpha) = 0$ if and only if $(\alpha^{q-1} - 1)(\alpha^2 - \alpha(\omega^4 + 1)) = 0$ if and only if $a^{q-1} = 1$ if and only if $\alpha \in \mathbb{F}_q$. □

With a similar proof to Theorem 2.1.8 we obtain the following result.

Theorem 2.5.9. *Let P be an irreducible polynomial of degree $3m$. Then $P|B_{q,k}$ if and only if $P = P^\tau$, m divides k and the type of P is congruent to k/m modulo 3.*

Theorem 2.5.10. *Consider $G_{20}(3m)$, $m \geq 1$. For every $k \geq 1$ we have*

$$q^k - (-1)^k = \sum_{d|k,\ \frac{k}{d} \not\equiv 0 \pmod 3} 3dG_{20}(3d),$$

if $x^2 - (\omega^4 + 1)(\omega + 1)x - 1$ is irreducible. Otherwise we have

$$q^k - 1 = \sum_{d|k,\ \frac{k}{d} \not\equiv 0 \pmod 3} 3dG_{20}(3d).$$

Proof. Let EB_k be the set of all irreducible polynomials of degree greater than 2 dividing $B_{q,k}$. From the previous theorem we have

$$E_k = \bigcup_{d|k,\ \frac{k}{d}\equiv 1 \pmod 3} ES_1(3d) \cup \bigcup_{d|k,\ \frac{k}{d}\equiv 2 \pmod 3} ES_2(3d),$$

where $ES_i(3d)$ is the set of all irreducible anti-invariant polynomials of degree $3d$ and type i dividing $B_{q,k}$. This implies

$$\sum_{Q\in EB_k} \deg Q = \sum_{d|k,\ \frac{k}{d}\equiv 1 \pmod 3} 3d|ES_1(3d)| + \sum_{d|k,\ \frac{k}{d}\equiv 2 \pmod 3} 3d|ES_2(3d)|.$$

According to Corollary 2.5.7 we have

$$\sum_{Q\in EB_k} \deg Q = \sum_{d|k,\ \frac{k}{d}\equiv 1 \pmod 3} 3dG_{20}(3d) + \sum_{d|k,\ \frac{k}{d}\equiv 2 \pmod 3} 3dG_{20}(3d).$$

Finally

$$\sum_{Q\in EB_k} \deg Q = \sum_{d|k,\ \frac{k}{d}\not\equiv 0 \pmod 3} 3dG_{20}(3d).$$

According to Proposition 2.5.8 we have

$$\sum_{Q\in EB_k} \deg Q = \begin{cases} q^k - (-1)^k & \text{if } x^2 - (\omega^4+1)(\omega+1)x - 1 \text{ is irreducible,} \\ q^k - 1 & \text{if } x^2 - (\omega^4+1)(\omega+1)x - 1 \text{ is reducible.} \end{cases}$$

□

Using Möbius inversion we obtain the following result.

Theorem 2.5.11. *$G_{20}(n) = 0$ if $n \not\equiv 0 \pmod 3$. Let $n = 3m$. Then we have*

$$G_{20}(3m) = \frac{1}{3m} \sum_{d|m,\ d\not\equiv 0 \pmod 3} \mu(d) \left(q^{m/d} - (-1)^{m/d}\right),$$

if $x^2 - (\omega^4+1)(\omega+1)x - 1$ is irreducible and

$$G_{20}(3m) = \frac{1}{3m} \sum_{d|m,\ d\not\equiv 0 \pmod 3} \mu(d) \left(q^{m/d} - 1\right)$$

otherwise.

Finally we note that $x^2 - (\omega^4+1)(\omega+1)x - 1$ and $x^2 - (\omega+1)^2 - \omega^2$ are in the same orbit, hence one is irreducible if and only if the other one is.

Considering now orbits of length 30 we have the following result.

Theorem 2.5.12. *We have*

$$G_{30}(2) = \frac{1}{4}(q - (-1)^{(q-1)/2}) - G_{10}(2) - G_{15}(2)$$

and

$$G_{30}(2m) = \frac{1}{4m}\left(q^m - 1\right)$$

if $m = 2^s, s \geq 2$ *and*

$$G_{30}(2m) = \frac{1}{4m} \sum_{d|m,\ d\equiv 1 \pmod 2} \mu(d) q^{m/d}$$

otherwise.

Proof. We consider the involution $x \mapsto -1/x$ and we use Theorem 1.2.7 in order to compute the number of polynomials fixed by it. If the degree of the polynomials is 2, we note that we have to exclude polynomials of that degree having orbits of length 10 and 15 and to consider whether x^2+1 is irreducible or not. If the degree is greater than 2 we know from the previous results that there is no polynomial of this degree fixed by an involution and another element of the group. Therefore the number of orbits is just half of the number of polynomials fixed by $x \mapsto -1/x$ because there are 15 conjugate subgroups of order 2, hence polynomials fixed by that involution come in pairs in the same orbit. □

2.6 General results

In this section we include some general results (of which existence we were unaware at the moment we were working on our results), obtained by Stichtenoth and Topuzoglu in [ST12]. While we focused our attention on specifics subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ and were able to obtain specific counting results for these cases, the two authors consider general subgroups of the projective linear group of dimension two. The goal of their paper is to obtain asymptotic enumerations results on the number of irreducible factors of a certain class of polynomials, generalizing known results, such as the number of irreducible self-reciprocal polynomials. We also recall the paper [Gar11], in which the author obtains results considering triangular and diagonal matrices.

We start with the following result.

Theorem 2.6.1. *Let* H *be a subgroup of* $\mathrm{PGL}_2(\mathbb{F}_q)$ *of order* $D \geq 2$*. Assume that* $f \in \mathcal{I}_n$ *is invariant under* H*, i.e.* $B \circ f = f$ *for every* $B \in H$*. Then either* $n = 2$ *or* n *is divisible by* D*.*

We showed (for example in the section of dihedral groups) that this result holds for cyclic groups. Here we see that it remains true in a more general context.

Corollary 2.6.2. *Suppose that $n \geq 2$ is relatively prime to $q(q^2-1)$. Then all orbits of $\mathcal{I}_n$ under the action of $\mathrm{PGL}_2(\mathbb{F}_q)$ have length $q(q^2-1)$.*

In their work they consider an action dual to the one we considered, namely to the matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$ they associate the following action:

$$A \circ f = (bx+d)^n f\left(\frac{ax+c}{bx+d}\right),$$

where $n = \deg f$.
To a matrix A of the previous form they associate the following polynomial

$$F_r(x) = bx^{q^r+1} - ax^{q^r} + dx - c.$$

It is shown that this polynomial is separable and that we have the following result.

Theorem 2.6.3. *Let $f \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree $n \geq 2$. The following are equivalent:*

1. *$f | F_r$, for some $r \geq 0$,*

2. *$A \circ f = f$.*

Corollary 2.6.4. *For every $A \in \mathrm{PGL}_2(\mathbb{F}_q)$ there exist infinitely many A-invariant irreducible polynomials in $\mathbb{F}_q[x]$.*

We can be more precise about the integer r occurring in Theorem 2.6.3 at point 1.

Theorem 2.6.5. *Let f be an A-invariant irreducible polynomial of degree $n \geq 2$ and suppose that $f(x) | F_r(x)$. Then the following holds:*

1. *For any integer $t \geq 0$ we have*

$$f(x) | F_t(x) \Leftrightarrow t \equiv r \pmod{n}.$$

Hence there is a unique $s \in \{0, 1, \ldots n-1\}$ such that $f(x) | F_s(x)$.

2. *If $n \geq 3$, then the order D of A divides n and*

$$r = m \cdot \frac{n}{D} \text{ with some integer } m \text{ satisfying } \gcd(m, D) = 1.$$

Hence the unique s of the previous point has the form

$$s = l \cdot \frac{n}{D} \quad \text{with } 1 \leq l \leq D-1 \text{ and } \gcd(l, D) = 1.$$

Using Theorem 2.6.5 we can obtain the following result.

Proposition 2.6.6. *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree $n \geq 2$. Suppose that $A \circ f = f$ for all $A \in \mathrm{PGL}_2(\mathbb{F}_q)$. Then $q = 2$ and $f = x^2 + x + 1$. Conversely, the polynomial $x^2 + x + 1$ is irreducible and invariant under $\mathrm{PGL}_2(\mathbb{F}_2)$.*

The two authors proved also some asymptotic results about the irreducible factors of $F_r(x)$. Define

$$\lambda(A, r) = |\{f \in \mathbb{F}_q[x] |\, f \text{ is irreducible, monic, } \deg f = Dr \text{ and } f | F_r(x)\}|.$$

Theorem 2.6.7. *Let $A \in \mathrm{PGL}_2(\mathbb{F}_q)$ and suppose A has order $D \geq 2$. Then we have*

$$\lambda(A, r) \approx \frac{q^r}{Dr} \quad \text{as} \quad r \to \infty.$$

In other words, almost all irreducible factors of $F_r(x)$ have degree Dr, for large values of r.

We obtain also an asymptotic formula for A-invariant polynomials. We define

$$\mu(A, n) = |\{f \in \mathbb{F}_q[x] | f \text{ is irreducible, monic, } \deg f = n \text{ and } A \circ f = f\}|.$$

Theorem 2.6.8. *Let $A \in \mathrm{PGL}_2(\mathbb{F}_q)$ and suppose A has order $D \geq 1$. Then we have*

$$\mu(A, r) \approx \phi(D) \cdot \frac{q^n}{Dn} \quad \text{as} \quad n \to \infty.$$

Chapter 3

Generalizing self-reciprocal polynomials

This chapter is completely devoted to present some results obtained with Sandro Mattarei. Starting from [Ahm11], we generalized some of its results. The original article deals with the transformation of irreducible polynomials by rational quadratic maps. The author considers irreducible polynomials that preserve this property after the transformation. This can be considered as a generalization of the concept of self-reciprocal polynomials, in fact the author recovers the number of these polynomials with his methods. In the first section of this chapter we use another method, namely certain canonical forms of rational quadratic maps, in order to recover Ahmadi's results. In the second section, according to our method, we are able to extend some of the results in the case of cubic rational maps. In the last section we give some counting results for polynomials transformed by cubic maps. It is worth mentioning the beautiful paper of Cohen, [Coh69], in which he recovered, using different techniques, the same results of Carlitz on the number of self-reciprocal polynomials and studied transformation of polynomials by maps of higher degrees.

3.1 A first generalization

We briefly present Ahmadi's results from [Ahm11]. We start with a simple known result, which motivated the idea behind his work.

Lemma 3.1.1. *Let K be a field and let $g(x) \in K[x]$ be a polynomial of degree $2n$. Then $x^{2n} \cdot g(1/x) = g(x)$ holds if, and only if, $g(x) = x^n \cdot f(x + x^{-1})$ for some $f \in K[x]$.*

What does that mean? We can study self-reciprocal polynomials in this new context, namely quadratic transformations.

Definition 3.1.2. Let $f \in K[x]$ be a polynomial of degree n and let $g, h \in K[x]$ coprime polynomials such that $\max\{\deg g, \deg h\} = 2$. We define the quadratic transformation p of f in the following way:

$$p(x) = h(x)^n f\left(\frac{g(x)}{h(x)}\right).$$

The idea is now the following: we can start from a polynomial of degree n and obtain a self-reciprocal polynomial using the quadratic transformation $x + 1/x$, i.e., with the notations of the previous definition, with $g = x^2 + 1$ and $h = x$. It is natural to ask if we can count the number of irreducible polynomials obtained applying an arbitrary quadratic transformation. The work of Ahmadi proved that a complete answer can be given. We will present his results with only the ideas behind the proofs, since we will then obtain the same results with another approach, which will lead us to another generalization.

The following result, which can be found for example in [Coh69], will be very useful.

Lemma 3.1.3 (Capelli)**.** *Let P be an irreducible polynomial of degree n over $\mathbb{F}_q[x]$ and let $g, h \in \mathbb{F}_q[x]$. Then $h(x)^n P(g(x)/h(x))$ is irreducible in $\mathbb{F}_q[x]$ if and only if $g(x) - \lambda h(x)$ is irreducible in $\mathbb{F}_{q^n}[x]$, where $\lambda \in \mathbb{F}_{q^n}$ is a root of P.*

Proof. Consider $Q(x) = h(x)^n P(g(x)/h(x))$ and let $t = \max\{\deg g, \deg h\}$. We have that $\deg Q = tn$. Let γ be a root of Q in the algebraic closure of $\mathbb{F}_q$. Then we must have $g(\gamma) = \lambda h(\gamma)$ for some root λ of P. This means that γ is a root of $g(x) - \lambda h(x)$, a polynomial of degree t in $\mathbb{F}_q(\lambda)[x]$. We note that $\mathbb{F}_q(\lambda) \subseteq \mathbb{F}_q(\gamma)$ and that $|\mathbb{F}_q(\lambda) : \mathbb{F}_q| = n$. Now we have

$$\begin{aligned} Q(x) \text{ is irreducible in } \mathbb{F}_q[x] &\Leftrightarrow |\mathbb{F}_q(\lambda) : \mathbb{F}_q| = tn \\ &\Leftrightarrow |\mathbb{F}_q(\lambda) : \mathbb{F}_q(\gamma)| = t \\ &\Leftrightarrow g(x) - \lambda h(x) \text{ is irreducible in } \mathbb{F}_q(\lambda)[x]. \end{aligned}$$

□

Lemma 3.1.3 shows us that we can restrict our attention to the polynomials of the form $g(x) - \lambda h(x)$, where $\lambda \in \mathbb{F}_{q^n}$ and it is not contained in any proper subfield.

Using some counting argument and some geometric tools, e.g. Hurwitz's formula, Ahmadi proves the following result.

Theorem 3.1.4 ([Ahm11]). *Let q be a prime power, and let $g(x) = a_1x^2 + b_1x + c_1$ and $h(x) = a_2x^2 + b_2x + c_2 \in \mathbb{F}_q[x]$ be relatively prime polynomials with $\max\{\deg g, \deg h\} = 2$. Also let $I_{(n,g,h)}$ be the set of monic irreducible polynomials $f(x)$ of degree $n > 1$ over $\mathbb{F}_q$ whose quadratic transformation by $g(x)$ and $h(x)$ is irreducible over $\mathbb{F}_q$. Then*

$$|I_{(n,g,h)}| = \begin{cases} 0 & \text{if } b_1 = b_2 = 0 \text{ and } q = 2^l \\ \frac{1}{2n}(q^n - 1) & \text{if } q \text{ is odd and } n = 2^m, m \geq 1 \\ \frac{1}{2n} \sum_{d|n,\, d \text{ odd}} \mu(d) q^{n/d} & \text{otherwise.} \end{cases}$$

We note that this result generalizes Carlitz's result on self-reciprocal polynomials. We will now present another method to prove the same result, and we will then use this method to generalize this result for cubic transformations.

The idea is to replace general quadratic maps with a simpler form.

Definition 3.1.5. Let K be a field and suppose R is a rational transformation of degree n. Let $(g, h) \in \mathrm{PGL}_2(K) \times \mathrm{PGL}_2(K)$. We define the (left) action of (g, h) on R by $g(R(h^{-1}(x)))$, obtained composing rational transformations. We call R and $g \circ R \circ h^{-1}$ equivalent.

Let R be a rational transformation of degree n, $R = t(x)/s(x)$ and let $f_R = s(x)^{\deg f} f(t(x)/s(x))$. We recall the following result.

Lemma 3.1.6. *If f_R is irreducible then $f_{R\circ A}$ is irreducible, for any linear rational expression $A(x)$.*

Since we have that $(f_B)_R = f_{B\circ R}$, where $B(x)$ is a rational transformation, we note that the map $f \mapsto f_B$ is a degree-preserving bijection from the set of polynomials f such that $f_{B\circ R\circ A}$ is irreducible, onto the set of polynomials f such that f_R is irreducible. Thus, for the purpose of counting the irreducible polynomials of the form f_R and a given degree over a finite field $K = \mathbb{F}_q$, we may take advantage of any normalization which replaces R with some $B \circ R \circ A$ having a simpler form. We now obtain the following result.

Proposition 3.1.7. *Let K be a field, and let g, h be coprime polynomials in $K[x]$ with $\max\{\deg g, \deg h\} = 2$. Then the rational expression $g(x)/h(x)$, upon composing on both sides with affine maps and the inversion map $x \mapsto 1/x$, repeatedly and in some order, can be taken to the form $x + \sigma x^{-1}$ for some $\sigma \in K^*$, or, when $\operatorname{char} K = 2$ only, to the form x^2.*

Proof. Write $g(x) = g_2x^2 + g_1x + g_0$ and $h(x) = h_2x^2 + h_1x + h_0$. Most of our work will serve to remove the quadratic term from the denominator, while leaving a linear term, if that is possible.

We first deal with the rather special case $g_2h_1 = g_1h_2$ and $g_1h_0 = g_0h_1$, whence $g_1 = h_1 = 0$. Any nonzero translation in x will get us away from this situation, except when K has characteristic two. In that case, if $h_2 = 0$ then multiplication by a scalar and addition of another bring the expression to the form x^2, as claimed. If $h_2 \neq 0$ then addition of a suitable constant will remove the quadratic term from the numerator, after which taking the reciprocal followed by post-composition with a suitable affine map lead again to the desired form x^2.

As we mentioned, if the characteristic of K is not two, then we may arrange for at least one of $g_2h_1 \neq g_1h_2$ and $g_1h_0 \neq g_0h_1$ to hold. Possibly after pre-composition with the inversion map $x \mapsto 1/x$, we may assume that the former holds. If $h_2 = 0$ then our expression has the form $(g_2x^2 + g_1x + g_0)/(h_1x + h_0)$, with $h_1 \neq 0$. Otherwise, by adding a suitable constant to $g(x)/h(x)$ we may arrange that $g(x)$ has no quadratic term, but has a nonzero linear term, and then the reciprocal $h(x)/g(x)$ will have that form.

Finally, a translation in x brings our expression to the form $(g_2x^2 + g_1x + g_0)/x$. Multiplication by a nonzero constant followed by addition of a suitable constant turn it into the desired form $x+\sigma x^{-1}$, for some $\sigma \in K^*$. □

Proposition 3.1.7 tells us that we can consider only two representatives for quadratic maps: if the characteristic is odd we have $x+1/x$ and $x+\sigma/x$, where $\sigma \in \mathbb{F}_q$ is not a square. If the characteristic is even we have x^2 and $x + 1/x$.

