A NUMBER THEORETICAL APPROACH TO POLYNOMIALS OVER FINITE FIELDS

by

Neslihan Girgin Öztürk

B.S., Mathematics, Dokuz Eylül University, 2011

M.S., Mathematics, Mimar Sinan Fine Arts University, 2015

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

Graduate Program in Mathematics

Boğaziçi University

2023

To my uncle, Mehmet Girgin, in loving memory.

ACKNOWLEDGEMENTS

First of all, I would like to express my most sincere gratitude to my advisor Assoc. Prof. Alp Bassa for his guidance, encouragement and contributions to my academic experience. I consider myself lucky to work with him and I have learned a lot from his comprehensive point of view.

I am honored to have Assoc. Prof. Ayhan Günaydın and Assoc. Prof. Ayberk Zeytin as members of my jury and my progress committee as well. I would like to thank them very much with all my gratitude, in addition to their helpful comments in our progress meetings, for giving their time since the beginning of my graduate process. I would like to extend my deepest thanks to my other jury member Prof. Ahmet Emrah Çakçak besides his remarkable comments, for introducing Number Theory to me, one of the most admirable areas of mathematics, in my master thesis period as being my advisor as well. I would also like to thank Assoc. Prof. Özlem Beyarslan for being a member of my jury and her valuable comments.

I would like to thank to the members of our group, Jacqueline Anderson, Irene Bouw, Ozlem Ejder, Valentijn Karemaker, and Michelle Manes for the joint work which was started at the Women in Numbers Europe II and resulted as a paper included as a part of my Ph.D. period. I would also like thank to Asst.Prof. Emrah Sercan Yılmaz for his contributions to a part of this thesis as another joint work.

I would like to thank sincerely each member of the Mathematics Department of MSGSU, where I am a research assistant, for giving the opportunity to work comfortably and providing a warm atmosphere to study for my thesis with endless understanding. I also would like to express my special thanks to Prof. Ayşe Berkman who is more than just the head of this department at that time for me, I always feel her continuous support throughout my academic life.

My hearty thanks go to my dear friends Melissa Nalbandiyan Özsahakyan and Eda Kırımlı not only for shares when we work but also for their enormous friendship with invaluable moral support. It would be harder for me to complete this process without their endless encouragement.

Without a doubt, my most special thanks go to my dear fellow Tekgül Kalaycı who is always more than a friend and even a sister to me. It is an undeniable fact that her never-ending support and encouragement helped me complete this work with such an inner peace. It is also certain that my words will not be enough to describe the importance her place in my life in every sense for the last sixteen years.

Last but not least, I am deeply grateful to my mother, my father, my sister and my brother who are always supported me throughout my life with their pure love unconditionally. Besides, how lucky am I to have my husband, İlker Öztürk, whose endless love, patience and understanding were one of my biggest supports in completing this process.

ABSTRACT

A NUMBER THEORETICAL APPROACH TO POLYNOMIALS OVER FINITE FIELDS

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. The explicit constructions of irreducible polynomials over $\mathbb{F}_q$ of high degree is one of the main problems in the arithmetic of finite fields which has many applications in several areas such as coding theory and cryptography. In general, some recursive methods are preferred to do these constructions using rational transformations. In particular, we are interested in methods that are obtained by using quadratic transformations. For doing this, we will first classify and normalize the rational transformations of degree 2 using the behaviour of the ramified places in the corresponding rational function field extensions over the finite field $\mathbb{F}_q$. Then we will investigate the constructions using Galois theory and some basic observations in group theory. This approach helps to better understand the iterative constructions and gives various generalisations of them. It also enables to determine the requirements put on the initial polynomials.

ÖZET

SONLU CİSİMLER ÜZERİNDEKİ POLİNOMLARA SAYI KURAMSAL BİR YAKLAŞIM

$\mathbb{F}_q$, q elemanlı sonlu cisim olsun. Yüksek dereceli indirgenemez polinomların inşası, kodlama teorisi ve kriptografi gibi birçok alanda uygulaması olan, sonlu cisim aritmetiğinin ana problemlerinden biridir. Genellikle bu inşalar için, rasyonel dönüşümleri kullanan, özyinelemeli metodlar tercih edilir. Özel olarak bu çalışmada, ikinci dereceden dönüşümleri kullanarak elde edilen yöntemlerle ilgileneceğiz. Bunu yapmak için, önce ikinci dereceden rasyonel dönüşümleri, karşılık gelen sonlu cisimler üzerinde fonksiyon cisimleri genişlemesindeki, dallanan yerlerin davranışlarına göre sınıflandırıp, normalleştireceğiz. Daha sonra Galois teori ve grup teoriden bazı temel gözlemleri kullanarak bu inşaları inceleyeceğiz. Bu yaklaşım, özyinelemeli yapıları daha iyi anlamaya yardımcı olurken, çeşitli genellemeleri veriyor. Ayrıca, başlangıç polinomu üzerine koyulması gereken koşulları belirlememizi sağlıyor.

TABLE OF CONTENTS

LIST OF SYMBOLS

c	A non-zero element of the finite field $\mathbb{F}_q$
$Con_{F'/F}(P)$	The conorm of the place P with respect to the extension F'/F
C_4	The cyclic group of order 4
$\deg g$	The degree of the polynomial g
$\mathrm{Diff}(F'/F)$	The different of F'/F
D_8	The dihedral group of order 8.
$d(P'\|P)$	The different exponent of $P'\|P$
$D(P'\|P)$	The decomposition group of $P'\|P$
$e(P'\|P)$	The ramification index of the place P' lying above P
$f(P'\|P)$	The inertia degree of the place P' lying above P
$f^Q(T)$	The Q-transform of f
$f^R(T)$	The R-transform of f
$f^*(T)$	The reciprocal of the polynomial f
F/K	An algebraic function field of one variable over K
F'/K'	An algebraic extension of F/K
F_P	The residue field of P
$\mathbb{F}_q$	The finite field with q elements.
$\mathbb{F}_q^*$	The multiplicative subgroup of the finite field $\mathbb{F}_q$
$\mathbb{F}_q[T]$	The polynomial ring over $\mathbb{F}_q$ in T
$\overline{\mathbb{F}}_q$	The algebraic closure of $\mathbb{F}_q$
$\mathbb{F}_{q^{n\cdot 2^\infty}}$,	An infinite subfield of the field $\overline{\mathbb{F}}_q$
$\mathbb{F}_q(w)$	A rational function field in w
g	The genus of a given function field
$Gal(F'/F)$	The Galois group of F'/F
$GL_2(K)$	The invertible 2×2 matrices group of entries in the field $\mathbb{F}_q$
$I(P'\|P)$	The inertia group of $P'\|P$
K	An arbitrary field
$\mathrm{N}_{F'/F}$	The norm map with respect to the extension F'/F

O	A valuation ring
P	A place in the given function field
$PGL_2(K)$	The 2×2 matrices group with determinant 1 and of entries from the field K (The automorphism group of K)
$P'\|P$	A place lying above P
$\mathbb{P}_F$	The set of all places of F
$\mathbb{P}^1(K)$	The projective line over K
q	A prime power
$\mathrm{Tr}_{F'/F}$	The trace map with respect to the extension F'/F
V	The Klein four group
Δ	The discriminant of a given polynomial
ξ	A primitive 4-th root of unity
ζ	A t^i-th root of unity

1. INTRODUCTION

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. The construction of high degree irreducible polynomials over $\mathbb{F}_q$ is one of the main problems in the arithmetic of finite fields, with many applications in several areas such as coding theory [1–3], cryptography [4–6], computer algebra systems [7]. The problem was initially studied for even characteristic. Later on extensive work was carried out for the case of odd characteristic, as well [4]. The explicit construction of such polynomials form a topic of interest and current research, especially because of these applications.

In general, the known constructions are based on the composition of a given irreducible polynomial with a rational function. Most results in this area are based on the following fundamental result of Capelli:

Theorem 1.1. *[8, 9] Let $f, g \in \mathbb{F}_q[T]$ be relatively prime polynomials and let $p \in \mathbb{F}_q[T]$ be an irreducible polynomial of degree n. Then the composition polynomial*

$$F(T) = (g(T))^n p(f(T)/g(T))$$

is irreducible over $\mathbb{F}_q$ if and only if the polynomial $f - \alpha g$ is irreducible over $\mathbb{F}_{q^n}$, for any root $\alpha \in \mathbb{F}_{q^n}$ of p.

In this context this result is usually used in an iterative manner to obtain an infinite sequence of irreducible polynomials over $\mathbb{F}_q$ of increasing degrees. Most of such constructions begin by taking a suitably chosen irreducible polynomial $p(T) \in \mathbb{F}_q[T]$ and a rational transformation. The polynomial $p(T)$ is repeatedly composed with the rational transformation, clearing denominators on the way. Hence a sequence of polynomials is obtained. The given conditions on $p(T)$ set at the beginning guarantee the irreducibility of each of the iterates.

Among the known transformations in the literature, the most well-known and most utilized one is the Q-transform. Besides giving irreducible polynomials, it also produces self-reciprocal ones, and furthermore N-polynomials. Recall that a nonzero polynomial $f(T)$ of degree n with $f(0) \neq 0$, is said to be *self-reciprocal* if it equals its reciprocal polynomial, $f^*(T) = T^n f(0)^{-1} f(\frac{1}{T})$. N-polynomials will be defined in Section 2.2 in the case of even characteristic.
The Q-transform is defined as follows:

$$f^Q(T) := T^{\deg f} \cdot f\left(T + \frac{1}{T}\right).$$

In the paper [10], Meyn gave some important results about the irreducibility of the self-reciprocal polynomial using of Q- transformation in detail. He also showed that these polynomials can be used to obtain explicit models for certain infinite subfields, $\mathbb{F}_{q^{n \cdot 2^\infty}}$, of the field $\overline{\mathbb{F}}_q$.

In general, self-reciprocal polynomials over finite fields have been studied extensively because of their rich algebraic structure and large scale applications in various branches of mathematics and engineering. In particular, in coding theory, self-reciprocal irreducible monic polynomials were used for characterizing and enumerating Euclidean self-dual cyclic codes and Euclidean complementary dual cyclic codes over finite fields in [11] and [12], respectively. Moreover, in [13], such polynomials have been characterized up to their degrees and in [14] the order and the number of these polynomials of a given degree over finite fields have been determined.

Moreover, these polynomials are used to generate reversible codes with a read-backward property in [13, 15, 16]. Also, there is a relation between irreducible self-reciprocal polynomials over finite fields and the class of primitive self-complementary necklaces consisting of beads colored with q colors [17]. The numbers of these polynomials are the same as the number of periodic sequences of some symmetry type [18].

The Q-transform was considered in characteristic 2 by Varshamov-Garakov in [19] and [20], Wiedemann in [21], and Kyuregyan in [22]. Their results togehter with results of Meyn from [10] can be summarized as follows:

Theorem 1.2. *(Varshamov-Garakov, Wiedemann, Meyn, Kyuregyan)*
Suppose $q = 2^r$ *and* $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0 \in \mathbb{F}_q[T]$ *is an irreducible polynomial with* $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a_{n-1}) = 1$ *and* $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\frac{a_1}{a_0}) = 1$. *Define*

$$f_0 = f \text{ and } f_k(T) = T^{\deg f_{k-1}} f_{k-1}\Big(\frac{T^2+1}{T}\Big) = f_{k-1}^Q(T),$$

for all $k \geqslant 1$. *Then* f_k *is an irreducible polynomial over* $\mathbb{F}_q$, *for all* $k \geqslant 0$.

Then, Kyuregyan [23] showed that this gives an N-polynomials sequence in characteristic 2, (Theorem 3.39). The normality of these polynomials in various cases is due to Gao [24], Scheerhorn [25], Schwartz [26] and Kyuregyan [27].

On the other hand, Meyn gave some results in [10] for odd characteristic as well. The irreducibility of the Q-transform of an irreducible polynomial was shown using the following result:

Theorem 1.3. *[10, Theorem 8] Let* q *be an odd prime power. If* f *is an irreducible polynomial of degree* n *over* $\mathbb{F}_q$ *then* f^Q *is irreducible if and only if the element* $f(2)f(-2)$ *is a non-square in* $\mathbb{F}_q$.

There are some incomplete results for the iterations in this paper, as well. In [28], Bassa and Menares also gave more explicit statements about the irreducibility of more than one iterations of this transformation.

The construction of N-polynomials is another significant problem in mathematics because of its use in various areas such as coding theory, cryptography, etc. In most cases the following is addressed:

A positive integer n is given and a finite field $\mathbb{F}_q$ is chosen as the ground field. Then, in order to construct a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, an N-polynomial in $\mathbb{F}_q[x]$ of degree n is constructed (in most cases this is done iteratively). There are several results for doing this efficiently by obtaining a sequence of N-polynomials over $\mathbb{F}_q$ [10, 24, 25, 27, 29–31].

Let us also mention the constructions of irreducible polynomials of 2-power degree over $\mathbb{F}_q$, with odd characteristic given by Cohen [32] and McNay's [33]. Since the Q-transform is less practical in odd characteristic, Cohen defined the R-transform as follows: For a polynomial $f(T)$, define

$$f^R(T) = (2T)^{\deg f} \cdot f\Big(\frac{T+T^{-1}}{2}\Big) = 2^{\deg f} \cdot f^Q\Big(\frac{T}{2}\Big).$$

Then Cohen gave the following result:

Theorem 1.4. *[32, Theorem 2], Let q be an odd prime power and f be a monic irreducible polynomial over $\mathbb{F}_q$ with $\deg f \geqslant 1$ and assume $\deg f$ is even whenever $q \equiv 3 \pmod q$. Suppose $f(1)f(-1)$ is not a square element in $\mathbb{F}_q$. Define $f_0 = f$ and $f_k = f_{k-1}^R$. Then for each $k \geqslant 0$, f_k is an irreducible polynomial over $\mathbb{F}_q$.*

Furthermore, Meyn in [34] showed that these polynomials are normal and Chapman [29] improved this by showing that they are in fact completely normal polynomials.

The research in this thesis is motivated by these results. We want to show how one can associate an extension of algebraic function fields to a given transformation and how these results can be interpreted by studying the given extension with the help of Galois theory. We show that all known results can be obtained more easily and intuitively using this approach.

We are particularly interested in methods that are obtained using quadratic transformations. For this, we will first classify the rational transformations of degree 2 using the behaviour of the ramified places in a quadratic rational function fields

extension over the finite field $\mathbb{F}_q$. Then we will try to understand the constructions using Galois theory and some basic observations from group theory and determine the requirements put on the initial polynomial.

Let us give more details about our approach: Define a rational function field extension $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(t)$ where $w = g(t)/h(t)$ for any relatively prime polynomials $g, h \in \mathbb{F}_q[T]$ with $\max\{\deg g, \deg h\} = 2$. By Corollary 2.7, the extension is always ramified. Let P be a place of $\mathbb{F}_q(w)$ and P' be a place of $\mathbb{F}_q(t)$ lying over P. By the Hurwitz Genus Formula in Theorem 2.5 and Dedekind's Different Theorem in 2.6, there can be three situations for the ramified places in the given extension:
First, there can be wildly ramified places in the case of even characteristic. On the other hand, for odd characteristic, there can be either two rational places, P_1 and P_2 that are (tamely) ramified, or a single place of degree 2, which is tamely ramified.

In this work, we are mostly interested in the case of odd characteristic. The case of two ramified rational places will be examined in detail, while the other case of a degree 2 ramified place is still in progress and we plan to address it in future work in more detail. We will need the following below definition:

Let $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_q)$. Action of this group on $\overline{\mathbb{F}}_q \cup \{\infty\}$ is defined by, for any $\alpha \in \overline{\mathbb{F}}_q$, $\sigma.\alpha = \frac{a\alpha+b}{c\alpha+d}$ if $c\alpha + d \neq 0$ and ∞ otherwise, with $\sigma.\infty = \frac{a}{c}$ if $c \neq 0$ and ∞ otherwise.

Fixing the transformation will fix the corresponding extension of function fields. Iterating the transformation will correspond to several extensions. This sequence of extensions can come together in several ways, depending on how the ramified places in one extensions are related to the ones in the following step. Accordingly, there are three possible cases for the behaviour of the ramified places in the extensions:

In the first case, the same places lie over P_1 and P_2 in the $\mathbb{F}_q(t)$, i.e., the places above the ramified places are again the ramified ones. With a Möbius transformation σ, we can carry them to the places 0 and ∞ to normalize the extension, i. e., $\sigma(P_1)$ is the place 0 in $\mathbb{F}_q(\sigma(w)) = \mathbb{F}_q(w)$ and $\sigma(P_2)$ is the place ∞ in $\mathbb{F}_q(\sigma(w)) = \mathbb{F}_q(w)$. Similarly for the places above of $\mathbb{F}_q(\sigma(t)) = \mathbb{F}_q(t)$. If we write the transformation corresponding to such an extension, we just find the power map transformation $cT^2,\ c \in \mathbb{F}_q^*$ which is almost the same as the R-transform:

Say $w = \frac{at^2+bt+d}{et^2+ft+g},\ a, b, d, e, f, g \in \mathbb{F}_q$. We can determine the transformation by just using Kummer's Theorem 2.3. Since ∞ lies over ∞, it will be a polynomial map, so the denominator is equal to 1. Now, consider $w = at^2 + bt + d$, for the place $(w = 0)$ of $\mathbb{F}_q(w)$, we must obtain the zero place $(t = 0)$ in $\mathbb{F}_q(t)$ with ramification index 2, that is, the equation must be of the form $0 = ct^2$ for some $c \in \mathbb{F}_q^*$. This case has already been considered in [35] and [28].

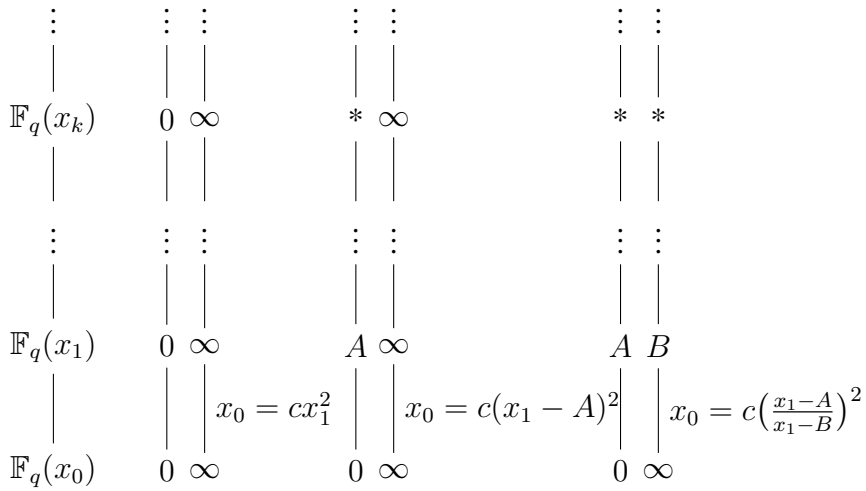
The second case occurs if one of the ramified places is again ramified in the next extension, i.e., one of the places of $\mathbb{F}_q(t)$ lying over P_1 and P_2 is the same as P_1 or P_2. Again, after a normalisation like above, if we carry P_1 and P_2 to the places 0 and ∞ of $\mathbb{F}_q(w)$, respectively, and let the place $(t = A), A \in \mathbb{F}_q^*$, lie over 0 and $(t = \infty)$ lies over $(w = \infty)$, we obtain the transformation $c(T - A)^2$, for some $c \in \mathbb{F}_q^*$.

In the last case, the neither of the ramified places is ramified in the next extension, i.e., the places of $\mathbb{F}_q(t)$ lying above P_1 and P_2 are not the same as them. If we again normalize such an extension carrying P_1 and P_2 to the 0 and ∞ places of $\mathbb{F}_q(w)$, respectively, with $(t = A), A \in \mathbb{F}_q^*$, and $(t = B), B \neq \infty$ places of $\mathbb{F}_q(t)$ lying over them, respectively, we obtain the transformation $c\left(\frac{T-A}{T-B}\right)^2$, for some $c \in \mathbb{F}_q^*$.

We can apply these transformations iteratively to obtain a sequence of polynomials in the following manner:

$$f_{i+1}(T) = h(T)^{\deg f_i} f_i\Big(\frac{g(T)}{h(T)}\Big),\ \text{for } i \geq 0.$$

Then we define the corresponding tower, $\mathbb{F}_q(x_0) \subseteq \mathbb{F}_q(x_1) \subseteq \cdots \mathbb{F}_q(x_n) \subseteq \cdots$, where $x_i = g(x_{i+1})/h(x_{i+1})$ for any relatively prime polynomials $g, h \in \mathbb{F}_q[T]$. We have the following situations for each case:



After this a classification we can benefit from the strength of Galois theory and use some basic fact from group theory. This approach allows us to obtain a better understanding of various iterative constructions and gives various generalizations of them, providing many new infinite sequence of irreducible polynomials over a given finite field. It also helps in to determining the necessary requirements put on the initial polynomials. In addition, we can also obtain some sequences of N-polynomials and self-reciprocal polynomials in certain situations.

We finish by giving a short outline of this thesis:

In the following part, chapter two, we recall some basic facts about function fields arithmetic, in particular, over the finite constant fields, mostly referring to [36].

In the main chapter, namely the third chapter, we describe our approach in detail. We consider three classes introduced above in detail. We show how well known results in the literature such as the R-transform, the Q-transform, and some

constructions of Kyuregyan fit nicely into this framework and how they just become particular cases. We also show how a celebrated result, Lemma 3.34, given by Jones and Boston in [37,38] about the the irreducibility of composition of quadratic polynomials can be obtained using our results.

Lastly, in chapter four, we give a joint work with Jacqueline Anderson, Irene Bouw, Ozlem Ejder, Valentijn Karemaker, and Michelle Manes which was started at the Women in Numbers Europe II workshop at the Lorentz Centre in Leiden, and resulted in the paper [39] [1] that was already carried out during this doctorate process. We study the dynamical properties of a large class of rational maps with exactly three ramification points. By constructing families of such maps, we obtain infinitely many conservative maps of degree d; this answers a question of Silverman. Rather precise results on the reduction of these maps yield strong information on the rational dynamics. Due to the relation of the iterative constructions of irreducible polynomials over finite fields with the arithmetical dynamical systems, it gives an extra motivation to investigate and explain their algebraic structure explicitly using the same number theoretical tools.

[1] 'Bu tez çalışması kapsamında ortaya çıkan ve telif hakkı yayınevine devredilen görseller, yayınevinin kendi ağ sayfasında bulunan "yazarın kendi ürettiği yazı ve grafiklerin tekrar kullanımı hakkında geçerli olan yayın politikası"na uygun olarak tez kitabında kullanılmıştır.'

2. PRELIMINARIES

Since our approach to the iterative constructions of irreducible polynomials is based on the arithmetic of function fields, in this section we first give some facts related to our work. For the details we refer to [36] as one of the main sources.

2.1. Function Fields

Let K be an arbitrary field and F/K be an algebraic function field of one variable over K. In particular, we are interested in the most basic example, the rational function field $F = K(t)$ where t is a transcendental over K. Any element $f \in F$ can be represented of the form $f = k.p_1(t)^{n_1} \cdots p_i(t)^{n_i} \cdots$ in which $0 \neq k \in K$ and $p_i(t) \in K[t]$ is monic, irreducible and pairwise distinct for all i with $n_i \in \mathbb{Z}$.

Theorem 2.1. *[36, Theorem 1.2.2] The rational function field, $K(t)/K$ has no places except the places*

$$\begin{aligned} P_{p(t)} &= \left\{ \frac{f(t)}{g(t)} \in K(t) : f(t), g(t) \in K[t], p(t) | f(t), p(t) \nmid g(t) \right\} \\ &= \left\{ \frac{f(t)}{g(t)} \in K(t) : \nu_{p(t)}\Big(\frac{f(t)}{g(t)}\Big) > 0 \right\} \end{aligned}$$

with its valuation ring

$$\begin{aligned} O_{p(t)} &= \left\{ \frac{f(t)}{g(t)} \in K(t) : f(t), g(t) \in K[t], p(t) \nmid g(t) \right\} \\ &= \left\{ \frac{f(t)}{g(t)} \in K(t) : \nu_{p(t)}\Big(\frac{f(t)}{g(t)}\Big) \geq 0 \right\} \end{aligned}$$

for a monic irreducible polynomial $p(t) \in K[t]$, where ν is the corresponding discrete valuation and

$$P_\infty = \left\{ \frac{f(t)}{g(t)} : f(t), g(t) \in K[t], \deg f < \deg g \right\}$$

with its valuation ring

$$O_\infty = \left\{ \frac{f(t)}{g(t)} : f(t), g(t) \in K[t], \deg f \leq \deg g \right\}.$$

This theorem implies that there is a one-to-one correspondence between the degree one places of the rational function field $K(t)$ and $K \cup \{\infty\}$. That is, if we look from the perspective of algebraic geometry, we say that the points of the set $K \cup \{\infty\}$ which is interpreted as the projective line $\mathbb{P}^1(K)$ over K with its automorphism group $PGL_2(K)$ acting on it faithfully and sharply 3-transitively, corresponds in a one-to-one way to the the degree 1 places of $K(t)$.

Proposition 2.2. *[36, Proposition 1.6.3] Let F be an algebraic function field over the finite field K with the genus g. Then F is rational if and only if $g = 0$.*

Let F'/K' be an algebraic extension of F/K. For a place $P \in \mathbb{P}_F$, the set of all places of F, we define the *conorm* with respect to the extension F'/F as $Con_{F'/F}(P) := \sum_{P'|P} e(P'|P) \cdot P'$, where the sum runs over all places $P' \in \mathbb{P}_{F'}$ lying above P which satisfies for the towers $F'' \supseteq F' \supseteq F$,

$$Con_{F''/F}(P) = Con_{F''/F'}(Con_{F'/F}(P)).$$

Let R be a subring of F/K and F'/K' be an algebraic extension of F/K. An element $y \in F$ is called *integral* over R, if for some monic polynomial $p(T) \in R[T]$, $p(y) = 0$. In particular, by Proposition 3.3.1 in [36], for an integrally closed subring R of F/K such that F is the quotient field of R, and an element $y \in F'$ with the minimal polynomial $p(T)$ over F, y is integral over R if and only if $p(T) \in R[T]$.

The next theorem is in the heart of our work. It shows the relation between the factorization of a polynomial after applying the given transformation and the

places lying over the associated place of the initial polynomial in the corresponding extension of the function fields.

Theorem 2.3. *(Kummer) [36, Theorem 3.3.7] Let P be a place of F and F'/F be its extension such that $F' = F(y)$ where y is an integral over the valuation ring O_P with the minimal polynomial $p(T) \in O_p[T]$ over F whereas its residue class, $\overline{p}(T) \in F_P$, is separable in F_P. Suppose that it factorizes into irreducible polynomials in the residue field $F_P = O_P/P$ such that $\overline{p}(T) = \prod_{i=1}^{r} p_i(T)$. Choose monic polynomial $q_i(T) \in O_P[T]$ with $\overline{q}_i(T) = p_i(T)$ and $\deg q_i(T) = \deg p_i(T)$. Then, there exists a places $P_i \in \mathbb{P}_{F'}$ such that $P_i|P,\ q_i(y) \in P_i$ and its inertia degree $f(P_i|P) = \deg p_i(T)$ for $i = 1, 2, \cdots, r$ with $P_i \neq P_j$ when $i \neq j$. Moreover, there is no other place of F' lying above P because of the fundamental equality which is given in Theorem 3.1.11 in [36].*

Definition 2.4. *[36, Definition 3.4.3] Let F'/K' be a finite separable extension of F/K, $P \in \mathbb{P}_F$ with the integral closure O'_P in F' and $C_P = t \cdot O'_P$ be the complementary module over O_P. The different exponent of $P'|P$ is defined as*

$$d(P'|P) := -\nu_{P'}(t)$$

and the different of F'/F is the divisor

$$\mathrm{Diff}(F'/F) := \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \cdot P'.$$

Theorem 2.5. *(Hurwitz Genus Formula) [36, Theorem 3.4.13] Let F'/K' be a finite separable extension of F/K. We have that*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \mathrm{Diff}(F'/F),$$

where g and g' are the genus of F and F', respectively,

Theorem 2.6. *(Dedekind's Different Theorem) [36, Theorem 3.5.1] Let F'/K' be a finite separable extension of F/K and $P \in \mathbb{P}_F$. For all $P'|P$,*

(i) $d(P'|P) \geq e(P'|P) - 1$.

(ii) $d(P'|P) = e(P'|P) - 1$ *if and only if the extension, F'/F, is tame.*

Corollary 2.7. *[36, Corollary 3.5.8] Let $F/K(x)$ be a finite separable extension of degree $[F : K(x)] > 1$ so that K is the constant field of F. Then $F/K(x)$ is ramified.*

2.1.1. Galois Extensions of Function Fields

Theorem 2.8. *[36, Theorem 3.7.1] Let F'/K' be a Galois extension of F/K and P_1, P_2 be extensions of P in F'. Then $P_2 = \sigma(P_1)$ for some $\sigma \in Gal(F'/F)$. In other words, the Galois group acts transitively on the set of extensions of P.*

Theorem 2.9 (Corollary 3.7.2)**.** *[36], Let F'/K' be a Galois extension of F/K and $P_1, \cdots, P_r$ be extensions of P in F'. Then*

$$e(P_i|P) = e(P_j|P) \text{ and } f(P_i|P) = f(P_j|P) \text{ for all } 1 \leq i, j \leq r.$$

For the following definitions and results we refer to the Section 3.8 and Theorem 3.8.2 in [36]. Let F'/K' be a Galois extension of F/K and P' be an extension of P in F'.

Decomposition group : $D(P'|P) = \{\sigma \in Gal(F'/F) | \sigma(P') = P'\}$ which is a subgroup of $Gal(F'/F)$, with $|D(P'|P)| = e(P'|P)f(P'|P)$, then it is just equal to $f(P'|P)$ for the unramified places. Also, $D(P'|P) \cong Gal(F_{P'}/F_P)$ thus, in particular if K is a finite field and $P'|P$ is unramified, $D(P'|P)$ is a cyclic subgroup of $Gal(F'/F)$ of order $f(P'|P)$.

Inertia group : $I(P'|P) = \{\sigma \in Gal(F'/F) | \sigma(x) = x \mod P' \ \forall x \in O_{P'}\}$ which is normal subgroup of $D(P'|P)$, with $|I(P'|P)| = e(P'|P)$.