In the special case of $K = \mathbb{F}_q$, we obtain the same result using the orbit-stabilizer theorem.

Lemma 3.1.8. *The number of quadratic maps from $\mathbb{P}^1(\mathbb{F}_q)$ to itself is $q^3(q^2-1)$.*

Proof. We note that the result can be obtained by dividing by $q - 1$ the number of ordered pairs of coprime (nonzero) polynomials of degree at most two, and not both of degree less than two. There are $(q^3 - 1)^2$ pairs of nonzero polynomials of degree at most two, $(q^3 - 1)(q - 1)$ of which consist of proportional polynomials. Of the remaining pairs, those with greatest common divisor of degree one (which can be taken to be monic) are easily seen to be in number of $q(q^2-q)(q^2-1)$. What is left are the pairs of coprime polynomials of degree at most two, and we still have to subtract from those the number of pairs of coprime polynomials of degree less than two, which is $(q^2 - q)(q^2 - 1)$. We are left with $q^3(q^2 - 1)(q - 1)$ pairs, which proves our claim. □

Now, we list stabilizers of certain maps, in order to use the orbit-stabilizer theorem to conclude. We omit the computations used to obtain these stabilizers, noting that they can be computed knowing that an element of the stabilizer acts as the identity on ramification points and on their corresponding branch points.

Theorem 3.1.9. *Suppose q is odd. Then we have only two equivalence classes, namely $x \mapsto x^2$ and $x \mapsto (x^2+\sigma)/(2x)$, where σ is not a square.*

Proof. The stabilizer of the map $x \mapsto x^2$ consist of all pairs $(x \mapsto \alpha x, y \mapsto y/\alpha^2)$ and all pairs $(x \mapsto \alpha/x, y \mapsto \alpha^2/y)$ with $\alpha \in \mathbb{F}_q^*$. Hence this stabilizer has order $2(q-1)$, and the orbit has length $q^2(q^2-1)(q+1)/2$. Consider now the map $x \mapsto (x^2+\sigma)/(2x)$. Its stabilizer consists of all pairs

$$\left(x \mapsto \frac{\alpha x + \sigma\beta}{\beta x + \alpha}, y \mapsto \frac{(\alpha^2+\sigma\beta^2)y - 2\sigma\alpha\beta}{-2\alpha\beta y + (\alpha^2+\sigma\beta^2)}\right)$$

and of all pairs

$$\left(x \mapsto \frac{\alpha x + \sigma\beta}{-\beta x - \alpha}, y \mapsto \frac{(\alpha^2+\sigma\beta^2)y + 2\sigma\alpha\beta}{-2\alpha\beta y - (\alpha^2+\sigma\beta^2)}\right),$$

for $\alpha, \beta \in \mathbb{F}_q$ and $\alpha^2 - \sigma\beta^2 \neq 0$, where proportional pairs (α, β) give rise to the same pair of maps. Since σ is a non-square, the condition $\alpha^2 - \sigma\beta^2 \neq 0$ is equivalent to $(\alpha, \beta) \neq (0,0)$, and we conclude that the stabilizer has order $2(q^2-1)/(q-1) = 2(q+1)$. Hence the length of the orbit will be $q^2(q^2-1)(q-1)/2$. Now we see that the sum of the lengths of the two orbits is $q^3(q^2-1)$, hence there are only two of them. □

We note that the map $x \mapsto x^2$ and the map $x \mapsto x + 1/x$, which we considered in Proposition 3.1.7, are equivalent. In fact, if we consider $A = (x-1)/(x+1)$ and $B = (2x+2)/(-x+1)$, we have $B \circ x^2 \circ A = x + 1/x$. We prove now a similar result for finite fields of even characteristic.

Theorem 3.1.10. *Suppose q is even. Then we have only two equivalence classes, namely $x \mapsto x^2$ and $x \mapsto (x^2+1)/x$.*

Proof. The stabilizer of the map $x \mapsto x^2$ consist of all pairs

$$\left(x \mapsto \frac{ax+b}{cx+d}, y \mapsto \frac{d^2y + b^2}{c^2y + a^2}\right).$$

Hence this stabilizer is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$, and the orbit has length $q(q^2-1)$. Consider now the map $x \mapsto (x^2+1)/x$. Its stabilizer consists of all pairs

$$\left(x \mapsto \frac{x+c}{cx+1}, y \mapsto \frac{y}{ty+1}\right),$$

where $c \in \mathbb{F}_q \setminus \{1\}$ and $t = c/(1+c^2)$ and of the map $(x \mapsto 1/x, y \mapsto y)$. Hence this stabilizer has order q and the length of the orbit will be $q(q^2-1)^2$. Now we see that the sum of the lengths of the two orbits is $q^3(q^2-1)$,hence there are only two of them. □

Remark 3.1.11. One notable equivalence class of rational expressions $R(x) = g(x)/h(x)$ of degree r over $\mathbb{F}_q$ (say q odd for now), is the class of the polynomial x^r. Of course any such $R(x)$ can be also be viewed as a rational expression over a larger field, such as $\mathbb{F}_{q^2}$, but may be equivalent to x^r over $\mathbb{F}_{q^2}$ and inequivalent over $\mathbb{F}_q$.

When $R(x) = x^r$, letting

$$A(x) = \tau\frac{x+\tau}{x-\tau}, \quad B(x) = \tau\frac{x+\tau^r}{x-\tau^r},$$

one finds

$$(B \circ R \circ A)(x) = \frac{\sum_{k \text{ even}} \binom{r}{k} x^{r-k}\tau^k}{\sum_{k \text{ odd}} \binom{r}{k} x^{r-k}\tau^{k-1}}.$$

When $\tau^2 \in \mathbb{F}_q^*$ we have $(B \circ R \circ A)(x) \in \mathbb{F}_q(x)$, which is certainly equivalent to $R(x) = x^r$ over $\mathbb{F}_q$ if $\tau \in \mathbb{F}_q$, but is not otherwise (because its two ramification points do not belong to $\mathbb{F}_q$ then). In particular, $(B \circ R \circ A)(x) = \frac{1}{2}(x+\tau^2/x)$ when $r = 2$, and $(B \circ R \circ A)(x) = (x^3 + 3\tau^2 x)/(3x^2 + \tau^2)$ when $r = 3$.

We will now use Hurwitz's formula to obtain once again this classification of quadratic maps.

Proposition 3.1.12 ([Sil09])**.** *Let $f : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ a finite separable morphism. Then*

$$2\deg(f) - 2 \geq \sum_{P \in \mathbb{P}^1(K)} (e_f(P) - 1),$$

where $e_f(P)$ is the ramification index of f at P. Equality holds if and only if $\operatorname{char}(K) \nmid e_f(P)$ for every $P \in \mathbb{P}^1(K)$.

Thus let $\deg(f) = 2$ and suppose K has characteristic different from 2. Hurwitz's formula now tells us that f has exactly two ramification points with index 2. By composing on both sides with suitable projective linear maps we can assume the ramification points to be 0 and 1, and the corresponding branch points to be 0 and 1. In particular, our map has become a quadratic polynomial (a quadratic rational map without poles) and, actually, a multiple of the map x^2 (because it has 0 as a ramification point).

Consider now the not algebraically closed case and let $K = \mathbb{F}_q$ (the same works for the real field). We know that in the algebraic closure there are only two ramification points, hence, if they are not K-rational, they are roots of the same polynomial of degree 2 over K. Using the action considered in Remark 3.1.11, we obtain that the map x^2 splits in two orbits, namely x^2 and $x + \sigma/x$, where $\sigma \in K$ is not a square.

Consider now the characteristic 2 case. We know (e.g. considering the zeroes of the derivative) that we can have only one ramification point, hence it must be rational. We may assume that ∞ is ramified and thus the map is a

polynomial of degree 2. We have still the map x^2, which now is not a separable morphism, since $K(x)/K(x^2)$ is purely inseparable. The general case will be $f(x) = x^2 + ax$ and, precomposing with a suitable transformation, we can assume $f(x) = x^2 + x$. We note that this map has only one ramification point at infinity. This map is equivalent to $x + 1/x$, which we considered previously.

Now we are able to give a simpler proof of Ahmadi's result. We will need the following result, which is a simple generalization of Lemma 3.1.1.

Lemma 3.1.13. *Let K be a field, $\sigma \in K^*$, and let $g(x) \in K[x]$ be a polynomial of degree $2n$. Then $x^{2n} \cdot g(\sigma x^{-1}) = \sigma^n g(x)$ holds if, and only if, $g(x) = x^n \cdot f(x + \sigma x^{-1})$ for some $f \in K[x]$ of degree n.*

Proof. We first show that $K(x + \sigma/x)$ is the fixed subfield of the automorphism of $K(x)$ given by $x \mapsto \sigma/x$. In fact, it is clearly contained in the fixed subfield. However, because $K(x)$ is the splitting field over $K(x + \sigma/x)$ of the irreducible polynomial $(y - x)(y - \sigma/x) = y^2 - (x + \sigma/x) + \sigma$, we have $|K(x) : K(x + \sigma/x)| = 2$. This proves our claim.

If $g(x)/x^n = f(x + \sigma/x)$ for some $f \in K[x]$, then the left-hand side must be invariant under the substitution $x \mapsto \sigma/x$, which is equivalent to $x^{2n} \cdot g(\sigma/x) = \sigma^n g(x)$. Conversely, if $g(x)/x^n$ is invariant under the substitution $x \mapsto \sigma/x$, then the first part of the proof implies $g(x)/x^n = f(x + \sigma/x)$ for some rational function $f \in K(x)$, necessarily of degree n. We only need to show that f is actually a polynomial. If it were not, then it would have a pole at some $\eta \in \overline{K}$, the algebraic closure of K. But then $f(x + \sigma/x)$ would have a pole at any root $\xi \in \overline{K}$ of the polynomial $(x^2 + \sigma) - \eta x$. Because 0 cannot be a root of this polynomial, and $g(x)/x^n = f(x + \sigma/x)$ cannot have any pole except at 0, we get the desired contradiction and are forced to conclude that $f \in K[x]$. □

Lemma 3.1.13 told us that, as for the self-reciprocal case, we can associate to the quadratic rational map $x \mapsto x + \sigma/x$ a rational linear transformation, namely $x \mapsto \sigma/x$ and focus our attention to irreducible polynomials fixed by it. We use now Theorem 1.2.7 in order to obtain the desired results. Only one case is left, namely counting irreducible polynomials of the form $f(x^2)$ in even characteristic. Of course they cannot have this property and we are done.

3.2 Cubic maps

How can we try to generalize some of the previous results? We have at least two natural possibilities. The first is to consider elements of the projective linear group different from $x + \sigma/x$, for example considering rational transformations having order greater than or equal to 3. Otherwise we can try to replace quadratic transformations, considering polynomials g and h with

degree greater than 2. Let us start with the first idea.

We consider elements of $\mathrm{PGL}_2(\mathbb{F}_q)$ having order 3. For example we consider the element given by $\left[\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right]$, i.e. the rational transformation $x \mapsto (x-1)/x$. As for the case of self-reciprocal polynomials, we will prove a result which puts in correspondence this element with a map of degree 3. In fact, we have the following result.

Lemma 3.2.1. *Let K be a field and let $g(x) \in K[x]$ be a polynomial of degree $3n$. We have $(-x)^{3n} \cdot g\big((x-1)/x\big) = g(x)$ if, and only if,*

$$g(x) = x^n(x-1)^n \cdot f\left(\frac{x^3-3x+1}{x(x-1)}\right)$$

for some $f \in K[x]$ of degree n.

Proof. Consider the automorphism of the field $K(x)$ given by the substitution $x \mapsto (x-1)/x$, which has order three. The monic polynomial which has its distinct composition powers as its roots is

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

It has coefficients in the subfield $L = K\big(\frac{x^3-3x+1}{x(x-1)}\big)$ of $K(x)$, and is irreducible over L. Because $K(x)$ is a splitting field for it over L we have$|K(x) : L| = 3$, and hence L is the fixed subfield of $K(x)$ with respect to the automorphism considered.

If

$$\frac{g(x)}{x^n(x-1)^n} = f\left(\frac{x^3-3x+1}{x(x-1)}\right) \tag{3.2.1}$$

for some $f \in K[x]$, then the left-hand side must be invariant under the substitution $x \mapsto (x-1)/x$, and $(-x)^{3n} \cdot g\big((x-1)/x\big) = g(x)$ follows after a short calculation. Conversely, if the latter holds then Equation (3.2.1) holds for some rational function $f \in K(x)$, necessarily of degree n. If f were not a polynomial, then it would have a pole at some $\eta \in \overline{K}$, the algebraic closure of K. But then the right-hand side of Equation (3.2.1), and hence the left-hand side as well, would have a pole at any root $\xi \in \overline{K}$ of the polynomial $(x^3-3x+1) - \eta x(x-1)$. Because this polynomial cannot have 0 or 1 as roots, this is impossible. We conclude that $f \in K[x]$, as desired. □

We note that the rational expression $(x^3-3x+1)/(x(x-1))$ has two ramification points, with multiplicity 3, hence it is equivalent to x^3 in an algebraic closure of K.

We could now try to repeat the same ideas used for the quadratic case, i.e. associate an element of $\mathrm{PGL}_2(K)$ to every representative of quadratic maps

and count the number of polynomials fixed by the linear transformation. Alas, this is not the case. We have the following result, which can be found in [Bea10].

Theorem 3.2.2. *Suppose r is coprime with* $\mathrm{char}(K)$. *Then*

1. $\mathrm{PGL}_2(K)$ *contains only one conjugacy class of subgroups isomorphic to* $\mathbb{Z}/r$, $r > 2$.

2. *The conjugacy classes of cyclic subgroups of order* 2 *of* $\mathrm{PGL}_2(K)$ *are parametrized by* $K^*/(K^*)^2$*: to* $\alpha \in K^*(\mod (K^*)^2)$ *corresponds the involution* $z \mapsto \alpha/z$.

This shows that the previous method works only for quadratic maps. Any rational transformation of order 3 will correspond to a map of degree 3 with only two ramification points. We need to find another way to deal with this case. We will use again Hurwitz's formula.

3.2.1 Orbits

As in the quadratic case we will now consider representatives of cubic maps (under the action of $\mathrm{PGL}_2(\mathbb{F}_q) \times \mathrm{PGL}_2(\mathbb{F}_q)$) over algebraically closed fields. We start with characteristics greater than 3.

Proposition 3.2.3. *Any cubic map R over an algebraically closed field K of characteristic different from* 2 *and* 3, *is equivalent either to* x^3, *or to* $R_c(x) = \dfrac{x^3 + (c-2)x^2}{(2c-1)x - c}$ *for some* $c \in K$.

The rational function $R_c(x)$ has ramification points ∞, 0, 1, λ, *with corresponding branch points* ∞, 0, 1, μ, *where* $\lambda = -c(c-2)/(2c-1)$ *and* $\mu = -c(c-2)^3/(2c-1)^3$. *The four ramification points are distinct, and so are the four branch points, provided that* $c \notin \{-1, 0, 1/2, 1, 2\}$.

Moreover, those exceptional cases give all maps equivalent to $R_{1/2}(x) = -2x^3 + 3x^2$ *(whose ramification points are* $\infty, 0, 1$, *with* ∞ *of index three).*

Remark 3.2.4. Instead of $R_{1/2}(x) = -2x^3 + 3x^2$, for a representative of the unique equivalence classes of maps with three ramification points we will take $x^3 - 3x^2$, whose ramification points are $\infty, -2, 2$, with ∞ having index three.

Proof. According to Hurwitz's formula, $R(x)$ has at most four ramification points P_i, with ramification indices $(3,3)$, $(3,2,2)$, or $(2,2,2,2)$, and corresponding distinct branch points $R(P_i)$.
If $R(x)$ has only two ramification points, then after pre- and post-composition with suitable automorphisms of $\mathbb{P}^1(K)$ we may assume them to be 0 and ∞, and also that the corresponding branch points are 0 and ∞. Then $R(x)$ is a scalar multiple of x^3, and clearly is equivalent to x^3.

Now suppose that $R(x)$ has at least three ramification points. Assuming, as we may, that $R(x)$ has ∞ and 0 as ramification points with corresponding branch points ∞ and 0 (hence it has ∞ as a double pole and 0 as a double zero), it will have the form $R(x) = (x^3 + ax^2)/(bx - c)$, for some $a, b, c \in K$. Further imposing that f has 1 as a ramification point with corresponding branch point 1 amounts to $f(x-1) - 1$ having a double zero at 0. A short calculation then leads to

$$R(x) = R_c(x) := \frac{x^3 + (c-2)x^2}{(2c-1)x - c}.$$

Because the ramification points besides ∞ are the zeroes of $R'(x)$, one finds that the fourth ramification point is $\lambda = -c(c-2)/(2c-1)$, with corresponding branch point $\mu = -c(c-2)^3/(2c-1)^3$.

Now note that $\lambda \in \{\infty, 0, 1\}$ if and only if $c \in \{-1, 0, 1/2, 1, 2\}$. Because μ equals λ for each of those values of c, they yield equivalent functions, as one can change one to any other by suitably permuting the three ramification points, and the branch points correspondingly. In particular, $R_{1/2}(x) = -2x^3 + 3x^2$ has ramification points $\infty, 0, 1$, with ∞ of index three. Because its stabilizer in $PGL_2(K) \times PGL_2(K)$ can only permute the two ramification points with $e_R(P) = 2$, and the corresponding branch points accordingly, it must consist of the identity map together with the map given by pre- and post-composition with $1 - x$. □

Now, we study the orbits over fields of low characteristic. Hurwitz's formula will no longer hold but we will use some *direct* reasoning.

Proposition 3.2.5. *Any cubic map over an algebraically closed field K of characteristic 2 is equivalent to one of the following maps: x^3, $x^3 + x^2$, $(x^3 + 1)/x$ or $(x^3 + b^2)/(x + b^2)$, with $b \neq 1$.*

Proof. We can suppose that infinity is ramified and start with the case in which it has multiplicity three. We obtain a polynomial of the form $x^3 + a^2x^2 + b^2x$. If $a^2 = b$ this is equivalent to x^3, otherwise we obtain $x^3 + x^2$.