Let P_D denote the restriction of the place P' in the decomposition field F_D (which is the fixed field of the subgroup $D(P'|P)$ of $Gal(F'|F)$) , and P_I be the restriction of P' in the inertia field F_I (which is again the fixed field of the subgroup

$I(P'|P)$ of $Gal(F'|F)$, similarly). About the ramification and the inertia indices of the places $P'|P_D,\ P_D|P_I$ and $P_I|P$, we have the following figure:

$$\begin{array}{ccc} F' & P' & \\ | & | & e(P'|P_I) = e(P'|P) = [F' : F_I] \text{ and } f(P'|P_I) = 1 \\ F_I & P_I & \\ | & | & f(P_I|P_D) = f(P'|P) = [F_I : F_D] \text{ and } e(P_I|P_D) = 1 \\ F_D & P_D & \\ | & | & e(P_D|P) = f(P_D|P) = 1 \\ F & P & \end{array}$$

2.2. N-Polynomials

For a positive integer n, the field $\mathbb{F}_{q^n}$ is a cyclic Galois extension of $\mathbb{F}_q$ of degree n, with Galois group generated by the Frobenius automorphism $\alpha \to \alpha^q$ which is the cyclic group of order n. This extension field, $\mathbb{F}_{q^n}$, is a vector space over $\mathbb{F}_q$ of dimension n. A *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis consisting of the Galois conjugates of a given element $\alpha \in \mathbb{F}_{q^n}$, i.e., a basis of the form $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ for some element $\alpha \in \mathbb{F}_{q^n}$. Such an element α is said to be *normal* over $\mathbb{F}_q$ and its irreducible polynomial over $\mathbb{F}_q$ is called an *N-polynomial* or a *normal polynomial*. The existence of a normal basis for a given q and n is ensured by the *"Normal Basis Theorem"* [31, Corollary 4.13]. Furthermore, if for each divisor d of n, α is normal in the extension $\mathbb{F}_{q^n}/\mathbb{F}_{q^d}$, then α is called a *completely normal element* in the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ and its irreducible polynomial over the related field is called a *completely normal polynomial*.

The constructions of N-polynomials over the finite field $\mathbb{F}_q$ is one of the important problems in the arithmetic of finite fields. In general a positive integer n is given and a finite field $\mathbb{F}_q$ is chosen as a ground field. Then, in order to construct a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, an N-polynomial in $\mathbb{F}_q[T]$ of degree n is constructed. Especially, for the explicit constructions of irreducible polynomials

over $\mathbb{F}_q$, some recursive methods using rational transformations are preferred. In particular, in the following chapter, we will be interested in the methods that are obtained using quadratic transformations.

3. A CLASSIFICATION OF NORMALIZED QUADRATIC TRANSFORMATIONS

Let us define a function field extension $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(t)$ where $w = g(t)/h(t)$ for any relatively prime polynomials $g, h \in \mathbb{F}_q[T]$ with $\max\{\deg g, \deg h\} = 2$. By Corollary 2.7, the extension is always ramified. Let P be a place of $\mathbb{F}_q(w)$ and P' be a place of $\mathbb{F}_q(t)$ lying over P. Recall that the different of the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ is defined as $\sum_{P \in \mathbb{P}_{\mathbb{F}_q(w)}} \sum_{P'|P} d(P'|P).P'$ where $d(P'|P)$ is the different exponent of P' over P. By the Hurwitz Genus Formula in Theorem 2.5,

$$2g' - 2 = \frac{[\mathbb{F}_q(t) : \mathbb{F}_q(w)]}{[\mathbb{F}_q : \mathbb{F}_q]}(2g - 2) + \deg \mathrm{Diff}(\mathbb{F}_q(t)/\mathbb{F}_q(w))$$

where g and g' are the genus of $\mathbb{F}_q(w)$ and $\mathbb{F}_q(t)$, respectively, which are just equal to 0 since the function fields are rational. Thus we obtain that

$$\deg \mathrm{Diff}(\mathbb{F}_q(t)/\mathbb{F}_q(w)) = 2.$$

This implies that there can be three situations for the ramified places in the given extension: There is place P of $\mathbb{F}_q(w)$ which has different exponent 2, or there are two places which have different exponent 1, or there is one place of degree 2 which has different exponent one. By Dedekind's Different Theorem in 2.6, we know that $d(P'|P) \geqslant e(P'|P) - 1$ and equality holds if and only if $e(P'|P)$ is not divisible by the characteristic of $\mathbb{F}_q$. Thus, we see that there can be wildly ramified places for even characteristic. On the other hand, for odd characteristic, there can be two rational places, P_1 and P_2 or a place of degree 2, which are tamely ramified.

Even though we will consider the the situation in even characteristic at some points, for our work we are mostly interested in odd characteristic case. Especially, the case of two ramified rational places has been examined in detail. The other case of a degree 2 ramified place still in progress and will be considered in the future.

3.1. The General Approach for the Transformations of Degree 2 with Galois Theoretical Tools

Let us give some general observations and results that will explain our approach to these constructions: Let $g, h \in \mathbb{F}_q[T]$ be relatively prime polynomials. Define the map,

$$\begin{aligned} T_{g,h}(f): \quad \mathbb{F}_q[T]\backslash\{0\} &\to \mathbb{F}_q[T]\backslash\{0\} \\ f(T) &\mapsto h(T)^{\deg f} \cdot f\Big(\frac{g(T)}{h(T)}\Big). \end{aligned}$$

Observe that for any $f_1, f_2 \in \mathbb{F}_q[T] \setminus \{0\}, T_{g,h}(f_1 \cdot f_2) = T_{g,h}(f_1) \cdot T_{g,h}(f_2)$. Denote the n-fold composition of this map as $T^n_{g,h}$. We associate it with the extension of rational function fields $\mathbb{F}_q(t)/\mathbb{F}_q(w)$, where $w = g(t)/h(t)$. For any irreducible polynomial $f(T) \in \mathbb{F}_q[T]$ of degree d we know that there is a place P_f of degree d in $\mathbb{F}_q(w)$. Then we will show that the factorisation of $T_{g,h}(f)$ in $\mathbb{F}_q[T]$ is relevant to the splitting behaviour of P_f in the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$.

From now on we assume the places that we consider are unramified and none of the indeterminates has pole at these places.

As we said above we will consider the quadratic transformations which implies that $\max\{\deg g, \deg h\} = 2$. The extension corresponding to $T_{g,h}$ will satisfy $[\mathbb{F}_q(x) : \mathbb{F}_q(t)] = 2$. First we just examine two iterations to understand the behaviour of the place P_f in the extensions setting $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(t) \subseteq \mathbb{F}_q(x)$, where $t = g(x)/h(x)$ and $w = g(t)/h(t)$. We want that the place P_f is inert in the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$. Such an extension is either Galois or not. If it is a Galois extension, the Galois group has order 4, so it is either the cyclic group C_4 of order 4 or the Klein four group $V = \mathbb{Z}_2 \times \mathbb{Z}_2$. If it is not a Galois extension, its Galois closure has Galois group given by the dihedral group D_8 of order 8.

Let us examine these cases one by one:

Suppose the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ is Galois, and let Q_f be a place of $\mathbb{F}_q(x)$ lying above the place P_f. We know that the decomposition group $D(Q_f|P_f)$ is a cyclic subgroup of the Galois group since we are working with a finite field of constant fields. If P_f is inert in this extension, $D(Q_f|P_f)$ is equal to the whole Galois group. So, if the Galois group is the Klein-four group V, then P_f cannot be inert in the extension since V is not a cyclic group, which means that we cannot find an irreducible polynomial f with $T^2_{g,h}(f)$ is also irreducible (note that for a finite field there is always a unique extension of each degree and it is a cyclic Galois extension).

When the Galois group is C_4, since it has just one cyclic subgroup of order 2, we se that if the place P_f of $\mathbb{F}_q(w)$ is inert in $\mathbb{F}_q(t)/\mathbb{F}_q(w)$, then it has to be also inert in the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$.

Now suppose $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ is not a Galois extension. Its Galois closure has Galois group D_8 which implies that for an element η of the Galois closure $\mathbb{F}_q(x,\eta)$ of the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$, there is an extension $\mathbb{F}_q(w,\eta)$ of $\mathbb{F}_q(w)$ of degree 2, so that $\mathbb{F}_q(x,\eta)/\mathbb{F}_q(w,\eta)$ is a cyclic Galois extension with the Galois group C_4. Then if the place P_f of $\mathbb{F}_q(w)$ is inert in the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ then it splits in the extension $\mathbb{F}_q(w,\eta)/\mathbb{F}_q(w)$ if and only if P_f is inert in the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$.

Taking into account these ideas, we will consider the iterative constructions that were classified at the beginning. For a given transformation $T_{g,h}$, we will see that if the associated extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ satisfies certain properties (with respect to the places involved), then the same will hold for the extension $\mathbb{F}_q(x_{i+2})/\mathbb{F}_q(x_i)$, $i \geqslant 0$, in the tower $\mathbb{F}_q(x_0) \subseteq \mathbb{F}_q(x_1) \subseteq \cdots \mathbb{F}_q(x_n) \subseteq \cdots$, where
$x_i = g(x_{i+1})/h(x_{i+1})$ and $x_0 = w, x_1 = t, x_2 = x$.

Let us give further details of this approach. Recall the given tower of the rational function fields $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(t) \subseteq \mathbb{F}_q(x)$, where $t = g(x)/h(x)$ and $w = g(t)/h(t)$. Let $f(w) \in \mathbb{F}_q[w]$ be an irreducible polynomial, P_f be the associated place of $\mathbb{F}_q(w)$ and O_f be the associated valuation ring. Let Q_f be a place of $\mathbb{F}_q(t)$ lying over P_f which means Q_f is a zero of $f(w)$ in $\mathbb{F}_q(t)$ and v_{Q_f} be the corresponding valuation. We denote the ramification index with $e(Q_f|P_f)$ of Q_f over P_f and we have $e(Q_f|P_f) = v_{Q_f}(f(w)) = v_{Q_f}\big(f\big(\frac{g(t)}{h(t)}\big)\big)$. We start by assuming that t is regular at Q_f. Then Q_f will be an irreducible polynomial $f'(t) \in \mathbb{F}_q[t]$ and v_{Q_f} will be the f'-adic valuation $v_{f'}$ on $\mathbb{F}_q(t)$. Thus $e(Q_f|P_f) = v_{f'}\big(f\big(\frac{g(t)}{h(t)}\big)\big)$ and $e(Q_f|P_f)$ is the biggest power of $f'(t)$ occurring as a factor of the polynomial $T_{g,h}(f) = h(t)^{\deg f} \cdot f\big(\frac{g(t)}{h(t)}\big)$ since it is equal to the numerator of $f\big(\frac{g(t)}{h(t)}\big)$ that is in lowest term because of g, h are relatively prime.

We know that if t is integral over O_f, then t is regular at all places of $\mathbb{F}_q(t)$ lying over P_f. This implies that there is a one-to-one correspondence between the irreducible factors of $T_{g,h}(f)$ and the places of $\mathbb{F}_q(t)$ lying over P_f by the Kummer Theorem. That is, if $T_{g,h}(f) = f_1'(t)^{e_1} \cdot f_2'(t)^{e_2} \cdots f_s'(t)^{e_s}$ where $f_i(t)$'s are irreducible polynomials in $\mathbb{F}_q[t]$ and $Q_{f_i'}$ is the associated place of $\mathbb{F}_q(t)$ with $\deg Q_{f_i'} = \deg f_i'(x)$ then $Q_{f_1'}, \ldots, Q_{f_s'}$ will be all the places of $\mathbb{F}_q(t)$ lying over P_f with $e_i = e(Q_{f_i'}|P_f)$, and the inertia degrees are given by $f(Q_{f_i'}|P_f) = \deg f_i'(t)$.

Therefore we obtain the following result:

Theorem 3.1. *[28, Theorem 3] $T_{g,h}(f) = h(t)^{\deg f} f\big(\frac{g(t)}{h(t)}\big)$ is irreducible in $\mathbb{F}_q[t]$ if and only if the associated place P_f is inert in the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$, where $w = g(t)/h(t)$.*

This is a result of Kummer's Theorem 2.3 that is implied by the irreducibility of the polynomial $f(T) - \alpha \cdot g(T)$ over $O_f/P_f \cong \mathbb{F}_q(\alpha)$, where α is a root of $f(T)$, which is known as Capelli's Lemma (see also 1.1).

Since the transformation $T_{g,h}$ is multiplicative we also have the following:

Theorem 3.2. *[28, Theorem 4] Let $f(T)$ be any polynomial over $\mathbb{F}_q$ and let $D_0 = (f(t))$ be the zero divisor of $f(w)$ in $\mathbb{F}_q(w)$. If x is integral over O_f, then all places in the support of the conorm of D_0 with respect to the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$, $\mathrm{Con}_{\mathbb{F}_q(t)/\mathbb{F}_q(w)}(D_0)$ will be in one-to-one correspondence with the irreducible factors of $T_{g,h}(f)$ in $\mathbb{F}_q[t]$ with $\mathrm{Con}_{\mathbb{F}_q(t)/\mathbb{F}_q(w)}(D_0) = (T_{g,h}(f))_0$.*

By using this theorem repeatedly , we see that the factorization of $T^n_{g,h}(f)$ is just related to the splitting behaviour of the place P_f in a given tower of rational function fields.

Theorem 3.3. *[28, Theorem 5] Given a tower of rational function fields $\mathbb{F}_q(x_0) \subseteq \mathbb{F}_q(x_1) \subseteq \ldots \subseteq \mathbb{F}_q(x_n) \subseteq \ldots$ where $g(x_{i+1})/h(x_{i+1}) = x_i$, for $i \geqslant 0$. Let $f(T)$ be an irreducible polynomial over $\mathbb{F}_q$ and let the associated place of $\mathbb{F}_q(x_0)$ be given by P_f and let O_f be the its valuation ring. Assume that x_i is integral over O_f, for all i. For $n \geqslant 1$, let f' be any irreducible polynomial and $Q_{f'}$ be the associated place in $\mathbb{F}_q(x_n)$. Then $f'(T)$ is an irreducible factor of $T^n_{g,h}(f)$ with exponent $e = e(Q_{f'}|P_f)$ if and only if $Q_{f'}$ lies over P_f. In that case $f(Q_{f'}|P_f) = \deg f'(T)$.*

Corollary 3.4. *[28, Corollary 6] $T^n_{g,h}(f)$ is irreducible over $\mathbb{F}_q$ if and only if the place P_f is inert in the extension $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$ for any $n \geqslant 1$.*

The integrity of $x_1, x_1, x_2, \ldots, x_n, \ldots$ over O_f can be guaranteed by requiring $\deg f(t) > 1$ or $\deg g > \deg h$. If $\deg f(t) > 1$, then the pole of x_n in $\mathbb{F}_q(x_n)$ cannot lie above P_f since the pole of x_n is a rational place and $\deg P_f = \deg f(t) > 1$ for any $n \geqslant 1$. Thus x_n must be integral over O_f. Similarly, if $\deg g > \deg h$, the pole of x_n in $\mathbb{F}_q(x_n)$ lies just above P_∞ which is the pole of x_0 in $\mathbb{F}_q(x_0)$, thus cannot lie above the place P_f, for any $n \geqslant 1$.

Proposition 3.5. *[28, Proposition 8] Let $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(t) \subseteq \mathbb{F}_q(x)$ be given such that $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ and $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ are extensions of degree p, for a prime p not dividing the characteristic of $\mathbb{F}_q$. Assume also that $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ is a cyclic Galois extension. Let P be a place of $\mathbb{F}_q(w)$ which is unramified in $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ and is inert in $\mathbb{F}_q(t)/\mathbb{F}_q(w)$. Then P is inert in $\mathbb{F}_q(x)/\mathbb{F}_q(w)$.*

Proof. Let Q be a place of $\mathbb{F}_q(t)$ lying over P and $D = D(Q|P)$ be its decomposition group. As we know, D is a cyclic subgroup of $G = Gal(\mathbb{F}_q(x)/\mathbb{F}_q(w))$. By assumption G is a cyclic group of order p^2. Thus we have that either $D = \{e\}$ or $D \cong C_p$ or $D = G$. Again by assumption P is inert in $\mathbb{F}_q(t)/\mathbb{F}_q(w)$, that is D cannot be equal to $\{e\}$. Now suppose $D \cong C_p$. Since C_p is the unique subgroup of G and $[\mathbb{F}_q(x) : \mathbb{F}_q(t)] = p$, we must have that $\mathbb{F}_q(t)$ is the fixed field of D, that is $\mathbb{F}_q(t)$ is the decomposition field of Q over P, which contradicts that P is inert in $\mathbb{F}_q(t)/\mathbb{F}_q(w)$. Therefore $D = G$ which means that P is also inert in $\mathbb{F}_q(x)/\mathbb{F}_q(w)$. □

By using this proposition repeatedly, we obtain the following results:

Corollary 3.6. *[28, Corollary 9] Let $\mathbb{F}_q(x_0) \subseteq \mathbb{F}_q(x_1) \subseteq \ldots \subseteq \mathbb{F}_q(x_n) \subseteq \ldots$ be a given tower with $[\mathbb{F}_q(x_{n+1}) : \mathbb{F}_q(x_n)] = p$, for some prime p not dividing the characteristic of $\mathbb{F}_q$, $n = 0, 1, \ldots$. Assume $\mathbb{F}_q(x_{n+2})/\mathbb{F}_q(x_n)$ is cyclic Galois extension for all $n \geqslant 0$. If a place P of $\mathbb{F}_q(x_0)$ is unramified in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$ for $n \geqslant 1$ and is inert in $\mathbb{F}_q(x_1)/\mathbb{F}_q(x_0)$ then P is inert in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$ for all $n \geqslant 1$.*

Corollary 3.7. *[28, Corollary 11] Let $\mathbb{F}_q(x_0) \subseteq \mathbb{F}_q(x_1) \subseteq \ldots \subseteq \mathbb{F}_q(x_n) \subseteq \ldots$ be a given tower with $[\mathbb{F}_q(x_{n+1}) : \mathbb{F}_q(x_n)] = p$, for some prime p not dividing the characteristic of $\mathbb{F}_q$, $n = 0, 1, \ldots$. Suppose there is an element $\eta \in \overline{\mathbb{F}_q(x_0)}$ so that $\mathbb{F}_q(x_{n+1}, \eta)/\mathbb{F}_q(x_n, \eta)$ is a cyclic Galois extension for $n \geqslant 0$. If a place P of $\mathbb{F}_q(x_0)$ is unramified in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$ for $n \geqslant 1$, is inert in $\mathbb{F}_q(x_1)/\mathbb{F}_q(x_0)$ and splits in $\mathbb{F}_q(x_0, \eta)/\mathbb{F}_q(x_0)$, then P is inert in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$ for all $n \geqslant 1$.*

3.2. The Power Map Transformation, T^2

Let us give some results for the first case of our classification, the transformation $cT^2, c \in \mathbb{F}_q^*$. This is so classical method to construct a sequence of irreducible polynomials using power map transformations of any degree. A well-known result about it is the following ([9]):

Theorem 3.8. *[9, Theorem 1] Let $f(T) \in \mathbb{F}_q[T]$ be an irreducible polynomial of degree n and exponent e (which is te order of any root of f). Let t be a positive integer, the polynomial $f(T^t)$ is irreducible over $\mathbb{F}_q$ if and only if*

(i) $\gcd(t, (q^n - 1)/e) = 1$,
(ii) each prime factor of t divides e, and
(iii) if $4|t$ then $4|(q^n - 1)$.

Proposition 3.9. *[35, Proposition 2.2] Let $f(T) \in \mathbb{F}_q[T]$ be an irreducible polynomial of degree n and t be a positive integer. If t is even, assume also that $4|q^n - 1$. If $f(T^t)$ is irreducible over $\mathbb{F}_q$ then $f(T^{t^r})$ is irreducible over $\mathbb{F}_q$ for all $r \geqslant 0$.*

This result follows from the fact that the prime factors of t^r are the same as those of t. So if t satisfies the conditions of Theorem 3.8, then so does t^r.

Proposition 3.10. *[35, Proposition 2.3] Let $f(T) \in \mathbb{F}_q[T]$ be an irreducible polynomial of degree n and let t be a positive integer. If t is even, assume moreover that $4|q^n - 1$. Let $f_0(T) = f(T)$ and set $f_m(T) = f_{m-1}(T^t)$ for $m \geqslant 1$. Assume $f_1(T)$ is irreducible. Then $f_m(T)$ is irreducible of degree $\deg f \cdot t^m$ for all m.*

This is just obtained using the above Proposition 3.9, iteratively. Now let us give some notations and definitions from [35].

Let $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_q)$ and $f(T) \in \mathbb{F}_q[T]$ of degree n setting $f(\infty) := \infty$. Define

$$P_\sigma(f)(T) := (cT+d)^n f\Big(\frac{aT+b}{cT+d}\Big).$$

We say that $\deg P_\sigma(f)(x) = n \Leftrightarrow f(\sigma.\infty) \neq 0$. Also under the latter condition, for any $\tau \in GL_2(\mathbb{F}_q)$, $P_\sigma \circ P_\tau(f) = P_{\sigma.\tau}(f)$. If f is irreducible over $\mathbb{F}_q$ then so is $P_\sigma(f)$. Let t be a positive integer and define $S_t : \mathbb{F}_q[T] \to \mathbb{F}_q[T]$ such that $S_t(f)(T) := f(T^t)$. Using these maps we define a transformation as follows:

$$f^{R_{\sigma,t}}(T) := P_{\sigma^{-1}} \circ S_t \circ P_\sigma(f)(T).$$

For $f(a/c) \neq 0$, we also define an element of $\mathbb{F}_q$ by

$$\eta(f;\sigma) := (\sigma^{-1}.\infty)^n . \frac{f(\sigma.0)}{f(\sigma.\infty)} = \Big(-\frac{d}{c}\Big)^n f\Big(\frac{b}{d}\Big) f\Big(\frac{a}{c}\Big)^{-1},$$

if $c = 0$ then $\eta(f;\sigma) = (-d/a)^n f(b/d)$ and if $d = 0$, $\eta(f;\sigma) = (-b/c)^n f(a/c)^{-1}$.

Lemma 3.11. *[35, Lemma 3.2] Let $g(T)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n with $g(\sigma.\infty) \neq 0$ and set $f := P_\sigma(g)$. Then f is irreducible and $f(\sigma^{-1}.\infty) \neq 0$. Also, if $\alpha_1, \dots \alpha_n$ are the roots of f, then $\sigma.\alpha_i = \left(\frac{a\alpha_i+b}{c\alpha_i+d}\right)$ are the roots of g for $1 \leqslant i \leqslant n$.*

Theorem 3.12. *[35, Theorem 1.2] Let $t \geq 2$ be an integer such that every prime factor of t divides $q-1$. Let $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_q)$ and $f(T) \neq T - a/c$ be a monic irreducible polynomial over $\mathbb{F}_q$ of degree n. If $q \equiv 3 \mod 4$ and t is even assume also n is even. Suppose for all prime numbers $\ell | t$, the element $\eta(f;\sigma)$ is not an $\ell-$th power in $\mathbb{F}_q$. Define $f_0 = g$ and let $f_i = f_{i-1}^{R_{\sigma,t}}$ for $i \geq 1$. Then $(f_i)_{i\geq 0}$ is an infinite sequence of irreducible polynomials, with $\deg f_i = t^i n$.*

3.2.1. R-Transform

As en example of this case we can give the well-known R-transform of Cohen. For an odd prime power q, it gives a classical way for constructing a sequence of

irreducible polynomials. It is analogous to the transformation of Wiedemann and to Meyn's Q-transform which is defined as

$$f^Q(T) = T^{\deg f} f(T + T^{-1}),$$

for any polynomial f over a field of even characteristic. We will already mention this transform in our third class in detail.

Cohen's purpose was to find a similar way to do this in odd characteristic. Modifying Meyn's work, he defined the R-transform for a polynomial f as follows:

$$f^R(T) = (2T)^{\deg f} f\Big(\frac{T^2+1}{2T}\Big) = 2^{\deg f} f^Q\Big(\frac{T}{2}\Big).$$

Then he proved the following result, which was given in the introduction (see Theorem 1.4): *Let q be an odd prime power and f be a monic irreducible polynomial over $\mathbb{F}_q$ with $\deg f \geqslant 1$ and assume $\deg f$ is even whenever $q \equiv 3 \pmod q$. Suppose $f(1)f(-1)$ is not a square element in $\mathbb{F}_q$. Define $f_0 = f$ and $f_k = f_{k-1}^R$. Then for each $k \geqslant 0$, the polynomial f_k is irreducible over $\mathbb{F}_q$.*

He also showed that for any q, there exists an irreducible polynomial over $\mathbb{F}_q$ satisfying the hypotheses of this theorem.

Notice that for $\sigma = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $t = 2$ we obtain Cohen's R-transform: $T \to \frac{T^2+1}{2T}$. This means that the R-transform is just the power map transformation $T \to T^2$, with a change of coordinate by the linear fractional transformation

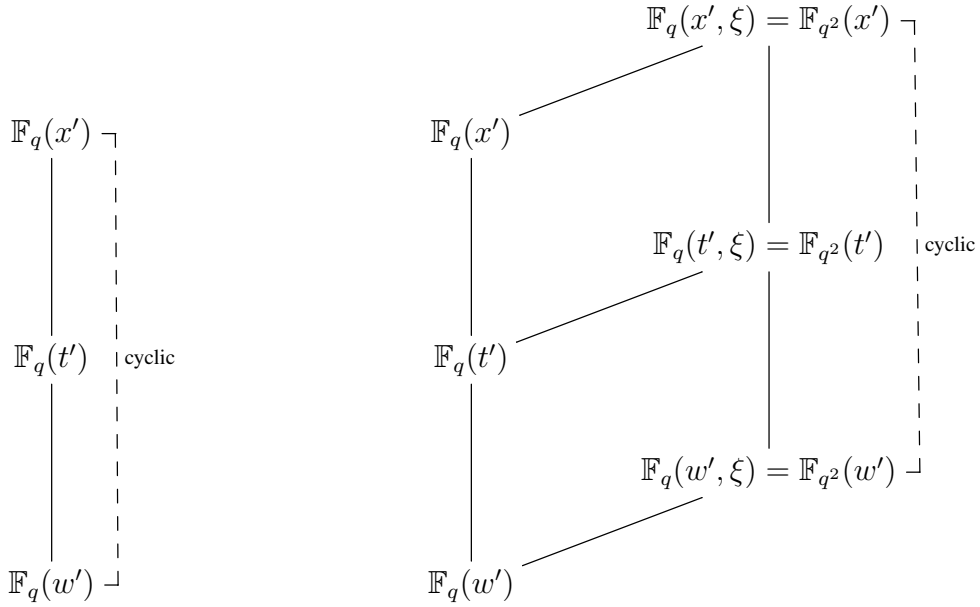
$$\sigma(T) = \frac{T+1}{T-1}.$$

Given an irreducible polynomial over $\mathbb{F}_q$ with $f(1) \neq 0$ (this guarantees that we start with an unramified place in the corresponding rational function field extension, which is already satisfied automatically by the following condition), if we compute the element $\eta(\sigma; f) = f(1).f(-1)^{-1}$, we see that it is equal to the condition given by Cohen in Theorem 1.4 up to a square element $f(-1)^2$.

To see the details Galois theoretically, let us consider the transformation for two iterations in the corresponding tower of the rational function fields:

Let $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(t) \subseteq \mathbb{F}_q(x)$ be the rational function field extensions with $w = \frac{t^2+1}{2t}$ and $t = \frac{x^2+1}{2x}$. Take the linear fractional transformation $\sigma(T) = \frac{T+1}{T-1}$ which implies that $\sigma\left(\frac{T^2+1}{T}\right) = (\sigma(T))^2$. Now say $w' = \sigma(w),\ t' = \sigma(t)$ and $x' = \sigma(x)$, then consider the extensions $\mathbb{F}_q(w') \subseteq \mathbb{F}_q(t') \subseteq \mathbb{F}_q(x')$ with $w' = t'^2$ and $t' = x'^2$. That is, the minimal polynomial of x' over $\mathbb{F}_q(w')$ is $Irr(x', \mathbb{F}_q(w')) = T^4 - w'$.

Thus the extension $\mathbb{F}_q(x')/\mathbb{F}_q(w')$ is cyclic Galois, i.e. $Gal(\mathbb{F}_q(x')/\mathbb{F}_q(w')) = C_4$ if $\mathbb{F}_q$ contains the 4-th roots of unity. This is equivalent to say that $q \equiv 1 \pmod 4$. However, whenever $q \equiv 3 \pmod 4$ then the extension $\mathbb{F}_q(x')/\mathbb{F}_q(w')$ can be lifted to a Galois extension adjoining a primitive 4-th root of unity ξ. That is the new extension $\mathbb{F}_q(x', \xi)/\mathbb{F}_q(w', \xi)$ is cyclic Galois extension now. In fact $\mathbb{F}_q(\xi) = \mathbb{F}_{q^2}$, so the extension $\mathbb{F}_q(w', \xi) = \mathbb{F}_{q^2}(w') \supseteq \mathbb{F}_q(w')$ is just a constant field extension.



$q \equiv 1 \mod 4$ $\qquad\qquad$ $q \equiv 3 \mod 4$

Let us start with an irreducible polynomial $f(T)$ over $\mathbb{F}_q$ with the associated place P_f of $\mathbb{F}_q(w)$ (i.e., the zero P_f of $f(w)$). If $\deg f$ is even then P_f splits in the

extension $\mathbb{F}_{q^2}(w)/\mathbb{F}_q(w)$. Now we can also determine when P_f is inert in the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$. Since $w' = \frac{w+1}{w-1}$, w' has a pole at P_{w-1}. Notice that the place P_{w-1} is already ramified in the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$, because

$$Irr(t, \mathbb{F}_q(w)) = T^2 - 2wT + 1 \equiv (T-1)^2 \mod P_{w-1},$$

so we take $f(w) \neq w - 1$. Say $\delta = w'(P_f)$ which the value of w' at P_f. Since $\{t', 1\}$ is an integral basis at P_f for the extension $\mathbb{F}_q(t) = \mathbb{F}_q(t') \supseteq \mathbb{F}_q(w') = \mathbb{F}_q(w)$ with $w' = t'^2$, by Kummer's Theorem P_f splits in the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ if and only if δ is a square element in $\mathbb{F}_q(\delta)$. This is equivalent to say that $\mathrm{N}_{\mathbb{F}_q(\delta)/\mathbb{F}_q}(\delta)$ is a square in $\mathbb{F}_q$ since the norm map is multiplicative. The irreducible polynomial of the element δ over $\mathbb{F}_q$ is given by $(T-1)^{\deg f} f\left(\frac{T+1}{T-1}\right)$ with the leading coefficient $f(1)$ and constant term $(-1)^{\deg f} f(-1)$. Thus $\mathrm{N}_{\mathbb{F}_q(\delta)/\mathbb{F}_q}(\delta) = \frac{f(-1)}{f(1)}$ and P_f is inert in the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ if $f(-1)f(1)$ is a non-square in $\mathbb{F}_q$. If $q \equiv 1 \mod 4$ by Corollary 3.6 and if $q \equiv 3 \mod 4$ by Corollary 3.7 we obtain Cohen's result in Theorem 1.4.

The existence of such a polynomial satisfying the conditions in the Theorem 1.4, ([32, Lemma 4]), can also be shown easily now. For a given $n \geqslant 1$, let σ be a primitive element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Obviously, σ is a non-square element in $\mathbb{F}_{q^n}$. Let $f(T)$ be the minimal polynomial of σ of $\deg f = n$ over $\mathbb{F}_q$. Then the polynomial $(T-1)^n f\left(\frac{T+1}{T-1}\right)$ is irreducible and satisfies the condition of the Cohen's result in Theorem 1.4.

In addition, Bassa and Menares also showed in the rest of their main theorem in [35] that, for $i \geqslant 0$ and a t^i-th root of unity, ζ, the set of the roots of f_i is invariant under the action of the order t^i matrix in $GL_2(\mathbb{F}_q(\zeta))$ given by

$$\mu_{\sigma,\zeta} = \begin{pmatrix} \zeta ad - bc & (1-\zeta)ab \\ (\zeta - 1)cd & ad - \zeta bc \end{pmatrix},$$

where $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $f_{i+1} = f_i^{R_{\sigma,t}},\ i \geqslant 0$.

For the R-transform, since $t = 2$ and $\sigma = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, we take $\zeta = -1$ then obtain the matrix $\mu_{\sigma,\zeta} = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$ that has the action $T \mapsto \frac{1}{T}$. This means that for all $i \geqslant 0$, the roots of the polynomial f_i in the sequence stated by the R-transform are invariant under the map $T \mapsto \frac{1}{T}$. Thus, these polynomials are also self-reciprocal for all $i \geqslant 0$.

Besides, in the paper [10], Meyn showed the following result:

Theorem 3.13. *[10, Theorem 1] Let $q \equiv 1 \mod 4$ be a prime power and $f \in \mathbb{F}_q[T]$ be a monic self-reciprocal N-polynomial of degree 2 such that $f(1)f(-1)$ is a non-square element of $\mathbb{F}_q$. Then for all $i \geqslant 0$, the polynomials defined as $f(T) = f_0(T)$ and $f_{i+1}(T) = f_i^R(T)$ are N-polynomials over $\mathbb{F}_q$.*

After that, in [29] Chapman showed that the roots of these polynomials are also completely normal in the corresponding extensions of the base field.

Theorem 3.14. *[29, Theorem 1] Let $q \equiv 1 \mod 4$ be a prime power and $f(T) = T^2 + aT + 1$ be an irreducible polynomial over $\mathbb{F}_q$. Define the sequence $f_0(T) = f(T)$ and $f_{i+1}(T) = f_i^R(T), i \geqslant 0$, with α_i is a root of the polynomial f_i for each $i \geqslant 0$. Then α_i is a completely normal element of $\mathbb{F}_{q^{2^i}}$ over $\mathbb{F}_q$.*

More generally, in [40], Aravena proved that the generalization of the power map transformation, $R_{\sigma,t}$ gives completely normal polynomials under suitable conditions:

Theorem 3.15. *[40, Theorem 1.3] Let $f(T) \neq T - a/c$, of degree 1, $t \geq 2$, $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_q)$. Let $(f_i)_{i\geq 0}$ be the sequence defined as $f_0 = f$ and $f_{i+1} = f_i^{R_{\sigma,t}}$. Suppose $dc \neq 0$, then we have the following:*

i) *If* $ab = 0$, *then* $(f_i)_{i\geq 0}$ *is a sequence of completely normal polynomials over* $\mathbb{F}_q[T]$.

ii) *If* $ab \neq 0$, *and the element* $\frac{bc}{ad}$ *is an* ℓ*-th power for some prime* ℓ *dividing* t, *then* $(f_i)_{i\geq 0}$ *is a sequence of completely normal polynomials over* $\mathbb{F}_q[T]$.

iii) *If* $ab \neq 0,\ d = -c$ *and* $f(T) \neq T$, *then* $(f_i)_{i\geq 0}$ *is a sequence of completely normal polynomials over* $\mathbb{F}_q[T]$.

Then he also proved the existence of a polynomial $f_0$of degree 1 over $\mathbb{F}_q$ such that $f_1 = f_0^R$ where f_1 is a given initial polynomial for Theorem 3.14 and f_0 satisfies the conditions of Theorem 3.12 which is given as $f_0(T) = T - \frac{\alpha+\alpha^{-1}}{2}$ where α is a root of the f_1. It is clear that $f_0(T) \in \mathbb{F}_q[T]$ since f_1 is a self-reciprocal polynomial and so $\frac{1}{\alpha}$ is also its root, i.e., the conjugate of α is just its reciprocal $\frac{1}{\alpha}$ which implies that their sum $\alpha + \frac{1}{\alpha} \in \mathbb{F}_q$. Moreover, $\eta(f_0, \sigma) = \left(\frac{1}{2-(\alpha+\alpha^{-1})}\right)^2((\alpha + \alpha^{-1})^2 - 4))$ which is not a square element in $\mathbb{F}_q$ since the given polynomial

$$f_1(T) = T^2 - (\alpha + \alpha^{-1})T + 1$$

is irreducible and its discriminant is equal to $(\alpha + \alpha^{-1})^2 - 4$.

3.2.2. Some Examples of Kyuregyan

Using the ideas leading to the above results, we can show that some other known iterative constructions of irreducible polynomials over finite fields can be recovered as examples of generalized power map transformations $R_{\sigma,t}$. In particular , we have considered the recurrent methods for odd characteristic which were constructed by Kyuregyan in [41]. First he states the following theorem:

Theorem 3.16. *[41, Theorem 3] Let* $f(T) \neq T$ *be an irreducible polynomial in* $\mathbb{F}_q[T]$ *with* $\deg f \geqslant 1$ *and assume* $q \equiv 3 \mod 4$ *if* $\deg f$ *is even,* $r \neq 0, \delta \neq 0,\ h \in \mathbb{F}_q$. *Suppose* $f\left(\frac{2\delta - rh}{r^2}\right) f\left(-\left(\frac{2\delta+rh}{r^2}\right)\right)$ *is a non-square element in* $\mathbb{F}_q$. *Define* $f_0(T) = f(T)$ *and* $f_k(T) = \left(2T + \frac{2h}{r}\right)^{\deg f_{k-1}} f_{k-1}\left(\frac{T^2 + \frac{4\delta^2 - (hr)^2}{r^4}}{2T + \frac{2h}{r}}\right),\ k \geqslant 1$. *Then* $(f_k(T))_{k\geqslant 0}$ *is a sequence of irreducible polynomials over* $\mathbb{F}_q$.

Kyuregyan gives a computational proof for this result. We will obtain a more conceptual proof using our approach.

Let us define the corresponding rational function field extension for the given transformation:

$$\begin{array}{c} \mathbb{F}_q(t) \\ \Big| \\ w = \frac{t^2+\frac{4\delta^2-(hr)^2}{r^4}}{2t+\frac{2h}{r}} \\ \Big| \\ \mathbb{F}_q(w) \end{array}$$

where $\delta, h, r \in \mathbb{F}_q$ satisfy the conditions in Theorem 3.16. Then the irreducible polynomial of t over $\mathbb{F}_q(w)$ is given by

$$Irr(t, \mathbb{F}_q(w)) = T^2 - 2wT - \frac{2h}{r}w + \frac{4\delta^2 - (hr)^2}{r^4}.$$

We can easily see that for the places $P_1 := \left(w = -\left(\frac{2\delta+rh}{r^2}\right)\right)$ of $\mathbb{F}_q(w)$ and $P_2 := \left(w = \frac{2\delta-rh}{r^2}\right)$, we obtain $Irr(t, \mathbb{F}_q(w)) \equiv \left(T - \left(\frac{2\delta-rh}{r^2}\right)\right)^2 \mod P_1$ and $Irr(t, \mathbb{F}_q(w)) \equiv \left(T + \left(\frac{2\delta+rh}{r^2}\right)\right)^2 \mod P_2$ in the corresponding residue fields $\mathbf{F}_{P_1}$ and $\mathbf{F}_{P_2}$, respectively. Since t is integral over $\mathbb{F}_q(w)$, we apply Kummer's Theorem to say that P_1 and P_2 are all ramified places of $\mathbb{F}_q(w)$ in the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ with $Q_1 := \left(t = -\left(\frac{2\delta+rh}{r^2}\right)\right)$ and $Q_2 := \left(t = \frac{2\delta-rh}{r^2}\right)$ i.e., the same places are lying over P_1 and P_2, respectively. Thus, this transformation is an example of the first class of the quadratic transformations which were normalized and classified at the beginning. We can determine the linear fractional map, $\sigma^{-1} \in PGL_2(\mathbb{F}_q)$ as carrying the ramified places P_1 and P_2 of $\mathbb{F}_q(w)$ to the places $(\sigma^{-1}(w) = 0)$ and $(\sigma^{-1}(w) = \infty)$, respectively, that is given by $\sigma^{-1} = \begin{pmatrix} 1 & \frac{2\delta+rh}{r^2} \\ 1 & -\left(\frac{2\delta-rh}{r^2}\right) \end{pmatrix}$. Then we normalize the given transformation in Theorem 3.16 with this change of coordinates just as the power map transformation $\sigma^{-1}(w) = (\sigma^{-1}(t))^2$. In other words, for any polynomial $f \in \mathbb{F}_q[T]$ we have

$$f^{R_{\sigma,2}}(T) := P_{\sigma^{-1}} \circ S_2 \circ P_\sigma(f)(T) = \Big(2T + \frac{2h}{r}\Big)^{\deg f} f\Big(\frac{T^2 + \frac{4\delta^2-(hr)^2}{r^4}}{2T + \frac{2h}{r}}\Big),$$

where $\sigma = \begin{pmatrix} -\left(\frac{2\delta - rh}{r^2}\right) & -\left(\frac{2\delta + rh}{r^2}\right) \\ -1 & 1 \end{pmatrix}$.

After that we use Theorem 3.12 to see that the conditions in Theorem 3.16 are already satisfied by its assumptions. First, we find the corresponding element $\eta(f, \sigma) \in \mathbb{F}_q$.

$$\eta(f,\sigma) = (\sigma^{-1}.\infty)^n f(\sigma.0) f(\sigma.\infty)^{-1} = f\Big(-\Big(\frac{2\delta + rh}{r^2}\Big)\Big) f\Big(\frac{2\delta - rh}{r^2}\Big)^{-1}$$

which is a non-square in $\mathbb{F}_q$ if and only if $f\Big(-\Big(\frac{2\delta+rh}{r^2}\Big)\Big) f\Big(\frac{2\delta-rh}{r^2}\Big)$ is a non-square in $\mathbb{F}_q$. And starting with an initial polynomial $f(T) neq T$ guarantees to take an unramified place in $\mathbb{F}_q(w)$, i.e., the corresponding place P_f is not equal to the zero place or the infinity place of $\mathbb{F}_q$. Thus, the assumptions of Theorem 3.16 already cover the conditions of Theorem 3.12.

Besides, we can also say that the transformation given in Theorem 3.16 even gives an infinite completely normal polynomials sequence by the result of Aravena, Theorem 3.15, if we start with a polynomial of degree 1 since for the associated linear fractional transformation $\sigma = \begin{pmatrix} -\left(\frac{2\delta - rh}{r^2}\right) & -\left(\frac{2\delta + rh}{r^2}\right) \\ -1 & 1 \end{pmatrix}$ with entries satisfying the necessary conditions in part (iii). This property was not mentioned by Kyuregyan in the paper [41].

In the paper [41], there are also some other results which can be obtained with the same method as above. One of them is given as follows:

Theorem 3.17. *[41, Theorem 3] Let $f(T) \neq T$ be an irreducible polynomial in $\mathbb{F}_q[T]$ with $\deg f \geqslant 1$ and assume $q \equiv 3 \mod 4$ if $\deg f$ is even. Let $aT^2 + 2hT$ and $dT^2 + h,\ h \neq 0$ be relatively prime polynomials over $\mathbb{F}_q$. Suppose $0 \neq \delta \in \mathbb{F}_q$, $\delta^2 - (ah)^2$ is a non-zero square and $f\Big(-\frac{2h^2}{\delta+ah}\Big) f\Big(\frac{2h^2}{\delta-ah}\Big)$ is a non-square element in*

$\mathbb{F}_q$. *Define* $f_0(T) = f(T)$ *and* $f_k(T) = (dT^2+h)^{\deg f_{k-1}} f_{k-1}\Big(\frac{aT^2+2hT}{dT^2+h}\Big),\ k \geqslant 1$. *Then* $(f_k(T))_{k\geqslant 0}$ *is a sequence of irreducible polynomials over* $\mathbb{F}_q$.

Following the same procedure as above, taking the linear fractional transformation $\sigma = \begin{pmatrix} \frac{2h^2}{\delta+ah} & -\frac{2h^2}{\delta+ah}-1 \\ -\Big(\frac{\delta-ah}{\delta+ah}\Big) & \end{pmatrix} \in GL_2(\mathbb{F}_q)$ we obtain that, for any polynomial $f \in \mathbb{F}_q[T]$,

$$f^{R_{\sigma,2}}(T) := P_{\sigma^{-1}} \circ S_2 \circ P_\sigma(f)(T) = (dT^2+h)^{\deg f} f\Big(\frac{aT^2+2hT}{dT^2+h}\Big).$$

Then we have $\eta(f,\sigma) = \Big(\frac{\delta-ah}{\delta+ah}\Big)^n f\Big(\frac{2h^2}{\delta-ah}\Big) f\Big(-\frac{2h^2}{\delta+ah}\Big)^{-1}$. If we multiply by the non-zero square element $(\delta^2-(ah)^2)^n f\Big(-\frac{2h^2}{\delta+ah}\Big)^2 \in \mathbb{F}_q$, we obtain

$$\eta(f,\sigma)(\delta^2-(ah)^2)^n f\Big(-\frac{2h^2}{\delta+ah}\Big)^2 = ((\delta-ah)^n)^2 f\Big(\frac{2h^2}{\delta-ah}\Big) f\Big(-\frac{2h^2}{\delta+ah}\Big).$$

That is, $\eta(f,\sigma)$ is a non-square element of $\mathbb{F}_q$ if and only if $\delta^2-(ah)^2$ is a square and $f\Big(\frac{2h^2}{\delta-ah}\Big) f\Big(-\frac{2h^2}{\delta+ah}\Big)$ is a non-square in $\mathbb{F}_q$ as given in the conditions of Theorem 3.17. Again by Theorem 3.15, part (ii), this transformation gives a sequence of completely normal polynomials, if we start with a polynomial of degree 1.

Similary, the following result in [41] is also just the power map transformation with a change of coordinates.

Theorem 3.18. *[41, Theorem 3] Let* $f(T)$ *be an irreducible polynomial in* $\mathbb{F}_q[T]$ *with* $\deg f \geqslant 1$ *and assume* $q \equiv 3 \mod 4$ *if* $\deg f$ *is even,* $b \in \mathbb{F}_q$. *Suppose* $f\Big(-\frac{b}{2}\Big)$ *is a non-square element in* $\mathbb{F}_q$. *Define*

$$f_0(T) = f(T) \text{ and } f_k(T) = f_{k-1}\Big(T^2+bT+\frac{b^2}{4}-\frac{b}{2}\Big),\ k \geqslant 1.$$

Then $(f_k(T))_{k\geqslant 0}$ *is a sequence of irreducible polynomials over* $\mathbb{F}_q$.

With the change of coordinates matrix $\sigma = \begin{pmatrix} 1 & -\frac{b}{2} \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_q)$ and the element $\eta(f,\sigma) = (-1)^{\deg f} f\Big(-\frac{b}{2}\Big) \in \mathbb{F}_q$ which is a non-square if and only if $f\Big(-\frac{b}{2}\Big) \in \mathbb{F}_q$ is a non-square when $q \equiv 1 \mod 4$ since -1 is already a square in this case, otherwise we take $\deg f$ as even by assumption.

3.2.3. Consideration over a Quadratic Extension of the Field $\mathbb{F}_q$

We can consider the generalization of the power map transformation over a quadratic extension of $\mathbb{F}_q$ as well. For such a construction, Bassa and Menares improved some expressions. Some results in [35] as follows:

Let $\sigma \in GL_2(\mathbb{F}_{q^2})$ and $t \geqslant 2$. Let $f(T) \in \mathbb{F}_q[T]$ with $f(\sigma.\infty) \neq 0$. We say that $R_{\sigma,t}$ is defined over $\mathbb{F}_q$ if there is an element $\kappa \in \mathbb{F}_{q^2}^*$ such that

$$\kappa \cdot f^{R_{\sigma,t}}(T) \in \mathbb{F}_q[T].$$

We know that if f is an irreducible over $\mathbb{F}_q$ and $\deg f$ is odd, then f is also irreducible over $\mathbb{F}_{q^2}$, but if $\deg f$ is even, there are two irreducible factors $r(T), s(T)$ in $\mathbb{F}_{q^2}[T]$, both of degree $(\deg f)/2$.

Now assume $R_{\sigma,t}$ is defined over $\mathbb{F}_q$ and set the sequence $f_0 = f$ and $f_i = f_{i-1}^{R_{\sigma,t}}$ for $i \geq 1$. If $\deg f$ is even, define the sequences r_i and s_i similarly, with the initial polynomial r and s, respectively. Notice that $g_i = r_i.s_i$ for any $i \geqslant 0$.

Theorem 3.19. *[35, Theorem 4.1] Let $\sigma \in GL_2(\mathbb{F}_{q^2})$ and $t \geq 2$ be such that $R_{\sigma,t}$ is defined over $\mathbb{F}_q$. Assume that each of prime factors of t is a divisor of $q^2 - 1$. Let $f(T) \in \mathbb{F}_q[T]$ be an irreducible polynomial of degree n such that $f(\sigma.\infty) \neq 0$. Consider the sequence defined as above f_i and r_i if $\deg f$ is even. If $\deg f$ is odd (resp. even), assume that for all prime factors ℓ of t , $\eta(f;\sigma)$ (resp. $\eta(r;\sigma)$) is not an ℓ-th power in $\mathbb{F}_{q^2}$. Then, if $\deg f$ is odd or if $4 \mid \deg f.t$, we have that a nonzero multiple of $f_i(x)$ is an irreducible polynomial in $\mathbb{F}_q[T]$ for all $i \geqslant 0$. If $\deg f$ is even, a nonzero multiple of r_i is an irreducible polynomial in $\mathbb{F}_{q^2}[T]$ for all $i \geqslant 0$.*

3.2.3.1. McNay's Transformation. The well-known transformation by McNay's is an example of this situation. It is defined as follows:

For a non-square element $c \in \mathbb{F}_q$ satisfying $c = \delta^2,\ \delta \in \mathbb{F}_{q^2}$, and a polynomial $f(T) \in \mathbb{F}_q[T]$,

$$f_c(T) = (2T)^{\deg f} f\Big(\frac{T^2 + c}{2T}\Big).$$

Then we can easily see that, for $\sigma = \begin{pmatrix} \delta & \delta \\ -1 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_{q^2})$, $f_c(T) = (2\delta)^{\deg f} f^{R_\sigma,2}(T)$. We assume that $f(\sigma.\infty) = f(-\delta) \neq 0$ and observe that $\eta(f, \sigma) = f(\delta)f(-\delta)^{-1}$ is a non-square element in $\mathbb{F}_{q^2}$. By Theorem 3.19 we have the following result:

Theorem 3.20. *Let $f(T)$ be an irreducible polynomial in $\mathbb{F}_q[T]$ and $c \in \mathbb{F}_q$ a non-square element with $c = \delta^2,\ \delta \in \mathbb{F}_{q^2}$. Assume $f(\delta)f(-\delta)$ is not a square in $\mathbb{F}_{q^2}$ and if $\deg f$ is even, let $r(T) \in \mathbb{F}_{q^2}[T]$ be an irreducible factor of $f(T)$ assuming $r(\delta)r(-\delta)$ is not a square in $\mathbb{F}_{q^2}$. Define $f_0(T) = f(T)$ and $f_k(T) = (f_{k-1})_c(T)$, $k \geqslant 1$. Then $(f_k(T))_{k\geqslant 0}$ is a sequence of irreducible polynomials over $\mathbb{F}_q$.*

McNay showed in [33] that if we assume $q \equiv 3 \mod 4$ and $c, 1-c$ are non-square elements in $\mathbb{F}_q$ and $f_0(T) = T^2+2T+c$, we obtain an irreducible polynomial sequence $f_{k+1}(T) = (f_k)_c(T)$ for all $k \geqslant 0$. It is easily shown by Theorem 3.20 as follows:

Since $1 - c$ is a non-square in $\mathbb{F}_q$ we have the given polynomial $f_0(T)$ is irreducible over $\mathbb{F}_q$. We also see that $f_0(T)$ factors over $\mathbb{F}_{q^2}$, because $\deg f$ is even which is given as $f_0(T) = (T + 1 - \sqrt{1-c})(T + 1 + \sqrt{1-c})$. Without loss of generality, assume $r(T) := T + 1 - \sqrt{1-c}$ and consider the element $r(\delta)r(-\delta) = 2(1 - c - \sqrt{1-c})$. Suppose for the contrary that this element is a square in $\mathbb{F}_{q^2}$. That is, there are $a,\ b \in \mathbb{F}_q$ such that $2(1-c-\sqrt{1-c}) = (a(1-c)+b\sqrt{1-c})^2$, since $\{1-c, \sqrt{1-c}\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. We obtain $a^2(1-c)+b^2 = 2,\ 2ab(1-c) = -2$, then we have the equality $(1-c)^3a^4 - 2(1-c)^2a^2 + 1 = 0$ which is polynomial in a^2 over $\mathbb{F}_q$. This means

that its discriminant, $-4c(1-c)^3$, must be a square element in $\mathbb{F}_q$ since $a^2 \in \mathbb{F}_q$, which is satisfied if and only if -1 is a square in $\mathbb{F}_q$, i.e., $q \equiv 3 \mod 4$.

Afterwards Chapman showed in [29] that this construction gives a completely normal polynomials sequence as well.

Theorem 3.21. *[29, Theorem 2] Let $q \equiv 3 \mod 4$ be a prime power and $f_0(T) = T^2+bT+c$ be an irreducible polynomial over $\mathbb{F}_q$ with the nonzero element b and a non-square element c in $\mathbb{F}_q$. Define the sequence $f_{k+1}(T) = (f_k)_c(T), k \geqslant 0$, with α_k is a root of the polynomial f_k for each $k \geqslant 0$. Then α_k is a completely normal element of $\mathbb{F}_{q^{2^k}}$ over $\mathbb{F}_q$.*

Using this approach, such a transformation can be generalized as a degree t power map for any $t \mid q^2-1$ relating to Singer subgroups. In fact, this corresponds to starting with a degree 2 place in the initial extension of the corresponding rational function fields. Nevertheless, this part of the work is in progress, we will give some details in the following section.

3.2.3.2. Starting with a Degree 2 Places and its Relation with Singer Subgroups. Let $D > 1$ and consider the extension $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ with $t = x^D$. If $D \mid q-1$, i.e., $\mathbb{F}_q$ contains the D-th roots of unity, this is a Galois extension of degree D. Otherwise it can be turned into a Galois extension after extending the field of constants. The only ramified places are $(t=0)$ and $(t=\infty)$. Both are totally ramified with ramification index D and above them are the rational places $(x=0)$ and $(x=\infty)$. Now let $p(T) \in \mathbb{F}_q[T]$ be an irreducible polynomial of degree 2 and denote its roots in $\mathbb{F}_{q^2}$ by θ and $\overline{\theta} = \theta^q$. We want to find $\sigma \in PGL_2(\mathbb{F}_{q^2})$ such that $\sigma.0 = \theta$ and $\sigma.\infty = \overline{\theta}$.

It can be verified that $\sigma = \begin{pmatrix} 1 & -\theta \\ 1 & -\overline{\theta} \end{pmatrix}$ has the desired property and the corresponding fractional linear transformation is given by $\frac{T-\theta}{T-\overline{\theta}}$. We have $\sigma^{-1} = \begin{pmatrix} \overline{\theta} & -\theta \\ 1 & -1 \end{pmatrix}$

in $PGL_2(\mathbb{F}_{q^2})$. We use σ to obtain an extension with ramified places given by θ and $\overline{\theta}$. Namely, let

$$x' = \sigma(x) = \frac{\overline{\theta} \cdot x - \theta}{\theta \cdot x - 1} \quad \text{and} \quad t' = \sigma(t) = \frac{\overline{\theta} \cdot t - \theta}{\theta \cdot t - 1}.$$

Clearly $\mathbb{F}_q(x) = \mathbb{F}_q(x')$ and $\mathbb{F}_q(t) = \mathbb{F}_q(t')$. In the extension $\mathbb{F}_q(x') = \mathbb{F}_q(t')$ the ramified places are $(t' = 0)$ and $(t' = \infty)$, with $(x' = 0)$ and $(x' = \infty)$ lying above these. The extension is given by

$$t' = \sigma(t) = \sigma(x^D) = \sigma\big((\sigma^{-1}(x'))^D\big) = \frac{\overline{\theta}(x' - \theta)^D - \theta(x' - \overline{\theta})^D}{(x' - \theta)^D - (x' - \overline{\theta})^D}.$$

Let us denote this map by $\psi_{D,p(T)}$, that defines an extension of degree D ramified at the place defined by $p(T)$.

More specifically, take as $p(T) = T^2 - AT + B$ such that $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\theta) = A$ and $\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\theta) = B$.

As an example of this construction, for our approach we consider the case $D = 2$. It can be verified that $\psi_{D,p(T)} = \frac{x^2 - B}{2x - A}$. If c is a non-square in $\mathbb{F}_q$, then $p(T)$ can be chosen as $p(T) = T^2 - c$ and $\psi_{2,T^2-c} = \frac{x^2+x}{2x}$. This corresponds to the transformation given by McNay.

In these examples $\psi_{D,p(T)}$ is defined over $\mathbb{F}_q$. This is true in general. We have $\psi(x) = \frac{\overline{\theta}(x-\theta)^D - \theta(x-\overline{\theta})^D}{(x-\theta)^D - (x-\overline{\theta})^D}$ If we use binomial theorem, we see that all terms have the factor $\theta - \overline{\theta}$. After cancelling, all other terms can be written in terms of the norm and trace of θ^i.

The case $D = q + 1$ is more interesting. It corresponds to the norm map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ and it is easily seen that $\psi(x)$ has a pole at all $\alpha \in \mathbb{F}_q$. Also, $\psi(\infty) = \infty$. So all rational places lie over the pole ∞ in the extension defined by ψ.

Such a construction brings out some questions: When is the extension $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ with $t = \psi_{D,p(t)}(x)$ cyclic? What is ramified in this extension? What happens for $D > q + 1$? Is it true that $\psi_{D_1,p(T)} \circ \psi_{D_2,p(T)} = \psi_{D_1 \cdot D_2,p(T)}$? What

can be said about the normality? Besides ψ is closely related to the power map and normality of twists of the power map by Möbius transformations are understood in certain cases. Moreover, doing iterations of the transformation ψ will also raise new questions.

3.2.3.3. Other Examples from Kyuregyan's Results. It is possible to find some other constructions in the literature as an example of such a situation. In [30], Kyuregyan stated the following result:

First, define the polynomial

$$g_f(T) = (-1)^n \sum_{j=0}^{n} \sum_{u=0}^{2j} (-1)^u a_u a_{2j-u} T^j,$$

for $f(T) = \sum_{u=0}^{n} a_u T^u \in \mathbb{F}_q[T]$.

Proposition 3.22. *[41, Theorem 8] Let $f(T) = \sum_{u=0}^{n} a_u T^u \in \mathbb{F}_q[T]$ be an irreducible polynomial of degree $n > 1$, with at least one coefficient $a_{2i+1} \neq 0$, $(0 \leqslant i \leqslant \lfloor \frac{n}{2} \rfloor)$ and order e. Then the polynomial $g_f(T)$ of degree n is irreducible over $\mathbb{F}_q$ and has the order $\frac{e}{\gcd(e,2)}$. Moreover, $g_f(T)$ is the minimal polynomial of the element α^2 if α is a root of $f(T)$.*

Theorem 3.23. *[30, Theorem 2] Let $f_0(T) = \sum_{u=0}^{n} a_u T^u \in \mathbb{F}_q[T]$ be an irreducible polynomial of degree $n > 1$, with at least one coefficient $a_{2i+1} \neq 0$, $(0 \leqslant i \leqslant \lfloor \frac{n}{2} \rfloor)$. Let $aT^2 + 2hT + ahd^{-1}$ and $dT^2 + 2aT + h$ be relatively prime, where $a,\ d,\ h \in \mathbb{F}_q^*$ and $a^2 \neq hd$. Suppose that the element $(hd^{-1})^n$ is a non-zero square in $\mathbb{F}_q$ and the element $(hd - a^2)^n g_{f_0}(\frac{h}{d})$ is non-square in $\mathbb{F}_q$. Define*

$$f_k(T) = (dT^2 + 2aT + h)^{\deg f_{k-1}} f_{k-1}\Big(\frac{aT^2 + 2hT + ahd^{-1}}{dT^2 + 2aT + h}\Big), k \geqslant 1. \qquad (3.1)$$

Then $f_k(T)$ is an irreducible polynomial over $\mathbb{F}_q$ for every $k \geqslant 0$.

Let $\sigma = \begin{pmatrix} -\sqrt{\frac{h}{d}} & -\left(\frac{a+\sqrt{hd}}{a-\sqrt{hd}}\right)\sqrt{\frac{h}{d}} \\ -1 & \left(\frac{a+\sqrt{hd}}{a-\sqrt{hd}}\right) \end{pmatrix}$ where $a, d, h \in \mathbb{F}_q^*$ and $a^2 \neq hd$. Notice that, $\sigma \in GL_2(\mathbb{F}_{q^2})$ if and only if $\frac{h}{d}$ is a non-square in $\mathbb{F}_q$, otherwise $\sigma \in GL_2(\mathbb{F}_q)$. We observe that, for any polynomial $f(T) \in \mathbb{F}_q[T]$ of degree n with $f\left(\sqrt{\frac{h}{d}}\right) \neq 0$,

$$f^{R_{\sigma,2}}(T) = P_{\sigma^{-1}} \circ S_2 \circ P_\sigma(f)(T) = (dT^2 + 2aT + h)^n f\Big(\frac{aT^2 + 2hT + ahd^{-1}}{dT^2 + 2aT + h}\Big).$$

Then $\eta(f, \sigma) = \left(\frac{a+\sqrt{hd}}{a-\sqrt{hd}}\right)^n f\left(-\sqrt{\frac{h}{d}}\right) f\left(\sqrt{\frac{h}{d}}\right)^{-1}$. If $\frac{h}{d}$ is a square in $\mathbb{F}_q$ (so $\sigma \in GL_2(\mathbb{F}_q)$) and $\eta(f, \sigma)$ is a non-square in $\mathbb{F}_q$, then by Theorem 3.12 $(f_k(T))_{k \geqslant 0}$ forms an infinite sequence of irreducible polynomials. If $\frac{h}{d}$ is not a square in $\mathbb{F}_q$ then $\sigma \in GL_2(\mathbb{F}_{q^2})$ and consider the sequence f_k as well as r_k which is a factor of f_k over $\mathbb{F}_{q^2}$ when n is even. If n is odd (respectively, even) and $\eta(f, \sigma)$ (respectively $\eta(r, \sigma)$) is not a square in $\mathbb{F}_{q^2}$, by Theorem 3.19 $f_k(T)$ is irreducible polynomials in $\mathbb{F}_q[T], \forall k \geqslant 0$ (respectively, a nonzero multiple of r_k is irreducible polynomials in $\mathbb{F}_{q^2}[T], \forall k \geqslant 0$).

The assumptions in Theorem 3.23 are satisfied from the assumptions in Theorem 3.12 and Theorem 3.19.