Suppose now that infinity is ramified with multiplicity two. Up to some pre- and post-composition we can suppose that $f = (x^3 + ax^2 + b)/x$, with $b \neq 0$. Its derivative is $f'(x) = (ax^2 + b)/x^2$. If $a = 0$ the only ramification is at infinity and we see that this map is equivalent to $(x^3 + 1)/x$. If $a \neq 0$ we can suppose that it is one, and the other ramification point is for $x = d$ with $d^2 = b$. We obtain a family of maps of the form $f(x) = (x^3 + x^2 + b^2)/x$. We note that if $b = 1$ the map is equivalent to $x^3 + x^2$. Now we note that this map is equivalent to $(x^3 + b^2)/(x + b^2)$.

□

Proposition 3.2.6. *Any cubic map over an algebraically closed field K of characteristic 3 is equivalent to one of the following maps: x^3, $x^3 + x^2$, $x^3 + x$ or the 1-parameter family $(x^3 + (1 + \lambda)x^2)/((1 + \lambda)x + \lambda)$, with $\lambda \neq -1$.*

Proof. We start supposing that infinity is ramified with multiplicity 3, hence our map becomes a polynomial of the form $x^3 + ax^2 + bx$. If $a = b = 0$ we obtain the non-separable map x^3. If $a \neq 0$ the map is equivalent to $x^3 + x^2$. If $a = 0, b \neq 0$ we obtain $x^3 + x$. We see that these three maps are not equivalent, since x^3 is not separable, $x^3 + x^2$ has two ramification points and $x^3 + x$ has only one ramification point.

Suppose now that ∞ is ramified with multiplicity 2, therefore the map, up to pre- and post-compositions, has the form $f(x) = (x^3 + ax^2 + 1)/x$. Its derivative is $(2x^3 + ax^2 + 2)/x^2$. If $a = 0$ we have only one other ramification point and it has multiplicity 3. It can be shown that this map is equivalent to $x^3 + x^2$. Hence suppose $a \neq 0$. We see that in this case $2x^3 + ax^2 + 2$ has three different roots, hence we have four simple ramification points. As in [Oss06], we obtain a family of maps depending on one parameter, namely $(x^3 + (1 + \lambda)x^2)/((1 + \lambda)x + \lambda)$, with $\lambda \neq -1$. □

Since we are interested in the classification of cubic maps over finite fields and not only over algebraically closed ones, we will present now some results for finite fields of arbitrary characteristic.

Proposition 3.2.7. *Suppose we are in characteristic greater than* 3 *and consider maps over the finite fields* $\mathbb{F}_q$ *of degree* 3 *with at most three ramification points. Then they are equivalent to one of the following:* x^3, $(x^3 + 3\tau^2 x)/(3x^2 + \tau^2)$, $x^3 - 3x$ *or* $x^3 - 3\epsilon^2 x$, *where* $\tau, \epsilon \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Proof. If the map has only two ramification points we know that in the algebraic closure is equivalent to x^3 and, as we have seen in Remark 3.1.11, we obtain the other map, $(x^3 + 3\tau^2 x)/(3x^2 + \tau^2)$, conjugate to x^3 over $\mathbb{F}_{q^2}$ but not over $\mathbb{F}_q$.

If the map has three ramification points, we can always assume that the one with multiplicity 3 is in $\mathbb{F}_q$, since it is fixed by Frobenius, hence we can assume that we have a ramification at infinity. The other two ramification points are either in $\mathbb{F}_q$, thus we obtain the map $x^3 - 3x$, or are in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and we can assume that they are ϵ and $-\epsilon$. Then, we obtain the map $x^3 - 3\epsilon^2 x$, whose derivative has precisely those two elements as roots. □

We will also prove results for characteristic 2 and 3. We start with the latter.

Proposition 3.2.8. *Suppose we are in characteristic* 3 *and consider maps of degree* 3 *with at most three ramification points. Then they are equivalent to one of the following:* x^3, $x^3 + x^2$, $x^3 + x$ *and* $x^3 + ax$, *where* a *is not a square in* $\mathbb{F}_q$.

Proof. The non-separable map is still x^3, as in the algebraically closed case. If we consider a map with two ramification points of multiplicities 3 and 2 they must be in $\mathbb{F}_q$, hence the map will be equivalent to $x^3 + x^2$. If the map

is separable with only one ramification point, we can assume that it is at infinity and the map is equivalent to $x^3 + x$ or to $x^3 + ax$, where a is not a square in $\mathbb{F}_q$. We note that these two maps are not equivalent, since $x^3 + x$ is equivalent only to maps of the form $x^3 + c^2x$. □

Now, we focus our attention to characteristic 2. In this case we are able to give a complete classification of the orbits over finite fields. This is due to the fact that we have at most two ramification points.

Proposition 3.2.9. *Suppose we are in characteristic* 2 *and let* f *be a cubic map over* $\mathbb{F}_q$*, with* $q = 2^k$*. Then* f *will be equivalent to one of the following maps:*

1. x^3;
2. $W(c) = \dfrac{x^3 + xc^{q+1} + (c + c^q)c^{q+1}}{x^2 + x(c + c^q) + (c^2 + c^{2q} + c^{q+1})}$, *with* $c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$;
3. $x^3 + x^2$;
4. $\dfrac{x^3 + a}{x}$, *with* $a \in \mathbb{F}_q$;
5. $\dfrac{x^3 + b^2}{x + b^2}$, *with* $b \in \mathbb{F}_q, b \neq 1$;
6. $U(b) = \dfrac{t_1x^3 + t_2x^2 + t_3x + t_4}{t_5x^2 + t_6x + t_7}$, *with* $t_1 = b(c + c^q)$, $t_2 = c^2 + c^{2q}$, $t_3 = b(c^{q+2}+c^{2q+1})$, $t_4 = (b+1)(c^{q+3}+c^{3q+1})$, $t_5 = b(c+c^q)$, $t_6 = b(c^2+c^{2q})$ *and* $t_7 = c^{q+2} + c^{2q+1} + (b + 1)(c^3 + c^{3q})$.

Proof. Consider the map $f = x^3$. We have another map, conjugate to x^3 on $\mathbb{F}_{q^2}$ but not over $\mathbb{F}_q$. In fact, consider the rational transformations

$$A(x) = \frac{x + c}{x + c^q} \quad \text{and} \quad B(x) = \frac{c^q x + c}{x + 1},$$

where $c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then, we consider

$$B \circ f \circ A(x) = \frac{x^3(c + c^q) + x(c + c^q)c^{q+1} + (c^2 + c^{2q})c^{q+1}}{x^2(c + c^q) + x(c^2 + c^{2q}) + (c^3 + c^{3q})}.$$

This map is defined over $\mathbb{F}_q$ and its ramification points are c and c^q, therefore it cannot be equivalent to x^3 over $\mathbb{F}_q$.
Now, the map x^3+x^2 has two ramification points with different multiplicities, thus this map does not split in different orbits over $\mathbb{F}_q$.
Consider now the maps $g_a = (x^3 + a)/x$. They have only one ramification point at infinity, hence we can suppose that the ramification point is rational.

We note that g_a and g_b are in the same orbit if and only if a and b differ by some third power. Thus, if $q \not\equiv 1 \pmod 3$, we have only one orbit, the one given by $(x^3+1)/x$. Otherwise the orbit splits in three different ones, parametrized by $K^*/(K^*)^3$.

At last, we have the family of maps of the form $(x^3+b^2)/(x+b^2)$, with $b \neq 1$, ramified at ∞ and 1. Their orbit splits in two over $\mathbb{F}_q$, the other one having the two ramification points in $\mathbb{F}_{q^2}$ but not in $\mathbb{F}_q$. In fact, let $c \in \mathbb{F}_{q^2}$ be an element of nonzero trace. We consider the transformations

$$A(x) = \frac{bx + c(b+1) + c^q}{x + c^q} \quad \text{and} \quad B(x) = \frac{c^q x + c(b+1) + c^q}{x+b},$$

We obtain

$$B \circ f \circ A(x) = \frac{t_1 x^3 + t_2 x^2 + t_3 x + t_4}{t_5 x^2 + t_6 x + t_7},$$

where $t_1 = b(c+c^q)$, $t_2 = c^2 + c^{2q}$, $t_3 = b(c^{q+2} + c^{2q+1})$, $t_4 = (b+1)(c^{q+3} + c^{3q+1})$, $t_5 = b(c+c^q)$, $t_6 = b(c^2+c^{2q})$ and $t_7 = c^{q+2}+c^{2q+1}+(b+1)(c^3+c^{3q})$. These maps are defined over $\mathbb{F}_q$ and ramified at c and c^q. □

As in the quadratic case, we also use orbits and stabilizers to obtain another proof of the fact that the previous ones are the only equivalence classes. We need first the following result.

Lemma 3.2.10. *The number of cubic maps from $\mathbb{P}^1(\mathbb{F}_q)$ to itself is $q^5(q^2-1)$.*

Proof. We note that the result can be obtained by dividing by $q-1$ the number of ordered pairs of coprime (nonzero) polynomials of degree at most three, and not both of degree less than three. There are $(q^4-1)^2$ pairs of nonzero polynomials of degree at most three, $(q^4-1)(q-1)$ of which consist of proportional polynomials. Of the remaining pairs, those with greatest common divisor of degree one (which can be taken to be monic) are easily seen to be in number of qr_2, where r_2 is the number of of coprime polynomials of degree at most two, and from Lemma 3.1.8 we know that $r_2 = q^6+q-q^5-q^2$. We have to subtract now the polynomials with greatest common divisor of degree two which are in number of $q^2(q^2-q)(q^2-1)$. What is left are the pairs of coprime polynomials of degree at most three, and we still have to subtract from those the number of pairs of coprime polynomials of degree less than three, which is again r_2. We are left with $q^5(q^2-1)(q-1)$ pairs, which proves our claim. □

In the following proposition we list the stabilizers for the representatives of the equivalence classes and use orbit-stabilizer theorem to prove that the previous ones are the only equivalence classes. As in the quadratic case, we will exhibit a list of all stabilizers without the explicit computations, using again the fact that an element of the stabilizer acts as the identity on ramification points and on their corresponding branch points.

Proposition 3.2.11. *The equivalence classes in Proposition 3.2.9 cover all orbits for cubic maps in characteristic* 2.

Proof. The stabilizer of the map $x \mapsto x^3$ consists of all pairs $(x \mapsto \alpha x, y \mapsto y/\alpha^3)$ and all pairs $(x \mapsto \alpha/x, y \mapsto \alpha^3/y)$ with $\alpha \in \mathbb{F}_q^*$. Hence this stabilizer has order $2(q-1)$ and the orbit has length $q^2(q^2-1)(q+1)/2$. Consider now the maps $x \mapsto W(c)$. Their stabilizer consists of all pairs

$$\left(x \mapsto \frac{(u(c+c^q)+v)x + uc^{q+1}}{ux+v}, y \mapsto \frac{(s(c+c^q)+t)y + sc^{q+1}}{sy+t}\right)$$

and of all pairs

$$\left(x \mapsto \frac{vx + v(c+c^q) + uc^{q+1}}{ux+v}, y \mapsto \frac{\tilde{t}y + \tilde{t}(c+c^q) + \tilde{s}c^{q+1}}{\tilde{s}y+\tilde{t}}\right),$$

where $s = v^2u+(c+c^q)vu^2+(c^2+c^{2q}+c^{q+1})u^3$, $t = v^3+(c+c^q)v^2u+(c^2+c^{2q}+c^{q+1})vu^2+(c^{q+2}+c^{2q+1}+c^3+c^{3q})u^3$, $\tilde{s} = u^3(c^2+c^{2q}+c^{q+1})+u^2v(c+c^q)+uv^2$ and $\tilde{t} = u^3(c^{q+2}+c^{2q+1}) + u^2vc^{q+1} + v^3$. The determinant of the maps is nonzero for $(u,v) \neq (0,0)$ since $c \notin \mathbb{F}_q$. We note that proportional pairs (u,v) give rise to the same pair of maps. We can conclude that the stabilizers have order $2(q^2-1)/(q-1) = 2(q+1)$ and the length of the orbits will be $q^2(q^2-1)(q-1)/2$. Consider now the map $x \mapsto x^3+x^2$. Its stabilizer consists only of the identity, hence its orbit has length $q^2(q^2-1)^2$. The stabilizer of the map $x \mapsto (x^3+a)/x$ consists of the pairs $(x \mapsto \alpha x, y \mapsto \alpha y)$, where $\alpha \in \mathbb{F}_q$ and $\alpha^3 = 1$. Thus, if $q \not\equiv 1 \pmod 3$, we have only one orbit, whose stabilizer has order 1, otherwise we have three orbits whose stabilizers have order three. Hence we obtain one or three orbits whose total length is $q^2(q^2-1)^2$. Consider now the maps $x \mapsto (x^3+b^2)/(x+b^2)$. The stabilizer consists of $(x \mapsto x, y \mapsto y)$ and $(x \mapsto (x+b^2)/(x+1), y \mapsto (y+b^2)/(y+1))$. The orbit has length $q^2(q^2-1)^2/2$. If we consider finally the maps $x \mapsto U(b)$ we have that their stabilizer consists of the maps $(x \mapsto x, y \mapsto y)$ and $(x \mapsto x+c+c^q, y \mapsto y+c+c^q)$. The orbit has then length $q^2(q^2-1)^2/2$. If now we sum the length of all orbits we obtain $q^5(q^2-1)$. □

Remark 3.2.12. We are not able to give the same results over finite fields for maps with four ramification points. The difficulties arise in trying to *move* these points in a smart way. In fact we have the following possibilities for the location of the points:

1. they can be all in an extension of degree 4 of $\mathbb{F}_q$.
2. they are roots of two distinct irreducible polynomials of degree 2 over $\mathbb{F}_q$.
3. two of them are rational and the other two are roots of an irreducible polynomial of degree 2.

4. three of them are roots of an irreducible polynomial of degree 3 over $\mathbb{F}_q$ and the other one is rational.

5. they are all rational.

3.3 Some counting

Using the previous results we now focus our attention on polynomials obtained by cubic transformations. As for the quadratic case we would like to count the number of irreducible polynomials $f \in \mathbb{F}_q[x]$ of degree n, such that $h^n f(g/h)$ is still irreducible. As before, we call $I_{(n,g,h)}$ this set.

Recalling Lemma 3.1.3, we need to study the irreducibility of the polynomial $r_\beta(x) = g(x) - \beta h(x)$, with $\beta \in \mathbb{F}_{q^n}$ and not contained in proper subfields.

Throughout this section we will assume, up to some post-composition, that $\deg g = 3$ and $\deg h = 2$. We recall here a result, which can be found for example in [PCo89] that we will use in the following.

Lemma 3.3.1. *Suppose* $\mathrm{char}(K) \neq 2$ *and let* $f \in K[x]$ *be a polynomial of degree* n*. Let* Δ *be its discriminant. Then* Δ *is a square in* K *if and only if the group of* f *over* K*, regarded as premutation group of the roots, is contained in the alternating group of degree* n*.*

We will now introduce some notation, following Ahmadi.
Let $\tau(m,q) = \mathbb{F}_{q^m} \setminus \bigcup_{d|m,d<m} \mathbb{F}_{q^d}$ be the set of elements of $\mathbb{F}_{q^m}$ not contained in some proper subfield. We define now some sets, that will help us in our counting.
First, we define

$$U(m,q) = \{\beta : \beta \in \tau(m,q), r_\beta \text{ is irreducible over } \mathbb{F}_{q^m}\}.$$

Using Lemma 3.1.3, we see that $|I_{(n,g,h)}| = |U(n,q)|/n$, since we need to consider only one root for every irreducible polynomial of degree n over $\mathbb{F}_q[x]$. In order to count the cardinality of this set, we introduce now another set, which can be seen as a generalization of the latter one. Namely, we define

$$\bar{U}(m,q) = \{\beta : \beta \in \mathbb{F}_{q^m}, r_\beta \text{ is irreducible over } \mathbb{F}_{q^m}\}.$$

The difference here is that we consider all the elements of $\mathbb{F}_{q^m}$, not only the ones of degree m. Consider now the set

$$V(n,q) = \{\beta : \beta \in \mathbb{F}_{q^n} \text{ and } \exists \gamma \in \mathbb{F}_{q^n} \text{ such that } r_\beta(\gamma) = 0\}.$$

This is the set of β, such that r_β has a root. Now, since r_β is never constant and of degree 3 we have $|V(n,q)| = q^n - |\bar{U}(n,q)|$.
We try now to compute $|V(n,q)|$ and we introduce the following set.

$$W(m,q) = \{(\gamma,\beta) : \gamma,\beta \in \mathbb{F}_{q^n}, r_\beta(\gamma) = 0\}.$$

We note that, when γ is not a root of h, for every $\gamma \in \mathbb{F}_{q^n}$ there is a unique $\beta \in \mathbb{F}_{q^n}$, namely $g(\gamma)/h(\gamma)$, such that $r_\beta(\gamma) = 0$. Therefore $|W(n,q)| = q^n - a$, where a is the number of roots of h in $\mathbb{F}_{q^n}$.
Now we see that

$$|V(n,q)| = \frac{|W(n,q)| + 2m + 2c + b}{3}, \tag{3.3.1}$$

where b is the number of $\mathbb{F}_{q^n}$-rational branch points whose corresponding ramification points have multiplicity 2, i.e. the number of β, such that $r_\beta = (x-s)^2(x-r)$, m is the number of β for which $f - \beta g$ factorizes as $(x-s)r$ with r irreducible of degree 2 and c is the number of β such that $f - \beta g = (x-\gamma)^3$, i.e. c is the number of branch points with exactly one (finite) preimage.

We consider now the discriminant $\Delta = \Delta(\beta)$ of $r_\beta(x)$ (taken with respect to the variable x). We know from Lemma 3.3.1 that Δ is a square if and only if the group G of permutation of the roots of r_β is contained in $\mathcal{A}_3$. In term of reducibility of r_β we have two possibilities: if G is the trivial group, then r_β splits in $\mathbb{F}_{q^n}$. If $G = \mathcal{A}_3$, cyclic of order 3, then r_β is irreducible. Suppose now that Δ is not a square. It must then contain some odd permutation. Anyway, since Galois groups over finite fields are cyclic, it must then have order 2, generated by a transposition. In this case we have that $r_\beta = (x-s)r$, where r is irreducible of degree 2.

We see now how we can proceed, using the discriminant. We note that m is equal to the number of β, for which Δ is not a square. Thus, let N be the number of points of the plane curve given by the equation $y^2 - \Delta$.