First, notice that the fact that $f_0(T) = \sum_{u=0}^{n} a_u T^u \in \mathbb{F}_q[T]$ is an irreducible polynomial of degree $n > 1$, with at least one coefficient $a_{2i+1} \neq 0, (0 \leqslant i \leqslant \lfloor \frac{n}{2} \rfloor)$ implies that the polynomial $g_{f_0(T)}$ is of degree n irreducible over $\mathbb{F}_q$ and it is the minimal polynomial of the element α^2 if α is a root of $f_0(T)$ by Proposition 3.22.

Now let n be even. Then $(\frac{h}{d})^n$ is already a square in $\mathbb{F}_q$ whether $\frac{h}{d}$ is a square in $\mathbb{F}_q$ or not. If $\frac{h}{d}$ is a square in $\mathbb{F}_q$, then $\sigma \in GL_2(\mathbb{F}_q)$ as we mentioned above.

Observe that $\eta(f_0, \sigma) = \left(\frac{a+\sqrt{hd}}{a-\sqrt{hd}}\right)^n f_0\left(-\sqrt{\frac{h}{d}}\right) f_0\left(\sqrt{\frac{h}{d}}\right)^{-1}$ is a non-square in $\mathbb{F}_q$ if and only if $\left((a - \sqrt{hd})^n f_0\left(\sqrt{\frac{h}{d}}\right)\right)^2 \eta(f_0, \sigma) = (a^2 - hd) f_0\left(-\sqrt{\frac{h}{d}}\right) f_0\left(\sqrt{\frac{h}{d}}\right)$ is a non-square in $\mathbb{F}_q$. Let α be a root of $f_0(x)$ in $\mathbb{F}_{q^n}$. Then

$$
\begin{aligned}
f_0(T) = \prod_{i=0}^{n-1}(T-\alpha^{q^i}) \;\Rightarrow\; & f_0\Big(-\sqrt{\frac{h}{d}}\Big) f_0\Big(\sqrt{\frac{h}{d}}\Big) \\
= \; & \prod_{i=0}^{n-1}\Big(-\sqrt{\frac{h}{d}} - \alpha^{q^i}\Big) \prod_{i=0}^{n-1}\Big(\sqrt{\frac{h}{d}} - \alpha^{q^i}\Big) \\
= \; & (-1)^n \prod_{i=0}^{n-1}\Big(-\frac{h}{d} - (\alpha^2)^{q^i}\Big) \\
= \; & (-1)^n g_{f_0}\Big(\frac{h}{d}\Big).
\end{aligned}
$$

We see that $\eta(f_0, \sigma)$ is a non-square in $\mathbb{F}_q$ if and only if

$$
(a^2 - hd) f_0\Big(-\sqrt{\frac{h}{d}}\Big) f_0\Big(\sqrt{\frac{h}{d}}\Big) = (hd - a^2) g_{f_0}\Big(\frac{h}{d}\Big)
$$

is a non-square in $\mathbb{F}_q$. That is, all assumptions in Theorem 3.23 are satisfied by the assumptions of Theorem 3.12 for this case. Let n be even and $\frac{h}{d}$ is a non-square in $\mathbb{F}_q$. Then $\sigma \in GL_2(\mathbb{F}_{q^2})$. Since n is even, $f_0(T)$ has exactly two irreducible factors $r(T), s(T)$ in $\mathbb{F}_{q^2}[x]$ both of degree $\frac{n}{2}$. We have

$$
\eta(r, \sigma) = \Big(\frac{a + \sqrt{hd}}{a - \sqrt{hd}}\Big)^n r\Big(-\sqrt{\frac{h}{d}}\Big) r\Big(\sqrt{\frac{h}{d}}\Big)^{-1}
$$

is a non-square in $\mathbb{F}_{q^2}$ if and only if

$$
\Big(\Big(a - \sqrt{hd}\Big)^n r\Big(\sqrt{\frac{h}{d}}\Big)\Big)^2 \eta(r, \sigma) = (a^2 - hd) r\Big(-\sqrt{\frac{h}{d}}\Big) r\Big(\sqrt{\frac{h}{d}}\Big)
$$

is a non-square in $\mathbb{F}_{q^2}$. Notice that $(a^2 - hd)^n \in \mathbb{F}_q$, that is, it is already a square in $\mathbb{F}_{q^2}$. Thus, $\eta(r, \sigma)$ is a non-square in $\mathbb{F}_{q^2}$ if and only if $r\Big(-\sqrt{\frac{h}{d}}\Big) r\Big(\sqrt{\frac{h}{d}}\Big)$ is a non-square in $\mathbb{F}_{q^2}$. For the latter we have

$$
\Big(r\Big(-\sqrt{\frac{h}{d}}\Big) r\Big(\sqrt{\frac{h}{d}}\Big)\Big)^{\frac{q^2-1}{2}} = -1 \Leftrightarrow \Big(\Big(r\Big(-\sqrt{\frac{h}{d}}\Big) r\Big(\sqrt{\frac{h}{d}}\Big)\Big)^{q+1}\Big)^{\frac{q-1}{2}} = -1
$$

which means that $r\Big(-\sqrt{\frac{h}{d}}\Big) r\Big(\sqrt{\frac{h}{d}}\Big)$ is a non-square in $\mathbb{F}_{q^2}$ if and only if $\Big(r\Big(-\sqrt{\frac{h}{d}}\Big) r\Big(\sqrt{\frac{h}{d}}\Big)\Big)^{q+1}$ is a non-square in $\mathbb{F}_q$. Observe that

$$\begin{aligned}\Big(r\Big(-\sqrt{\frac{h}{d}}\Big)r\Big(\sqrt{\frac{h}{d}}\Big)\Big)^{q+1} &= r\Big(-\sqrt{\frac{h}{d}}\Big)\Big(r\Big(-\sqrt{\frac{h}{d}}\Big)\Big)^{q} r\Big(\sqrt{\frac{h}{d}}\Big)\Big(r\Big(\sqrt{\frac{h}{d}}\Big)\Big)^{q} \\ &= (-1)^{\frac{n}{2}} g_r\Big(\frac{h}{d}\Big)\Big((-1)^{\frac{n}{2}} g_r\Big(\frac{h}{d}\Big)\Big)^{q} \\ &= (-1)^{n} g_r\Big(\frac{h}{d}\Big) g_s\Big(\frac{h}{d}\Big) \\ &= (-1)^{n} g_{f_0}\Big(\frac{h}{d}\Big),\end{aligned}$$

where $r(A) = (s(A))^q, \forall A \in \mathbb{F}_q$. Thus, in this case we can say that the sequence $r_k(T)$ consists polynomials where their nonzero multiples are irreducible over $\mathbb{F}_{q^2}$, $\forall k \geqslant 0$ by 3.19 which gives something more than Kyuregyan. Since in our case $t = 2,\ 4|nt$ when n is even, then by the assumptions of 3.19 we already obtain the nonzero multiples of the polynomials in the sequence $f_k(x), \forall k \geqslant 0$ are irreducible over $\mathbb{F}_q$.

Lastly, if n is odd, then $\left(\frac{h}{d}\right)^n$ is a square in $\mathbb{F}_q$ if and only if $\frac{h}{d}$ is a square in $\mathbb{F}_q$, that is $\sigma \in PGL_2(\mathbb{F}_q)$, which is the same as the first case.

Therefore, Theorem 3.12 and 3.19 just imply then Theorem 3.23 which shows that the transformation in (3.1) is just the power map, $T \mapsto T^2$, with a change of coordinates.

Besides, using the result of Aravena in Theorem 3.15, we can say that the polynomials in (3.1) are also completely normal for certain q's with an initial polynomials of degree 1 . Since n is odd in this situation, we have that $\sigma \in PGL_2(\mathbb{F}_q)$, then by part (ii) of the Theorem 3.15, the polynomials are completely normal over $\mathbb{F}_q$ for q's which in -1 is a square in $\mathbb{F}_q$, i.e. , for $q \equiv 1 \mod 4$.

In the paper [30], there are also some other results which can be obtained with this method as well.

Theorem 3.24. *[30, Theorem 3] Let* $f_0(T) = \sum_{u=0}^{n} a_u T^u \in \mathbb{F}_q[T]$ *be an irreducible polynomial of degree* $n > 1$, *with at least one coefficient* $a_{2i+1} \neq 0$, $(0 \leqslant i \leqslant \lfloor \frac{n}{2} \rfloor)$. $a,\ d,\ h \in \mathbb{F}_q^*$ *and* $a^2 \neq hd$. *Suppose* $a,\ c \in \mathbb{F}_q^*$ *and the element* $(ac)^n$ *is a square in* $\mathbb{F}_q$ *and the element* $(-1)^n g_{f_0}(\frac{c}{a})$ *is non-square in* $\mathbb{F}_q$. *Define* $f_k(T) = (2aT)^{\deg f_{k-1}} f_{k-1}\left(\frac{aT^2+c}{2aT}\right), k \geqslant 1$. *Then* $f_k(T)$ *is an irreducible polynomial over* $\mathbb{F}_q$ *for every* $k \geqslant 0$.

For $\sigma = \begin{pmatrix} \sqrt{\frac{c}{a}} & \sqrt{\frac{c}{a}} \\ 1 & -1 \end{pmatrix}$, we do a similar consideration like in the above result and then obtain a completely normal polynomial sequence for $q \equiv 1 \mod 4$ which again says more than Kyuregyan's result. Notice that this is a kind of generalization of McNay's result.

Similarly, we consider another result from the paper [30] as follows:

Theorem 3.25. *[30, Theorem 5] Let* $f_0(T) = \sum_{u=0}^{n} a_u T^u \in \mathbb{F}_q[T]$ *be an irreducible polynomial of degree* $n > 1$, *with at least one coefficient* $a_{2i+1} \neq 0$, $(0 \leqslant i \leqslant \lfloor \frac{n}{2} \rfloor)$. $a,\ d,\ h \in \mathbb{F}_q^*$ *and* $a^2 \neq hd$. *Suppose* $h,\ d \in \mathbb{F}_q^*$ *and the element* $(hd)^n$ *is a square in* $\mathbb{F}_q$ *and the element* $g_{f_0}(\frac{h}{d})$ *is non-square in* $\mathbb{F}_q$. *Define* $f_k(T) = (dT^2 + h)^{\deg f_{k-1}} f_{k-1}\left(\frac{2hT}{dT^2+h}\right), k \geqslant 1$. *Then* $f_k(T)$ *is an irreducible polynomial over* $\mathbb{F}_q$ *for every* $k \geqslant 0$.

For $\sigma = \begin{pmatrix} -1 & -1 \\ \sqrt{\frac{d}{h}} & -\sqrt{\frac{d}{h}} \end{pmatrix}$, again doing a similar consideration as above we obtain a completely normal polynomials sequence for $q \equiv 1 \mod 4$ as well.

3.3. Transformations of the Form, $c(T - A)^2$

Now we start to discuss the second case of our classification which is given by the transformation $c(T-A)^2, c, A \in \mathbb{F}_q^*$ for $A = 1$ to make the calculations easier.

First, we just examine two iterations like before to understand the behaviour of any place P_f associated to the irreducible polynomial of $f(T) \in \mathbb{F}_q[T]$ of degree n. Set the extension as $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(t) \subseteq \mathbb{F}_q(x)$, with $t = c(x-1)^2$ and $w = c(t-1)^2$, $c \in \mathbb{F}_q^*$. Recall that the ramified places of $\mathbb{F}_q(w)$ in the extensions $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ is $(w = 0)$ and $(w = \infty)$ with $(t = 1)$ and $(t = \infty)$ lying above them respectively in $\mathbb{F}_q(t)$.

$$\begin{array}{rccc} \mathbb{F}_q(x) & * & \infty \\ t = c(x-1)^2 \,\Big| & \Big| & \Big| \\ \mathbb{F}_q(t) & 1 & \infty \\ w = c(t-1)^2 \,\Big| & \Big| & \Big| \\ \mathbb{F}_q(w) & 0 & \infty \end{array}$$

Let $\mathbb{F}_q(w_0) \subseteq \mathbb{F}_q(t_0) \subseteq \mathbb{F}_q(x_0)$, with $t_0 = c_0(x_0-1)^2$ and $w_0 = c_0(t_0-1)^2$, for an element $c_0 \in \mathbb{F}_q^*$. be another tower in this case. Assume that there is a Möbius transformation which is given by an element $\sigma = \begin{pmatrix} a & b \\ c' & d \end{pmatrix} \in GL_2(\mathbb{F}_q)$ between these two towers such that $\sigma(w_0) = w,\ \sigma(t_0) = t$ and $\sigma(x_0) = x$ fixing the points $0,\ 1$ and ∞. It will be of the form $\sigma = k \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ with $k \neq 0$. These equality is satisfied if and only if $c = c_0$ which implies that the towers are the same.

This means that, under the action of $PGL_2(\mathbb{F}_q)$ on the projective line $\mathbb{P}^1(\mathbb{F}_q)$, such extensions are equivalent if and only if the scalars of the transformations are the same, that is, they are the same extensions. This fact implies that there are $q-1$ many different extensions, which vary according to the scalar $c \in \mathbb{F}_q^*$ each having the ramified places ∞ of $\mathbb{F}_q(w)$ which stay ramified in the all functions fields of the tower and the ramified place 0 of $\mathbb{F}_q(w)$ which lies under the place 1 of the function field $\mathbb{F}_q(t)$. Let us consider such extensions Galois theoretically. Since $w = c(c(x-1)^2-1)^2$, the irreducible polynomial of x over $\mathbb{F}_q(w)$ is

$$\begin{aligned} Irr(x,\mathbb{F}_q(w))(T) &= T^4-4T^3+\Big(6-\frac{2}{c}\Big)T^2+\Big(-4+\frac{4}{c}\Big)T+\Big(\frac{1}{c}-1\Big)^2-\frac{w}{c^3} \\ &= (T-x)(T+(x-2))\Big(T^2-2T+\Big(x^2-2x+2-\frac{2}{c}\Big)\Big). \end{aligned}$$

Galois theory of the polynomials of degree 4 is can be understood with the help of the cubic resolvent of quartic polynomials, see Kaplansky [42] and Kappe and Waren [43] for details. The cubic resolvent of this polynomial is obtained as follows:

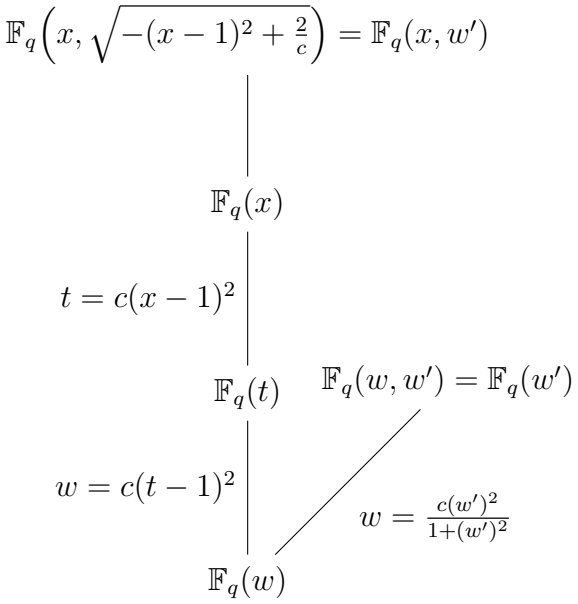
- T^3 if the characteristic of $\mathbb{F}_q$ is even,
- $(T+2(\frac{1}{c}-1))(T^2-4T-4(\frac{1}{c^2}-1-\frac{w}{c^3}))$ if the characteristic of $\mathbb{F}_q$ is odd.

In the first situation we have that the extension is Galois with Galois group given by the Klein-4 group, which means that there is not an inert place of $\mathbb{F}_q(w)$ in the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ as was mentioned at the beginning. Thus we are not interested in this case.

For the latter situation, let $g(T)=T^2-4T-4(\frac{1}{c^2}-1-\frac{w}{c^3})$. If $g(T)$ has a root in $\mathbb{F}_q(w)$, the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ is Galois with Galois group again given by Klein-4 group. If it has no root in $\mathbb{F}_q(w)$, the splitting field of the polynomial $Irr(x,\mathbb{F}_q(w))(T)$ contains the roots of $g(T)$. In this case, after adjoining the roots of $g(T)$ to the field $\mathbb{F}_q(w)$, if $f(T)$ is reducible in this field the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ is Galois with Galois group C_4. Otherwise, the extension is not Galois and its Galois closure has Galois group D_8.

To consider the roots of $g(T)$, let us compute its discriminant, $\delta=\frac{16}{c^2}(1-\frac{w}{c})$. Since the characteristic is odd, δ is not a square in $\mathbb{F}_q(w)$ since $\Delta:=1-\frac{w}{c}$ is not a square in $\mathbb{F}_q(w)$. Using the relation $w=c(c(x-1)^2-1)^2$, we obtain that $\delta=16(x-1)^2(-(x-1)^2+\frac{2}{c})$. Adjoining the roots of the polynomial $g(T)$ to the field $\mathbb{F}_q(w)$, we obtain the field $\mathbb{F}_q\Big(w,\sqrt{1-\frac{w}{c}}\Big)=\mathbb{F}_q\Big(w,\sqrt{-(x-1)^2+\frac{2}{c}}\Big)$ and the polynomial $Irr(x,\mathbb{F}_q(w))(T)$ is still not reducible in this field since x is not

in $\mathbb{F}_q\Big(w, \sqrt{-(x-1)^2+\frac{2}{c}}\Big)$. This means that the Galois group of the polynomial $Irr(x, \mathbb{F}_q(w))(T)$ is D_8 with Galois closure $\mathbb{F}_q\Big(x, \sqrt{-(x-1)^2+\frac{2}{c}}\Big)$.



3.3.1. The Special Case for $c = 2$

First we will try to use Corollary 3.7 to obtain an inert place P of $\mathbb{F}_q(w)$ in the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$, which is already assumed inert in $\mathbb{F}_q(t)/\mathbb{F}_q(w)$. Then we will continue to do this iteratively whenever it is possible. For doing this, let us consider the element w' which is a root of the irreducible polynomial $T^2 - \frac{w}{w-c}$ over $\mathbb{F}_q(w)$ and generates the fixed field $\mathbb{F}_q(w, w') = \mathbb{F}_q(w')$ of the cyclic subgroup of D_8 of order 4. Since this subgroup is a normal subgroup of D_8, it is clear that, the function field

$$\mathbb{F}_q\Big(x, \sqrt{-(x-1)^2+\frac{2}{c}}\Big) = \mathbb{F}_q\Big(x, \sqrt{\frac{c-w}{c}}\Big) = \mathbb{F}_q\Big(x, \sqrt{\frac{w}{w-c}}\Big) = \mathbb{F}_q(x, w')$$

is a cyclic Galois extension of the field $\mathbb{F}_q(w, w')$. Thus applying the Corollary 3.7, for a place P of $\mathbb{F}_q(w)$ which is inert in the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ and splits in the extension $\mathbb{F}_q(w, w')/\mathbb{F}_q(w)$, we say that P is inert in $\mathbb{F}_q(x)/\mathbb{F}_q(w)$. Lets say Q is a place of $\mathbb{F}_q(t)$ lying over P. To continue iteratively, we need that the place Q splits in the extension $\mathbb{F}_q(t, t')$ where t' is a root of the polynomial $T^2 - \frac{t}{t-c}$ over $\mathbb{F}_q(t)$.

In general $\mathbb{F}_q(t,t')$ will be a different function field from $\mathbb{F}_q(t,w')$. Let us determine when $\mathbb{F}_q(t,t') = \mathbb{F}_q(t,w')$ is satisfied.

For doing this we use the irreducible polynomial of w' over $\mathbb{F}_q(w)$ and the relations $w = c(t-1)^2$, $(t'^2) = \frac{t}{c-t}$. Then we obtain that

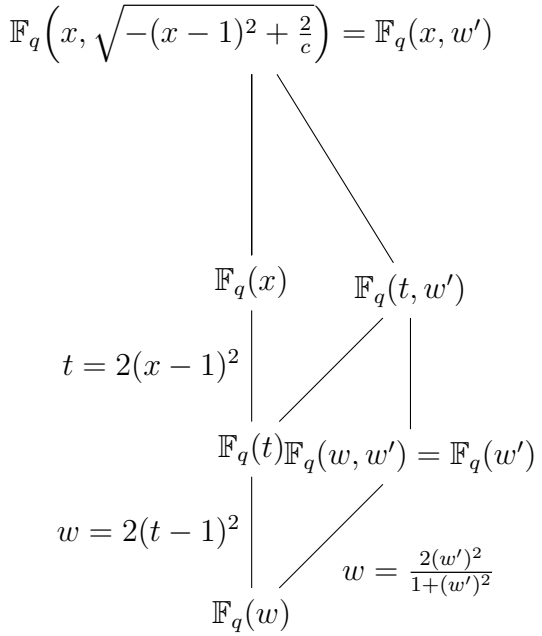
$$T^2 - \frac{w}{c-w} = T^2 - \frac{((c-1)(t')^2-1)^2}{((t')^2+1)^2-((c-1)(t')^2-1)^2}.$$

If this polynomial is reducible over $\mathbb{F}_q(t')$ we say that $w' \in \mathbb{F}_q(t,t') = \mathbb{F}_q(t')$, i.e., $\mathbb{F}_q(t,w') \subseteq \mathbb{F}_q(t,t')$. This is possible if the constant term is a square in $\mathbb{F}_q(t')$. Since the numerator is already a square in $\mathbb{F}_q(t')$ we should just consider the denominator. This element is a square in $\mathbb{F}_q(t')$ if and only if $c((2-c)t'^2+2)$ is a square in $\mathbb{F}_q(t')$. Since it is a polynomial in t' of degree 2, it would be a square if and only if its discriminant $8c^2(c-2)$ is equal to 0 which is satisfied for $c = 2$ or $c = 0$.The latter gives a contradiction. Thus $w' \in \mathbb{F}_q(t,t')$, i.e., $\mathbb{F}_q(t,w') \subseteq \mathbb{F}_q(t,t')$.

Now assuming $c = 2$, we will also show that $t' \in \mathbb{F}_q(t,w')$. Observe that

$$w = \frac{2w'}{1+w'^2} = 2(t-1)^2 \Rightarrow (w')^2 = \frac{(t-1)^2}{t(2-t)}.$$

Consider $(w' + \frac{w'}{t-1})^2 - \frac{t}{2-t}$ substituting previous relation, we obtain that it is equal to zero which means $w' + \frac{w'}{t-1}$ satisfies the irreducible polynomial of t' over $\mathbb{F}_q(t)$, i.e., $t' = w' + \frac{w'}{t-1}$ (or its conjugate which does not change anything). Thus $t' \in \mathbb{F}_q(t,w')$. We conclude that $\mathbb{F}_q(t') = \mathbb{F}_q(t,w')$ if and only if $c = 2$. With similar calculations we also obtain $\mathbb{F}_q(x') = \mathbb{F}_q(x,w')$ for $c = 2$.



This makes the case $c = 2$ special also in general: to have an element w' of degree 2 over $\mathbb{F}_q(x_0)$ such that the Galois closure of the extension $\mathbb{F}_q(x_{i+2})/\mathbb{F}_q(x_i)$ is given by $\mathbb{F}_q(x_{i+2}, w')$ for all i. Then we can shift the tower

$$\mathbb{F}_q(x_0) \subseteq \mathbb{F}_q(x_1) \subseteq \cdots \subseteq \mathbb{F}_q(x_n) \subseteq \cdots$$

to the new tower

$$\mathbb{F}_q(x_0, w') \subseteq \mathbb{F}_q(x_1, w') \subseteq \cdots \subseteq \mathbb{F}_q(x_n, w') \subseteq \cdots$$

with the property that $\mathbb{F}_q(x_{i+2}, w')/\mathbb{F}_q(x_i, w')$ has Galois group C_4.

Let us rephrase this result in terms of the coefficients of the corresponding irreducible polynomial, say f, to the place P of $\mathbb{F}_q(w)$ of degree n. Let α be any of its root in $\mathbb{F}_{q^n}$. By Theorem 3.1 $2(t-1)^2 - \alpha$ is irreducible over $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$ if and only if P is inert in the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$. Considering that, we obtain $2(t-1)^2 - \alpha = 2t^2 - 4t + (2-\alpha)$ is irreducible over $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$ if and only if its discriminant is a non-square in $\mathbb{F}_q(\alpha)$. Then the discriminant, 8α, is a non-square in $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$ if and only if 2α is a non-square in $\mathbb{F}_{q^n}$ if and only if $(2\alpha)^{\frac{q^n-1}{2}} = -1$ in $\mathbb{F}_{q^n}$. Observe that, $(2\alpha)^{\frac{q^n-1}{2}} = ((2\alpha)^{q^{n-1}+\cdots q+1})^{\frac{q-1}{2}}) = (2^n(-1)^n f(0))^{\frac{q-1}{2}}$. That is, 2α is a non-square in $\mathbb{F}_{q^n}$ if and only if $2^n(-1)^n f(0)$ is a non-square in $\mathbb{F}_q$.

Following a similar argumentation, we can also see that $2(w')^2-\alpha(1+(w')^2)$ splits in $\mathbb{F}_q(\alpha)$ if and only if the place P splits in the extension $\mathbb{F}_q(w')/\mathbb{F}_q(w)$. Then consider the following: $2(w')^2-\alpha(1+(w')^2)=(2-\alpha)(w')2-\alpha$ splits in $\mathbb{F}_q(\alpha)=\mathbb{F}_{q^n}$ if and only if $\frac{\alpha}{2-\alpha}$ is a square in $\mathbb{F}_q(\alpha)$ if and only if $(\frac{\alpha}{2-\alpha})^{\frac{q^n-1}{2}}=1$ in $\mathbb{F}_q(\alpha)$. Again observe that, $(\frac{\alpha}{2-\alpha})^{\frac{q^n-1}{2}}=(\frac{(-1)^nf(0)}{f(2)})^{\frac{q-1}{2}}$, since

$$(2-\alpha)^{q^{n-1}+\cdots q+1}=\prod_{i=0}^{n-1}(2-\alpha)^{q^i}=\prod_{i=0}^{n-1}(2-\alpha^{q^i})=f(2).$$

Thus $\frac{\alpha}{2-\alpha}$ is a square in $\mathbb{F}_q(\alpha)=\mathbb{F}_{q^n}$ if and only if $\frac{(-1)^nf(0)}{f(2)}$ is a square in $\mathbb{F}_q$. If we assume $(-1)^n2^nf(0)$ and $2^nf(2)$ are a non-square in $\mathbb{F}_q$ then $\frac{(-1)^nf(0)}{f(2)}=\frac{(-1)^n2^nf(0)}{2^nf(2)}$ is already a square in $\mathbb{F}_q$. Therefore we obtain the following result:

Theorem 3.26. *Let $f(T)\neq T$ be an irreducible polynomial of degree $n\geqslant 1$ over $\mathbb{F}_q$. Suppose the elements $(-1)^n2^nf(0)$ and $2^nf(2)$ are non-squares in $\mathbb{F}_q$. Define $G_0(T)=f(T)$, $G_k(T)=G_{k-1}(2(T-1)^2), k\geqslant 1$. Then for all $k\geqslant 1$, $G_k(T)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree $n2^k$.*

Proof. The condition $f(T)\neq T$ guarantees that we will not start with a ramified place. Following the above considerations we obtain the result by Corollary 3.7. □

3.3.1.1. An example of Kyuregyan. This special case corresponds to a result of Kyuregyan in [41] and it works even with weaker conditions, so we obtain a generalization of it. Let us recall this result of Kyuregyan from [41].

Theorem 3.27 ([41], Theorem 6)**.** *Let $r,\ h\in\mathbb{F}_q^*$. Let $f(T)\neq T$ be an irreducible polynomial of degree $n\geqslant 1$ over $\mathbb{F}_q$. Suppose the elements $f(0),\ h^n,\ (2r)^n$ are squares and $f(\frac{2h}{r})$ is non-square in $\mathbb{F}_q$. Define $f_0(T)=f(T)$,*

$$f_k(T)=\Big(\frac{(rT+2h)^2}{4h}\Big)^{\deg f_{k-1}}f_{k-1}\Big(\frac{(4h)^2T}{(rT+2h)^2}\Big), k\geqslant 1.$$

Then for all $k\geqslant 0$, $f_k(T)$ is an irreducible polynomial over $\mathbb{F}_q$.

We can obtain this easily by using our previous method, even with weaker conditions:

Let $\sigma = \begin{pmatrix} 2h & -4h \\ r & 0 \end{pmatrix} \in GL_2(\mathbb{F}_q)$ with $h, r \neq 0$ and consider its action on the extension that we define above as $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(t)$ and $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(w')$. Then we obtain after some calculations $\sigma(w) = \frac{(4h)^2\sigma(t)}{(r\sigma(t)+2h)^2}$. Notice that, it is just the transformation in the Theorem 3.27. Using the irreducible polynomial of w' over $\mathbb{F}_q(w)$ we obtain

$$Irr(\sigma(w'), \mathbb{F}_q(\sigma(w))) = T^2 - \frac{\sigma^{-1}(\sigma(w))}{2 - \sigma^{-1}(\sigma(w))} = T^2 - \frac{2h}{-r\sigma(w)}.$$

This splits modulo the place P_f over $\mathbb{F}_q(\sigma(w))$ if and only if $\frac{2h}{-r\alpha}$ is a square in $\mathbb{F}_{q^n}$ if and only if $\frac{(2h)^n}{r^n f(0)}$ is square in $\mathbb{F}_q$. This is equal to $\frac{(2^n)^2 h^n}{(2r)^n f(0)}$ which is already square in $\mathbb{F}_q$ with the conditions in Theorem 3.27.

In a similar way, we have

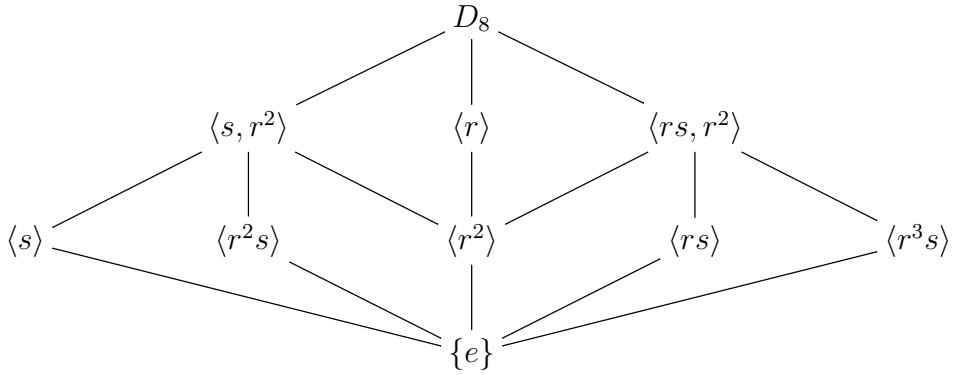
$$Irr(\sigma(t), \mathbb{F}_q(\sigma(w))) = T^2 - 2T + \frac{2 - \sigma^{-1}(\sigma(w))}{2} = T^2 - 2T + \frac{\sigma(w)}{-\sigma(w) + \frac{2h}{r}}.$$

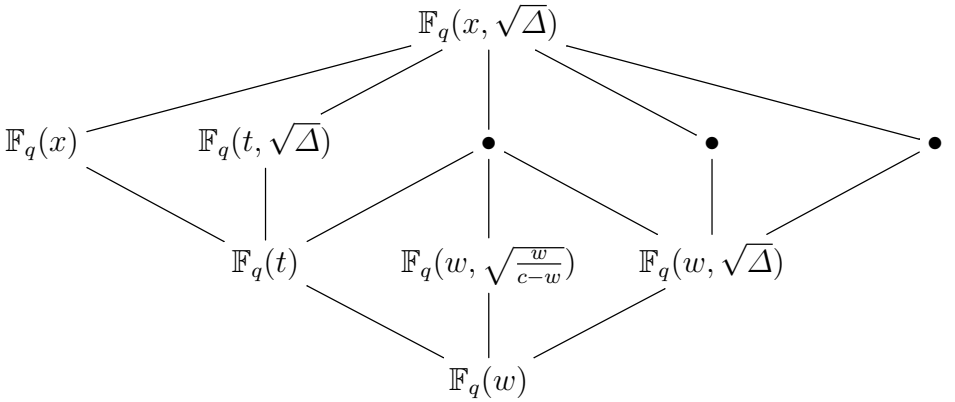
Its reduction modulo the place P_f is irreducible over $\mathbb{F}_q(\sigma(w))$ if and only if the discriminant $4\left(\frac{\frac{2h}{r}}{-\alpha+\frac{2h}{r}}\right)$ is a non-square in $\mathbb{F}_{q^n}$ if and only if $\left(\frac{\frac{2h}{r}}{-\alpha+\frac{2h}{r}}\right)$ is non-square in $\mathbb{F}_{q^n}$ if and only if $\left(\frac{(\frac{2h}{r})^n}{f(\frac{2h}{r})}\right)$ is non-square in $\mathbb{F}_q$ which is already satisfied with the conditions in Theorem 3.27. Then, by using Corollary 3.7 we can easily obtain the Kyuregyan's result in Theorem 3.27.

3.3.2. Other Cases for $c \neq 2$

Now we will also consider the case $c \neq 2$, in the transformation $c(T-1)^2$. In this situation, there does not exists a single element x_0' which lifts the tower to have the property that any two levels extension are cyclic of order 4. Nevertheless we can still determine some proper conditions for the initial place of the first function field of the tower to go on being inert in the above extensions. To do this we again start by considering just two steps as above. Recall $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(t) \subseteq \mathbb{F}_q(x)$, with $t = c(x-1)^2$ and $w = c(t-1)^2, c \in \mathbb{F}_q^*$ with the Galois closure $\mathbb{F}_q(x, \Delta)$ where $\Delta = \sqrt{1 - \frac{w}{c}} = \sqrt{-(x-1)^2 + \frac{2}{c}}$ with Galois group D_8. Let P be an unramified place of $\mathbb{F}_q(w)$ in the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ and inert in $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ and Q be

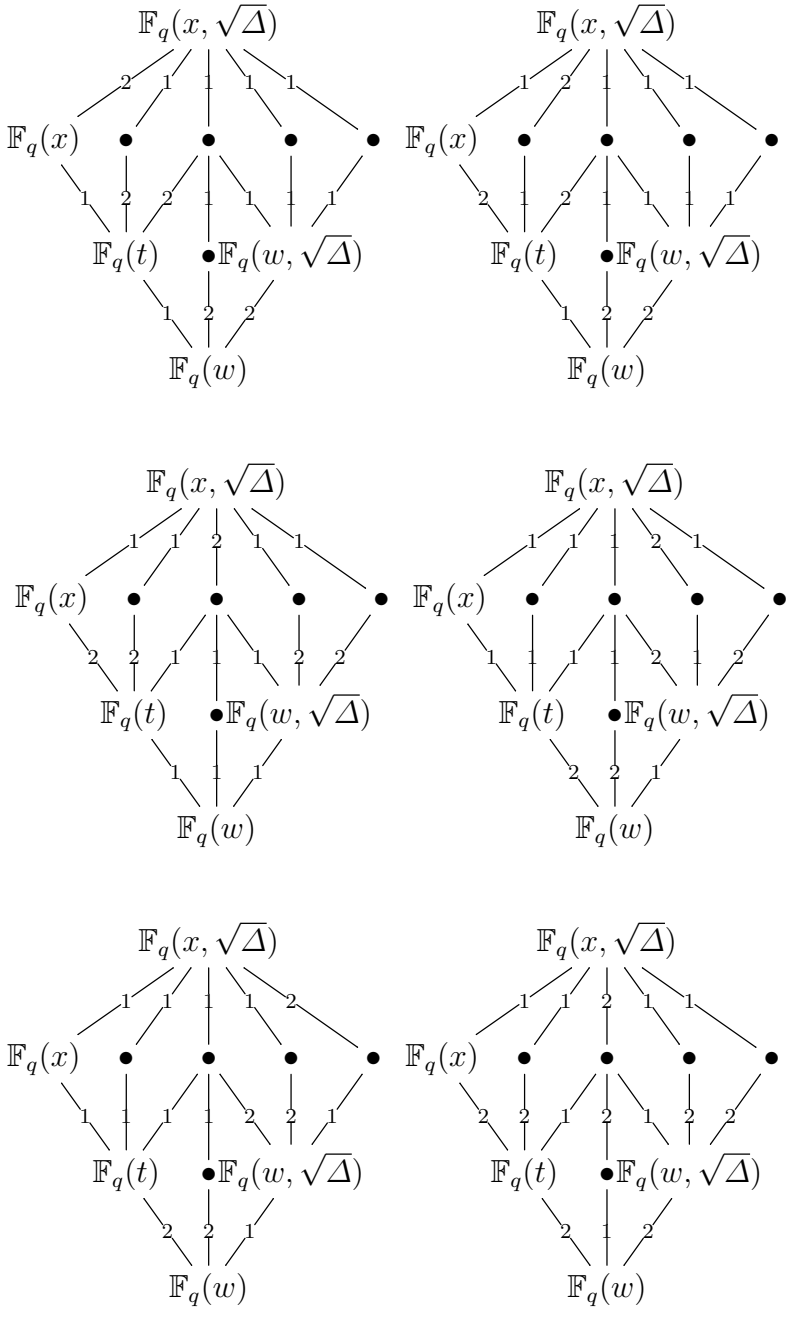
a place of $\mathbb{F}_q(t)$ lying over P. We try to understand the splitting behaviour of Q in $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ which is just determined by the splitting behaviour of P in the extension $\mathbb{F}_q(w, \sqrt{\Delta})/\mathbb{F}_q(w)$. This comes from the subgroup lattice of D_8 and the associated fixed fields extensions which are given below. It is clear that since $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ is not Galois, $\mathbb{F}_q(x)$ is the fixed field of a non-normal subgroup of D_8 of order 2. If we present the group D_8 as $D_8 = \langle r, s | r^4 = e = s^2, rsr^{-1} = s \rangle$, without loss of generality we can assume that the non-normal subgroup of order 2 is given by $\langle s \rangle$. Since the resolvent cubic splits over $\mathbb{F}_q(w, \sqrt{\Delta})$, this field is the fixed field of the subgroup of D_8 which is isomorphic to the Klein-4 group not intersecting with the group $\langle s \rangle$, that is equal to $\langle rs, r^2 \rangle$.





Let Q' be a place of $\mathbb{F}_q(x, \sqrt{\Delta})$ lying over P (that is also over Q). Since P is inert in $\mathbb{F}_q(t)/\mathbb{F}_q(w)$, the inertia group $I(Q'|P)$ is a non-trivial subgroup of D_8.

Since the constant field is a finite field, $I(Q'|P)$ has to be cyclic. Hence $I(Q'|P)$ can be equal to $\langle s\rangle, \langle r^2 s\rangle, \langle r\rangle, \langle r^2\rangle, \langle rs\rangle$ or $\langle r^3 s\rangle$. Using these we determine the inertia degree of the restriction of Q' on the fixed fields as follows:



The first three of the diagrams are not for the inert P in the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ since their inertia degree is not equal to 2. For the others, clearly P is inert in $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ and the splitting behaviour of Q in $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ is the

same as the splitting behaviour of P in $\mathbb{F}_q(w, \sqrt{\Delta})/\mathbb{F}_q(w)$. Notice that Δ is just the norm with respect to the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ of the discriminant of the minimal polynomial of x over $\mathbb{F}_q(t)$. Then we obtain the following lemma:

Lemma 3.28. *Let q be an odd prime power and $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(t) \subseteq \mathbb{F}_q(x)$, with $t = c(x-1)^2$ and $w = c(t-1)^2, c \in \mathbb{F}_q^*$ be a function field tower and Δ' be the discriminant of the minimal polynomial of x over $\mathbb{F}_q(t)$. Let $\Delta = \mathrm{N}_{\mathbb{F}_q(t)/\mathbb{F}_q(w)}(\Delta')$ and Q be a place of $\mathbb{F}_q(t)$ with the restriction P in $\mathbb{F}_q(w)$. Assume P is unramified in $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ and inert in $\mathbb{F}_q(t)/\mathbb{F}_q(w)$. Then Q is inert in $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ if and only if P is inert in $\mathbb{F}_q(w, \sqrt{\Delta})/\mathbb{F}_q(w)$.*

If we continue to consider this situation iteratively we must check for the same in each two level of the tower. As doing this Δ will change at each time. That is, for the tower $\mathbb{F}_q(x_0) \subseteq \mathbb{F}_q(x_1) \subseteq \cdots \subseteq \mathbb{F}_q(x_n) \subseteq \cdots$ where $x_n = c(x_{n+1}-1)^2$ for all $n \geqslant 1$, let P be an unramified place in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$, for all $n \geqslant 1$ and inert in $\mathbb{F}_q(x_1)/\mathbb{F}_q(x_0)$. According to our method above, P is inert in the extensions $\mathbb{F}_q(x_n, \sqrt{\Delta_n})/\mathbb{F}_q(x_n)$ with $\Delta_n = (\frac{16}{c^2})(-\frac{1}{c})(x_n - c)$ for all $n \geqslant 0$ if and only if P is inert in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$ for all $n \geqslant 1$ by the iteration. To consider all of Δ_n, we will find a recursive relation among them.

Say $p(T) = -\frac{1}{c}(T-c)$ and set the sequence $(\alpha(n))_{n\geqslant 0}$ in $\mathbb{F}_q^* \cup \{\infty\}$ such that $\alpha(0) = c$ and $\alpha(n+1) = c(\alpha(n)-1)^2$ for $n \geqslant 0$. Notice that $(\alpha(n))_{n\geqslant 0}$ is periodic since $\mathbb{F}_q$ is finite. Define the polynomials $p_r(T) = -\frac{1}{c}(T - \alpha(r))$ then $(p_r(T))_{r\geqslant 0}$ is also periodic with $p_0(T) = p(T) = -\frac{1}{c}(T-c)$. We will observe for the sequence of polynomials that $\mathrm{N}_{\mathbb{F}_q(x_n)/\mathbb{F}_q(x_{n-r})}(p(x_n))$ is equal to $p_r(x_{n-r})$, up to a square in $\mathbb{F}_q$ for any $0 \leqslant r \leqslant n$. First compute that,

$$\begin{aligned} \mathrm{N}_{\mathbb{F}_q(x_n)/\mathbb{F}_q(x_{n-1})}(p(x_n)) &= \left(-\frac{1}{c}\right)^2 (x_n - c)(-x_n + 2 - c) \\ &\quad \left(-\frac{1}{c}\right)^2 p_1(x_{n-1}), \end{aligned}$$

$$\mathrm{N}_{\mathbb{F}_q(x_{n-1})/\mathbb{F}_q(x_{n-2})}\Big(\Big(-\frac{1}{c}\Big)^2 p_1(x_{n-1})\Big)= \Big(-\frac{1}{c}\Big)^{2^2+2} p_2(x_{n-2}).$$

Doing these iteratively we obtain that,

$$\mathrm{N}_{\mathbb{F}_q(x_n)/\mathbb{F}_q(x_{n-r})}\Big(\Big(-\frac{1}{c}\Big)^{2k} p_{r+1}(x_{n-r-1})\Big) = \Big(-\frac{1}{c}\Big)^{2k'} p_r(x_{n-r}), k, k' \in \mathbb{Z}.$$

By the transitivity of the norm map, we have

$$\mathrm{N}_{\mathbb{F}_q(x_n)/\mathbb{F}_q(x_{n-r})}(p(x_n)) = \Big(-\frac{1}{c}\Big)^{2s} p_r(x_{n-r}), s \in \mathbb{Z}.$$

Also notice that, because of this equality, $\mathrm{N}_{\mathbb{F}_q(x_n)/\mathbb{F}_q(x_{n-r})}(p(x_n))$ is not a square in $\mathbb{F}_q(x_{n-r})$ for any $0 \leqslant r \leqslant n$.

Now we also guarantee that we do not choose a ramified place in the extension $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$ for any $n \geqslant 1$ at the beginning.

Lemma 3.29. *Let P be a place of $\mathbb{F}_q(x_0)$ which is not a pole at x_0. If $x_0(P)$ is not in the sequence $(\alpha(n))_{n\geqslant 0}$ then P is not ramified in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$ for any $n \geqslant 1$.*

Proof. In the extension $\mathbb{F}_q(x_{n+1})/\mathbb{F}_q(x_n)$ we know that x_n and $\frac{1}{x_n}$ ramified and the latter is the pole of x_n. If we compute the restriction of these places on $\mathbb{F}_q(x_0)$ we obtain that $x_0 - \alpha(n)$ and $\frac{1}{x_0}$, respectively. □

Let us now consider the extensions $\mathbb{F}_q\Big(x_0, \sqrt{p_n(x_0)}\Big)/\mathbb{F}_q(x_0)$ for $n \geq 0$. Since the sequence $(p_n(T))_{n\geqslant 0}$ is periodic, there are finitely many such extensions.

Define $M_q := \min\Big\{s \mid \alpha(s) = \pm\alpha(r) \text{ for some } 0 \leq r < s)\Big\}$. For any i, j such that $0 \leqslant i \neq j \leqslant M_q$, $p_i(T)$ and $p_j(T)$ do not have a common root, so the extensions $\mathbb{F}_q\Big(x_0, \sqrt{p_i(x_0)}\Big)/\mathbb{F}_q(x_0)$ and $\mathbb{F}_q\Big(x_0, \sqrt{p_j(x_0)}\Big)/\mathbb{F}_q(x_0)$ are disjoint. Thus we obtain the following result:

Theorem 3.30. *Let P be a place of $\mathbb{F}_q(x_0)$ which is not a pole of x_0 and $x_0(P)$ is not in $(\alpha(n))_{n\geq 0}$. Suppose that P is inert in the extensions $\mathbb{F}_q(x_1)/\mathbb{F}_q(x_0)$ and $\mathbb{F}_q\Big(x_0, \sqrt{p_n(x_0)}\Big)/\mathbb{F}_q(x_0)$, for all $0 \leq n \leq M_q$. Then P is inert in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$ for all $n \geq 1$.*

Proof. We will give the proof by induction on n. For the initial step $n = 1$, the place P is already given as inert in $\mathbb{F}_q(x_1)/\mathbb{F}_q(x_0)$. Now, assume that it is true for n, i.e., P is inert in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$. Let Q_n be the place of $\mathbb{F}_q(x_n)$ lying over P and for $0 \leq r \leq n$, Q_r be its restriction in $\mathbb{F}_q(x_r)$. By assumption P is unramified in $\mathbb{F}_q(x_{n+1})/\mathbb{F}_q(x_0)$.

$Irr(x_{n+1}, \mathbb{F}_q(x_n)) = T^2 - 2T + 1 - \frac{x_n}{c}$ and with discriminant, say Δ', is equal to $\frac{4}{c}x_n$ and $\mathrm{N}_{\mathbb{F}_q(x_n)/\mathbb{F}_q(x_{n-1})}(\Delta') = (\frac{4}{c})^2 x_n(-x_n + 2) = \frac{16}{c^2}(1 - \frac{x_{n-1}}{c})$ which is not a square in $\mathbb{F}_q(x_{n-1})$, then by Lemma 3.28 Q_n is inert in $\mathbb{F}_q(x_{n+1})/\mathbb{F}_q(x_n)$ if and only if Q_{n-1} is inert in $\mathbb{F}_q(x_{n-1}, \mathrm{N}_{\mathbb{F}_q(x_n)/\mathbb{F}_q(x_{n-1})}(\Delta'))/\mathbb{F}_q(x_{n-1})$. If we repeat this, we obtain that Q_n is inert in $\mathbb{F}_q(x_{n+1})/\mathbb{F}_q(x_n)$ if and only if P_{n-2} is inert in $\mathbb{F}_q(x_{n-2}, \mathrm{N}_{\mathbb{F}_q(x_n)/\mathbb{F}_q(x_{n-2})}(\Delta'))/\mathbb{F}_q(x_{n-2})$. Continuing repeatedly, we see that the latter condition is equivalent to saying that the place P is inert in $\mathbb{F}_q(x_0, \mathrm{N}_{\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)}(\Delta'))/\mathbb{F}_q(x_0)$. The norm $\mathrm{N}_{\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)}(\Delta')$ is equal to $p_n(x_0)$ up to a square in $\mathbb{F}_q$. Thus this condition is equivalent P being inert in $\mathbb{F}_q(x_0, \sqrt{p_n(x_0)})/\mathbb{F}_q(x_0)$ which is given in the assumptions. Therefore P is inert in the extension $\mathbb{F}_q(x_{n+1})/\mathbb{F}_q(x_n)$, so is intert in $\mathbb{F}_q(x_{n+1})/\mathbb{F}_q(x_0)$. □

We want to express the statement of this theorem in terms of the coefficients of the initial irreducible polynomial associated to the place P of $\mathbb{F}_q(x_0)$. Let $f(T) \in \mathbb{F}_q[T]$ be an irreducible polynomial of degree d and $f(\alpha(n)) \neq 0$ for all $n \geqslant 0$. To guarantee that we can make a choice so that $\deg f \geqslant 2$ or $f(T) \neq T - \alpha(n)$ for any n. Let γ be a root of f in $\overline{\mathbb{F}_q}$. Observe that

$$\mathbb{F}_q\Big(x_0, \sqrt{p_0(x_0)}\Big) = \mathbb{F}_q\Big(x_0, \sqrt{-\frac{1}{c}(x_0 - c)}\Big).$$

Then P is inert in $\mathbb{F}_q\Big(x_0, \sqrt{p_0(x_0)}\Big) = \mathbb{F}_q(x_0)$ if and only if $-\frac{1}{c}(\gamma - c)$ is not a square in $\mathbb{F}_q(\gamma)$ by Kummer's theorem. Since the norm map is multiplicative, it preserves being a square. That is, if $-\frac{1}{c}(\gamma - c)$ is a non-square in $\mathbb{F}_q(\gamma)$, then $\mathrm{N}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}(-\frac{1}{c}(\gamma - c))$ cannot be a square in $\mathbb{F}_q$. Let us determine the norm of this element. Notice that the minimal polynomial of the element $-\frac{1}{c}(\gamma - c)$ over $\mathbb{F}_q$ is

given by $f(-cT+c)$, where the leading coefficient is $(-c)^d$ times the leading coefficient of f, and $f(c)$ is the constant term. Hence

$$\mathrm{N}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\Big(-\frac{1}{c}(\gamma-c)\Big) = \frac{(-1)^d f(c)}{lc(f)(-c)^d} = \frac{f(c)}{lc(f)c^d}.$$

Thus P is inert in the extension $\mathbb{F}_q\Big(x_0, \sqrt{p_0(x_0)}\Big)/\mathbb{F}_q(x_0)$ if and only if $f(c)/lc(f)c^d$ is a non-square in $\mathbb{F}_q$. In a similar way, for $n \geqslant 1$ we want P to be inert in $\mathbb{F}_q\Big(x_0, \sqrt{p_n(x_0)}\Big)/\mathbb{F}_q(x_0)$, that is $-\frac{1}{c}(\gamma-\alpha(n))$ is a non-square in $\mathbb{F}_q$. Then the minimal polynomial of the element $-\frac{1}{c}(\gamma-\alpha(n))$ is just $f(-cT+\alpha(n))$ with the leading coefficient $(-c)^d$ times the leading coefficient of f and the constant term $(-1)^d f(\alpha(n))$. Thus P is inert in $\mathbb{F}_q\Big(x_0, \sqrt{p_n(x_0)}\Big)/\mathbb{F}_q(x_0)$ if and only if $\frac{f(\alpha(n))}{lc(f)c^d}$ is not a square in $\mathbb{F}_q$.

For the other assumption, namely, the assumption that P is inert in $\mathbb{F}_q(x_1)/\mathbb{F}_q(x_0)$ again by Kummer's Theorem we require that $T^2-2T+1-\frac{\gamma}{c}$ is irreducible over $\mathbb{F}_q(\gamma)$ which is satisfied if and only if its discriminant $4\frac{\gamma}{c}$ is not a square in $\mathbb{F}_q(\gamma)$. Omitting the square factors we want $\frac{\gamma}{c}$ to be a non-square in $\mathbb{F}_q(\gamma)$. Again using the multiplicativity of the norm map we see that $\frac{\gamma}{c}$ is a non-square in $\mathbb{F}_q(\gamma)$ if and only if

$$N_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\Big(\frac{\gamma}{c}\Big) = (\frac{1}{c})^d \,\mathrm{N}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}(\gamma) = (\frac{1}{c})^d(-1)^d f(0)/lc(f)$$

is a non-square in $\mathbb{F}_q$, where $lc(f)$ is the leading coefficient of the polynomial f. Hence we have that P is inert in $\mathbb{F}_q(x_1)/\mathbb{F}_q(x_0)$ if and only if $\frac{(-1)^d}{lc(f)c^d}f(0)$ is a non-square in $\mathbb{F}_q$. Therefore we rephrase the above theorem as follows:

Theorem 3.31. *Let $f(T)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree d with the leading coefficient $lc(f)$ such that $f(\alpha(n)) \neq 0$ for $n \geqslant 0$ with $f(\sigma.\infty) \neq 0$. Suppose that $\frac{(-1)^d}{lc(f)c^d}f(0)$ and $\frac{f(\alpha(n))}{lc(f)c^d}$ are non-square elements of $\mathbb{F}_q$, for $0 \leqslant n \leqslant M_q$. Define the sequence of polynomials*

$$f_0(T) = f(T) \text{ and } f_k(T) = f_{k-1}(c(T-1)^2), k \geqslant 1.$$

Then $f_k(T)$ is an irreducible polynomials over $\mathbb{F}_q$ of degree $d2^k$ for all $k \geqslant 0$. Other direction of the statement is also true.

We can construct a more general result as well.

Theorem 3.32. *Let* $\sigma = \begin{pmatrix} a & b \\ d & e \end{pmatrix} \in GL_2(\mathbb{F}_q)$ *and* $f(T) \in \mathbb{F}_q[T]$ *be an irreducible polynomial of* $\deg f \geqslant 1$ *with the leading coefficient* $lc(f)$ *over* $\mathbb{F}_q$ *satisfying that* $f(\sigma.\infty) \neq 0$ *and* $f(\alpha(n)) \neq 0$ *for* $n \geqslant 0$. *Suppose that, for* $e \neq 0$ *and* $d\alpha(n)+e \neq 0$ *for all* $n \geqslant 0$, *the elements* $\left(-\frac{e}{c}\right)^{\deg f} \frac{1}{lc(f)} f\left(\frac{b}{e}\right)$ *and* $\left(\frac{d\alpha(n)+e}{c}\right)^{\deg f} \frac{1}{lc(f)} f\left(\frac{a\alpha(n)+b}{d\alpha(n)+e}\right)$ *are non-square elements in* $\mathbb{F}_q$ *for* $0 \leqslant n \leqslant M_q$. *Define,* $f_0(T) = f(T)$ *and the polynomials* $f_k(T) = P_{\sigma^{-1}} \circ S_{c,(T-1)^2} \circ P_\sigma(f_{k-1})(T), k \geqslant 1$, *where the map,* $S_{c,(T-1)^2} : \mathbb{F}_q[T] \to \mathbb{F}_q[T]$, *is defined as* $S_{c,(T-1)^2}(g)(T) = g(c(T-1)^2)$, *for any polynomial* $g \in \mathbb{F}_q[T]$. *Then for all* $k \geqslant 0$, $f_k(T)$ *is an irreducible polynomial over* $\mathbb{F}_q$. *The converse is true as well.*

Proof. Just observe that we should consider the transformation, for the initial polynomial $P_{\sigma^{-1}}(g)(T) = g(\sigma^{-1}(T)).(-dT+a)^{\deg g} := f(T)$ where $g(T) \in \mathbb{F}_q[T]$ is an initial polynomial like in Theorem 3.31, now. So we have the modified conditions so that, $\left(-\frac{1}{c}\right)^{\deg g} \frac{1}{lc(g)} g(0) = \left(-\frac{1}{c}\right)^{\deg f} \frac{1}{lc(f)} e^{\deg f} f\left(\frac{b}{e}\right)$ and $\frac{1}{lc(g)} \frac{g(\alpha(n))}{c^{\deg g}} = \frac{1}{c^{\deg f}} \frac{1}{lc(f)} (d\alpha(n)+e)^{\deg f} f\left(\frac{a\alpha(n)+b}{d\alpha(n)+e}\right)$ are non-squares in $\mathbb{F}_q$. □

Remark 3.33. *The above result can be improved also for the cases* $e = 0$, $d\alpha(n)+e = 0$. *Let* $e = 0$ *and* $f(T) = a_s T^s + \cdots + a_1 T + a_0$ *over* $\mathbb{F}_q$. *Observe that* $e^s f(\frac{b}{e}) = a_s b^s + \cdots + a_1 b e^{s-1} + a_0 e^s = a_s b^s$. *Thus, if* $\left(-\frac{1}{c}\right)^s a_s b^s$ *is a non-square in* $\mathbb{F}_q$ *the result follows. Similarly for the case* $d\alpha(n)+e = 0$, *if* $\left(\frac{1}{c}\right)^s a_s (a\alpha(n)+b)^s$ *is a non-square in* $\mathbb{F}_q$ *the result follows.*

3.3.3. A Corollary: the Result of Jones and Boston

Another remarkable result about the construction of irreducible polynomials is given by Jones and Boston in [37] with a correction in [38]. Here one iterates quadratic polynomials over a finite field. We can summarize the part of their results which are of interested as follows:

Lemma 3.34. *[37, Lemma 2.5] Let q be an odd prime power and $g(T) = a_1T^2 + a_2T + a_3 \in \mathbb{F}_q[T]$ with the unique critical point $\gamma = -\frac{a_2}{2a_1}$. Suppose $f(T) \in \mathbb{F}_q[T]$ is an irreducible polynomial with leading coefficient $lc(f)$ and $\deg f \geqslant 1$. Then $f(g^n)$ is irreducible over $\mathbb{F}_q$ for all $n \geqslant 1$ if and only if the set*

$$\{(-a_1)^{\deg f} lc(f) f(g(\gamma))\} \cup \{a_1^{\deg f} lc(f) f(g^k(\gamma)) : i = 2, 3, \cdots\}$$

does not contain a square element in $\mathbb{F}_q$.

Using our approach given in Theorem 3.31, we can give a brief proof for this result. First, observe that any quadratic polynomial $g(T) = a_1T^2+a_2T+a_3 \in \mathbb{F}_q[T]$ with the unique critical point $\gamma = -\frac{a_2}{2a_1}$ can be written as $g(T) = a_1\left(T + \frac{a_2}{2a_1}\right)^2$. Then, with a Möbius twist using the element $\begin{pmatrix} -\frac{a_2}{2a_1} & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_q)$, we obtain that $P_{\sigma^{-1}} \circ S_{-\frac{a_2}{2},(T-1)^2} \circ P_\sigma(f)(T) = f\left(a_1\left(T + \frac{a_2}{2a_1}\right)^2\right)$. That is, taking the constant as $c = -\frac{a_2}{2}$, we see that the transformation $T \mapsto a_1\left(T + \frac{a_2}{2a_1}\right)^2$ is equivalent to the transformation $T \mapsto -\frac{a_2}{2}(T-1)^2$ under the action of $PGL_2(\mathbb{F}_q)$ on the set $\overline{\mathbb{F}_q} \cup \{\infty\}$. As we have shown before, that for each $c \in \mathbb{F}_q^*$, there is only one transformation, $T \mapsto c(T-1)^2$ in the corresponding orbit. Thus $T \mapsto -\frac{a_2}{2}(T-1)^2$ is the same transformation with $T \mapsto a_1\left(T + \frac{a_2}{2a_1}\right)^2$ under this action, i.e., in fact $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, is nothing but the unit linear fractional map. Then we can apply Theorem 3.31 to see that, for any irreducible polynomial f over $\mathbb{F}_q$ of $\deg f \geqslant 1$ with the leading coefficient $lc(f)$ satisfying $f(\alpha(n)) \neq 0$ for $n \geqslant 0$ where $\alpha(0) = -\frac{a_2}{2}$ and $\alpha(n+1) = -\frac{a_2}{2}(\alpha(n)-1)^2$. If the elements $\left(-\frac{1}{(-\frac{a_2}{2})}\right)^{\deg f} \frac{1}{lc(f)} f(0)$ and $\left(\frac{1}{(-\frac{a_2}{2})}\right)^{\deg f} \frac{1}{lc(f)} f(\alpha(n)), n \geqslant 0$ are non-squares in $\mathbb{F}_q$. Notice that these elements are just the squares, $lc(f)^2\left(\frac{a_2}{2}\right)^{2\deg f}$ and $lc(f)^2\left(-\frac{a_2}{2}\right)^{2\deg f}, n \geqslant 0$, multiplied by the elements in the set given in Theorem 3.34, respectively. Therefore, this theorem can be seen as a corollary of Theorem 3.31.

3.4. The Transformations of the Form $c\left(\frac{T-A}{T-B}\right)^2$

For the last case of our classification we will again use the same method. Recall that in this case we consider ramified places not staying the same in each level of the tower. In this case the transformation is given by $c\left(\frac{T-A}{T-B}\right)^2$ with $c, A \in \mathbb{F}_q^*$. We will take $A = 1$ to make the calculations easier, as in the second case. So, B cannot be equal to 1 from now on. At first we again consider two iterations to understand the behaviour of the places. Set the extension as $\mathbb{F}_q(w) \subseteq \mathbb{F}_q(t) \subseteq \mathbb{F}_q(x)$, where $t = c\left(\frac{x-1}{x-B}\right)^2$ and $w = c\left(\frac{t-1}{t-B}\right)^2$ with the ramified places of $\mathbb{F}_q(w)$ in the extensions $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ is $(w = 0)$ and $(w = \infty)$ with $(t = 1)$ and $(t = B)$ lying above them respectively in $\mathbb{F}_q(t)$.

$$
\begin{array}{rccc}
 & \mathbb{F}_q(x) & * & * \\
t = c\left(\frac{x-1}{x-B}\right)^2 & | & | & | \\
 & \mathbb{F}_q(t) & 1 & B \neq 1 \\
w = c\left(\frac{t-1}{t-B}\right)^2 & | & | & | \\
 & \mathbb{F}_q(w) & 0 & \infty
\end{array}
$$

Let $\mathbb{F}_q(w_0) \subseteq \mathbb{F}_q(t_0) \subseteq \mathbb{F}_q(x_0)$, with $t_0 = c_0\left(\frac{x_0-1}{x_0-B}\right)^2$ and $w_0 = c_0\left(\frac{t_0-1}{t_0-B}\right)^2$ for some $c_0 \in \mathbb{F}_q^*$ be another tower in this case. Assume that there is a Möbius transformation which is given by an element $\sigma = \begin{pmatrix} a & b \\ c' & d \end{pmatrix} \in GL_2(\mathbb{F}_q)$ between these two towers such that $\sigma(w_0) = w,\ \sigma(t_0) = t$ and $\sigma(x_0) = x$ fixing the points $0,\ 1$ and ∞. It will be of the form $\sigma = k \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ with $k \neq 0$. Consider that $w = c\left(\frac{t-1}{t-B}\right)^2 = w_0 = c_0\left(\frac{t_0-1}{t_0-B}\right)^2$. Then this equality is satisfied if and only if $c = c_0$ implying that the towers are the same.