We note that the number of β, for which Δ is a nonzero square, is $(N - b - c)/2$, since the discriminant has for roots the branch points of $g(x)/h(x)$. Adding $b + c$ we have that the number of squares is $(N + b + c)/2$, hence we obtain $m = q^n - (N + b + c)/2$. Using now Equation (3.3.1) we see that

$$|V(n,q)| = q^n - (N + a - c)/3$$

and finally

$$|\bar{U}(n,q)| = (N + a - c)/3.$$

Now we see that

$$|\bar{U}(n,q)| = \sum_{d|n, d\not\equiv 0 \pmod 3} |U(n/d,q)|.$$

If $\beta \in \tau(m,q)$ with $m|n$ we have that $\beta \in \bar{U}(n,q)$ if and only if n/m is not divisible by 3 otherwise $\mathbb{F}_{q^n}$ contains a cubic extension of $\mathbb{F}_{q^m}$ and r_β would not be irreducible.
We now use Möbius inversion to obtain

$$|U(n,q)| = \sum_{d|n, d\not\equiv 0 \pmod 3} \mu(d)|\bar{U}(n/d,q)|. \tag{3.3.2}$$

We now use this method to count $I_{(n,g,h)}$ in some cases and to approximate it in other ones. We start with the map with at most 3 ramification points. The first result, for the map $x \mapsto x^3$, is a special form of a result of Cohen, who studied the map $x \mapsto x^r$. We will now give the more general result. We denote with w' the product of the distinct primes appearing in the factorization of w.

Theorem 3.3.2 ([Coh69]). *Suppose that the integer $r > 1$ and the field $\mathbb{F}_q$ are given and suppose $\gcd(r,q) = 1$. Then, if $r'|q^n - 1, 4 \nmid \gcd(r, q^n + 1)$ and n is written as $n = kcc_1$, where k is the order of $q \pmod{r'}$, $\gcd(r,n) = 1$ and $c_1'|r$. Then*

$$I_{(n,x^r,1)} = \begin{cases} \dfrac{\phi(r)}{rn}(q^n - 1) & \text{if } c = 1, \\ \dfrac{\phi(r)}{rn} \displaystyle\sum_{s|c} \mu(s) q^{n/s} & \text{if } c > 1. \end{cases}$$

Otherwise, we have $I_{(n,x^r,1)} = 0$.

Now we consider the other map, in characteristic greater than 3, with two ramification points, namely

$$f(x) = \frac{x^3 + 3\tau^2 x}{3x^2 + \tau^2},$$

with $\tau \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $\tau^2 \in \mathbb{F}_q$.

Theorem 3.3.3. *Let $g = x^3 + 3\tau^2 x$ and $h = 3x^2 + \tau^2$, with $\tau \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $\tau^2 \in \mathbb{F}_q$. Write $n = 3^k 2^t s$, with $(s,6) = 1$. If $q \equiv 1 \pmod 3$ we have*

$$|I_{(n,g,h)}| = \begin{cases} 0 & 2 \nmid n, \\ (2/3n) \displaystyle\sum_{d|n, 3\nmid d, 2|n/d} \mu(d) q^{n/d} & s = 1, t \geq 2 \text{ or } s \neq 1, \\ (2/3n)(q^n - 1) & s = 1, t = 1. \end{cases}$$

If $q \equiv 2 \pmod 3$*, we have*

$$|I_{(n,g,h)}| = \begin{cases} \dfrac{2q+2}{3} & n = 1, \\ (2/3n)(q^n+1) & n = 3^k, k \geq 1, \\ (2/3n)(q^n - q^{n/2} - 2) & n = 2 \cdot 3^k, k \geq 0, \\ (2/3n) \displaystyle\sum_{d|n, 3\nmid d} \mu(d) q^{n/d} & \textit{otherwise.} \end{cases}$$

Proof. The discriminant Δ of $(x^3 + 3\tau^2 x) - \beta(3x^2 + \tau^2)$ equals $-108\tau^2(\beta^2 - \tau^2)^2$. We note that -108 is a square in $\mathbb{F}_q$ if and only if -3 is and this happens if and only if $q \equiv 1 \pmod 3$. We consider first this case. We want to compute $|\bar{U}(n,q)|$. Suppose that n is even. Then $3x^2 + \tau^2$ has two roots, hence $a = 2$ and the number c of rational branch points is 2. We have to compute the number N of points of the curve given by the equation $y^2 + 108\tau^2(\beta^2 - \tau^2)^2$. Since $\beta^2 - \tau^2 = 0$ for 2 values of β, we have $2(q^n - 2)$ nonzero values for y and 2 zero values corresponding to those roots. Hence $N = 2q^n - 2$ and $|\bar{U}(n,q)| = N/3$. If n is odd we have $c = 0$, since $\tau \notin \mathbb{F}_q$, and $a = 0$, since $-\tau^2/3$ is not a square. For the same reason $-3\tau^2$ is not a square and therefore $N = 0$.

Consider now the case $q \equiv 2 \pmod 3$. If n is even, as before, we obtain $|\bar{U}(n,q)| = N/3 = (2q^n - 2)/3$. If n is odd we have $c = 0$ and $a = 2$, since $-\tau^2/3$ is a square. Let us now consider the curve given by $y^2 - \Delta$. We have that $\beta^2 - \tau^2$ is never zero, hence $N = 2q^n$. Putting all together we obtain $|\bar{U}(n,q)| = (2q^n + 2)/3$.
Using Möbius inversion we obtain the conclusion. □

We focus now our attention to the maps with three ramification points.

Lemma 3.3.4. *Let* $f = x^3 - 3\tau x$ *and* $g = 1$*. Writing* $n = 3^k 2^t s$*, with* $(s, 6) = 1$*, we have:*

$$|I_{(n,g,h)}| = \begin{cases} \dfrac{q-1}{3} & n = 1, \\ (1/3n)(q^n - 1) & n = 3^k, k \geq 1, \\ (1/3n) \displaystyle\sum_{d|n, 3\nmid d} \mu(d) q^{n/d} & \textit{otherwise,} \end{cases}$$

if $q \equiv 1 \pmod 3$ *and*

$$|I_{(n,g,h)}| = \begin{cases} \dfrac{q+1}{3} & n = 1, \\ (1/3n)(q^n + 1) & n = 3^k, k \geq 1, \\ (1/3n)(q^n - q^{n/2} - 2) & n = 2 \cdot 3^k, k \geq 1, \\ (1/3n) \displaystyle\sum_{d|n, 3\nmid d} \mu(d) q^{n/d} & \textit{otherwise}, \end{cases}$$

if $q \equiv 2 \pmod 3$.

Proof. The discriminant of $f - \beta$ equals $9(12\tau^3 - 3\beta^2)$. We need now to compute the number of squares of the form $12\tau^3 - 3\beta^2$. We know, e.g. from [LN83], that $\sum_{\beta \in \mathbb{F}_{q^n}} \eta(12\tau^3 - 3\beta^2) = -\eta(-3)$, where η is the quadratic character. Let m_1 be the number of non-zero squares. We have $m_1 - m = -\eta(-3)$ and $m_1 + m = q^n - b$, where b is the number of $\mathbb{F}_{q^n}$-rational branch points, corresponding to the roots of $12\tau^3 - 3\beta^2$. We obtain $m = (q^n - b + \eta(-3))/2$. Now we have

$$|\bar{U}(n,q)| = \frac{q^n - \eta(-3)}{3}.$$

The conclusion follows by Möbius inversion, noting that $\eta(-3) = 1$ if and only if $q^n \equiv 1 \pmod 3$. □

We give now some results for the characteristic 3 case. We note that the case x^3 is surely covered by Theorem 3.3.2, but of course $f(x^3)$ will be reducible, thus $I_{(n,x^3,1)} = 0$ for every n.

We consider now the map $x^3 + x^2$.

Theorem 3.3.5. *Let* $f = x^3 + x^2$ *and* $g = 1$. *Then*

$$|I_{(n,g,h)}| = \frac{1}{3n} \sum_{d|n, 3\nmid d} \mu(d) q^{n/d}.$$

Proof. The discriminant of $f - \beta$ equals β. Therefore the number of points N of the curve given by $y^2 - \beta$ in $\mathbb{F}_{q^n}$ is q^n, hence $|\bar{U}(n,q)| = q^n/3$. □

We have now the map $x^3 + \sigma x$.

Theorem 3.3.6. *Let* $f = x^3 + \sigma x$ *and* $g = 1$. *Then*

$$|I_{(n,g,h)}| = \begin{cases} (2/3n) \displaystyle\sum_{d|n, 3\nmid d} \mu(d) q^{n/d} & (A), \\ (2/3n) \displaystyle\sum_{d|n, 3\nmid d, 2|n/d} \mu(d) q^{n/d} & \textit{otherwise}, \end{cases}$$

where condition (A) *is true if* $q \equiv 1 \pmod 4$ *and* σ *is a square or* $q \equiv 3 \pmod 4$ *and* σ *is not a square.*

Proof. The discriminant of $f - \beta$ is $-\sigma^3$, hence it does not depend on β. If $-\sigma$ is a square we have $2q^n$ solutions (two for each β), otherwise we have no solution. Suppose $q \equiv 1 \pmod 4$. Then, if σ is a square we have $\eta(-\sigma) = 1$ in every extension of $\mathbb{F}_q$. Otherwise, if σ is not a square, $\eta(-\sigma) = 1$ in extensions of even degree and $\eta(-\sigma) = -1$ for extensions of odd degree. Suppose $q \equiv 3 \pmod 4$. Then, if σ is a square we have $\eta(-\sigma) = (-1)^k$ in $\mathbb{F}_{q^k}$. If σ is not a square we always have $\eta(-\sigma) = 1$. Again the conclusion follows using Möbius inversion formula. □

We give an estimate for $|I_{(n,g,h)}|$ in the case when four distinct ramification points.

Theorem 3.3.7. *Suppose* f *is a rational function of degree* 3 *with four ramification points. Then we have* $|I_{(n,g,h)}| = q^n/3n + O(q^{n/2}/3n)$.

Proof. Consider the curve with equation $y^2 - \Delta$. It is smooth since the zeroes of Δ are exactly the branch points and it has genus 1 since the discriminant has degree 4 if infinity is not a branch point and 3 otherwise. Then, we apply the Hasse-Weil bound to obtain

$$|N - q^n - 1| < 2\sqrt{q^n}.$$

Using this bound and Equation (3.3.2) we see that $|I_{(n,g,h)}| = q^n/3n + O(q^{n/2}/n)$. □

Chapter 4

PN functions

In this chapter we will introduce and discuss the theory of PN functions over finite fields. These are functions such that their finite difference in every nonzero direction is a permutation polynomial of the field. The main interest for these functions arises in the cryptographic context, which occurs mostly in characteristic two. However, a lot of work has been done in odd characteristic as well, because the topic is quite interesting as an independent object of study. Some interesting results on this topic could be found for example in the following papers, where the authors studied property of PN functions and present classes of polynomials satisfying these properties: in [RS89], [Joh87], [Hir89] and [Glu90] we have the first important results, showing that only quadratic polynomials are PN functions over prime fields of odd characteristic. Since in this chapter we are mainly interested in PN monomials, we cite the interesting paper [CM97], in which we can find some interesting results on PN monomials and some necessary conditions they must satisfy. In [Cou06], the author shows that essentially the only PN monomial over fields of prime square order is x^2. We proved a similar result for finite fields $\mathbb{F}_{p^4}$, unaware of the paper [CL12]. A lot of papers shows that certain classes of polynomials have the PN property. Among others we may cite [LHT13], [PZ11], in which the authors use some interesting ideas of character theory, [DY06], [ZW09] and [ZKW09]. Finally we would like to cite [Zie13], in which the author proved interesting asymptotic results for PN monomials.
In the first section we give the formal definition of PN function and previously known results about permutation polynomials, such as the Hermite-Dickson criterion. In the second section we give some known results about PN monomials, in particular some necessary conditions. The last section contains our original results. We tried to generalize the concept of PN functions for higher order finite differences, asking the k-th finite difference to be a permutation polynomial for every possible n-tuple of directions. We proved results for fields of order p, p^2, p^4 and partial results for fields of order p^3.

4.1 Preliminaries

We start with the definition of the object we want to study.

Definition 4.1.1. Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a map from a finite field to itself. Denote with $N(a, b)$ the number of solutions of $f(x + a) - f(x) = b$, with $a, b \in \mathbb{F}_q$ and let $\Delta_f = \max\{N(a, b)|a, b \in \mathbb{F}_q, a \neq 0\}$. We say that f is differentially k-uniform if $\Delta_f = k$. If $\Delta_f = 2$ we say that f is almost perfect non-linear (APN) and if $\Delta_f = 1$ we say that it is perfect non-linear (PN).

We note immediately that in characteristic 2 we cannot have PN functions, since if x is a solution of $f(x + a) - f(x) = b$, then $x + a$ is also a solution. Hence APN functions is the best we can obtain in even characteristic. A lot of work has been done in this case, since cryptographic systems need functions with a low differential uniformity in order to be safer against certain types of attacks.

We concentrate now on PN functions in odd characteristic.

Definition 4.1.2. Let $f \in \mathbb{F}_q[x]$ be a polynomial over a finite field. We say that f is a permutation polynomial of $\mathbb{F}_q$ if the function associated to it is bijective.

We note now that the condition of differentially 1-uniform means that $f(x + a) - f(x)$ is a permutation polynomial, for every $a \in \mathbb{F}_q, a \neq 0$. We consider now a family of polynomials, namely q-polynomials. They have the form

$$L(x) = \sum_{i=0}^{m-1} a_i x^{q^i},$$

where the coefficients are in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$.

From the identity $c^q = c$ for $c \in \mathbb{F}_q$ and $(a + b)^q = a^q + b^q$ it follows that q-polynomials satisfy

1. $L(\alpha + \beta) = L(\alpha) + L(\beta)$ for $\alpha, \beta \in F$,

2. $L(c\beta) = cL(\beta)$ for all $c \in \mathbb{F}_q$ and $\beta \in F$,

where F is a field extension of $\mathbb{F}_q$.
Using the linearity of the functions associated to a q-polynomial, we note that a p-polynomial is a permutation polynomial of $\mathbb{F}_q$ if and only if it has only the root 0 in $\mathbb{F}_q$.

One of the main results regarding permutation polynomials is the following:

Theorem 4.1.3 (Hermite-Dickson criterion, [LN83]). *Let $\mathbb{F}_q$ be of characteristic p. Then $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions hold:*

1. *f has exactly one root in $\mathbb{F}_q$,*
2. *for each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t \pmod{x^q - x}$ has degree less than or equal to $q-2$.*

4.2 Some known results

In this section we present some known results regarding PN functions, which will serve as introduction for what we have done. We are interested mainly in PN monomials, i.e. PN functions of the form x^n. The first important result, which can be found in [Glu90], [Hir89] and in [Joh87] is the following.

Theorem 4.2.1 ([RS89], [Joh87], [Hir89] and [Glu90]). *Let f be a PN function over $\mathbb{F}_p$ and suppose f has degree less than p. Then f is a quadratic polynomial.*

This theorem essentially says that over the prime field the only PN functions are the obvious ones. If f is quadratic, then $f(x+a) - f(x)$ will be a linear polynomial, which is clearly bijective.

This result, with some immediate considerations, will give some necessary conditions for PN monomials over $\mathbb{F}_q$. The following Proposition can be found in [CM97].

Proposition 4.2.2 ([CM97]). *The polynomial x^n is PN over $\mathbb{F}_q$ if and only if $(x+1)^n - x^n$ is a permutation polynomial of $\mathbb{F}_q$. Also, if x^n is PN we have $n \equiv 2 \pmod{p-1}$ and $\gcd(n, q-1) = 2$.*

Proof. We know that x^n is PN if and only if $(x+a)^n - x^n$ is a permutation polynomial of $\mathbb{F}_q$ for every $a \in \mathbb{F}_q, a \neq 0$. Because

$$(x+a)^n - x^n = a^n \left((x/a + 1)^n - (x/a)^n \right),$$

and because affine transformations preserve bijectivity, we obtain that x^n is PN if and only if $g(x) = (x+1)^n - x^n$ is a permutation polynomial of $\mathbb{F}_q$. Now, since $g(K) \subset K$ for every subfield K of $\mathbb{F}_q$, we see that $(x+1)^n - x^n$ must also in particular be a permutation polynomial of the prime field. From Theorem 4.2.1, reducing modulo $x^p - x$ we obtain $n \equiv 2 \pmod{p-1}$.
Suppose now x^n is PN. Then there exists only one $c \in \mathbb{F}_q$ such that $(c+1)^n = c^n$. Dividing by c we obtain $(1+1/c)^n = 1$, hence there exists only one $y \in \mathbb{F}_q$, with $y^n = 1$ and $y \neq 1$. Therefore there are only two solutions in $\mathbb{F}_q$ of the equation $y^n - 1$ and this implies $\gcd(n, q-1) = 2$. □

We note that if $f = x^n$ is PN, then also $g = x^{pn}$ has this property. In fact $g(x+1)-g(x) = (f(x+1)-f(x))^p$ and the p-th power maps in characteristic p are automorphisms.

We will now present here the class of Dembowski-Ostrom polynomials. They have the form

$$f(x) = \sum_{i,j=0}^{e-1} a_{ij} x^{p^i+p^j},$$

where $q = p^e$ and $a_{i,j} \in \mathbb{F}_q$.

We have then the following result, which can be found in [DO68].

Proposition 4.2.3. *Suppose $f \in \mathbb{F}_q[x]$ is a Dembowski-Ostrom polynomial as described above. Then f is PN if it satisfies the following condition:*

$$\sum_{i,j=0}^{e-1} a_{ij}(t^{p^i}s^{p^j} + s^{p^i}t^{p^j}) = 0 \text{ if and only if } s = 0 \text{ or } t = 0, \text{ with } s,t \in \mathbb{F}_q.$$

One of the main conjectures in this field asks if every PN function, up to addition of an additive polynomial, is a Dembowski-Ostrom polynomial. This fails in characteristic 3, but it is still open for larger characteristics.

A special class of Dembowski-Ostrom polynomials are monomials of the form $x^{p^\alpha+1}$ over $\mathbb{F}_q$. For this class we have a complete result.

Proposition 4.2.4 ([CM97])**.** *Let $f = x^{p^\alpha+1}$. Then f is PN over $\mathbb{F}_{p^e}$ if and only if $e/(\alpha, e)$ is odd.*

Suppose now that $q = p^2, p \geq 3$. Then a result of Coulter tells us that the previous conjecture holds in this case.

Theorem 4.2.5 ([Cou06])**.** *The monomial x^n is PN over $\mathbb{F}_{p^2}$, p an odd prime, if and only if $n \equiv 2 \pmod{p^2-1}$ or $n \equiv 2p \pmod{p^2-1}$.*

Thus the only PN monomials of degree less than p^2 over $\mathbb{F}_{p^2}$ are x^2 and x^{2p}, the trivial ones.

In order to prove the theorem the author uses condition $n \equiv 2 \pmod{p-1}$ and the Hermite-Dickson criterion. The latter is used to exclude some cases, looking for some t such that $((x+1)^n - x^n)^t$ has degree $q-1$ and therefore it cannot be a permutation polynomial.

In 2012, Coulter and Lazebnik published an article, namely [CL12], in which they prove the corresponding result over $\mathbb{F}_{p^4}$. While unaware of their article we obtained the same result. Because our proof of Theorem 4.2.6 is, up to organization, very similar to that of Coulter and Lazebnik, we limit ourselves to providing a sketch of the argument, which will be useful in order to understand the structure of the proofs presented in the next section.

Theorem 4.2.6. *The monomial x^n is PN over $\mathbb{F}_{p^4}$, for $p > 3$, if and only if $n \equiv 2, 2p, 2p^2, 2p^3 \pmod{p^4-1}$.*

The following lemma is well known.

Lemma 4.2.7 ([Luc78a], [Luc78c], [Luc78b])**.** *Let p be a prime and let α, β be non-negative integers with base p expansions $\alpha = \sum_i \alpha_i p^i$ and $\beta = \sum_j \beta_j p^j$. Then*

$$\binom{\alpha}{\beta} \equiv \prod_i \binom{\alpha_i}{\beta_i} \pmod{p},$$

where we use the convention $\binom{n}{k} = 0$, if $n < k$.

Sketch of proof of 4.2.6. Since we are interested in functions rather than polynomials, we can suppose $n \leq p^4 - 1$. We then write n in base p. Hence we have $n = a + bp + cp^2 + dp^3$. Since $n \equiv 2 \pmod{p-1}$, we have four cases: $a + b + c + d \in \{2, p+1, 2p, 3p-1\}$. We start with the first case.

Case 1. Suppose $a + b + c + d = 2$. Then we have the possibilities $(a, b, c, d) = (2, 0, 0, 0)$, $(a, b, c, d) = (1, 1, 0, 0)$, $(a, b, c, d) = (1, 0, 1, 0)$ and $(a, b, c, d) = (1, 0, 0, 1)$. Here we used the fact that x^n is PN if and only if x^{pn} is, hence we can assume n not divisible by p. The first case corresponds to $n = 2$, the others to $1 + p, 1 + p^2$ and $1 + p^3$, respectively. In these three last cases x^n is not a PN function by Proposition 4.2.4 therefore x^2 is the only PN function in this case.

Case 2. We suppose now $a + b + c + d = p + 1$, say $a + c = k$ and $b + d = p + 1 - k$. Using the fact that x^n is a PN function over the subfield $\mathbb{F}_{p^2}$, we must have $n \equiv 2 \pmod{p^2-1}$ or $n \equiv 2p \pmod{p^2-1}$. If $k = 0$ or $k = p + 1$ we obtain $n \equiv p + 1 \pmod{p^2-1}$ and x^n is not PN over $\mathbb{F}_{p^2}$. Suppose $2 \leq k \leq p - 1$. Considering $n \pmod{p^2-1}$ we obtain that it is congruent to $a+c+(b+d)p$. Therefore $n \equiv k+(p+1-k)p \pmod{p^2-1}$ and x^n with this choice is not PN over $\mathbb{F}_{p^2}$. If $k = 1$ we obtain $n \equiv 1 + p^2 \equiv 2 \pmod{p^2-1}$ and for $k = p$, by symmetry, we obtain $n \equiv 2p \pmod{p^2-1}$. We consider the case $a + c = 1$ (the other is obtained multiplying this one by p or p^3) and we assume that $a = 1$ and $c = 0$. We need only to show that all the possible values $n = 1 + bp + (p - b)p^3$ give rise to monomials which are not PN.
There are three subcases, namely $b \in \{2, \ldots, p-2\}$, $b = 1$ and $b = p - 1$. In the first case the conclusion is reached considering $((x+1)^n - x^n)^{1+p+p^2+p^3}$ and showing that this polynomial has degree $p^4 - 1$, hence by the Hermite-Dickson criterion it is not a permutation polynomial. We write the explicit computations for the term $(x+1)^{n(1+p)}x^{n(p^2+p^3)}$ to show how we use the binomial theorem and Lemma 4.2.7. We can expand the term using the

binomial theorem and obtain

$$\sum_{(\alpha_i),(\beta_i),(\gamma_i)} c_{\alpha_i,\beta_i,\gamma_i} x^{\alpha_1+\gamma_2+b+(\beta_1+\alpha_2+p-b)p+(\beta_2+1+p-b)p^2+(\gamma_1+b+1)p^3},$$

where $i \in \{1,2\}, \alpha_i \in \{0,1\}, \beta_i \in \{0,\dots,b\}, \gamma_i \in \{0,\dots,p-b\}$ and

$$c_{\alpha_i,\beta_i,\gamma_i} = \prod_{i=1}^{2} \binom{1}{\alpha_i}\binom{b}{\beta_i}\binom{p-b}{\gamma_i}.$$

The coefficient of the monomial of degree p^4-1 is obtained when we consider $\alpha_1+\gamma_2+b = p-1, \beta_1+\alpha_2+p-b = p-1, \beta_2 = b-2$ and $\gamma_1 = p-b-2$. We expand it and obtain

$$\left(\binom{1}{0}\binom{p-b}{p-b-1} + \binom{1}{1}\binom{p-b}{p-b-2}\right)\left(\binom{1}{0}\binom{b}{b-1} + \binom{1}{1}\binom{b}{b-2}\right)\cdot$$

$$\cdot\binom{b}{b-2}\binom{p-b}{p-b-2} \equiv$$

$$\equiv \left(-b+\frac{b(b+1)}{2}\right)\left(b+\frac{b(b-1)}{2}\right)\frac{b(b-1)}{2}\frac{b(b+1)}{2} \equiv \frac{b^4(b^2-1)^2}{16} \pmod{p}.$$

To reach the conclusion we have to argue in a similar way for every term.

If $b = 1$ we can reach the conclusion applying the Hermite-Dickson criterion using the exponent $1+2p+p^2+2p^3$ (we note that in this case Coulter and Lazebnik used the exponent p^2-1).
If $b = p-1$ we consider the exponent p^2-1 and this allows us to conclude.

Case 3. We have $a+b+c+d = 2p$. Suppose $a+c = k$ and $b+d = 2p-k$. We use the fact that x^n is a PN function over the subfield $\mathbb{F}_{p^2}$. Suppose $2 \le k \le p-2$. Considering $n \pmod{p^2-1}$ we obtain $a+c+(b+d)p$. Hence $n \equiv k+(2p-k)p \equiv k+1+(p-k)p$. This is not PN over $\mathbb{F}_{p^2}$ by Theorem 4.2.5. By symmetry if $p+2 \le k \le 2p-2$ we obtain $n \equiv k-p+(2p-k+1)p \pmod{p^2-1}$ and for the same reason this is not PN. If $k = p$ we have $n \equiv 1+p \pmod{p^2-1}$ and this is not PN. Thus there are only the two cases $k \in \{p-1, p+1\}$, which correspond to $n \equiv 2p$ and $n \equiv 2$, respectively. Up to multiplying by p^2 we can consider the first case only, namely $a+c = p-1$ and $b+d = p+1$. We can now exclude that $f = (x+1)^n - x^n$ is a permutation polynomial considering $f^{p^2+1} \pmod{x^{p^4}-x}$ and showing that it has degree p^4-1.

Case 4. We have $a+b+c+d = 3p-1$. This implies $a+c \ge p+1$ and $b+d \ge p+1$. Now we use the fact that x^n is a PN function over the subfield $\mathbb{F}_{p^2}$. If we consider $n \pmod{p^2-1}$ we obtain $a+c+(b+d)p$. Thus,

suppose $a+c = p+1+k$, with $0 \leq k \leq p-3$. We obtain $a+c+(b+d)p \equiv 1+k+(2p-1-k)p \equiv 2+k+(p-1-k)p$. Now, from Theorem 4.2.5 we have that $x^{2+k+(p-1-k)p}$ is not a planar function over $\mathbb{F}_{p^2}$ and we are done. □

The hypothesis on the characteristic in Theorem 4.2.6 is fundamental.

Proposition 4.2.8 ([CM97]). *Let $q = 3^e$ and $\alpha \in \mathbb{N}$. Then the polynomial $x^{(3^\alpha+1)/2}$ is PN over $\mathbb{F}_q$ if and only if $\gcd(\alpha, e) = 1$ and α is odd. Moreover, let $n = (3^\alpha + q)/2$, with $\alpha \in \mathbb{N}$. Then x^n is PN over $\mathbb{F}_q$ if and only if $\gcd(\alpha, e) = 1$ and $\alpha - e$ is odd.*

We note immediately that these PN polynomials are not Dembowki-Ostrom. Anyway, for larger characteristics the conjecture still holds. Zieve recently proved the following results.

Theorem 4.2.9 ([Zie13]). *Suppose x^n is PN over $\mathbb{F}_{p^r}$, where $p^r \geq (n-1)^4$ and $p \nmid n$. Then, either $n = p^i + 1$ with $0 \leq i < r$ and $r/(i, r)$ is odd, or $n = (3^i + 1)/2$ if $p = 3$ with $2 < i < r$ and $\gcd(i, 2r) = 1$.*

Corollary 4.2.10 ([Zie13]). *For any prime p and any positive integer n, the function $x \mapsto x^n$ is PN over $\mathbb{F}_{p^k}$ for infinitely many k if and only if either*

1. *$n = p^i + p^j$ where p is odd and $i \geq j \geq 0$, or*
2. *$n = \dfrac{3^i + 3^j}{2}$ where $p = 3$ and $i > j \geq 0$ with $i \not\equiv j \pmod 2$.*

This important result implies that the conjecture is true for all large q.

It is worth noting that, while we have results for $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^4}$, the conjecture is still open over $\mathbb{F}_{p^3}$. The method used by Coulter and Matthews, based on Hermite's criterion, does not apply well in this last case.

4.3 A generalization

In this section we try to generalize the results of the previous section for higher order *derivatives*.

Definition 4.3.1. Let f be a polynomial over $\mathbb{F}_q$. We define the k-th finite difference in directions $(a_1, \ldots, a_k)$ as:

$$\nabla^k_{a_1,\ldots,a_k} f = g(x + a_k) - g(x),$$

where $g(x) = \nabla^{k-1}_{a_1,\ldots,a_{k-1}} f$ and $\nabla^1_a f = f(x + a) - f(x)$. Now we say that a polynomial $f \in \mathbb{F}_q[x]$ is k-PN over $\mathbb{F}_q$ if the function associated to $\nabla^k_{a_1,\ldots,a_k} f$ is a bijection for every choice of $(a_1, \ldots, a_k)$, with $a_i \in \mathbb{F}_q, a_i \neq 0$, for all i.

For example we see immediately that the $(k-1)$-finite difference of x^k is $k!a_1a_2\cdots a_kx+c$, where c is a constant, hence x^k is $(k-1)$-PN over $\mathbb{F}_q$ as long as $p\nmid k!$. Consider now for example the second derivative in directions $(1,1)$ in characteristic 3. We obtain $\nabla^2_{1,1}f = f(x+2)+f(x+1)+f(x)$. Therefore, we note that if a is a solution of $f(a+2)+f(a+1)+f(a)=b$ for some $b\in\mathbb{F}_q$ we have that $a+1$ and $a+2$ are solutions of the same equation. Hence the map cannot be a bijection. The same thing happens for higher characteristic. This is nothing but the generalization of the fact that in even characteristic there cannot be PN functions.

We focus our attention to k-PN monomials and we see the first results we have. We need a lemma.

Lemma 4.3.2. *Let f be a polynomial in $\mathbb{F}_{p^k}[x]$ and suppose $\gcd(\deg(f),p)=1$. Then $f(x+a)-f(x)$ with $a\in\mathbb{F}_{p^k}, a\neq 0$ has degree $\deg(f)-1$.*

Proof. Since the finite difference operator is linear, we consider a monomial x^n, where $p\nmid n$. Then we have that the monomial of highest degree in $(x+a)^n-x^n$ is nax^{n-1}, and we are done. □

Theorem 4.3.3. *Suppose x^n is k-PN over $\mathbb{F}_p$, where $n\leq p-1$ and $p\geq k+2$. Then $n=k+1$.*

Proof. We know from Theorem 4.2.1 that a polynomial f such that $f(x+a)-f(x)$ is a permutation polynomial for every $a\in\mathbb{F}_q, a\neq 0$ must be a quadratic polynomial. This implies that $\nabla^{k-1}_{a_1,\cdots,a_{k-1}}x^n$ has degree 2. Every time we apply the finite difference operator the degree drops by 1. Therefore we must have that $n=k+1$. □

Theorem 4.3.3 says that over the prime field only the trivial k-PN monomial has this property. Consider now a quadratic extension of this field. Thus we are trying to determine k-PN monomials over $\mathbb{F}_{p^2}$.

Theorem 4.3.4. *Suppose x^n is a k-PN monomial over $\mathbb{F}_{p^2}$ with $p\geq 2k+2$ and $n\leq p^2-1$. Then, writing $n=a+bp$, we have $a+b=k+1$.*

Proof. Consider $g=\nabla^k_{a_1,\ldots,a_k}f$, where $a_i\in\mathbb{F}_p$. Since g is defined over $\mathbb{F}_p$ we have that $g(\mathbb{F}_p)\subset\mathbb{F}_p$, hence g should be a permutation polynomial of the prime field for every choice of the k directions. From Theorem 4.3.3 we know that $n\equiv k+1 \pmod{p-1}$.
Let now $f(x)$ be the k-th derivative (always in direction 1) of x^n. We have

$$f(x)=(-1)^k\sum_{i=0}^{k}(-1)^i\binom{k}{i}(x+i)^n.$$

If we write $n=a+bp$ we have two possible cases, $a+b=k+1$ and $a+b=p+k$. We want to exclude the latter. We consider $f^{1+p} \pmod{x^{p^2}-x}$ and show

that it has degree p^2-1. Then, by the Hermite-Dickson Criterion, f cannot be a permutation polynomial.
We have

$$f(x)^{1+p}=\sum_{i=0}^{k}\sum_{j=0}^{k}(-1)^{i+j}\binom{k}{i}\binom{k}{j}(x+i)^n(x+j)^{pn}.$$

Consider now the single term $(x+i)^n(x+j)^{pn}$, $i,j\neq 0$. Expanding it we obtain

$$\sum_{\alpha=0}^{a}\sum_{\beta=0}^{b}\sum_{\gamma=0}^{a}\sum_{\delta=0}^{b}\binom{a}{\alpha}\binom{b}{\beta}\binom{a}{\gamma}\binom{b}{\delta}i^{a-\alpha+(b-\beta)p}j^{a-\gamma+(b-\beta)p}x^{\alpha+\delta+(\beta+\gamma)p}.$$

Since $\alpha+\delta+(\beta+\gamma)p<(p+(p-1)/2)+(p+(p-1)/2)p<2(p^2-1)$ for $p\geq 5$, we need to consider only the case $\alpha+\delta=\beta+\gamma=p-1$.
Hence the coefficient c of the term of degree p^2-1 will be

$$\sum_{\alpha=a-k-1}^{a}\sum_{\beta=b-k-1}^{b}\binom{a}{\alpha}\binom{b}{\beta}\binom{a}{p-1-\beta}\binom{b}{p-1-\alpha}i^{a-\alpha+b-\beta}j^{a-\gamma+b-\beta}.$$

We rewrite this sum as C_1C_2 where

$$C_1=\left(\sum_{\alpha=a-k-1}^{a}\binom{a}{\alpha}\binom{b}{\alpha+1+k-a}i^{a-\alpha}j^{\alpha+1+k-a}\right)$$

and

$$C_2=\left(\sum_{\beta=b-k-1}^{b}\binom{b}{\beta}\binom{a}{\beta+1+k-a}i^{b-\beta}j^{\beta+1+k-b}\right).$$

Finally we obtain

$$\left(\sum_{l=0}^{k+1}\binom{a}{k+1-l}\binom{b}{l}i^{k+1-l}j^{l}\right)\left(\sum_{l=0}^{k+1}\binom{b}{k+1-l}\binom{a}{l}i^{k+1-l}j^{l}\right).$$

Consider the single term $\binom{a}{k+1-l}\binom{b}{l}$. Using the fact that $a+b\equiv k \pmod p$ we have

$$\binom{b}{l}=\frac{b(b-1)\cdots(b-l+1)}{l!}\equiv(-1)^l\frac{(a-k)(a-k+1)\cdots(a-k+l-1)}{l!}.$$

Therefore

$$\binom{a}{k+1-l}\binom{b}{l}\equiv(-1)^l\binom{a}{k+1}\binom{k+1}{l}\pmod p.$$

Finally, we see that c is equivalent modulo p to

$$\left(\binom{a}{k+1}\sum_{l=0}^{k+1}(-1)^l\binom{k+1}{l}i^{k+1-l}j^l\right)\left(\binom{b}{k+1}\sum_{l=0}^{k+1}(-1)^l\binom{k+1}{l}i^{k+1-l}j^l\right).$$

Noting that $\binom{b}{k+1} \equiv (-1)^{k+1}\binom{a}{k+1} \pmod p$ we have that

$$c \equiv (-1)^{k+1}\binom{a}{k+1}^2(i-j)^{2k+2} \pmod p.$$

Consider now the term $x^n(x+j)^{pn}$. Expanding it we obtain

$$\sum_{\alpha=0}^{a}\sum_{\beta=0}^{b}\binom{a}{\alpha}\binom{b}{\beta}j^{a-\alpha+(b-\beta)p}x^{a+\beta+(\alpha+b)p}.$$

As before we need only to consider the case $a+\beta = \alpha+b = p-1$. Thus the coefficient c of the term of degree p^2-1 will be

$$c = \binom{a}{k+1}\binom{b}{k+1}j^{2k+2} \equiv (-1)^{k+1}\binom{a}{k+1}^2 j^{2k+2}.$$

In the same way we see that the monomial of degree p^2-1 of $x^{np}(x+i)^n$ has the same coefficient.