This means that, under the action of $PGL_2(\mathbb{F}_q)$ on the projective line $\mathbb{P}^1(\mathbb{F}_q)$, such extensions are equivalent if and only if the scalars of the transformations are the same.

Let us consider such extensions Galois theoretically. Recall that we did this in the previous case while considering the element Δ which is the norm with respect to the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ of the discriminant of the minimal polynomial of x over $\mathbb{F}_q(t)$.

Since $t = c\Big(\frac{x-1}{x-B}\Big)^2$ we have $Irr(x, \mathbb{F}_q(t)) = T^2 - 2\Big(\frac{c-Bt}{c-t}\Big)T + \Big(\frac{c-B^2t}{c-t}\Big)$ with the discriminant $\Delta' = \Big(\frac{4(B-1)^2ct}{(c-t)^2}\Big)$. Then the norm of Δ' with respect to the extension $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ is equal to $(w-c)(w-\frac{c}{B^2})$ up to a square in $\mathbb{F}_q(t)$ or is equal to $t((B+1)t-2B)(2t-(B+1))$ in terms of t again up to a square in $\mathbb{F}_q(t)$. If we work in even characteristic or $B=-1$ in any characteristic, Δ is a square in $\mathbb{F}_q(w)$ and in this situation the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ is Galois with Galois group V, the Klein-4 group. As we observed before we are not interested in this case. Otherwise the extension is not Galois with Galois closure $\mathbb{F}_q(x, \sqrt{\Delta})$ and its Galois group is D_8. In a similar way, with the help of the subgroup diagram of D_8 and the Galois correspondence with the fixed subfields extensions of $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ we have the following:

For an unramified place P of $\mathbb{F}_q(w)$ in the extension $\mathbb{F}_q(x)/\mathbb{F}_q(w)$ which is inert in $\mathbb{F}_q(t)/\mathbb{F}_q(w)$ is inert in the extension $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ if and only if it is inert in $\mathbb{F}_q(w, \sqrt{\Delta})/\mathbb{F}_q(w)$ as in Lemma 3.28.

Let us do this iteratively for the tower $\mathbb{F}_q(x_0) \subseteq \mathbb{F}_q(x_1) \subseteq \cdots \subseteq \mathbb{F}_q(x_n) \subseteq \cdots$ where $x_n = c\Big(\frac{x_{n+1}-1}{x_{n+1}-B}\Big)^2, B \neq \pm 1, c \in \mathbb{F}_q^*$ for all $n \geqslant 0$. Let P be an unramified place in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$, for all $n \geqslant 1$ and inert in $\mathbb{F}_q(x_1)/\mathbb{F}_q(x_0)$. Then P is inert in the extensions $\mathbb{F}_q(x_n, \sqrt{\Delta})/\mathbb{F}_q(x_n)$ for all $n \geqslant 0$ if and only if P is inert in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$ for all $n \geqslant 1$.

Set the recursive relations

$$\alpha(0) = c, \alpha(n+1) = c\Big(\frac{\alpha(n)-1}{\alpha(n)-B}\Big)^2 \text{ and } \beta(0) = \frac{c}{B^2}, \beta(n+1) = c\Big(\frac{\beta(n)-1}{\beta(n)-B}\Big)^2$$

and define the polynomials

$$p_n(T) = (T - \alpha(n))(T - \beta(n)) \text{ with } p_0(T) = p(T) := (T - c)(T - \frac{c}{B^2}).$$

The relation between the polynomials $p_n(T), n \geqslant 0$ is given again using the norm map such that $\mathrm{N}_{\mathbb{F}_q(x_n)/\mathbb{F}_q(x_{n-r})} = kp_r(x_{n-r})$, for some square $k \in \mathbb{F}_q$, thus any of them is not a square in $\mathbb{F}_q(x_{n-r})$. Notice also that $(p_n(T))_{n\geqslant 0}$ is periodic. To guarantee starting with an unramified place we have to take P which is not a pole of x_0 and $x_0(P)$ is not in the sequences $(\alpha(n))_{n\geqslant 0}$ and $(\beta(n))_{n\geqslant 0}$.

Remark 3.35. *The sequences $(\alpha(n))_{n\geqslant 0}$ and $(\beta(n))_{n\geqslant 0}$ can have common elements, so the polynomials $p_r(T)$ may have common roots, for some r. But we must have that $\alpha(n) \neq \beta(n)$ for all n.*

Theorem 3.36. *Let P be a place of $\mathbb{F}_q(x_0)$ which is not a pole of x_0 and $x_0(P)$ is not in $(\alpha(n))_{n\geq 0}$ and $(\beta(n))_{n\geq 0}$. Suppose that P is inert in the extensions $\mathbb{F}_q(x_1)/\mathbb{F}_q(x_0)$ and $\mathbb{F}_q(x_0, \sqrt{p_n(x_0)})/\mathbb{F}_q(x_0)$, for all $0 \leq n \leq M_q$. Then P is inert in $\mathbb{F}_q(x_n)/\mathbb{F}_q(x_0)$ for all $n \geq 1$.*

The proof is just the analogous of the proof of the Theorem 3.30.

Now let $f(T)$ be the irreducible polynomial associated to the place P of $\mathbb{F}_q(x_0)$ of degree d over $\mathbb{F}_q$ with a root $\gamma \in \mathbb{F}_{q^d}$. Observe that,

$$\mathbb{F}_q\Big(x_0, \sqrt{p_0(x_0)}\Big) = \mathbb{F}_q\Big(x_0, \sqrt{(x_0 - c)(x_0 - \frac{c}{B^2})}\Big) = \mathbb{F}_q\Big(x_0, \sqrt{\frac{x_0 - c}{x_0 - \frac{c}{B^2}}}\Big).$$

P is inert in $\mathbb{F}_q(x_0, \sqrt{p_0(x_0)})/\mathbb{F}_q(x_0)$ if and only if $\frac{\gamma - c}{\gamma - \frac{c}{B^2}}$ is not a square in $\mathbb{F}_q(\gamma)$, equivalently if and only if $\mathrm{N}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\Big(\frac{\gamma - c}{\gamma - \frac{c}{B^2}}\Big)$ is not a square in $\mathbb{F}_q$. The minimal polynomial of the element $\frac{\gamma - c}{\gamma - \frac{c}{B^2}}$ over $\mathbb{F}_q$ is $(-T + 1)^d f\Big(\frac{-\frac{c}{B^2}T + c}{-T + 1}\Big)$ with the leading coefficient $(-1)^d f(\frac{c}{B^2})$ and the constant term $(-1)^d f(c)$. Then

$$\mathrm{N}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\Big(\frac{\gamma - c}{\gamma - \frac{c}{B^2}}\Big) = \frac{f(c)}{f(c/B^2)}.$$

For $n \geqslant 1$, P is inert in $\mathbb{F}_q(x_0, \sqrt{p_0(x_0)})/\mathbb{F}_q(x_0)$, i.e., $\frac{\gamma - \alpha(n)}{\gamma - \beta(n)}$ is not a square in $\mathbb{F}_q(\gamma)$ or equivalently $\mathrm{N}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\Big(\frac{\gamma - \alpha(n)}{\gamma - \beta(n)}\Big) = \frac{f(\alpha(n))}{f(\beta(n))}$ is not a square in $\mathbb{F}_q$.

For the other assumption that P is inert in $\mathbb{F}_q(x_1)/\mathbb{F}_q(x_0)$ by using Kummer's Theorem we require that $T^2-2(\frac{c-B\gamma}{c-\gamma})T+(\frac{c-B^2\gamma}{c-\gamma})$ is irreducible over $\mathbb{F}_q(\gamma)$ which is satisfied if and only if the non-square factor of its discriminant $c\gamma$ is not a non-square in $\mathbb{F}_q(\gamma)$ which is equivalent to say that $\mathrm{N}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}(c\gamma) = (-c)^d\frac{f(0)}{lc(f)}$ is a non-square in $\mathbb{F}_q$. Hence we have P is inert in $\mathbb{F}_q(x_1)/\mathbb{F}_q(x_0)$ if and only if $(-c)^d\frac{1}{lc(f)}f(0)$ is a non-square in $\mathbb{F}_q$.

Theorem 3.37. *Let $f(T)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree d such that $f(\alpha(n)) \neq 0$, $f(\beta(n)) \neq 0$ for $n \geqslant 0$ and $\alpha(n) \neq \beta(n)$ for all n. Assume $(-c)^d\frac{1}{lc(f)}f(0)$ and $\frac{f(\alpha(n))}{f(\beta(n))}$ are non-square elements of $\mathbb{F}_q$ for $n \geqslant 0$. Define the sequences of polynomial $f_0(T) = f(T)$ and*

$$f_k(T) = ((T-B)^2)^d f_{k-1}\Big(c\Big(\frac{T-1}{T-B}\Big)^2\Big), k \geqslant 1.$$

Then $f_k(T)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree $d2^k$ for all $k \geqslant 0$. The converse of the statement is true as well.

We can state a more general result like Theorem 3.32 as follows:

Theorem 3.38. *Let $\sigma = \begin{pmatrix} a & b \\ d & e \end{pmatrix} \in GL_2(\mathbb{F}_q)$, $\alpha(n) \neq \beta(n)$, $\forall n$ and $f(T) \in \mathbb{F}_q[T]$ be an irreducible polynomial of $\deg f \geqslant 1$ with the leading coefficient $lc(f)$ over $\mathbb{F}_q$ satisfying that $f(\sigma.\infty) \neq 0$, $f(\alpha(n)) \neq 0$ and $f(\beta(n)) \neq 0$ for $n \geqslant 0$. Suppose that, for $e \neq 0$, $d\beta(n)+e \neq 0$ and $d\alpha(n)+e \neq 0$ for all $n \geqslant 0$, the elements $\Big(-\frac{e}{c}\Big)^{\deg f}\frac{1}{lc(f)}f\Big(\frac{b}{e}\Big)$ and $\Big(\frac{d\alpha(n)+e}{d\beta(n)+e}\Big)^{\deg f}\Big(\frac{f\Big(\frac{a\alpha(n)+b}{d\alpha(n)+e}\Big)}{f\Big(\frac{a\beta(n)+b}{d\beta(n)+e}\Big)}\Big)$ are non-square elements in $\mathbb{F}_q$ for $n \geqslant 0$. Define,*

$$f_0(T) = f(T) \text{ and } f_k(T) = P_{\sigma^{-1}} \circ S_{c,(\frac{T-1}{T-B})^2} \circ P_\sigma(f_{k-1})(T), k \geqslant 1,$$

where the map, $S_{c,(\frac{T-1}{T-B})^2} : \mathbb{F}_q[T] \to \mathbb{F}_q[T]$, is defined as

$$S_{c,(\frac{T-1}{T-B})^2}(g)(T) = ((T-B)^2)^{\deg g} g\Big(c\Big(\frac{T-1}{T-B}\Big)^2\Big),$$

for any polynomial $g \in \mathbb{F}_q[T]$. Then for all $k \geqslant 0$, $f_k(T)$ is an irreducible polynomial over $\mathbb{F}_q$. The converse is also true as well.

3.4.1. Q-Transform

The well-known Q-transformation, $T \to \left(\frac{T^2+1}{T}\right)$, is an example of the third case which is special because of its role in obtaining self-reciprocal polynomials. As we have mentioned in the introduction, this transform was considered in characteristic 2 by Varshamov-Garakov in [19] and [20], Wiedemann in [21], Meyn in [10] and Kyuregyan in [22], explicitly. Recall that we have the following result in the Theorem 1.2: *Suppose* $q = 2^r$ *and* $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0 \in \mathbb{F}_q[T]$ *is an irreducible polynomial with* $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a_{n-1}) = 1$ *and* $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\frac{a_1}{a_0}) = 1$. *Define*

$$f_0 = f \text{ and } f_k(T) = T^{\deg f_{k-1}} f_{k-1}\Big(\frac{T^2+1}{T}\Big) = f_{k-1}^Q(T),$$

for all $k \geqslant 1$. *Then* f_k *is an irreducible polynomial over* $\mathbb{F}_q$, *for all* $k \geqslant 0$.

Moreover, Kyuregyan showed in [23] that the Q-transform gives asequence of N-polynomials in characteristic 2:

Theorem 3.39. *[23, Theorem] For* $q = 2^s$, *let* $f_0(T) = \sum_{i=0}^n c_iT^i$, *be an* N*-polynomial of degree* n *over* $\mathbb{F}_q$ *whose coefficients satisfy the conditions*

$$\sum_{i=0}^{s-1}\Big(\frac{c_1}{c_0}\Big)^{2^i} = 1, \quad \sum_{i=0}^{s-1}\Big(\frac{c_{n-1}}{c_n}\Big)^{2^i} = 1. \tag{3.2}$$

Then $(f_k(T))_{k\geqslant 0}$ *recursively defined by* $f_{k+1}(T) = T^{n2^k} f_k(T + T^{-1})$, $k \geqslant 0$, *is a sequence of* N*-polynomials* $\mathbb{F}_q$ *with* f_k *of degree* $2^k n$.

In addition to the works of Gao [24], Scheerhorn [25], Schwartz [26] and Kyuregyan [27], recently, Alizadeh and Mehrabi [44] gave a new explicit construction of a sequence of normal polynomials over $\mathbb{F}_{2^s}$.

Theorem 3.40. *[44, Theorem 4.1] Let* $G_0(T) = \sum_{i=0}^n d_iT^i \neq T$ *be an* N*-polynomial of degree* n *over* $\mathbb{F}_{2^s}$ *such that* $G_0(T+1)$ *is a self-reciprocal polynomial over* $\mathbb{F}_{2^s}$. *Define*

$$G_{k+1}(T) = T^{n2^{k+1}} G_k\Big(\frac{T^2+T+1}{T^2}\Big), \quad k \geqslant 0.$$

Then $\big(G_k(T)\big)_{k\geqslant 0}$ *and* $\big(G_k(T+1)\big)_{k\geqslant 0}$ *are sequences of* N*-polynomials and self-reciprocal* N*-polynomials of degree* $n2^k$ *over* $\mathbb{F}_{2^s}$*, respectively, if and only if*

$$\mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}\Big(\frac{G_0'(1)}{G_0(1)}\Big) = \mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}\Big(\frac{d_{n-1}}{d_n} + n\Big) = 1, \tag{3.3}$$

where $G_0'(1)$ *is the formal derivative of* $G_0(T)$ *evaluated at* 1.

We show that this new construction is in fact just the Q-transform in disguise. We give a simpler and more conceptual proof of Theorem 3.40 as follows: First, let us remind a lemma of Jungnickel in [45] about the normality of polynomials.

Lemma 3.41. *[45, Proposition 3.1] Let* $\alpha \in \mathbb{F}_{q^n}$ *be normal over* $\mathbb{F}_q$ *and* a, b *elements of* $\mathbb{F}_q$ *with* $a \neq 0$*. Then* $\gamma = a\alpha + b$ *is a normal element of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$ *if and only* $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq -n\frac{b}{a}$.

We will show that Theorem 3.40 is an immediate consequence of Theorem 3.39 and Lemma 3.41 and generalize it. Let $F_0(T) = \sum_{\nu=0}^{n} c_\nu T^\nu$, be a self-reciprocal N-polynomial of degree n over $\mathbb{F}_{2^s}$ whose coefficients satisfy the conditions in (3.2), that is, $\mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}(\frac{c_1}{c_0}) = 1$ and $\mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}(\frac{c_{n-1}}{c_n}) = 1$. Define

$$F_{k+1}(T) = F_k^Q(T) \text{ for } k \geqslant 0.$$

Notice that, by the definition of the Q-transform, substituting $\frac{1}{T}$ in place of T and multiplying by T^{n2^k} both sides of this equation, we obtain

$$T^{n2^k}.F_{k+1}(\frac{1}{T}) = T^{n2^k}(\frac{1}{T})^{n2^k}F_k\Big(\frac{1}{T}+T\Big) = T^{n2^k}F_k\Big(\frac{1}{T}+T\Big) = F_{k+1}(T),$$

i.e., $F_k(T)$ is a self-reciprocal polynomial for all $k \geqslant 0$. Then by Theorem 3.39, $F_k(T) \in \mathbb{F}_{2^s}[T]$ is a self-reciprocal N-polynomial of degree $n2^k$ for $k \geqslant 0$. Let α_k be a root of $F_k(T)$. Since $F_k(T)$ is a self-reciprocal N-polynomial, $\frac{1}{\alpha_k}$ is also a root of $F_k(T)$ and a normal element in $\mathbb{F}_{2^{sn2^k}}$ over $\mathbb{F}_{2^s}$. We have

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_{2^{sn2^k}}/\mathbb{F}_{2^s}}\Big(\frac{1}{\alpha_k}\Big) &= \mathrm{Tr}_{\mathbb{F}_{2^{sn2^k}}/\mathbb{F}_{2^s}}(\alpha_k)\\ &= \alpha_k + \alpha_k^{2^s} + \cdots + \alpha_k^{2^{s(n2^k-1)}}\end{aligned}$$

$$
\begin{aligned}
&= (\alpha_k + \alpha_k^{2^{sn2^{k-1}}}) + (\alpha_k^{2^s} + \alpha_k^{2^{sn2^{k-1}+1}}) + \cdots \\
&\quad \cdots + (\alpha_k^{2^{s(n2^{k-1}-1)}} + \alpha_k^{2^{s(n2^k-1)}}) \\
&= \Big(\alpha_k + \frac{1}{\alpha_k}\Big) + \Big(\alpha_k + \frac{1}{\alpha_k}\Big)^{2^s} + \cdots + \Big(\alpha_k + \frac{1}{\alpha_k}\Big)^{2^{s(n2^{k-1}-1)}} \\
&= \alpha_{k-1} + (\alpha_{k-1})^{2^s} + \cdots + (\alpha_{k-1})^{2^{s(n2^{k-1}-1)}} \\
&= \mathrm{Tr}_{\mathbb{F}_{2^{sn2^{k-1}}}/\mathbb{F}_{2^s}}(\alpha_{k-1}).
\end{aligned}
$$

Note that the equation $\alpha_k + \frac{1}{\alpha_k} = \alpha_{k-1}$ just comes from the definition of the Q-transform. Continuing this way, we obtain

$$\mathrm{Tr}_{\mathbb{F}_{2^{sn2^k}}/\mathbb{F}_{2^s}}(\alpha_k) = \mathrm{Tr}_{\mathbb{F}_{2^{sn2^{k-1}}}/\mathbb{F}_{2^s}}(\alpha_{k-1}) = \cdots = \mathrm{Tr}_{\mathbb{F}_{2^{sn}}/\mathbb{F}_{2^s}}(\alpha_0) = \frac{c_{n-1}}{c_n}.$$

Since by (3.2) we have $\mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{2^{sn}}/\mathbb{F}_{2^s}}(\alpha_0)) = \mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}\big(\frac{c_{n-1}}{c_n}\big) = 1$, we see that $\mathrm{Tr}_{\mathbb{F}_{2^{sn}}/\mathbb{F}_{2^s}}(\alpha_0)$ is not equal to 0. Thus, by Lemma 3.41 with $a = b = 1$ and by using the self-reciprocity of $F_k(T)$ for all $k \geqslant 0$, the polynomials

$$G_k(T) = (T+1)^{n2^k} F_k\Big(\frac{1}{T+1}\Big), \quad k \geqslant 0$$

are N-polynomials of degree $n2^k$ over $\mathbb{F}_{2^s}$. Then $T^{n2^k} G_k\Big(\frac{T+1}{T}\Big) = F_k(T)$. One verifies that

$$
\begin{aligned}
T^{n2^{k+1}} G_{k+1}\Big(\frac{T+1}{T}\Big) &= F_{k+1}(T) = T^{n2^k} F_k\Big(T + \frac{1}{T}\Big) \\
&= T^{n2^k}\Big(T + \frac{1}{T}\Big)^{n2^k} G_k\Big(\frac{(T+\frac{1}{T})+1}{T+\frac{1}{T}}\Big) \\
&= (T^2+1)^{n2^k} G_k\Big(\frac{T^2+T+1}{T^2+1}\Big)
\end{aligned}
$$

Substituting $\frac{1}{T+1}$ in place of T, one obtains

$$
\begin{aligned}
\Big(\frac{1}{T+1}\Big)^{n2^{k+1}} G_{k+1}\Big(\frac{\frac{1}{T+1}+1}{\frac{1}{T+1}}\Big) &= \Big((\frac{1}{T+1})^2+1\Big)^{n2^k} G_k\Big(\frac{(\frac{1}{T+1})^2+(\frac{1}{T+1})+1}{(\frac{1}{T+1})^2+1}\Big) \\
\Rightarrow G_{k+1}(T) &= (\frac{T}{T+1})^{n2^{k+1}} (T+1)^{n2^{k+1}} G_k\Big(\frac{T^2+T+1}{T^2}\Big) \\
\Rightarrow G_{k+1}(T) &= (T^2)^{n2^k} G_k\Big(\frac{T^2+T+1}{T^2}\Big) \quad \text{for } k \geqslant 0.
\end{aligned}
$$

We recover the sequence from Theorem 3.40. The polynomial

$$G_0(T) = (T+1)^n F_0\Big(\frac{1}{T+1}\Big)$$

is the initial polynomial in Theorem 3.40 and

$$T^n G_0\Big(\frac{T+1}{T}\Big) = F_0(T)$$

is a self-reciprocal polynomial by assumption, i.e.,

$$T^n G_0\Big(\frac{T+1}{T}\Big) = T^n\Big(\frac{1}{T}\Big)^n G_0\Big(\frac{\frac{1}{T}+1}{\frac{1}{T}}\Big) = G_0(T+1)$$

is self-reciprocal, as in the initial assumptions of Theorem 3.40. This implies that all members of the sequence $(G_k(T+1))_{k\geqslant 0}$ are also self-reciprocal. The condition (3.3) in Theorem 3.40 corresponds to the condition (3.2) in Theorem 3.39:

As $G_0(T+1) = F_0(T)$, we have $G_0(1) = F_0(0) = c_0$, $G_0'(1) = F_0'(0) = c_1$, $c_n = d_n$ and $c_{n-1} = d_{n-1} + nd_n$. Then $\mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}\Big(\frac{G_0'(1)}{G_0(1)}\Big) = \mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}(\frac{c_1}{c_0})$ and $\mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}\big(\frac{d_{n-1}}{d_n} + n\big) = \mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}\big(\frac{c_{n-1}}{c_n}\big)$.

We can obtain a more general result for the construction of sequences of N-polynomials in even characteristic as an immediate consequence of Theorem 3.39 and Lemma 3.41:

Theorem 3.42. *Let $\mathbb{F}_q$ be a finite field with q elements of even characteristic.*

(i) Let $H_0(T) = \sum_{i=0}^n a_i T^i$ be an N-polynomial of degree n over $\mathbb{F}_q$ such that $H_0(aT+b)$ is a self-reciprocal polynomial over $\mathbb{F}_q$ with elements $a \neq 0, b \in \mathbb{F}_q$ and $nba_n + a_{n-1} \neq 0$. Define

$$H_{k+1}(T) = (T+b)^{n2^k} \cdot H_k\Big(\frac{T^2+bT+a^2}{T+b}\Big), k \geqslant 0.$$

Then $\big(H_k(T)\big)_{k\geqslant 0}$ and $\big(H_k(aT+b)\big)_{k\geqslant 0}$ are sequences of N-polynomials and self-reciprocal N-polynomials of degree $n2^k$ over $\mathbb{F}_q$, respectively, if and only if

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\Big(\frac{aH_0'(b)}{H_0(b)}\Big) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\Big(\frac{a_{n-1}}{aa_n} + \frac{b}{a}n\Big) = 1, \tag{3.4}$$

(ii) Let $S_0(T) = \sum_{i=0}^{n} b_i T^i$ *be an* N*-polynomial of degree* n *over* $\mathbb{F}_q$ *such that* $S_0(\frac{eT+f}{T})(\frac{T}{f})^n$ *is a self-reciprocal polynomial over* $\mathbb{F}_q$ *with elements* $f \neq 0$, $e \in \mathbb{F}_q$ *and* $neb_n + b_{n-1} \neq 0$*. Define*

$$S_{k+1}(T) = (T^2 + f^2 + e^2)^{n2^k} \cdot S_k\Big(\frac{eT^2 + f^2T + e^3}{T^2 + f^2 + e^2}\Big), \;\; k \geqslant 0.$$

Then $\big(S_k(T)\big)_{k\geqslant 0}$ *and* $\big((\frac{T}{f})^n S_k(\frac{eT+f}{T})\big)_{k\geqslant 0}$ *are sequences of* N*-polynomials and self-reciprocal* N*-polynomials of degree* $n2^k$ *over* $\mathbb{F}_q$*, respectively, if and only if*

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\Big(\frac{fS_0'(e)}{S_0(e)}\Big) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\Big(\frac{b_{n-1}}{fb_n} + \frac{e}{f}n\Big) = 1, \tag{3.5}$$

Proof. (i) Let $F_0(T) = \sum_{i=0}^{n} c_i T^i$ be an N-polynomial in $\mathbb{F}_q[T]$ and define $F_{k+1}(T) = F_k^Q(T)$ for $k \geqslant 0$. Set $H_k(T) = F_k(\frac{T+b}{a})$ for all k. Let $H_0(T) = \sum_{i=0}^{n} a_i T^i$. Then consider that

$$\begin{aligned} H_{k+1}(T) &= F_{k+1}\Big(\frac{T+b}{a}\Big) \\ \Rightarrow H_{k+1}(aT+b) &= F_{k+1}(T) = T^{n2^k} F_k\Big(T + \frac{1}{T}\Big) \\ &= T^{n2^k} H_k\Big(a\Big(T + \frac{1}{T}\Big) + b\Big) \\ &= T^{n2^k} H_k\Big(\frac{aT^2 + bT + a}{T}\Big). \end{aligned}$$

Substituting $\frac{T+b}{a}$ in place of T, we obtain

$$\begin{aligned} H_{k+1}(T) &= \Big(\frac{T+b}{a}\Big)^{n2^k} H_k\Big(\frac{a(\frac{T+b}{a})^2 + b(\frac{T+b}{a}) + a}{\frac{T+b}{a}}\Big) \\ &= \Big(\frac{T+b}{a}\Big)^{n2^k} H_k\Big(\frac{T^2 + bT + a^2}{T+b}\Big). \end{aligned}$$

That is,

$$H_{k+1}(T) = \Big(\frac{T+b}{a}\Big)^{n2^k} H_k\Big(\frac{T^2 + bT + a^2}{T+b}\Big), \;\; k \geqslant 0.$$

Since $H_0(aT+b) = F_0(T)$ we can easily see that the coefficients satisfying $c_n = a^n a_n$, $c_{n-1} = a^{n-1}(nba_n + a_{n-1})$, $c_1 = F_0'(0) = aH_0'(b)$ and

$c_0 = F_0(0) = H_0(b)$ which recover the conditions in (3.4) by Lemma 3.41 and Theorem 3.39.

(ii) Similar as in (i) let $F_0(T) = \sum_{i=0}^{n} c_i T^i$ be an N-polynomial in $\mathbb{F}_q[T]$ and define $F_{k+1}(T) = F_k^Q(T)$ for $k \geqslant 0$. Set $S_k(T) = (T+e)^{n2^k} F_k(\frac{f}{T+e})$ for all k. Let $S_0(T) = \sum_{i=0}^{n} b_i T^i$. Then consider that

$$\begin{aligned} S_{k+1}(T) &= (T+e)^{n2^{k+1}} F_{k+1}\Big(\frac{f}{T+e}\Big) \\ \Rightarrow \Big(\frac{T}{f}\Big)^{n2^{k+1}} S_{k+1}\Big(\frac{eT+f}{T}\Big) &= F_{k+1}(T) \\ &= T^{n2^k} F_k\Big(T+\frac{1}{T}\Big) \\ &= T^{n2^k}\Big(\frac{T+\frac{1}{T}}{f}\Big)^{n2^k} S_k\Big(\frac{e(T+\frac{1}{T})+f}{T+\frac{1}{T}}\Big) \\ \Rightarrow S_{k+1}\Big(\frac{eT+f}{T}\Big) &= \frac{(f(T^2+1))^{n2^k}}{T^{n2^{k+1}}} S_k\Big(\frac{eT^2+fT+e}{T^2+1}\Big). \end{aligned}$$

Substituting $\frac{f}{T+e}$ in place of T, we obtain

$$S_{k+1}(T) = \Big(\frac{T^2+e^2+f^2}{f}\Big)^{n2^k} S_k\Big(\frac{eT^2+f^2T+e^3}{T^2+e^2+f^2}\Big), k \geqslant 0.$$

Notice that

$$\Big(\frac{T}{f}\Big)^{n} S_0\Big(\frac{eT+f}{T}\Big) = F_0(T) \tag{3.6}$$

Since $F_0(T)$ is self-reciprocal, i.e., $F_0(T) = T^n F_0 = (\frac{1}{T})$, substituting $\frac{1}{T}$ in place of T and multiplying both sides by T^n of (3.6), we have

$$\Big(\frac{1}{f}\Big)^{n} S_0(e+fT) = T^n F_0(\frac{1}{T}) = F_0(T).$$

Then, the rest of the proof is the same with part (i) for $a = f, b = e$ and $a_i = \frac{b_i}{f^n}$ for all i, giving the conditions in (3.5).

□

Notice that, taking $e = f = 1$ in the second part of the theorem, we recover Theorem 3.40.