We have seen that the coefficient modulo p of the term of degree p^2-1 of $(x+i)^n(x+j)^{pn} \pmod{x^{p^2}-x}$ equals $(-1)^{k+1}\binom{a}{k+1}^2(i-j)^{2k+2}$. Summing up all the terms we obtain that the coefficient of the term of degree p^2-1 of $f(x)^{1+p} \pmod{x^{p^2}-x}$ is

$$(-1)^{k+1}\binom{a}{k+1}^2\sum_{i=0}^{k}\sum_{j=0}^{k}(-1)^{i+j}\binom{k}{i}\binom{k}{j}(i-j)^{2k+2}.$$

According to the following Lemma this sum is not zero, for the given choice of $p \geq 2k+2$. □

To conclude the proof we only need the following result.

Lemma 4.3.5. *Let*

$$S(k,r) = \sum_{i=0}^{k}\sum_{j=0}^{k}(-1)^{i+j}\binom{k}{i}\binom{k}{j}(i-j)^r.$$

Then $S(k,r) = 0$ *if* r *is odd or if* $r < 2k$,

$$S(k,2k) = (-1)^k(2k)!$$

and

$$S(k,2k+2) = (-1)^k(2k)!k(k+1)(2k+1)/6 = (-1)^k(2k)!(1+2^2+\cdots+k^2).$$

Proof. We note that when r is odd the given sum is zero, since the coefficient of $(i-j)^r$ and $(j-i)^r$ is the same.
Changing indices of the sum we obtain

$$S(k,r) = \sum_{j=0}^{k} \sum_{i=-j}^{k-j} (-1)^i \binom{k}{j} \binom{k}{j+i} i^r = \sum_j \binom{k}{j} \sum_i (-1)^i \binom{k}{j+i} i^r.$$

This is the evaluation in $x=-1$ of the polynomial

$$\sum_{j=0}^{k} \binom{k}{j} (xD)^r \sum_{i=-j}^{k-j} \binom{k}{j+i} x^i = \sum_{j=0}^{k} \binom{k}{j} (xD)^r \frac{(1+x)^k}{x^j},$$

where $(xD)(f) = xD(f)$ and D is the standard derivative. By linearity of this operator we can exchange the sums and we obtain that $S(k,r)$ is the evaluation at $x=-1$ of

$$(xD)^r (1+1/x)^k (1+x)^k = (xD)^r \frac{(1+x)^{2k}}{x^k}.$$

By direct computation we see that

$$(xD)\frac{(1+x)^i}{x^j} = \frac{i(1+x)^{i-1}}{x^{j-1}} - \frac{j(1+x)^i}{x^j}.$$

Since the exponent of $(1+x)$ in the numerator decreases at most by one every time we apply the operator xD, we have that, if $r < 2k$, the numerator of $(xD)^r \frac{(1+x)^{2k}}{x^k}$ is divisible by $1+x$ and therefore, evaluating at -1, we obtain zero.
From the above formula we see that applying $k-1$ times the operator we obtain $(2k)_{k-1} \frac{(1+x)^{k+1}}{x} + p$, where p is divisible by $(1+x)^{k+2}$. Now $(xD)(1+x)^i/x = i(1+x)^{i-1} - (1+x)^i/x$. From this we have that

$$(xD)^k \frac{(1+x)^{2k}}{x^k} = (2k)_k (1+x)^k + q,$$

where q is divisible by $(1+x)^{k+1}$.

Now $(xD)(1+x)^i = ix(1+x)^{i-1}$ and $(xD)(ix(1+x)^{i-1}) = i(i-1)x^2(1+x)^{i-2} + ix(1+x)^i$. From this formula we immediately see that

$$(xD)^{2k} \frac{(1+x)^{2k}}{x^k} = (2k)! x^k + s,$$

where s is divisible by $(1+x)$. Thus, evaluating it at $x=-1$, we obtain $S(k,2k) = (-1)^k (2k)!$.
To prove the thesis for $r = 2k+2$ we will use induction. By direct computation we see that the conclusion is true for $k \in \{1,2,3\}$.

Taking the second derivative, we have to consider the evaluation at $x = -1$ of

$$(xD)^{2k}\left((xD)^2\frac{(1+x)^{2k}}{x^k}\right) = (xD)^{2k}\left(k^2\frac{(1+x)^{2k}}{x^k} - 2k(2k-1)\frac{(1+x)^{2k-2}}{x^{k-1}}\right).$$

The first term is $k^2S(k,2k) = (-1)^k k^2(2k)!$. We apply now the inductive hypothesis on the second term and we obtain $-2k(2k-1)(-1)^{k-1}(2k-2)!(1+2^2+\cdots+(k-1)^2)$. Summing these two terms we get $(-1)^k(2k)!(1+2^2+\cdots+k^2)$ and the conclusion has been proved. □

In general we cannot obtain a complete classification of k-PN over $\mathbb{F}_{p^2}$ for arbitrary k, but we can complete the discussion for $k = 2$ and $k = 3$, considering the cases left.

Proposition 4.3.6. *Suppose x^n is 2-PN over $\mathbb{F}_{p^2}, p \geq 5$, and $n \leq p^2 - 1$. Then $n \in \{3, 3p\}$ if $p \equiv -1 \pmod 3$, and $n \in \{3, 3p, 1+2p, 2+p\}$ if $p \equiv 1 \pmod 3$. If x^n is 3-PN over $\mathbb{F}_{p^2}$ and $n \leq p^2 - 1$, then $n \in \{4, 4p\}$.*

Note that, differently from the PN case, we now have some results depending on the value modulo 3 of the prime p.

Proof. If $f = x^3$, its second derivative in directions d and e is $6dex + s$ for some constant s and that is clearly a permutation polynomial. Now, consider the case $n = 2 + p$, the other case being obtained by taking the p-th power.

Thus, let $f = x^{2+p}$. Then we have $\nabla_{d,e}f = 2dex^p + (2de^p + 2d^pe)x + s$ for some constant s. We know that a p-polynomial is permutation if and only if it has only one zero. Therefore $\nabla_{d,e}f$ is a permutation polynomial if and only if the equation $u^{p-1} + y^{p-1} + z^{p-1} = 0$ has no solution with $u, y, z \in \mathbb{F}_{p^2}^*$. Dividing by z^{p-1} this is equivalent to requiring that the equation $u^{p-1} + y^{p-1} + 1 = 0$ has no solution with $u, y \in \mathbb{F}_{p^2}^*$. Suppose now (u, y) is such a solution and let $z = u^{p-1}$. Then $y^{p-1} = -1 - z$. Since the $(p-1)$-th powers in $\mathbb{F}_{p^2}^*$ are precisely elements of norm 1 we have $z^{p+1} = (-1-z)^{p+1} = 1$. From these equations we obtain $z^p + z = -1$. Hence z has norm 1 and trace -1. Its minimal polynomial is $z^2 + z + 1$, thus z is a primitive third root of unity and we must have $p \equiv -1 \pmod 3$, since z is not an element of the prime field. Conversely, if $p \equiv -1 \pmod 3$, let z be a primitive third root of unity in $\mathbb{F}_{p^2}$. Since $p - 1 \equiv 1 \pmod 3$ we have that $z^{p-1} = z$. Hence, taking $u = z$ and $y = z^p$ we obtain a solution of $u^{p-1} + y^{p-1} + 1 = 0$.

Now, let $k = 3$. If $f = x^4$ we have $\nabla_{c,d,e}f = 24cdex + s$ for some constant s and this is a permutation polynomial. Now, let $n = 3 + p$. We have $\nabla_{c,d,e}x^n = 6cdex^p + (6c^pde + 6cd^pe + 6cde^p)x + s$ for some constant s.

This is a permutation polynomial if and only if the equation $u^{p-1} + v^{p-1} + w^{p-1} + t^{p-1} = 0$ has no solutions in $\mathbb{F}_{p^2}^*$. But -1 has norm 1, hence there is $z \in \mathbb{F}_{p^2}$ such that $z^{p-1} = -1$. Then $(1, 1, z, z)$ is a solution of the previous equation.

The last case is $n = 2 + 2p$. We have $\nabla_{1,1,1} x^n = 12x^p + 12x + s$ for some constant s. But now $x^p + x$ is not a permutation polynomial of $\mathbb{F}_{p^2}$ since, as before, there exists z with $z^{p-1} = -1$.
For $p = 5$ and $p = 7$ the conclusion of the theorem follows by direct computation. □

Remark. It is worth mentioning the recent work of Voloch and Zieve, [VZ13], where the two authors describe accurately the points of Fermat curves and surfaces.

As in the PN case, we obtain some results over $\mathbb{F}_{p^4}$ when $k = 2$ or $k = 3$. We need the following result.

Lemma 4.3.7. *Suppose $p \geq 5$ and consider the field extension $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$. Then there exists a non-square element m in $\mathbb{F}_{p^2}$ such that* $\mathrm{Norm}(1+m) = 4$.

Proof. Consider the basis $(1, s)$ of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$, where $s^2 = t$, a non-square element in the base field. We write $m = m_1 + m_2 s$ and let $k = \mathrm{Norm}(1+m) = m_1^2 - t m_2^2$. We need to find m_1 and m_2 in $\mathbb{F}_p$ such that m is not a square and $(1 + m_1 + m_2 s)(1 + m_1 + m_2 s)^p = 4$. If we expand it we obtain the equation $2m_1 + k - 3 = 0$. Consider the following system:

$$\begin{cases} 2m_1 + k - 3 = 0 \\ m_1^2 - t m_2^2 = k \end{cases}$$

We need to find a solution (m_1, m_2, k) such that k is not a square in $\mathbb{F}_p$. From the first equation we obtain $2m_1 = 3 - k$. Substituting in the second one we obtain

$$4t m_2^2 = k^2 - 10k + 9.$$

If we find $k \in \mathbb{F}_p$ such that both k and $k^2 - 10k + 9$ are not squares we are done, since we can take m_2 satisfying $m_2^2 = (k^2 - 10k + 9)/4t$. We note that $f(k) = k^2 - 10k + 9 = (k-1)(k-9)$. Because the equation $k^2 - 10k + 9 = h^2$ can be written as $(k + h - 5)(k - h - 5) = 16$, it has exactly $p - 1$ solutions $(k, h) \in \mathbb{F}_p^2$. Four of them are $(1, 0)$, $(9, 0)$ and $(0, \pm 3)$. Hence the equation can have at most $p - 5$ solutions where k is not a square. Because those come in pairs $(k, \pm h)$, there are at least two of the $(p-1)/2$ non-squares k in $\mathbb{F}_p$ such that $k^2 - 10k + 9$ is not a square. □

Theorem 4.3.8. *Let $f = x^n$ be a 2-PN monomial over $\mathbb{F}_{p^4}, p \geq 5$, $\deg(f) \leq p^4 - 1$ and suppose n not divisible by p. Then $n \in \{3, 2 + p^2, 1 + 2p^2\}$.*

Proof. Let $f = x^n$ and $n = a + bp + cp^2 + dp^3$. From Theorem 4.3.3 we know that $n \equiv 3 \pmod{p-1}$. Hence we have that $a+b+c+d \in \{3, p+2, 2p+1, 3p\}$. We consider each case separately.

Case 1. Suppose $a+b+c+d = 3$. We can assume $a \neq 0$, thus we have, up to multiplying by some power of p, that $n \in \{3, 2+p, 2+p^2, 2+p^3, 1+p+p^2\}$. Suppose $n = 2 + p$. We have

$$\nabla_{u,v} f = 2uvx^p + (2uv^p + 2u^p v)x + s,$$

for some constant s. This is a permutation polynomial if and only if the equation $y^{p-1} + z^{p-1} + t^{p-1} = 0$ has no solutions in $\mathbb{F}^*_{p^4}$. We recall Weil's bound for the number of $\mathbb{F}_q$-rational projective points N of a smooth curve in $\mathbb{P}^2(\mathbb{F}_q)$. We have

$$|N - q - 1| \leq 2g\sqrt{q},$$

where $g = \frac{(d-1)(d-2)}{2}$ is the genus of the curve and d is the degree of the defining polynomial. In our case the lower bound reads $N \geq 5p^3 - 6p^2 + 1$. We are interested in solutions (y, z, t), where $yzt \neq 0$. The equation $y^{p-1} + z^{p-1} = 0$ has $p - 1$ (projective) solutions, hence in total we have to exclude $3(p - 1)$ solutions from the number obtained before. But $5p^3 - 6p^2 + 1 > 3(p - 1)$, therefore we always have solutions in $\mathbb{F}^*_{p^4}$.

Suppose $n = 2 + p^3$. We have

$$\nabla_{u,v} f = 2uvx^{p^3} + (2uv^{p^3} + 2u^{p^3} v)x + s,$$

for some constant s. This is a permutation polynomial if and only if $y^{p^3-1} + z^{p^3-1} + t^{p^3-1} = 0$ has no solutions in $\mathbb{F}^*_{p^4}$. Since $\gcd(p^3 - 1, p^4 - 1) = p - 1$ the number of solutions of this equation is the same as in the previous case, hence we can conclude as before.

Suppose $n = 2 + p^2$. We have

$$\nabla_{u,v} f = 2uvx^{p^2} + (2uv^{p^2} + 2u^{p^2} v)x + s,$$

for some constant s. This is a permutation polynomial if and only if $y^{p^2-1} + z^{p^2-1} + t^{p^2-1} = 0$ has no solution with $y, z, t \in \mathbb{F}^*_{p^4}$, if and only if $y^{p^2-1} + z^{p^2-1} + 1 = 0$ has no solution with $y, z \in \mathbb{F}^*_{p^4}$. Suppose (y, z) is a solution and let $w = y^{p^2-1}$. We have $w^{p^2+1} = 1$. We also have $(-1 - w)^{p^2+1} = 1$. Substituting the first equation in the last one we obtain $w^{p^2} + w + 1 = 0$. Therefore $w^{p^2} = -1 - z$ and this gives, using the first equation, $w(-1-w) = 1$, i.e. $w^2 + w + 1 = 0$. This is an equation of degree 2 over $\mathbb{F}_p$, therefore $w \in \mathbb{F}_{p^2}$. But then $w^{p^2} = z$ and $w^{p^2} + w + 1 = 2w + 1$. This is zero if and only if $w = -1/2$. Since w has norm 1 we must have $2^4 \equiv 1 \pmod{p}$, therefore $p = 5$. But in $\mathbb{F}_5$ we have that $x^2 + x + 1$ is irreducible, therefore

$w = -1/w \equiv 2 \pmod 5$ cannot satisfy $w^2 + w + 1 = 0$. Hence we do not have a solution and the polynomial is a permutation polynomial.

Suppose now $n = 1 + p + p^2$. We have

$$\nabla_{1,v} f = (v + v^p)x^{p^2} + (v + v^{p^2})x^p + (v^p + v^{p^2})x + s,$$

for some constant s. We will now find a solution $(v, x), vx \neq 0$, for the equation $\nabla_{1,v} f - s = 0$ proving that, as a function of x, it is not a permutation polynomial. We consider $\mathbb{F}_{p^4}$ as a vector space of dimension 2 over $\mathbb{F}_{p^2}$ and take $(1, t)$ as basis, with $t^2 = m$, a non-square in F_{p^2}. Let now $v = v_1 + v_2 t$ and $x = x_1 + x_2 t$ the decomposition of v and x over our basis. Rewriting the previous equation we obtain the following system of two equations:

$$\begin{cases} x_1 v_1 + x_1^p v_1 + x_1 v_1^p - m v_2 x_2 = 0 \\ c v_1 x_2^p + c x_1 v_2^p = 0 \end{cases}$$

where $c = t^{p-1} \in \mathbb{F}_{p^2}$.

Set now $v_1 = v_2 = 1$. We have $x_2^p = -x_1$, hence $x_2 = -x_1^p$. Putting it in the first equation we obtain

$$(1 + m)x_1^p + 2x_1 = 0.$$

We know that this equation has a solution in $\mathbb{F}_{p^2}$ if and only if $2/(1+m)$ (as element of $\mathbb{F}_{p^2}$) has norm 1 over $\mathbb{F}_p$. Since by Lemma 4.3.7 we can choose a non-square m with this property, we solve the system, hence proving that x^{1+p+p^2} is not 2-PN over $\mathbb{F}_{p^4}$.

Case 2. Suppose now $n = a + bp + cp^2 + dp^3$ and $a + b + c + d = p + 2$. We will show that $g = (\nabla_{1,t} f)^{1+p+p^2+p^3}$ has degree $p^4 - 1$ for some direction t, hence it is not a permutation polynomial. We have $\nabla_{1,t} f = x^n - (x+1)^n - (x+t)^n + (x+1+t)^n$. Hence g will consist of 4^4 terms of the form

$$(x + i)^n (x + j)^{np} (x + k)^{np^2} (x + l)^{np^3},$$

where $i, j, k, l \in \{0, 1, t, 1 + t\}$. Expanding the previous term using the binomial theorem we obtain

$$\sum_{(\alpha_i),(\beta_i),(\gamma_i),(\delta_i)} s x^{\alpha_1+\delta_2+\gamma_3+\beta_4+(\beta_1+\alpha_2+\delta_3+\gamma_4)p+(\gamma_1+\beta_2+\alpha_3+\delta_4)p^2+(\delta_1+\beta_2+\gamma_3+\alpha_4)p^3} I,$$

where $I = i^{e_i} j^{e_j} k^{e_k} l^{e_l}, 0 \leq \alpha_i \leq a, 0 \leq \beta_i \leq b, 0 \leq \gamma_i \leq c, 0 \leq \delta_i \leq d, e_i = a - \alpha_1 + (b - \beta_1)p + (c - \gamma_1)p^2 + (d - \delta_1)p^3, e_j = d - \delta_2 + (a - \alpha_2)p + (b - \beta_2)p^2 + (c - \gamma_2)p^3, e_k = c - \gamma_3 + (d - \delta_3)p + (a - \alpha_3)p^2 + (b - \beta_3)p^3, e_l = b - \beta_4 + (c - \gamma_4)p + (d - \delta_4)p^2 + (a - \alpha_4)p^3$ and

$$s = \prod_{i=1}^{4} \binom{a}{\alpha_i} \prod_{i=1}^{4} \binom{b}{\beta_i} \prod_{i=1}^{4} \binom{c}{\gamma_i} \prod_{i=1}^{4} \binom{d}{\delta_i}.$$

Since $\alpha_1+\delta_2+\gamma_3+\beta_4+(\beta_1+\alpha_2+\delta_3+\gamma_4)p+(\gamma_1+\beta_2+\alpha_3+\delta_4)p^2+(\delta_1+\beta_2+\gamma_3+\alpha_4)p^3<2(p^4-1)$, in order to compute the coefficient M of degree p^4-1 we need to consider only the terms with $\alpha_1+\delta_2+\gamma_3+\beta_4=\beta_1+\alpha_2+\delta_3+\gamma_4=\gamma_1+\beta_2+\alpha_3+\delta_4=\delta_1+\beta_2+\gamma_3+\alpha_4=p-1$. Thus we have that $M=M_1M_2M_3M_4$, where

$$M_1=\sum_{\alpha_1+\delta_2+\gamma_3+\beta_4=p-1}\binom{a}{\alpha_1}\binom{b}{\beta_4}\binom{c}{\gamma_3}\binom{d}{\delta_2}i^{a-\alpha_1}j^{d-\delta_2}k^{c-\gamma_3}l^{b-\beta_4},$$

$$M_2=\sum_{\alpha_2+\delta_3+\gamma_4+\beta_1=p-1}\binom{a}{\alpha_2}\binom{b}{\beta_1}\binom{c}{\gamma_4}\binom{d}{\delta_3}i^{p(b-\beta_1)}j^{p(a-\alpha_2)}k^{p(d-\delta_3)}l^{p(c-\gamma_4)},$$

$$M_3=\sum_{\alpha_3+\delta_4+\gamma_1+\beta_2=p-1}\binom{a}{\alpha_3}\binom{b}{\beta_2}\binom{c}{\gamma_1}\binom{d}{\delta_4}i^{p^2(c-\gamma_1)}j^{p^2(b-\beta_2)}k^{p^2(a-\alpha_3)}l^{p^2(d-\delta_4)},$$

$$M_4=\sum_{\alpha_4+\delta_1+\gamma_2+\beta_3=p-1}\binom{a}{\alpha_4}\binom{b}{\beta_3}\binom{c}{\gamma_2}\binom{d}{\delta_1}i^{p^3(d-\delta_1)}j^{p^3(c-\gamma_2)}k^{p^3(b-\beta_3)}l^{p^3(a-\alpha_4)}.$$

Consider $g=\nabla_{a_1,a_2}f$, where $a_i\in\mathbb{F}_{p^2}$. We have $g(\mathbb{F}_{p^2})\subset\mathbb{F}_{p^2}$, hence f has to be a 2-PN monomial over $\mathbb{F}_{p^2}$. Hence we must have, up to multiplying n by some power of p and reducing modulo $x^{p^4}-x$, $a+c=2$ and $b+d=p$, $a+c=1$ and $b+d=p+1$ or $a+c=0$ and $b+d=p+2$. Except for the last case we can suppose without loss of generality that $a\neq 0$. We then have four possibilities for n: $n=bp+(p+2-b)p^3, 3\leq b\leq p-1$, $n=1+bp+(p+1-b)p^3, 2\leq b\leq p-1$, $n=2+bp+(p-b)p^3, 1\leq b\leq p-1$ and $n=1+bp+p^2+(p-b)p^3, 1\leq b\leq p-1$. We consider each of them in order.

Let $n=bp+(p+2-b)p^3$. We use the previous formula with $a=0, c=0$ and $d=p+2-b$ and we compute M. Let $S(i,j)=\binom{b}{3}(i-j)^3$. Then we have $M_1=S(l,j), M_2=S(i,k)^p, M_3=S(j,l)^{p^2}$ and $M_4=S(k,i)^{p^3}$. Therefore we have

$$M=\binom{b}{3}^4(i-k)^6(j-l)^6.$$

We need now to sum all these terms and we obtain that the coefficient of degree p^4-1 of $\nabla_{1,1}f$ is $14400\binom{b}{3}^4$. For $p\geq 7$ this coefficient is not zero and we are done.

Suppose now $n=1+bp+(p+1-b)p^3$. Now we use the previous formula with $a=1, c=0$ and $d=p+1-b$ and we compute M. Let

$$S(i,j,k,l)=\binom{b}{3}l^3-(b-1)\binom{b}{2}l^2j+b\binom{b}{2}lj^2-\binom{b+1}{3}j^3+\binom{b}{2}i(l-j)^2.$$

Then we have $M_1 = S(i,j,k,l), M_2 = S(j,k,l,i)^p, M_3 = S(k,l,i,j)^{p^2}$ and $M_4 = S(l,i,j,k)^{p^3}$. Summing all these terms, a computer computation shows that the coefficient of degree $p^4 - 1$ of $\nabla_{1,t} f$ is

$$r_1 = \frac{4}{9} b^4 (b-2)(b+1)(b-1)^4 (25b^2 - 25b - 59)$$

when $t = 1$ and

$$r_2 = \frac{8}{9} b^4 (b-1)^4 (1250b^4 - 2500b^3 - 4362b^2 + 5612b + 5981)$$

when $t = 2$. We have $r_2(2) = r_2(-1) = -3456$, which is not zero since $p \geq 5$. This implies that we can exclude the cases $b = 2$ and $b = p - 1$, because they produce polynomials that are not 2-PN. Suppose now $3 \leq b \leq p - 2$. We will show that $p_1 = 25x^2 - 25x - 59$ and $p_2 = 1250x^4 - 2500x^3 - 4362x^2 + 5612x + 5981$ cannot have a common root b in the prime field $\mathbb{F}_p$. Suppose that $p_1(b) \equiv p_2(b) \equiv 0 \pmod{p}$. Suppose $p \neq 5$ and consider $p_3 = p_2 - 50x^2 p_1 + 50x p_1 = -2662x^2 + 2662x + 5981$. We must have $p_3(b) \equiv 0 \pmod{p}$. Suppose $p \neq 11$. Considering $2662p_1 + 25p_3$ we obtain that p must divide $-7533 = -3^5 \cdot 31$. A computer computation shows that p_1 and p_2 are coprime if $p \in \{5, 11\}$. When $p = 31$ their greatest common divisor is $x^2 + 30x + b$, which is irreducible over $\mathbb{F}_{31}$, hence it has no roots in that field. Putting all together we see that, with this choice of n, f cannot be 2-PN.

Let now $n = 2 + bp + (p-b)p^3, 1 \leq b \leq p - 1$. As before, let

$$S(i,j,k,l) = \binom{b}{3} l^3 - b\binom{b}{2} l^2 j + b\binom{b+1}{2} l j^2 - \binom{b+2}{3} j^3 +$$

$$+2i\left(\binom{b}{2} l^2 - b^2 l j + \binom{b+1}{2} j^2\right) + i^2 b(l - j).$$

We have $c_1 = S(i,j,k,l), c_2 = S(j,k,l,i)^p, c_3 = S(k,l,i,j)^{p^2}$ and $c_4 = S(l,i,j,k)^{p^3}$. As in the previous case a computer computation shows that the coefficient of degree $p^4 - 1$ of $(\nabla_{1,t} f)^{1+p+p^2+p^3}$ is

$$r_1 = \frac{4}{9} b^4 (b-1)(b-2)(b+2)(b+1)(25b^4 - 197b^2 + 100)$$

when $t = 1$ and

$$r_2 = \frac{16}{9} b^4 (625b^8 - 8518b^6 + 31641b^4 - 32452b^2 + 10648)$$

when $t = 2$. We have $r_2(1) = r_2(-1) = 3456$ and $r_2(2) = r_2(-2) = 55296$, which are not zero since $p \geq 5$. With the Euclidean algorithm we see that $25x^4 - 197x^2 + 100$ and $625x^8 - 8518x^6 + 31641x^4 - 32452x^2 + 10648$ are coprime modulo p, unless $p \in \{19, 156797\}$. If $p = 19$ their greatest common

divisor is x^2+5, which is irreducible over $\mathbb{F}_{19}$. If $p=156797$ the greatest common divisor is $x^2+79228$ and this is irreducible over $\mathbb{F}_{156797}$. Hence x^n cannot be 2-PN with this choice of n.

Finally, let $n=1+bp+p^3+(p-b)p^3, 1\leq b\leq p-1$. Consider

$$S(i,j,k,l)=\binom{b}{3}l^3-b\binom{b}{2}l^2j+b\binom{b+1}{2}lj^2-\binom{b+2}{3}j^3+$$

$$+(i+k)\left(\binom{b}{2}l^2-b^2lj+\binom{b+1}{2}j^2\right)+ikb(l-j).$$

We have $M_1=S(i,j,k,l), M_2=S(j,k,l,i)^p, M_3=S(k,l,i,j)^{p^2}$ and $M_4=S(l,i,j,k)^{p^3}$. As in the previous cases a computer computation shows that the coefficient of degree p^4-1 of $(\nabla_{1,t}f)^{1+p+p^2+p^3}$ is

$$r_1=\frac{4}{9}b^4(b-1)^2(b+1)^2(25b^4-2b^2+49)$$

when $t=1$ and

$$r_2=\frac{16}{9}b^4(625b^8-1138b^6+2238b^4-1834b^2+2053)$$

when $t=2$. We have $r_2(1)=r_2(-1)=3456$, which is not zero since $p\geq 5$. With the Euclidean algorithm we see that $625x^8-1138x^6+2238x^4-1834x^2+2053$ and $25x^4-2x^2+49$ are coprime modulo p, unless $p=12497$. In this case the greatest common divisor is x^2+9356 and this is irreducible over $\mathbb{F}_{12497}$. Therefore x^n cannot be 2-PN with this choice of n.

Case 3. Let $n=a+bp+cp^2+dp^3$ with $a+b+c+d=2p+1$. We will show that $g=(\nabla_{1,1}f)^{1+p^2}$ has degree p^4-1, hence it is not a permutation polynomial. As before we use the binomial theorem to expand g, obtaining terms of the form

$$(x+i)^n(x+j)^{np^2}=\sum_{(\alpha_i),(\beta_i),(\gamma_i),(\delta_i)} sx^{\alpha_1+\gamma_2+(\beta_1+\delta_2)p+(\gamma_1+\alpha_2)p^2+(\delta_1+\beta_2)p^3}i^{e_i}j^{e_j},$$

where $0\leq\alpha_i\leq a, 0\leq\beta_i\leq b, 0\leq\gamma_i\leq c, 0\leq\delta_i\leq d, e_i=a-\alpha_1+(b-\beta_1)p+(c-\gamma_1)p^2+(d-\delta_1)p^3, e_j=c-\gamma_2+(d-\delta_2)p+(a-\alpha_2)p^2+(b-\beta_2)p^3$ and

$$s=\prod_{i=1}^{2}\binom{a}{\alpha_i}\prod_{i=1}^{2}\binom{b}{\beta_i}\prod_{i=1}^{2}\binom{c}{\gamma_i}\prod_{i=1}^{2}\binom{d}{\delta_i}.$$

Since $\alpha_1+\gamma_2+(\beta_1+\delta_2)p+(\gamma_1+\alpha_2)p^2+(\delta_1+\beta_2)p^3<2(p^4-1)$, in order to compute the coefficient M of degree p^4-1 we need to consider only the

terms with $\alpha_1+\gamma_2=\beta_1+\delta_2=\gamma_1+\alpha_2=\delta_1+\beta_2=p-1$. Thus we have that $M=M_1M_2M_3M_4$, where

$$M_1=\sum_{\alpha_1+\gamma_2=p-1}\binom{a}{\alpha_1}\binom{c}{\gamma_2}i^{a-\alpha_1}j^{c-\gamma_2},$$

$$M_2=\sum_{\beta_1+\delta_2=p-1}\binom{b}{\beta_1}\binom{d}{\delta_2}i^{p(b-\beta_1)}j^{p(d-\delta_2)},$$

$$M_3=\sum_{\alpha_2+\gamma_1=p-1}\binom{a}{\alpha_2}\binom{c}{\gamma_1}i^{p^2(c-\gamma_1)}j^{p^2(a-\alpha_2)},$$

$$M_4=\sum_{\delta_1+\beta_2=p-1}\binom{b}{\beta_2}\binom{d}{\delta_1}i^{p^3(d-\delta_1)}j^{p^3(b-\beta_2)}.$$

As before we reduce $n \pmod{p^2-1}$ since f should be 2-PN over the subfield $\mathbb{F}_{p^2}$. Let $a+c=k$ and $b+d=2p+1-k$. If $3\le k\le p-2$ we have that $n\equiv k+1+(p+1-k)p \pmod{p^2-1}$ and, with this choice of n, f is not 2-PN. If $p+3\le k\le 2p-2$ we have $n\equiv(k-p)+(2p+2-k)p \pmod{p^2-1}$ and we conclude as before. We have four cases left, i.e. $k\in\{p-1,p,p+1,p+2\}$. Without loss of generality we consider only $k=p-1$ and $k=p$, the other two being obtained considering $f^{np^2} \pmod{x^{p^4}-x}$.
Suppose $a+c=p-1$ and $b+d=p+2$. We see immediately that $M_1=M_3=1$. Then we have that M_2 would be equal to

$$\binom{b}{3}i^3+\binom{b}{2}(p+2-b)i^2j+b\binom{p+2-b}{2}ij^2+\binom{p+2-b}{3}j^3\equiv\binom{b}{3}(i-j)^3.$$

Exchanging i and j we obtain M_4, which is then equal to $-\binom{b}{3}(i-j)^3 \pmod p$. Hence we obtain $M\equiv-\binom{b}{3}^2(i-j)^6$. Summing up all the terms in order to obtain the coefficient of degree p^4-1 of $(\nabla_{1,1}f)^{1+p^2}$ we notice that this equals $-\binom{b}{3}^2S(2,6)$ where $S(k,r)$ is the sum we studied in Lemma 4.3.5. Finally we obtain $M\equiv-120\binom{b}{3}^2 \pmod p$. This is nonzero for $p\ge7$.
Now, suppose $a+c=p$ and $b+d=p+1$. Then we have $M_1=ai+cj\equiv a(i-j) \pmod p$ and $M_3\equiv-a(i-j) \pmod p$. Expanding M_2 we obtain

$$\binom{b}{2}i^2+b(p+1-b)ij+\binom{p+1-b}{2}j^2\equiv\binom{b}{2}(i-j)^2 \pmod p.$$

Exchanging i and j we obtain that $M_4\equiv M_2 \pmod p$. Now

$$M=M_1M_2M_3M_4\equiv-a^2\binom{b}{2}^2(i-j)^6.$$

As before, considering all the terms, we have that the coefficient of degree p^4-1 of $(\nabla_{1,1}f)^{1+p^2}$ is $-a^2\binom{b}{2}^2S(2,6)=-120a^2\binom{b}{2}^2$, which is not zero when

$p \geq 7$.

Case 4. Suppose $a+b+c+d = 3p$. Let $a+c = k$ and $b+d = 3p-k$. We have $p+2 \leq k \leq 2p-2$. Reducing modulo p^2-1 we obtain $n \equiv k+1-p+(2p-k+1)p \pmod{p^2-1}$ and, with this choice of n, f is not 2-PN over $\mathbb{F}_{p^2}$.

A computer computation shows that the same conclusion of the theorem holds for $p = 5$. □

Now, we enounce and prove the corresponding theorem for $k = 3$.

Theorem 4.3.9. *Let $f = x^n$ be a 3-PN monomial over $\mathbb{F}_{p^4}, p \geq 5$, $\deg(f) \leq p^4-1$ and suppose n not divisible by p. Then $n = 4$.*

Proof. Let $f = x^n$ and $n = a+bp+cp^2+dp^3$. We know that $n \equiv 4 \pmod{p-1}$. Hence we have that $a+b+c+d \in \{4, p+3, 2p+2, 3p+1\}$. We consider each case separately.

Case 1. Suppose $a+b+c+d = 4$. Up to multiplying by some power of p and reducing modulo p^4-1, we have $n \in \{4, 3+p, 3+p^2, 3+p^3, 2+p+p^2, 2+p+p^3, 2+p^2+p^3, 2+2p, 2+2p^2, 1+p+p^2+p^3\}$. Reducing modulo p^2-1 we can exclude, according to Proposition 4.3.6, all these cases except for $n = 4$, $n = 3+p^2$ and $n = 2+2p^2$.
Let $n = 3+p^2$. Then we have

$$\nabla_{1,u,v} f = 6uvx^{p^2} + x(6uv + 6uv^{p^2} + 6u^{p^2}v) + s,$$

for some constant s. This is a permutation polynomial if and only if the equation $y^{p^2-1} + z^{p^2-1} + t^{p^2-1} + 1 = 0$ has no solutions with $y, z, t \in \mathbb{F}_{p^4}^*$. We note that elements of the form y^{p^2-1} have norm 1. In $\mathbb{F}_{p^4}$ we have that -1 has norm 1, hence we can take w such that $w^{p^2-1} = -1$ and $(w, w, 1)$ is a solution of the previous equation.
Suppose now $n = 2+2p^2$. We have

$$\nabla_{1,1,1} f = 12x^{p^2} + 12x + 36$$

and $x^{p^2} + x$ is not a permutation polynomial of $\mathbb{F}_{p^4}$.