On the other hand, Meyn gave some results in [10] for odd characteristic as well. Let us recall the irreducibility of the Q-transform of an irreducible polynomial which is given in Theorem 1.3: *Let q be an odd prime power. If f is an irreducible polynomial of degree n over $\mathbb{F}_q$ then f^Q is irreducible if and only if the element $f(2)f(-2)$ is a non-square in $\mathbb{F}_q$.* There are some incomplete results for the iterations in this paper as well. In [28], Bassa and Menares also gave more explicit statements about the irreducibility of more than one iterations of this transformation. In our work, the Q-transform is just an specific example of Theorem 3.38 with the constant $c = -27,\ B = 9$ and $\sigma = \begin{pmatrix} 2 & -6 \\ 1 & 3 \end{pmatrix} \in GL_2(\mathbb{F}_q)$, in the sense that if $w = -27\left(\frac{t-1}{t-9}\right)^2$ then $\sigma(w) = \frac{\sigma(t)^2+1}{\sigma(t)}$. That is, the given results about Q-transform in odd characteristic can be obtained as a corollary of Theorem 3.38. In particular we consider the condition in Theorem 1.3 just for one iteration with our approach as follows: Let $f(T) = a_nT^n+a_{n-1}T^{n-1}+\cdots+a_1T+a_0$ be an irreducible polynomial in $\mathbb{F}_q$. The leading coefficient of f, a_n, is the constant term of its reciprocal,

$$T^n f\left(\frac{1}{T}\right) = a_n + a_{n-1}T + \cdots + a_0T^n.$$

That is, for the linear fractional map given by the element $\delta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{F}_q)$, we have that

$$P_\delta(f) = T^n f(\delta(T)) = T^n f\left(\frac{1}{T}\right),$$

then $a_n = P_\delta(f)(0)$. Thus we obtain the element, in the condition of Theorem 3.38 for the irreducibility of the first iteration so that

$$\left(-\frac{3}{-27}\right)^{\deg f} \frac{1}{P_{\sigma\cdot\delta}(f)(0)} f\left(\frac{-6}{3}\right) = \left(\frac{1}{3^2}\right)^{\deg f} \frac{f(-2)}{f(2)}$$

which is a non-square in $\mathbb{F}_q$ if and only if $f(-2)f(2)$ is a non-square in $\mathbb{F}_q$.

4. DYNAMICAL BELYI MAPS

In this chapter, we give a joint work with Jacqueline Anderson, Irene Bouw, Ozlem Ejder, Valentijn Karemaker, and Michelle Manes which was started at the Women in Numbers Europe II workshop at the Lorentz Centre in Leiden, and resulted in the paper [39] that was already carried out during this doctorate process. We study the dynamical properties of a large class of rational maps with exactly three ramification points. By constructing families of such maps, we obtain infinitely many conservative maps of degree d; this answers a question of Silverman. Rather precise results on the reduction of these maps yield strong information on the rational dynamics. Due to the relation of the iterative constructions of irreducible polynomials over finite fields with the arithmetical dynamical systems, it gives an extra motivation to investigate and explain their algebraic structure explicitly using the same number theoretical tools.

A *Belyi map* is a finite cover $f : X \to \mathbb{P}^1$ of smooth projective curves defined over $\mathbb{C}$ that is branched exactly at $0, 1, \infty$. Belyi maps can be described topologically as *dessins d'enfants* or combinatorially in terms of generating systems.

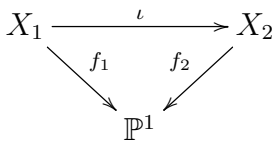
Definition 4.1. *Fix an integer $d > 1$. A generating system of degree d is a triple $\boldsymbol{\rho} = (\rho_1, \rho_2, \rho_3)$ of permutations $\rho_i \in S_d$ that satisfy*

- $\rho_1\rho_2\rho_3 = 1$,
- $G := \langle \rho_1, \rho_2, \rho_3 \rangle \subset S_d$ *acts transitively on* $\{1, 2, \ldots, d\}$.

The combinatorial type of $\boldsymbol{\rho}$ is a tuple $\underline{C} := (d; C(\rho_1), C(\rho_2), C(\rho_3))$, where d is the degree and $C(\rho_i)$ is the conjugacy class of ρ_i in S_d.

Two generating systems $\boldsymbol{\rho}$ and $\boldsymbol{\rho}'$ are *equivalent* if there exists a permutation $\tau \in S_d$ such that $\rho_i' = \tau\rho_i\tau^{-1}$ for $i = 1, 2, 3$. Furthermore, two Belyi maps

$f_i : X_i \to \mathbb{P}^1$ are *isomorphic* if there exists an isomorphism $\iota : X_1 \to X_2$ making



commutative. In particular, the f_i have the same branch locus. Riemann's Existence Theorem ([46, Theorem 2.13]) yields a bijection between equivalence classes of generating systems and isomorphism classes of Belyi maps $f : X \to \mathbb{P}^1$.

Let $\boldsymbol{\rho}$ be a generating system. The conjugacy class $C_i := C(\rho_i)$ of S_d corresponds to a partition $\sum_{j=1}^{r_i} n_j = d$ of d. The *length* $r_i = r(C_i)$ of C_i is the number of cycles of the elements of C_i. Note that we include the 1-cycles. The nonnegative integer $g := (d+2-r_1-r_2-r_3)/2$ is called the *genus* of the generating system. If $f : X \to \mathbb{P}^1$ is the Belyi map corresponding to $\boldsymbol{\rho}$ then $g = g(X)$ and $r_i = |f^{-1}(t_i)|$ is the cardinality of the inverse image of the ith branch point t_i.

We only consider the case that $g = g(X) = 0$. We write

$$f : \mathbb{P}^1_x \to \mathbb{P}^1_t, \qquad x \mapsto t = f(x);$$

the subscript indicates the coordinate of the corresponding projective line. Note that we write f both for the rational function $f(x) \in \mathbb{C}(x)$ and the cover defined by it.

We restrict, moreover, to the case that C_i is the conjugacy class of a single cycle, i.e. for each $i \in \{1,2,3\}$ the partition $\sum_j n_j$ corresponding to C_i contains a unique part n_j different from 1. We denote this part by e_i. Formulated differently, the corresponding Belyi map f has a unique ramification point above t_i, with ramification index e_i. The assumption that $g = g(X) = 0$ translates to the condition

$$2d + 1 = e_1 + e_2 + e_3.$$

We call this situation the *genus*-0 *single-cycle case*, and we write $(d; e_1, e_2, e_3)$ for

the combinatorial type of f. More generally, given four integers d, e_1, e_2, e_3 satisfying $2 \leq e_i \leq d$ and $2d + 1 = e_1 + e_2 + e_3$, we call $(d; e_1, e_2, e_3)$ an *abstract combinatorial type of genus* 0.

We say that a genus-0 single-cycle Belyi map f is *normalized* if its ramification points are $0, 1,$ and ∞, and if, moreover,

$$f(0) = 0, \quad f(1) = 1, \quad f(\infty) = \infty.$$

Since f has three ramification points, every isomorphism class of covers contains a unique normalized Belyi map.

The following proposition states that the triple of conjugacy classes corresponding to the combinatorial type $(d; e_1, e_2, e_3)$ is rigid and rational.

Proposition 4.2. *Let $\underline{C} := (d; e_1, e_2, e_3)$ be an abstract combinatorial type of genus 0. Then there exists a unique normalized Belyi map $f : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ of combinatorial type $\underline{C}$. Moreover, the rational map f may be defined over $\mathbb{Q}$.*

Remark 4.3. *Let $f : \mathbb{P}^1_x \to \mathbb{P}^1_t$ be a normalized Belyi map of combinatorial type $\underline{C} = (d; e_1, e_2, e_3)$, i.e. a genus-$0$ single-cycle map. The coordinates x and t are completely determined by the normalization of the ramification and branch points. Proposition 4.2 states that the (unique) rational function defining the Belyi map f satisfies $f(x) \in \mathbb{Q}(x)$.*

Normalized Belyi maps are examples of *conservative rational maps*, i.e. rational maps $f : \mathbb{P}^1 \to \mathbb{P}^1$ such that every ramification point is fixed. In [47, top of p. 110], Silverman asked if the number of PGL_2-equivalence classes of conservative maps $\mathbb{P}^1 \to \mathbb{P}^1$ of degree d in $\mathbb{Q}[z]$ or $\mathbb{Q}(z)$ may be bounded independently of d. We use Proposition 4.2 to answer this question.

Definition 4.4. *Two rational functions $f, g : \mathbb{P}^1_K \to \mathbb{P}^1_K$ are linearly conjugate over a field K if there is a $\phi \in Aut(\mathbb{P}^1_K) \cong PGL_2(K)$ such that $f^\phi := \phi^{-1} f \phi = g$.*

Note that linear conjugacy respects iteration; that is, if $f^\phi = g$, then $(f^n)^\phi = \left(f^\phi\right)^n = g^n$. Note also that for normalized genus-0 single-cycle Belyi maps Proposition 4.2 implies that linear conjugacy over $\mathbb{C}$ is the same as linear conjugacy over $\mathbb{Q}$, so we may omit the mention of the field.

Lemma 4.5. *Let $f : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ be a normalized Belyi map of combinatorial type $(d; e_1, e_2, e_3)$ and let g be a normalized Belyi map with combinatorial type $(d; e'_1, e'_2, e'_3)$. Then f and g are linearly conjugate over $\mathbb{C}$ if and only if there is some permutation $\sigma \in \mathcal{S}_3$ such that $e_i = e'_{\sigma(i)}$ for $i = 1, 2, 3$.*

Proof. The ramification index of a point is a dynamical invariant in the following sense: for a non-constant function $f : \mathbb{P}^1 \to \mathbb{P}^1$, any point $\alpha \in \mathbb{P}^1$, and any $\phi \in PGL_2$, the ramification indices satisfy $e_\alpha(f) = e_{\phi^{-1}(\alpha)}(f^\phi)$.

In the case of normalized Belyi maps, the only points of $\mathbb{P}^1$ with ramification index greater than one are $t_1 = 0$, $t_2 = 1$, and $t_3 = \infty$. Assume that f and g are normalized Belyi maps with $f^\phi = g$ for some $\phi \in PGL_2$. Then we may define a permutation $\sigma \in S_3$ by

$$e_i = \text{ ramification index of } f \text{ at } t_i \;=\; \text{ramification index of } g \text{ at } \phi^{-1}(t_i) \;= e'_{\sigma(i)}.$$

Conversely, given a permutation $\sigma \in S_3$ and a normalized Belyi map g of combinatorial type $(d; e_{\sigma(1)}, e_{\sigma(2)}, e_{\sigma(3)})$, there exists a unique $\phi \in PGL_2$ satisfying $\phi(t_i) = t_{\sigma(i)}$ for $i = 1, 2, 3$. Proposition 4.2 implies that $g = f^\phi$, since both normalized Belyi maps have the same combinatorial type. □

Lemma 4.5, together with the rationality result from Proposition 4.2, answers Silverman's question in the negative.

Corollary 4.6. *The number of PGL_2-conjugacy classes of conservative polynomials in $\mathbb{Q}[z]$ of degree $d \geq 3$ is at least $\left\lfloor \frac{d-1}{2} \right\rfloor$. The number of PGL_2-conjugacy classes of non-polynomial conservative rational maps in $\mathbb{Q}(z)$ of degree $d \geq 4$ is at least*

$$\sum_{i=1}^{\lfloor \frac{d-1}{3} \rfloor} \left\lfloor \frac{d+1-3i}{2} \right\rfloor. \tag{4.1}$$

Proof. We count the number of PGL_2-conjugacy classes of genus-0 single-cycle normalized Belyi maps in degree d, which serves as a lower bound for all conservative rational maps in the given degree, up to linear conjugacy. By Lemma 4.5, this equals the number of partitions of $2d+1$ into exactly three parts such that each part is at least 2 and none exceed d. The number of partitions equals the cardinality of

$$\{2 \leq e_1 \leq e_2 \leq e_3 \leq d \quad | \quad e_1 + e_2 + e_3 = 2d+1\}. \tag{4.2}$$

If f is a polynomial of degree d, then the ramification index $e_3 = e_\infty(f) = d$. Hence, it is enough to count pairs (e_1, e_2) such that $2 \leq e_1 \leq e_2 \leq d-1$ and $e_1+e_2 = d+1$. We see that e_1 can take on $\lfloor \frac{d-1}{2} \rfloor$ distinct values, and e_2 is determined by e_1.

To count nonpolynomial maps, we use the same strategy for every possible value of $e_3 \leq d-1$. Fixing $e_3 = d-i$, we count pairs (e_1, e_2) such that

$$2 \leq e_1 \leq e_2 \leq d-i \quad \text{and} \quad e_1 + e_2 = d+i+1.$$

These constraints give that $2i+1 \leq e_1 \leq \lfloor \frac{d+i+1}{2} \rfloor$, yielding $\lfloor \frac{d+1-3i}{2} \rfloor$ distinct possibilities.

Finally, the constraints in (4.2) require that $d-1 \geq e_3 \geq \lceil \frac{2d+1}{3} \rceil$. Writing $e_3 = d-i$ gives $1 \leq i \leq \lfloor \frac{d-1}{3} \rfloor$, and the result follows. □

4.1. Families of Dynamical Belyi Maps

In this section we determine some families of normalized dynamical Belyi maps explicitly. These results yield infinitely many explicit maps to which we can apply the dynamical system results from Section 4.4.

Proposition 4.7. *If a normalized Belyi map f has combinatorial type $(d; d-k, k+1, d)$, then $f(x)$ is given by*

$$f(x) = cx^{d-k}(a_0x^k + \ldots + a_{k-1}x + a_k),$$

where

$$a_i := \frac{(-1)^{k-i}}{(d-i)}\binom{k}{i} \text{ and } c = \frac{1}{k!}\prod_{j=0}^{k}(d-j).$$

Proof. It is clear that the ramification index e_3 is d, since f is a polynomial, and that e_1 is $d-k$. We need to show that the ramification index of e_2 is $k+1$. The derivative of f is given by

$$\begin{aligned} f'(x) &= c\sum_{i=0}^{k}\frac{(-1)^{k-i}}{(d-i)}\binom{k}{i}(d-i)x^{d-i-1} \\ &= cx^{d-k-1}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}x^{k-i} \\ &= (-1)^k cx^{d-k-1}(x-1)^k. \end{aligned}$$

Hence the only ramification points of f are $0, 1$ and ∞ and the ramification index e_2 is equal to $k+1$. We are left to show that $f(1) = 1$ which is equivalent to showing that

$$\sum_{i=0}^{k}\left(a_i\prod_{j=0}^{k}(d-j)\right) = \sum_{i=0}^{k}\left((-1)^{k-i}\binom{k}{i}\prod_{\substack{j=0\\ j\neq i}}^{k}(d-j)\right) = k!.$$

We first show that in the above sum, the coefficients of d^l for each $1 \leq l \leq k$ are 0 and the constant term is $k!$. Notice that the coefficient of d^k is $\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}$, which is 0 since this is the binomial expansion of $(x-1)^k$ evaluated at 1. Similarly, for the other terms d^l for $l \geq 1$, we obtain a sum $\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}p(i)$ where $p(x)$ is a polynomial of degree less than k. This sum is also zero. The constant coefficient is

$$\sum_{i=0}^{k}\left((-1)^i\binom{k}{i}\prod_{\substack{j=0\\ j\neq i}}^{k}(j)\right)=\binom{k}{0}k!=k!.$$

□

Remark 4.8. *We now provide an alternative proof of Proposition 4.7. A variant of this proof can be found in the unpublished master's thesis of Michael Eskin; his PhD-thesis [48, Proposition 5.1.2] contains a slightly weaker version of the result. To have the correct ramification at* 0, 1, *and* ∞, *we see that* f *must be of the form*

$$f(x)=x^{d-k}f_1(x) \tag{4.3}$$

for some $f_1(x)=\sum_{i=0}^{k}c_i(x-1)^i$, *such that*

$$f'(x)=(-1)^k c x^{d-k-1}(x-1)^k$$

for some $c\in\mathbb{C}^\times$. *This implies that*

$$c(x-1)^k=(d-k)f_1+xf_1'=c_k d(x-1)^k+\sum_{i=0}^{k-1}\left((d-k+i)c_i+(i+1)c_{i+1}\right)(x-1)^i.$$

This yields a recursive formula for the c_i, *from which it follows that*

$$c_i=(-1)^i\binom{d-k+i-1}{i}$$

for all $i=0,\ldots,k$, *and*

$$c=\binom{d-1}{k}d.$$

Substituting these values for c_i *and* c *back into Equation* (4.3), *the reader may check we obtain the claimed result.*

Example 4.9. *The unique normalized Belyi map* f *of combinatorial type* $(d;d-1,2,d)$ *is given by*

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

Proposition 4.10. *The unique normalized Belyi map f of combinatorial type $(d; d-k, 2k+1, d-k)$ is given by*

$$f(x) = x^{d-k}\left(\frac{a_0x^k - a_1x^{k-1} + \ldots + (-1)^k a_k}{(-1)^k a_k x^k + \ldots - a_1 x + a_0}\right),$$

where

$$a_i := \binom{k}{i} \prod_{k+i+1 \le j \le 2k} (d-j) \prod_{0 \le j \le i-1} (d-j) = k! \binom{d}{i} \binom{d-k-i-1}{k-i}.$$

Proof. The combinatorial type $(d; d-k, 2k+1, d-k)$ is characterized by the fact that the ramification at $x = 0, \infty$ is given by the same conjugacy class in the sense of Definition 4.1. This implies that the Belyi map f admits an automorphism in the following sense: Write $\psi(x) = 1/x$. Then $f^\psi = \psi^{-1} \circ f \circ \psi$ has the same combinatorial type as f. By Proposition 4.2, f is the unique normalized Belyi map of the given type, so $\psi^{-1} \circ f \circ \psi = f$.

From this, it immediately follows that we may write

$$f = x^{d-k} f_1/f_2, \qquad \text{with} \qquad f_2(x) = x^k f_1(1/x).$$

Let $f = g/h$ with

$$g(x) = x^{d-k} \sum_{i=0}^{k} (-1)^{k-i} a_{k-i} x^i \quad \text{and} \quad h(x) = \sum_{j=0}^{k} (-1)^j a_j x^j,$$

where the a_i are as in the statement of the proposition. It is clear that the ramification at $x = 0, \infty$ is as required. Moreover, we see that 0, 1, and ∞ are fixed points of f.

It therefore remains to determine the ramification at $x = 1$. More precisely, we need to show that the derivative satisfies

$$f'(x) = \frac{cx^{d-k-1}(x-1)^{2k}}{h(x)^2}, \tag{4.4}$$

for some non-vanishing constant c. Write $g'h - gh' = x^{d-k-1}\sum_l c_l x^l$. We have

$$c_l = (-1)^{k+l}\sum_{j=0}^{l}(d-k+l-2j)a_{k-l+j}a_j.$$

Here we have used the convention that $a_i = 0$ if $i > k$ or $i < 0$. Equation (4.4) on the a_i therefore translates to

$$\begin{aligned} c &= c_{2k} = (-1)^k(d-k)a_0a_k, \\ c_l &= (-1)^l c\binom{2k}{l} = (-1)^{k+l}\binom{2k}{l}(d-k)a_0a_k, \qquad l = 0,\ldots,2k. \end{aligned} \tag{4.5}$$

Hence, to prove (4.5) it suffices to prove the following:

$$\sum_{j=0}^{l}(d-k+l-2j)a_{k-l+j}a_j = \binom{2k}{l}(d-k)a_ka_0 \tag{4.6}$$

for every $l \leq k$. (In fact, l runs from 0 to $2k$, but by symmetry it suffices to look at $l \leq k$.)

Here and for the rest of the proof, we use the convention that $\binom{n}{m} = 0$ if $m \leq 0$ or $m \geq n$. Hence, the right hand side of (4.6) translates to

$$\begin{aligned} \binom{2k}{l}(d-k)a_ka_0 &= \binom{2k}{l}(d-k)k!\binom{d}{k}k!\binom{d-k-1}{k} \\ &= d(k!)^2\binom{2k}{l}\binom{d-1}{2k}\binom{2k}{k}. \end{aligned}$$

We write $d-k+l-2j$ as the difference of $d-k+l-j$ and j. Then the left hand side of (4.6) becomes

$$d(k!)^2\sum_{j=0}^{l}\left(\binom{d}{j}\binom{d-1}{k-l+j} - \binom{d-1}{j-1}\binom{d}{k-l+j}\right)\binom{d-2k+l-j-1}{l-j} \binom{d-k-j-1}{k-j}.$$

Hence, dividing both sides of (4.6) by $d(k!)^2$, we find that we need to prove that the following equation holds for all integers d, k and l such that $d \geq 2k+1$ and $l \leq k$:

$$\begin{aligned}\sum_{j=0}^{l} \left(\binom{d}{j}\binom{d-1}{k-l+j} - \binom{d-1}{j-1}\binom{d}{k-l+j} \right) \\ \binom{d-2k+l-j-1}{l-j}\binom{d-k-j-1}{k-j} \\ = \binom{2k}{l}\binom{d-1}{2k}\binom{2k}{k}.\end{aligned} \tag{4.7}$$

We fix k, l such that $l \leq k$ and define $F_{k,l}(d, j)$ as the quotient of the jth term in the sum on the left hand side of Equation (4.7) by $\binom{2k}{k}\binom{d-1}{2k}\binom{2k}{l}$.
Note that $F_{k,l}(d, j) = 0$ when $j > l$; this allows us to restate Equation (4.7) in the following form:

$$\sum_{j=0}^{\infty} F_{k,l}(d, j) = 1. \tag{4.8}$$

To prove that Equation (4.7), or equivalently (4.8), holds for every value of $d \geq 2k+1$, we first prove it for $d = 2k+1$, and then show that

$$\sum_{j=0}^{\infty} F_{k,l}(d+1, j) = \sum_{j=0}^{\infty} F_{k,l}(d, j)$$

for any $d \geq 2k+1$.

So first suppose that $d = 2k+1$. Then Equation (4.7) holds, since

$$\begin{aligned}\sum_{j=0}^{l} \left(\binom{2k+1}{j}\binom{2k}{k-l+j} - \binom{2k}{j-1}\binom{2k+1}{k-l+j} \right) \\ = \sum_{j=0}^{l} \binom{2k}{j}\binom{2k}{k-l+j} - \sum_{j=0}^{l-1} \binom{2k}{j}\binom{2k}{k-l+j} = \binom{2k}{l}\binom{2k}{k}.\end{aligned}$$

Next, to show that $\sum_{j=0}^{\infty} F_{k,l}(d+1, j) = \sum_{j=0}^{\infty} F_{k,l}(d, j)$, we write

$$\sum_{j=0}^{\infty} \left(F_{k,l}(d+1, j) - F_{k,l}(d, j) \right)$$

as a telescoping series. More explicitly, running this algorithm in Maple produces an explicit function $G_{k,l}(d,j)$ which satisfies

$$F_{k,l}(d+1,j) - F_{k,l}(d,j) = G_{k,l}(d,j+1) - G_{k,l}(d,j).$$

One may check that $G_{k,l}(d,0) = 0$. Moreover, $G_{k,l}(d,j) = 0$ for all $j > l$ since the same is true for $F_{k,l}(d,j)$. Hence, $\sum_{j=0}^{\infty}(F_{k,l}(d+1,j) - F_{k,l}(d,j))$ equals

$$\sum_{j=0}^{\infty}(G_{k,l}(d,j+1) - G_{k,l}(d,j)) = G_{k,l}(d,l+1) - G_{k,l}(d,0) = 0.$$

Example 4.11. *If a normalized Belyi map f has combinatorial type $(d; d-1, 3, d-1)$, then $f(x)$ is given by*

$$f(x) = x^{d-1}\frac{(d-2)x - d}{-dx + (d-2)}.$$

(Note that necessarily $d \geq 3$ in this case.)

Example 4.12. *If a normalized Belyi map f has combinatorial type $(d; d-2, 5, d-2)$, then $f(x)$ is given by*

$$f(x) = x^{d-2}\left(\frac{(d-3)(d-4)x^2 - 2d(d-4)x + d(d-1)}{d(d-1)x^2 - 2d(d-4)x + (d-3)(d-4)}\right).$$

(Note that necessarily $d \geq 5$ in this case.)

4.2. Reduction Properties of Normalized Belyi Maps

Let

$$f : \mathbb{P}^1_x \to \mathbb{P}^1_t, \qquad x \mapsto f(x) := t$$

be a normalized Belyi map of combinatorial type $\underline{C} := (d; e_1, e_2, e_3)$. Proposition 4.2 implies that $f(x) \in \mathbb{Q}(x)$ is a rational function with coefficients in $\mathbb{Q}$. We start by defining the reduction of f at a rational prime p. Since we assume that the rational function f is normalized, we may write

$$f(x) = \frac{f_1(x)}{f_2(x)},$$

where $f_1, f_2 \in \mathbb{Q}[x]$ are polynomials that are relatively prime. Multiplying numerator and denominator by a common constant $c \in \mathbb{Q}_{>0}$, we may assume that $f_1, f_2 \in \mathbb{Z}[x]$.

For $k = 1, 2$, write

$$f_k = c_k \tilde{f}_k, \quad \text{with } \tilde{f}_k \in \mathbb{Z}[x] \text{ a polynomial of content } 1 \tag{4.9}$$

Let $c = c_1/c_2$. The assumption that $f(1) = 1$ translates to

$$\tilde{f}_2(1) = c\tilde{f}_1(1) \in \mathbb{Z}.$$

Note that $\tilde{f}(x) := \frac{\tilde{f}_1(x)}{\tilde{f}_2(x)}$ need no longer be normalized. The ramification points of $\tilde{f}$ are still $0, 1, \infty$ but $\tilde{f}(1)$ need not be 1. Nonetheless, it makes sense to consider the reduction of $\tilde{f}$ modulo p. We denote the reduction of $\tilde{f}_k$ by $\overline{f}_k$ and put

$$\overline{f} = \frac{\overline{f}_1}{\overline{f}_2}, \qquad \overline{f}_k \in \mathbb{F}_p[x].$$

The definition of $\tilde{f}$ implies that $\overline{f} \neq 0$. We claim that in our situation $\overline{f}$ is not a constant. The proof below is inspired by a remark in [49, Section 4]; note however that Osserman works only with maps in characteristic p, while we consider reduction to characteristic p of maps in characteristic zero.

Proposition 4.13. *Let f be a normalized Belyi map of combinatorial type $\underline{C} := (d; e_1, e_2, e_3)$.*

(1) The reduction $\overline{f}$ is nonconstant.

(2) We have $\overline{f}(0) = 0$ and $\overline{f}(\infty) = \infty$.

(3) We have $\overline{f}(1) \neq 0, \infty$.

Proof. Define $\tilde{f}_1$ and $\tilde{f}_2$ as in Equation (4.9). Let i (resp. j) be maximal such that the coefficient of x^i in $\tilde{f}_1$ (resp. of x^j in $\tilde{f}_2$) is a p-adic unit. Note that the reduction $\overline{f}$ of f is constant if and only if $\tilde{f}_1 \equiv a\tilde{f}_2 \pmod{p}$ or $a\tilde{f}_1 \equiv \tilde{f}_2 \pmod{p}$ for some constant a. It follows that if $\overline{f}$ is constant, then $i = j$.

The definition of the combinatorial type implies that

$$e_1 \leq i \leq d = \deg(\tilde{f}_1), \qquad 0 \leq j \leq d - e_3 = \deg(\tilde{f}_2).$$

Since e_2 is a ramification index, we have that

$$e_2 = 2d + 1 - (e_1 + e_3) \leq d.$$

This implies that $e_1 + e_3 - d > 0$. It follows that

$$i \geq e_1 > d - e_3 \geq j. \tag{4.10}$$

This implies that $\overline{f}$ is nonconstant, and (1) is proved.

Equation (4.10) also implies that

$$\deg(\overline{f}_1) = i > j = \deg(\overline{f}_2).$$

This implies that $\overline{f}(\infty) = \infty$.

Applying the same argument to the minimal i' (resp. j') such that the coefficient of $x^{i'}$ in $\tilde{f}_1$ (resp. the coefficient of $x^{j'}$ in $\tilde{f}_2$) is a p-adic unit shows that

$$ord_0(\overline{f}_1) = i' > j' = ord_0(\overline{f}_2).$$

We conclude that $\overline{f}(0) = 0$, thus proving (2).

It remains to show that $\mu := \overline{f}(1) \neq 0, \infty$. We have

$$ord_0(\overline{f}_1) \geq e_1, \qquad ord_1(\overline{f}_1) \geq e_2.$$

We assume that $\mu = 0$, i.e. $\overline{f}(0) = \overline{f}(1) = 0$. This implies that

$$e_1 + e_2 \leq \deg(\overline{f}_1) \leq \deg(f_1) = d.$$

This yields a contradiction with $e_3 = 2d + 1 - (e_1 + e_2) \leq d$. We conclude that $\mu \neq 0$. Similarly, we conclude that $\mu \neq \infty$. This finishes the proof of (3). □

The following example shows that the reduction of f may be a constant if we omit the assumption on the combinatorial type of f.

Example 4.14. *We consider the rational function*

$$f(x) = \frac{px^4 + x^2}{x^2 + p}.$$

The corresponding cover $f : \mathbb{P}^1 \to \mathbb{P}^1$ is ramified at 6 points, each with ramification degree 2, so it is not a Belyi map as considered in this paper. Moreover, $x = 1$ is not a ramification point. Both the numerator and the denominator of f have content 1. Therefore with our definition of the reduction we obtain

$$\overline{f} = \frac{x^2}{x^2} = 1.$$

Remark 4.15. *In [50, Section 2.3] Silverman gives a different definition of the reduction of f. The difference between Silverman's definition and ours is (roughly speaking) that he does not divide f by the constant c before reducing, as we do in passing from f to $\tilde{f}$. Instead, Silverman only multiplies f_1 and f_2 by a common constant to assume that at least one of the polynomials f_1 or f_2 has content 1.*

We claim that in the case of a normalized Belyi map of ramification type $(d; e_1, e_2, e_3)$, Silverman's definition agrees with ours. To see this, let p be a prime. Recall that

$$1 = f(1) = c\tilde{f}(1) = c\frac{\tilde{f}_1(1)}{\tilde{f}_2(1)}.$$

Then Proposition 4.13.(3) implies that $\tilde{f}_1(1)$ and $\tilde{f}_2(1)$ have the same p-adic valuation, so $\tilde{f}(1)$ is a p-adic unit. Hence, $c = 1/\tilde{f}(1)$ is a p-adic unit, as well.

Note that $c = c_1/c_2$, where c_i is the content of the polynomial f_i, so in particular c is positive. We conclude that $c \in \mathbb{Q}_{>0}$ is a p-adic unit for all primes p, and hence that $c = 1$.

Let $g \in \overline{\mathbb{F}}_p(x)$ be a rational function. We say that the map $\mathbb{P}^1 \to \mathbb{P}^1$ defined by g is *(in)separable* if g is (in)separable. Recall that $g \in \overline{\mathbb{F}}_p(x)$ is inseparable if and only if it is contained in $\overline{\mathbb{F}}_p(x^p)$.

Definition 4.16. *Let $f : \mathbb{P}^1 \to \mathbb{P}^1$ have combinatorial type $(d; e_1, e_2, e_3)$. Let p be a prime. We say that f has good reduction if the reduction $\overline{f}$ also has degree d. If $\overline{f}$ is additionally (in)separable, we say that f has good (in)separable reduction. If f does not have good reduction, we say it has bad reduction.*

In Corollary 4.18 we show that if f has bad reduction, then $\overline{f}$ is inseparable. In particular, we do not have to consider the case of bad separable reduction.

Definition 4.16 is the definition of good reduction used in the theory of arithmetic dynamics. From the point of view of Galois theory, one usually defines "good reduction" to mean good and separable reduction. In our terminology f has bad reduction if and only if $\deg(\overline{f}) < \deg(f)$.