Case 2. Let $n = a+bp+cp^2+dp^3$ with $a+b+c+d = p+3$. We will show that $g = (\nabla_{1,1,t} f)^{1+p+p^2+p^3}$ has degree p^4-1 for some direction t, hence it is not a permutation polynomial. We have

$$\nabla_{1,1,t} f = -x^n + (x+t)^n - 2(x+1+t)^n + (x+2+t)^n + 2(x+1)^n - (x+2)^n.$$

Thus g will consist of 6^4 terms of the form

$$(x+i)^n (x+j)^{np} (x+k)^{np^2} (x+l)^{np^3},$$

where $i,j,k,l \in \{0,t,1+t,2+t,1,2\}$. We will use the same formulae seen in Theorem 4.3.8 in order to compute the coefficient of degree p^4-1 of these terms.
Consider $g = \nabla_{a_1,a_2,a_3} f$, where $a_i \in \mathbb{F}_{p^2}$. We have $g(\mathbb{F}_{p^2}) \subset \mathbb{F}_{p^2}$, hence f has to be a 3-PN monomial over $\mathbb{F}_{p^2}$. Hence we must have, up to multiplying n by some power of p and reducing modulo $x^{p^4}-x$, $a+c=3$ and $b+d=p$. We suppose without loss of generality that $a \neq 0$. We then have three possibilities for n: $n = 3+bp+(p-b)p^3, 1 \leq b \leq p-1$, $n = 2+bp+p^2+(p-b)p^3, 1 \leq b \leq p-1$ and $n = 1+bp+2p^2+(p-b)p^3, 1 \leq b \leq p-1$. We note that the last two are the same modulo multiplying by p^2, hence we will consider only one of them.
Thus, suppose $n = 3+bp+(p-b)p^3$. We use the formulae of the previous section with $a=3, c=0$ and $d=p-b$ and we compute M. Let

$$S(i,j,k,l) = i^3 b(l-j) + 3i^2\left(\binom{b}{2}l^2 - b^2 lj + \binom{b+1}{2}j^2\right) +$$

$$+3i\left(\binom{b}{3}l^3 - b\binom{b}{2}l^2 j + b\binom{b+1}{2}lj^2 - \binom{b+2}{3}j^3\right) +$$

$$+\binom{b}{4}l^4 - b\binom{b}{3}l^3 j + \binom{b}{2}\binom{b+1}{2}l^2 j^2 - b\binom{b+2}{3}lj^3 + \binom{b+3}{4}j^4.$$

Then we have $M_1 = S(i,j,k,l), M_2 = S(j,k,l,i)^p, M_3 = S(k,l,i,j)^{p^2}$ and $M_4 = S(l,i,j,k)^{p^3}$. Summing all these terms, a computer computation shows that the coefficient of degree p^4-1 of $(\nabla_{1,1,t} f)^{1+p+p^2+p^3}$ is

$$r_1 = \frac{1}{4}b^4(1225b^{12} - 63280b^{10} + 798090b^8 - 3115120b^6 + 5525413b^4 - 5086440b^2 + 2479248)$$

when $t=1$ and

$$r_2 = 16b^4(1225b^{12} - 66745b^{10} + 868335b^8 - 3306955b^6 + 5775712b^4 - 5057460b^2 + 2542752)$$

when $t=2$. With the Euclidean algorithm we see that the two polynomials h_1 and h_2 of degree 12 in r_1 and r_2 are coprime unless

$$p \in \{5,7,17,233,239,937,28933,323339\}.$$

If $p \in \{5,7,239,28933\}$ the greatest common divisor is irreducible over $\mathbb{F}_p$, therefore it is always nonzero when $b \in \mathbb{F}_p$. Now, if $p=17$ we have $\gcd(h_1,h_2) = b^2+9$ which has roots ± 5. If $p=233$ then $\gcd(h_1,h_2) = b^2+229 = (b+2)(b-2)$. If $p=937$ then $\gcd(h_1,h_2) = (b+533)(b+404)$. If $p=323339$ then $\gcd(h_1,h_2) = (b+9299)(b+314040)$. A direct computer computation, considering different directions, shows that in these cases $\nabla_{1,1,t} f$ is not a permutation polynomial.

Suppose now $n = 2 + bp + p^2 + (p-b)p^3$. Let

$$S(i,j,k,l) = i^2kb(l-j) + (i^2+2ik)\left(\binom{b}{2}l^2 - b^2lj + \binom{b+1}{2}j^2\right) +$$

$$+(k+2i)\left(\binom{b}{3}l^3 - b\binom{b}{2}l^2j + b\binom{b+1}{2}lj^2 - \binom{b+2}{3}j^3\right) +$$

$$+\binom{b}{4}l^4 - b\binom{b}{3}l^3j + \binom{b}{2}\binom{b+1}{2}l^2j^2 - b\binom{b+2}{3}lj^3 + \binom{b+3}{4}j^4.$$

Then we have $M_1 = S(i,j,k,l), M_2 = S(j,k,l,i)^p, M_3 = S(k,l,i,j)^{p^2}$ and $M_4 = S(l,i,j,k)^{p^3}$. Summing all these terms, a computer computation shows that the coefficient of degree p^4-1 of $(\nabla_{1,1,t}f)^{1+p+p^2+p^3}$ is

$$r_1 = \frac{1}{4}b^4(1225b^{12} - 9380b^{10} + 47270b^8 - 80972b^6 + 9881b^4 - 368744b^2 + 939856)$$

when $t = 1$ and

$$r_2 = 16b^4(1225b^{12} - 9170b^{10} + 44330b^8 - 80678b^6 + 62969b^4 - 271556b^2 + 1009744)$$

when $t = 2$. With the Euclidean algorithm we see that the two polynomials h_1 and h_2 of degree 12 in r_1 and r_2 are coprime unless

$$p \in \{5, 7, 19, 29, 101, 41051, 15052321\}.$$

If $p = 5$ or $p = 7$ the greatest common divisor of h_1 and h_2 has no roots in $\mathbb{F}_p$, hence for every choice of b it cannot vanish. For $p = 19$ we have $\gcd(h_1, h_2) = (b+3)(b+16)$. For $p = 29$ we have $\gcd(h_1, h_2) = (b+27)(b+2)$. For $p = 101$ we have $\gcd(h_1, h_2) = (b+34)(b+67)$. For $p = 41051$ we have $\gcd(h_1, h_2) = (b+17388)(b+23663)$. For $p = 15052321$ we have $\gcd(h_1, h_2) = (b+3670586)(b+11381735)$. As before a direct computation shows that we can exclude also these cases, since x^n, with such choice of n, is not 3-PN over $\mathbb{F}_{p^4}$.

Case 3. Suppose $n = a + bp + cp^2 + dp^3$ with $a+b+c+d = 2p+2$. We will show that $g = (\nabla_{1,1,1}f)^{1+p^2}$ has degree p^4-1, hence it is not a permutation polynomial. As before we reduce n modulo p^2-1 and exclude some cases. Suppose $a+c = k$ and $b+d = 2p+2-k$. If $4 \le k \le p-2$ then $n \equiv k+1+(p+2-k)p \pmod{p^2-1}$ and f is not 3-PN. If $k = p$ we obtain $n \equiv 1+3p \pmod{p^2-1}$ and we exclude this value. If $k = p+1$ we have $n \equiv 2+2p \pmod{p^2-1}$ and also this case is not 3-PN. If $p+4 \le k \le 2p-2$ we have $n \equiv k-p+(2p+3-k)p$ and also this case is bad. We have, only two cases left, namely $a+c = p-1$ and $a+c = p+3$. We can suppose

without loss of generality that $a+c=p-1$. Using the formulae of Theorem 4.3.8 we conclude that $M_1 = M_3 = 1$ and

$$M_2 = \binom{b}{4} i^4 + \binom{b}{3}(p+3-b)i^3 j + \binom{b}{2}\binom{p+3-b}{2} i^2 j^2 + \\ + b\binom{p+3-b}{3} ij^3 + \binom{p+3-b}{4} j^4 \equiv \binom{b}{4}(i-j)^4,$$

where the equivalence is modulo p. Exchanging i and j we obtain M_4 and thus, as before, the coefficient of degree p^4-1 of $(\nabla_{1,1,1} f)^{1+p^2}$ is

$$\binom{b}{4}^2 S(3,8) = -10080\binom{b}{4}^2,$$

which is not zero for $p \geq 11$.

Case 4. Suppose $a+b+c+d = 3p+1$. Let $a+c=k$ and $b+d = 3p+1-k$. We have $p+3 \leq k \leq 2p-2$. Reducing modulo p^2-1 we obtain $n \equiv k+1-p+(2p-k+2)p \pmod{p^2-1}$ and, with this choice of n, f is not 3-PN over $\mathbb{F}_{p^2}$.

A computer computation shows that the same conclusion of the theorem holds for $p = 5, 7$. □

We present now some partial results for k-PN functions over $\mathbb{F}_{p^3}$. As in PN case, this method does not allow us to obtain a complete classification.

Proposition 4.3.10. *If x^n is a k-PN monomial over $\mathbb{F}_{p^3}, p \geq 2k+2$ and $n \leq p^3-1$ then, writing $n = a+bp+cp^2$, we have $a+b+c = k+1$ or $a+b+c = p+k$.*

Proof. Let $f(x)$ be the k-th derivative (always in direction 1) of x^n. We have that f is defined over $\mathbb{F}_p$, hence $f(\mathbb{F}_p) \subset \mathbb{F}_p$, hence f should be a permutation polynomial of the prime field. From Theorem 4.3.3 we obtain $n \equiv k+1 \pmod{p-1}$. If we write $n = a+bp+cp^2$ we have three possible cases, $a+b+c = k+1$, $a+b+c = p+k$ and $a+b+c = 2p+k-1$. To conclude we only need to exclude the last one.

Thus, suppose $a+b+c = 2p+k-1$ and let $f = \nabla_1^k x^n$ the k-th derivative of x^n, every time in direction 1. We will show that $f^{1+p} \bmod x^{p^3}-x$ has degree p^3-1. We have that

$$f(x) = (-1)^k \sum_{i=0}^{k} (-1)^i \binom{k}{i} (x+i)^n$$

and

$$f(x)^{1+p} = \sum_{i=0}^{k}\sum_{j=0}^{k}(-1)^{i+j}\binom{k}{i}\binom{k}{j}(x+i)^n(x+j)^{pn}.$$

Consider now the single term $(x+i)^n(x+j)^{pn}$. Expanding it we obtain

$$\sum_{\alpha_1=0}^{a}\sum_{\beta_1=0}^{b}\sum_{\gamma_1=0}^{c}\sum_{\alpha_2=0}^{a}\sum_{\beta_2=0}^{b}\sum_{\gamma_2=0}^{c}\binom{a}{\alpha_1}\binom{b}{\beta_1}\binom{c}{\gamma_1}\binom{a}{\alpha_2}\binom{b}{\beta_2}\binom{c}{\gamma_2}i^{e_i}j^{e_j}x^r,$$

where $r = \alpha_1+\gamma_2+(\beta_1+\alpha_2)p+(\gamma_1+\beta_2)p^2, e_i = a-\alpha_1+(b-\beta_1)p+(c-\gamma_1)p^2$ and $e_j = c-\gamma_2+(a-\alpha_2)p+(b-\beta_2)p^2$.
Since $\alpha_1+\gamma_2+(\beta_1+\alpha_2)p+(\gamma_1+\beta_2)p^2 < 2(p^3-1)$ for $p \geq 5$, we need to consider only the case $\alpha_1+\gamma_2 = \beta_1+\alpha_2 = \gamma_1+\beta_2 = p-1$.
We then write this sum as $C_1C_2C_3$ where

$$C_1 = \sum_{\alpha_1+\gamma_2=p-1}\binom{a}{\alpha_1}\binom{c}{\gamma_2}i^{a-\alpha_1}j^{c-\gamma_2},$$

$$C_2 = \sum_{\beta_1+\alpha_2=p-1}\binom{b}{\beta_1}\binom{a}{\alpha_2}i^{(b-\beta_1)p}j^{(a-\alpha_2)p},$$

$$C_3 = \sum_{\gamma_1+\beta_2=p-1}\binom{c}{\gamma_1}\binom{b}{\beta_2}i^{(c-\gamma_1)p^2}j^{(b-\beta_2)p^2}.$$

We note that $i,j \in \mathbb{F}_p$, hence $i^p \equiv i^{p^2} \equiv i \pmod p$, therefore we omit p and p^2 powers. We note that C_1, C_2 and C_3 are totally similar. We compute C_1 and, mutatis mutandis, we will obtain also the other two.
Suppose $a+c = p-1+z$. Then we have

$$C_1 = \sum_{s=0}^{z}\binom{a}{s}\binom{c}{z-s}i^s j^{z-s}.$$

Consider $\binom{c}{z-s}$. Expanding it we have

$$\frac{c(c-1)\cdots(c-z+s+1)}{(z-s)!}.$$

Using the relation $a+c = p-1+z$ and reducing modulo p we obtain

$$\binom{c}{z-s} \equiv (-1)^{k-s}\frac{(a-s)(a-s-1)\cdots(a-z+1)}{(z-s)!}.$$

Hence we have

$$\binom{a}{s}\binom{c}{z-s} \equiv (-1)^{z-s}\frac{a(a-1)\cdots(a-z+1)}{s!(z-s)!} = (-1)^{z-s}\binom{a}{z}\binom{z}{s}.$$

Therefore

$$C_1 \equiv \binom{a}{z} \sum_{s=0}^{z} (-1)^{z-s} \binom{z}{s} i^s j^{z-s} = \binom{a}{z} (i-j)^z.$$

From this we have

$$C_2 \equiv \binom{b}{a+b-p+1} (i-j)^{a+b-p+1}$$

and

$$C_3 \equiv \binom{c}{b+c-p+1} (i-j)^{b+c-p+1}.$$

Multiplying and reducing modulo p, we obtain that the coefficient we are looking for is equal to

$$\binom{a}{p+k-b} \binom{b}{p+k-c} \binom{c}{p+k-a} (i-j)^{2k+2}.$$

Summing all the terms when i and j varies we obtain that the coefficient of the monomial of degree p^3-1 of $f^{1+p} \pmod{x^{p^3}-x}$ equals

$$\binom{a}{p+k-b} \binom{b}{p+k-c} \binom{c}{p+k-a} S(k, 2k+2),$$

where $S(k,r)$ is the sum we considered before. This is not zero with the given bound on p. By direct computation the same conclusion holds for $k=1$ and $p=3$. □

Bibliography

[Ahm11] Omran Ahmadi. Generalization of a theorem of Carlitz. *Finite Fields Appl.*, 17(5):473–480, 2011.

[Bea10] Arnaud Beauville. Finite subgroups of $\mathrm{PGL}_2(K)$. In *Vector bundles and complex geometry*, volume 522 of *Contemp. Math.*, pages 23–29. Amer. Math. Soc., Providence, RI, 2010.

[Car67] L. Carlitz. Some theorems on irreducible reciprocal polynomials over a finite field. *J. Reine Angew. Math.*, 227:212–220, 1967.

[CL12] Robert S. Coulter and Felix Lazebnik. On the classification of planar monomials over fields of square order. *Finite Fields Appl.*, 18(2):316–336, 2012.

[CM97] Robert S. Coulter and Rex W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des. Codes Cryptogr.*, 10(2):167–184, 1997.

[Coh69] Stephen D. Cohen. On irreducible polynomials of certain types in finite fields. *Proc. Cambridge Philos. Soc.*, 66:335–344, 1969.

[Cou06] Robert S. Coulter. The classification of planar monomials over fields of prime square order. *Proc. Amer. Math. Soc.*, 134(11):3373–3378 (electronic), 2006.

[DO68] Peter Dembowski and T. G. Ostrom. Planes of order n with collineation groups of order n^2. *Math. Z.*, 103:239–258, 1968.

[DY06] Cunsheng Ding and Jin Yuan. A family of skew Hadamard difference sets. *J. Combin. Theory Ser. A*, 113(7):1526–1535, 2006.

[Gar11] Theodoulos Garefalakis. On the action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$. *J. Pure Appl. Algebra*, 215(8):1835–1843, 2011.

[Glu90] David Gluck. A note on permutation polynomials and finite geometries. *Discrete Math.*, 80(1):97–100, 1990.

[Hir89] Yutaka Hiramine. A conjecture on affine planes of prime order. *J. Combin. Theory Ser. A*, 52(1):44–50, 1989.

[Joh87] Norman L. Johnson. Projective planes of prime order p that admit collineation groups of order p^2. *J. Geom.*, 30(1):49–68, 1987.

[LHT13] Nian Li, Tor Helleseth, and Xiaohu Tang. Further results on a class of permutation polynomials over finite fields. *Finite Fields Appl.*, 22:16–23, 2013.

[LN83] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983. With a foreword by P. M. Cohn.

[Luc78a] Edouard Lucas. Theorie des Fonctions Numeriques Simplement Periodiques. *Amer. J. Math.*, 1(2):184–196, 1878.

[Luc78b] Edouard Lucas. Theorie des Fonctions Numeriques Simplement Periodiques. *Amer. J. Math.*, 1(4):289–321, 1878.

[Luc78c] Edouard Lucas. Theorie des Fonctions Numeriques Simplement Periodiques. [Continued]. *Amer. J. Math.*, 1(3):197–240, 1878.

[Mey90] Helmut Meyn. On the construction of irreducible self-reciprocal polynomials over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 1(1):43–53, 1990.

[MR10] Jean Francis Michon and Philippe Ravache. On different families of invariant irreducible polynomials over $\mathbb{F}_2$. *Finite Fields Appl.*, 16(3):163–174, 2010.

[Oss06] Brian Osserman. Rational functions with given ramification in characteristic p. *Compos. Math.*, 142(2):433–450, 2006.

[PCo89] P. M. Cohn. *Algebra. Vol. 2.* John Wiley & Sons Ltd., Chichester, second edition, 1989.

[PZ11] Alexander Pott and Yue Zhou. A character theoretic approach to planar functions. *Cryptogr. Commun.*, 3(4):293–300, 2011.

[RS89] L. Rónyai and T. Szőnyi. Planar functions over finite fields. *Combinatorica*, 9(3):315–320, 1989.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[ST12] Henning Stichtenoth and Alev Topuzoğlu. Factorization of a class of polynomials over finite fields. *Finite Fields Appl.*, 18(1):108–122, 2012.

[Tot02] Gabor Toth. *Glimpses of algebra and geometry.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 2002. Readings in Mathematics.

[VZ13] Michael Zieve. Rational points on some Fermat curves and surfaces over finite fields . *arXiv*, abs/1310.1772:1–8, 2013.

[Zie13] Michael Zieve. Planar functions and perfect nonlinear monomials over finite fields . *arXiv*, abs/1301.5004:1–10, 2013.

[ZKW09] Zhengbang Zha, Gohar M. Kyureghyan, and Xueli Wang. Perfect nonlinear binomials and their semifields. *Finite Fields Appl.*, 15(2):125–133, 2009.

[ZW09] Zhengbang Zha and Xueli Wang. New families of perfect nonlinear polynomial functions. *J. Algebra*, 322(11):3912–3918, 2009.

Acknowledgments

I thank everyone. I will miss everyone.