Proposition 4.17. *Let $f : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be a normalized Belyi map of combinatorial type $\underline{C} := (d; e_1, e_2, e_3)$. Assume that the reduction $\overline{f}$ of f to characteristic p is separable. Then*

(a) f has good reduction (i.e., $\overline{d} = d$), and
(b) $p \nmid e_i$ for all i.

Proof. Our definition of the reduction of f, together with the assumption that f is normalized, implies that the points $x = 0, 1, \infty$ on the source $\mathbb{P}^1_{\mathbb{Q}}$ specialize to pairwise distinct points of $\mathbb{P}^1_{\mathbb{F}_p}$ (by Proposition 4.13.(2,3)). In particular, multiplying $\overline{f}$ by a constant (if necessary), we may assume that $\overline{f}$ is also normalized.

We write $f = f_1/f_2$ and $d_1 = \deg(f_1), d_2 = \deg(f_2)$. We denote the degree of $\overline{f}_i$ by $\overline{d}_i$, and define $\overline{d} = \deg(\overline{f})$. The polynomials $\overline{f}_1$ and $\overline{f}_2$ are not necessarily relatively prime. Put $g = \gcd(\overline{f}_1, \overline{f}_2)$ and $\delta = \deg(g)$.

Let $\overline{e}_i$ be the ramification indices of $\overline{f}$ at $x = 0, 1, \infty$, respectively. Our first goal is to compare these to the ramification indices e_i of f. We start by considering

what happens at $x = 0$. For this we write

$$\overline{f}_i = gh_i, \qquad i = 1, 2.$$

Since $\gcd(h_1, h_2) = 1$ it follows that

$$\overline{e}_1 = ord_0(\overline{f}) = ord_0(h_1).$$

The definition of the reduction implies that

$$ord_0(\overline{f}_1) = ord_0(g) + ord_0(h_1) \geq ord_0(f_1) = e_1.$$

For the right-most equality we have used that $\gcd(f_1, f_2) = 1$. Defining $\varepsilon_1 := ord_0(g)$ we obtain

$$\overline{e}_1 + \varepsilon_1 \geq e_1. \tag{4.11}$$

Interchanging the roles of $x = 0$ and $x = 1$, we similarly obtain

$$\overline{e}_2 + \varepsilon_2 \geq e_2, \tag{4.12}$$

where $\varepsilon_2 := ord_1(g)$. Note that interchanging the roles of $x = 0$ and $x = 1$ corresponds to conjugating $\overline{f}$ by $\varphi(x) = 1 - x$. From the definitions it follows immediately that

$$\varepsilon_1 + \varepsilon_2 \leq \delta. \tag{4.13}$$

The definition of the reduction of f and our normalization implies that

$$d = d_1 \geq \overline{d}_1 = \overline{d} + \delta. \tag{4.14}$$

Finally, for the ramification index $\overline{e}_3$ of $\overline{f}$ at ∞ we have

$$d - e_3 = d_2 \geq \overline{d}_2 = \overline{d}_1 - \overline{e}_3 = \overline{d} + \delta - \overline{e}_3. \tag{4.15}$$

Since we assume that $\overline{f}$ is separable, the Riemann–Hurwitz formula applied to $\overline{f}$, together with the inequalities (4.11), (4.12), (4.13), (4.14), and (4.15), yields

$$\begin{aligned} -2 &\geq -2\overline{d} + (\overline{e}_1 - 1) + (\overline{e}_2 - 1) + (\overline{e}_3 - 1) \\ &= (\overline{e}_1 + \varepsilon_1 - 1) + (\overline{e}_2 + \varepsilon_2 - 1) + (\overline{e}_3 - \overline{d} - \delta - 1) + (\delta - \varepsilon_1 - \varepsilon_2) + (-\overline{d}) \\ &\geq -2d + (e_1 - 1) + (e_2 - 1) + (e_3 - 1) = -2. \end{aligned} \tag{4.16}$$

It follows that both inequalities are equalities. The fact that the last inequality is an equality implies that $\overline{d} = d$, and that the inequalities (4.11), (4.12), (4.13), (4.14), and (4.15) are also equalities. This proves Statement (a).

The first inequality in (4.16) is an equality if and only if all ramification of $\overline{f}$ is tame. Hence we have $p \nmid \overline{e}_i$ for all i. The statement $\overline{d} = d$ implies that $\varepsilon_1 = \varepsilon_2 = \delta = 0$. Hence $\overline{e}_i = e_i$ for all i. Statement (b) follows. □

The following is an immediate consequence of Lemma 4.17.

Corollary 4.18. *Let $f : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be a normalized Belyi map of combinatorial type $\underline{C} := (d; e_1, e_2, e_3)$. Assume that f has bad reduction to characteristic p. Then the reduction $\overline{f}$ is inseparable.*

4.3. Good Inseparable Monomial Reduction

In Section 4.4 we determine the dynamical behavior of separable covers f of degree d (of a given combinatorial type), whose reduction modulo p satisfies $\overline{f}(x) = x^d$. Since 1 is a ramification point of $\overline{f}$, it follows that $\overline{f}$ is inseparable, and hence that $p \mid d$. If this happens, we say that f has *good (inseparable) monomial reduction* to characteristic p. In Theorem 4.23 we prove necessary and sufficient conditions for this to occur.

Definition 4.19. *(i) A rational map ψ of degree d in characteristic p can be written uniquely as $\psi = \psi' \circ \phi^n$, where ϕ is the p-Frobenius map and ψ' is separable. Suppose that ψ' is a normalized Belyi map of combinatorial type $(d'; e_1', e_2', e_3')$. Then we call the $\overline{e}_i = p^n e_i'$ for $i = 1, 2, 3$ the* generalized ramification indices *of ψ; we allow d' and each of the e_i' to be trivial.*

(ii) Let $\underline{C} = (d; e_1, e_2, e_3)$ be a combinatorial type such that $e_1 + e_2 + e_3 = 2d + 1$. Then we define

$$S_{\underline{C},p} := \{\psi : \mathbb{P}^1_{\overline{\mathbb{F}}_p} \to \mathbb{P}^1_{\overline{\mathbb{F}}_p} \mid \psi \text{ satisfies the following combinatorial conditions}\}$$

(a) $\deg(\psi) := \overline{d} \leq d$, *and*

(b) there exist $\varepsilon_1, \varepsilon_2, \delta \geq 0$ such that

$$\varepsilon_1 + \varepsilon_2 \leq \delta \leq d - \overline{d}$$

and the generalized ramification indices $\overline{e}_i$ ($i = 1, 2, 3$) of ψ satisfy

$$\overline{e}_1 \geq e_1 - \varepsilon_1,$$

$$\overline{e}_2 \geq e_2 - \varepsilon_2,$$

$$\overline{e}_3 \geq e_3 - (d - \overline{d} - \delta).$$

The set $S_{\underline{C},p}$ may be considered as a characteristic-p analog of the set of normalized Belyi maps of combinatorial type $\underline{C}$. Lemma 4.20 and Proposition 4.21 below imply that this set consists of one element. Moreover, it follows that $\psi \in S_{\underline{C},p}$ is the reduction (in the sense of §4.2) of the (unique) normalized Belyi map of type $\underline{C}$ in characteristic zero. In particular, it follows that $\psi \in S_{\underline{C},p}$ may be defined over $\mathbb{F}_p$.

Lemma 4.20. *Let $f \colon \mathbb{P}^1 \to \mathbb{P}^1$ be a normalized cover in characteristic zero of combinatorial type $\underline{C} = (d; e_1, e_2, e_3)$. Its reduction $\overline{f}$ modulo p lies in $S_{\underline{C},p}$.*

Proof. If f has good reduction at p, choose $\varepsilon_1 = \varepsilon_2 = \delta = 0$ and the result is immediate. If f has bad reduction, the result follows immediately from the proof of Proposition 4.17, for δ and ε_i ($i = 1, 2$) as in that proof. □

The following proposition is a reformulation in our terminology of a result of Osserman.

Proposition 4.21. *[49, Theorem 4.2.(i)] For any combinatorial type $\underline{C}$ and prime number p, we have $|S_{\underline{C},p}| = 1$.*

We sketch the idea of Osserman's approach in his proof of Proposition 4.21. For details we refer to [49] Osserman interprets a rational map $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ (up to automorphisms of the image) of degree d over a field K as a linear series by associating with the rational map $f = f_1/f_2$ the 2-dimensional vector subspace $V := \langle f_1, f_2 \rangle$ of the polynomials of degree less than or equal to d. This linear series may be considered as a point on the Grasmannian $G(1, d)$. The condition that the map has ramification index at least e_i at the point P_i defines a Schubert cycle $\Sigma_{e_i-1}(P_i)$ on $G(1, d)$. Base points of the linear series correspond to common zeros of f_1 and f_2.

Consider an arbitrary linear series in positive characteristic, which we denote by $\langle \psi_1, \psi_2 \rangle$. The inequalities (a) and (b) in Definition 4.19 may be interpreted as conditions on the linear series. Note that we do not require the polynomials ψ_i to be relatively prime. The zeros of $g := \gcd(\psi_1, \psi_2)$ are base points of the linear series. (Compare to the proof of Proposition 4.17, where we denoted the orders of these zeros at $0, 1$ by $\varepsilon_1, \varepsilon_2$, respectively.)

Assume that $\langle \psi_1, \psi_2 \rangle$ is a linear series satisfying the inequalities (a) and (b) from Definition 4.19. The Riemann–Hurwitz formula, together with the condition that $2d + 1 = e_1 + e_2 + e_3$, implies that the linear series $\langle \psi_1, \psi_2 \rangle$ does not have base points if $\psi = \psi_1/\psi_2$ is separable. (This follows as in the proof of Proposition 4.17.) However, the linear series associated with the reduction of a normalized Belyi map (as defined above) may have base points. Moreover, the base-point divisor $D := \varepsilon_1[0] + \varepsilon_2[1] - \delta[\infty]$ need not be unique. (See Example 4.22 below for an example.)

Our Proposition 4.2 states that in characteristic zero the intersection of the three Schubert cycles $\Sigma_{e_1-1}(0) \cap \Sigma_{e_2-1}(1) \cap \Sigma_{e_3-1}(\infty)$ has dimension 0 and the intersection product is 1. In other words, the intersection consists of one point. Osserman gives an intersection-theoretic argument to prove the same statement in arbitrary characteristic. More precisely, he proves that the intersection product of the three Schubert cycles in positive characteristic is scheme-theoretically a point. The underlying point is the unique map $\psi \in S_{\underline{C},p}$.

In this work, we are mainly interested in the case of good inseparable reduction. In this case we have $\varepsilon_1 = \varepsilon_2 = \delta = 0$, hence the base-point divisor is unique in this situation.

We give an example of a combinatorial type $\underline{C}$ for which the reduction of the normalized dynamical Belyi map of this type has base points. Moreover, we will see in that in this case the linear series satisfying the inequalities (a) and (b) is not unique, even though the underlying rational function is.

Example 4.22. *This example is taken from Osserman [49, §2] (two paragraphs above Proposition 2.1). Let p be a prime and $\underline{C} = (d; e_1, e_2, e_3)$ be a type such that $d > p$ and $e_i < p$ for $i = 1, 2, 3$. Then*

$$x^p \in S_{\underline{C},p}$$

as one may verify directly.

We therefore have that $\overline{d} = p = \overline{e}_i$ for all i. The inequalities (a) and (b) from Definition 4.19 become

$$\varepsilon_1 \geq 0, \qquad \varepsilon_2 \geq 0, \qquad \delta \leq d - e_3, \qquad \varepsilon_1 + \varepsilon_2 \leq \delta.$$

We conclude that for a given combinatorial type $\underline{C}$ and prime p the base-point divisor $D = \varepsilon_1[0] + \varepsilon_2[1] - \delta[\infty]$ need not be unique. The linear series corresponding to a solution $(\varepsilon_1, \varepsilon_2, \delta)$ of the inequalities is

$$\langle x^p g, g \rangle, \qquad \text{with } g = x^{\varepsilon_1}(x-1)^{\varepsilon_2}.$$

Dynamical Belyi maps as considered in this example do exist. Here is a concrete instance. Choose $p \geq 7$ *and* d *with* $p < d < 3(p-1)/2$ *and* k *such that* $d - p < k < (p-1)/2$. *Let* $\underline{C} = (d; d-k, 2k+1, d-k)$. *The normalized Belyi map of this combinatorial type is given in Proposition 4.10. The expression for the coefficients* a_i *in that lemma shows both that* $p|a_i$ *for* $d - p + 1 \leq i \leq d$, *and that* $a_i \equiv (-1)^k a_{d-p-i} \bmod p$ *for* $0 \leq i \leq d - p$ *(these are non-zero modulo* p*). From this it follows that*

$$\overline{f} = x^p.$$

Moreover, it follows that

$$g = \gcd(\overline{f}_1, \overline{f}_2) = (-1)^{d-p} a_{d-p} x^{d-p} + \cdots + a_0 \in \mathbb{F}_p[x]$$

has degree $d - p$. *The roots of the polynomial* g *correspond to base points of the linear series.*

Theorem 4.23. *Suppose that* $f \colon \mathbb{P}^1 \to \mathbb{P}^1$ *is a normalized dynamical Belyi map of combinatorial type* $\underline{C} = (d = p^n d'; e_1, e_2, e_3)$, *where* $p \nmid d'$. *Then the reduction* $\overline{f}$ *of* f *modulo* p *satisfies* $\overline{f}(x) = x^d$ *if and only if* $e_2 \leq p^n$.

Proof. In the good monomial reduction case, i.e. where $\overline{f}(x) = x^d$, we have $\overline{d} = d$, and the generalized ramification indices are $\overline{e}_1 = \overline{e}_3 = d$, and $\overline{e}_2 = p^n$. Hence, $e_2 \leq p^n$ is a necessary condition for good inseparable monomial reduction.

Conversely, let f be of combinatorial type $\underline{C} = (d = p^n d', e_1, e_2, e_3)$ as in the statement of the theorem, and assume that $e_2 \leq p^n$. We claim that the map $g(x) = x^d$ lies in $S_{\underline{C},p}$.

As before, we write ψ as the composition of the purely inseparable map of degree p^n and the separable map $\psi'(x) = x^{d'}$, and we write e'_1, e'_2, e'_3 for the ramification indices of ψ' at $x = 0, 1, \infty$, respectively. Clearly, $\deg(\psi) =: \overline{d} = d$ satisfies

$\overline{d} \leq d$. Moreover, the ramification indices $\overline{e}_i$ of g satisfy

$$\begin{aligned}
\overline{e}_1 &:= p^n e_1' = d \geq e_1, \\
\overline{e}_2 &:= p^n \geq e_2, \qquad \text{(by assumption)}, \\
\overline{e}_3 &:= p^n e_3' = d \geq e_3.
\end{aligned}$$

Choosing $\varepsilon_1 = \varepsilon_2 = \delta = 0$, we see that ψ satisfies the combinatorial conditions in Definition 4.19, so indeed $\psi \in S_{\underline{C},p}$. By Lemma 4.20 and Proposition 4.21, we obtain that $\overline{f} = g$, i.e., that f has good inseparable monomial reduction modulo p. □

Example 4.24. *Consider the combinatorial type $\underline{C} = (d = 15; e_1, e_2, e_3 = d = 15)$. The equation for the associated cover is given in [48, Proposition 5.1.2], and can alternatively be determined from Proposition 4.7. Computing the reduction of f modulo the primes $p = 2, 3, 5,$ and 7 yields the following table. We immediately see that the results of the table are in accordance with Theorem 4.23.*

e_2	$\overline{f}(x)$ *at* $p=2$	*Reduction Type*
2	x^{14}	*bad*
3	$x^{15}+x^{14}+x^{13}$	*good separable*
4	x^{12}	*bad*
5	$x^{15}+x^{12}+x^{11}$	*good separable*
6	$x^{14}+x^{12}+x^{10}$	*bad*
7	$x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9$	*good separable*
8	x^8	*bad*
9	$x^{15}+x^8+x^7$	*good separable*
10	$x^{14}+x^8+x^6$	*bad*
11	$x^{15}+x^{14}+x^{13}+x^8+x^7+x^6+x^5$	*good separable*
12	$x^{12}+x^8+x^4$	*bad*
13	$x^{15}+x^{12}+x^{11}+x^8+x^7+x^4+x^3$	*good separable*
14	$x^{14}+x^{12}+x^{10}+x^8+x^6+x^4+x^2$	*bad*

e_2	$\overline{f}(x)$ *at* $p=3$	*Reduction Type*
$e_2 \leq p=3$	x^{15}	*good inseparable*
$p=3<e_2\leq 2p=6$	$2x^{15}+2x^{12}$	*good inseparable*
$2p=6<e_2\leq 3p=9$	x^9	*bad*
$3p=9<e_2\leq 4p=12$	$2x^{15}+x^9+x^6$	*good inseparable*
$4p=12<e_2<5p=d=15$	$x^{15}+x^{12}+x^9+2x^6+2x^3$	*good inseparable*

e_2	$\overline{f}(x)$ *at* $p=5$	*Reduction Type*
$e_2 \leq p=5$	x^{15}	*good inseparable*
$p=5<e_2\leq 2p=10$	$3x^{15}+3x^{10}$	*good inseparable*
$2p=10<e_2<3p=d=15$	$x^{15}+2x^{10}+3x^5$	*good inseparable*

e_2	$\overline{f}(x)$ *at* $p=7$	*Reduction Type*
$e_2\leq 7$	x^{14}	*bad*
$e_2=8$	$5x^{15}+x^{14}+2x^8$	*good separable*
$8<e_2\leq 14$	$6x^{14}+2x^7$	*bad*

4.4. Dynamics

Let $f : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map and let f^n denote the nth iterate of f. The *(forward) orbit* of a point P under f is the set $\mathcal{O}_f(P) = \{f^n(P) : n \geq 0\}$. The *backward orbit* of a point P under f is the set $\bigcup_{n=1}^{\infty}\{Q \in \mathbb{P}^1 : f^n(Q) = P\}$. We say a point $P \in \mathbb{P}^1$ is *periodic* if $f^n(P) = P$ for some positive integer n. The smallest such n is called the *exact period* of P. For a point P of exact period n, we define the *multiplier* of f at P to be the nth derivative of f evaluated at P, denoted by $\lambda_P(f)$. A point P is *preperiodic* if $f^n(P) = f^m(P)$ for some positive integers $n \neq m$. If P is preperiodic but not periodic, we say it is *strictly preperiodic*. Let PrePer$(f, \mathbb{Q})$ denote the set of all rational preperiodic points for f. Our goal is to determine PrePer$(f, \mathbb{Q})$ for an interesting class of Belyi maps.

Theorem 4.25. *Let f be a normalized Belyi map of combinatorial type $(d; e_1, e_2, e_3)$, where d satisfies at least one of the following conditions:*

(i) $p = 2$ *is a divisor of* d *with valuation* $\ell = \nu_2(d)$*,*
(ii) $p = 3$ *is a divisor of* d *with valuation* $\ell = \nu_3(d)$*,*
(iii) $d = p^\ell$ *for some prime* p*.*

Assume that $e_2 \leq p^\ell$. Then PrePer$(f, \mathbb{Q})$ consists entirely of all rational fixed points for f and their rational preimages.

Recall that the condition $e_2 \leq p^\ell$ implies that f has good monomial reduction modulo p (Theorem 4.23). To prove Theorem 4.25, we will use the following well-known theorem.

Theorem 4.26. *[50, Theorem 2.21] Let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a rational function of degree $d \geq 2$ defined over a local field K with residue field k of characteristic p.*

Assume that f has good reduction and that $P \in \mathbb{P}^1(K)$ is a periodic point for f of exact period n. Let m denote the exact period of $\overline{P}$ under the reduced map $\overline{f}$, and let r denote the order of the multiplier $\lambda_{\overline{f}}(\overline{P})$ in k^*. Then one of the following holds: $n = m$, $n = mr$ and $n = mrp^e, e \in \mathbb{Z}, e > 0$.

Proof of Theorem 4.25. Let p be a prime in one of the three cases of the statement. To apply Theorem 4.26, we consider f as element of $\mathbb{Q}_p(x)$.

First suppose that $d = p^\ell$. When we reduce f modulo p, we get $\overline{f}(x) = x^d$. All points in $\mathbb{P}^1(\mathbb{F}_p)$ are fixed points for $\overline{f}$. Moreover, they are all critical points because the derivative of $\overline{f}$ is identically zero, so the multiplier of any point in $\mathbb{F}_p$ is zero. In the language of Theorem 4.26, for any $\alpha \in \mathbb{Q}$ that is periodic under f, we have $m = 1$ and $r = \infty$. Therefore, $n = 1$, so any rational periodic point for f must be a fixed point.

If $2 \mid d$, reduce f modulo 2 to get $\overline{f}(x) = x^d$. All points in $\mathbb{P}^1(\mathbb{F}_2)$ are fixed and critical, so Theorem 4.26 implies that any periodic point for f in $\mathbb{Q}$ must also be fixed.

Now assume that $3 \mid d$. In the case that d is even, the points in $\mathbb{P}^1(\mathbb{F}_3)$ are all fixed under the reduction $\overline{f}$ of f modulo 3. In the case that d is odd, the points $0, 1, \infty$ are fixed and $\overline{f}(-1) = 1$. This implies that -1 is strictly preperiodic. In either case, the only periodic points for $\overline{f}$ are fixed and critical, so once again Theorem 4.26 implies that all rational periodic points for f must also be fixed points.

In all cases, the only periodic rational points for f are fixed points. Thus, PrePer$(f, \mathbb{Q})$ consists solely of rational fixed points and their rational preimages. □

Remark 4.27. *Each of the three conditions on primes dividing d in Theorem 4.25 ensures that all periodic points for the reduced map $\overline{f}$ are fixed points. This is not always true for arbitrary d and p. For example, if $d = 35$ and we reduce modulo 5, the resulting map $\overline{f}(x) = x^{35}$ on $\mathbb{F}_5$ contains a periodic cycle of length two: $\overline{f}(2) = 3$ and $\overline{f}(3) = 2$. If we instead reduce modulo 7, we see that $\overline{f}$ on $\mathbb{F}_7$ also has a 2-cycle: $\overline{f}(2) = 4$ and $\overline{f}(4) = 2$. Thus in this case, we cannot use Theorem 4.26 to deduce a statement analogous to that of Theorem 4.25 because it is possible that f contains a rational periodic point of exact period 2.*

The following proposition gives a slightly stronger statement than Theorem 4.25 in the first case of that theorem.

Proposition 4.28. *Let f be the unique normalized Belyi map of combinatorial type $(d; d-k, k+1, d)$. Write $\nu := \nu_2(d)$ for the 2-adic valuation of d. Assume that $k+1 \leq 2^\nu$. Then the only fixed points of f in $\mathbb{P}^1(\mathbb{Q})$ are $x = 0, 1, \infty$.*

Proof. Recall from Theorem 4.23 that the condition $k+1 \leq 2^\nu$ implies that f has good monomial reduction to characteristic 2. As in Remark 4.8, we write

$$f(x) = x^{d-k}\left(\sum_{i=0}^{k} c_i(x-1)^i\right), \qquad \text{with } c_i = (-1)^i\binom{d-k+i-1}{i}.$$

In particular, $c_0 = 1$. One easily checks that

$$h(x) := \frac{f(x)-x}{x(x-1)} = \left(\sum_{i=0}^{d-k-2} x^i + x^{d-k-1}\sum_{i=0}^{k-1} c_{i+1}(x-1)^i\right).$$

Since f is branched at 3 points, we have that $d-k \geq 2$. It follows that

$$h(0) \equiv 1 \pmod 2, \qquad h(1) = d-k-1-\binom{d-k}{1} \equiv 1 \pmod 2.$$

Therefore the reduction $\overline{h}(x)$ of $h(x)$ modulo 2 does not have any roots in $\mathbb{F}_2$, and hence h does not have any roots in $\mathbb{Q}$. Here we have used that h has good reduction to characteristic 2, i.e. $\deg(h) = \deg(\overline{h})$. This implies that h does not have any rational roots that specialize to ∞ when reduced modulo 2. □

We will now look at one particular family of normalized Belyi maps and use Theorem 4.25 to determine PrePer$(f, \mathbb{Q})$. Let $d \geq 3$ be the degree of f. Consider the following family:

$$f(x) = -(d-1)x^d + dx^{d-1}. \tag{4.17}$$

Recall from Example 4.9 that this is the unique normalized Belyi map of combinatorial type $(d; d-1, 2, d)$.

Proposition 4.29. *Let f be defined as in Equation* (4.17)*. Then:*

(i) The only fixed points for f in $\mathbb{P}^1(\mathbb{Q})$ are $0, 1$ and ∞ (for all d) and $\frac{1}{2}$ (for $d = 3$).

(ii) The only additional rational points in the backward orbits of these fixed points are $\frac{d}{d-1}$ (for all d) and $-\frac{1}{2}$ (for $d = 3$).

Proof. (i) The fixed points of f are the roots of $f(x)-x = -(d-1)x^d+dx^{d-1}-x$, which factors as follows:

$$f(x) - x = x(x-1)(-(d-1)x^{d-2} + x^{d-3} + x^{d-4} + \ldots + x + 1).$$

By the rational root theorem, any nonzero rational zero of the above polynomial is of the form $\frac{1}{b}$, where b divides $d-1$. If $\frac{1}{b}$ is a root of $f(x) - x$, then b satisfies:

$$\frac{b^{d-1} - 1}{b - 1} = b^{d-2} + b^{d-3} + \ldots + b + 1 = d. \tag{4.18}$$

Claim: Equation (4.18) does not have any integer solutions for $d \geq 4$.

Statement (1) immediately follows from the claim.

By inspection, it follows that $b \notin \{0, \pm 1\}$, so we may assume $|b| \geq 2$. Note that we must have $b \leq -2$ because if $b > 1$, the left hand side of Equation (4.18) is strictly greater than d. Moreover, since b is negative, d must be even, since the left hand side of Equation (4.18) is positive. Since $d \geq 4$ and

$b \leq -2$, we have:

$$\sum_{i=0}^{d-2} b^i > b^{d-2} + b^{d-3} = (-b)^{d-3}(-b+1) \geq 3 \cdot 2^{d-3} > d.$$

The claim follows.

(ii) We have the following by direct calculation:

$$f^{-1}(0) = \left\{0, \frac{d}{d-1}\right\}.$$

If $d = 3, f^{-1}(1) = \{1, -\frac{1}{2}\}$. Otherwise, if $d > 3$, an argument similar to that in Part 1 shows that $f^{-1}(1) \bigcap \mathbb{Q} = \{1\}$: Suppose that $f(\frac{1}{b}) = 1$, where $b \in \mathbb{Z}$. (By the rational root theorem, any such rational preimage is of this form.) Then, $f(\frac{1}{b}) - 1 = 0$, which, after factoring $(x-1)$ from the left hand side, gives the following equation:

$$\sum_{i=0}^{d-1} b^i = d.$$

Note that $b = 1$ is one solution to this equation. Any other solution for b would require $b < 0$ and in particular, $b \leq -2$. Therefore, d must be odd for the sum to be positive. If $d \geq 5$, we have the following:

$$\sum_{i=0}^{d-1} b^i \geq b^{d-1} + b^{d-2} \geq |b|^{d-2} \geq 2^{d-2} > d.$$

Thus, $f^{-1}(1) \bigcap \mathbb{Q} = \{1\}$.

A direct calculation also shows that if $d = 3$, then $-\frac{1}{2}$ has no rational preimages, and $\frac{1}{2}$ has no rational preimages except itself. It remains to show that $\frac{d}{d-1}$ has no rational preimages. Suppose $f(\frac{a}{b}) = \frac{d}{d-1}$ for some relatively prime integers a and b. The rational root theorem implies that $a|d$ and $b|(d-1)^2$. After clearing denominators, we have the following equation:

$$-(d-1)^2 a^d + d(d-1)a^{d-1}b - db^d = 0. \tag{4.19}$$

Reducing modulo $d-1$ yields $-b^d \equiv 0$, so $(d-1)|b^d$. Reducing modulo d yields $-a^d \equiv 0$, so $d|a^d$. Let p be a prime dividing d. Suppose that the valuation $\nu_p(d) = k \geq 1$ and $\nu_p(a) = \ell$, for $1 \leq \ell \leq k$. Then
$\nu_p(-(d-1)^2 a^d + d(d-1)a^{d-1}b - db^d) = k$ because $\nu_p(db^d) = k$ and

$\nu_p(-(d-1)^2a^d + d(d-1)a^{d-1}b) \geq \max\{\ell^d, k+\ell^{d-1}\} > k$. This contradicts Equation (4.19).

□

Corollary 4.30. *Let f be the polynomial of degree d in the family defined in Equation* (4.17)*, where either $2 \mid d, 3 \mid d$, or $d = p^\ell$ for some prime p. Then:*

(i) $\mathit{PrePer}(f, \mathbb{Q}) = \{0, 1, \frac{3}{2}, \frac{1}{2}, -\frac{1}{2}, \infty\}$ *if* $d = 3$.

(ii) $\mathit{PrePer}(f, \mathbb{Q}) = \left\{0, 1, \frac{d}{d-1}, \infty\right\}$ *if* $d \neq 3$.

Proof. Theorem 4.25 states that $\mathrm{PrePer}(f, \mathbb{Q})$ consists solely of fixed points for f and their rational preimages. Proposition 4.29 then completely describes all rational preperiodic points for f. □

Remark 4.31. *The statement of Proposition 4.29.(2) may be partially generalized. For simplicity we restrict to the case that f is the unique normalized Belyi map of combinatorial type $(d; d-k, k+1, d)$. An explicit formula for f was determined in Proposition 4.7. We use the terminology of that result.*

In the proof of Proposition 4.7 we showed that the derivative of f satisfies

$$f'(x) = (-1)^k c x^{d-k-1}(x-1)^k, \qquad \text{with } c > 0.$$

Distinguishing 4 cases depending on whether k and d are even or odd and considering the sign of f' yields the following statement for the real elements in the fibers $f^{-1}(0)$ and $f^{-1}(1)$.

(i) Suppose that d and k are both even. Then $f^{-1}(0) \cap \mathbb{R} = \{0\}$ and $f^{-1}(1) \cap \mathbb{R} = \{1, \beta\}$ for some $\beta < 0$.

(ii) Suppose that d is odd and k is even. Then $f^{-1}(0) \cap \mathbb{R} = \{0\}$ and $f^{-1}(1) \cap \mathbb{R} = \{1\}$.

(iii) Suppose that d is even and k is odd. Then $f^{-1}(0) \cap \mathbb{R} = \{0, \gamma\}$ for some $\gamma > 1$ and $f^{-1}(1) \cap \mathbb{R} = \{1\}$.

(iv) Suppose that d and k are both odd. Then $f^{-1}(0) \cap \mathbb{R} = \{0, \gamma\}$ for some $\gamma > 1$ and $f^{-1}(1) \cap \mathbb{R} = \{1, \beta\}$ for some $\beta < 0$.

In particular, this determines the rational values in $f^{-1}(0)$ and $f^{-1}(1)$ in the case that d is odd and k is even. In the other cases, in principle it is possible to analyze when the real roots β, γ are rational, similarly to the proof of Proposition 4.29. In Proposition 4.7 we showed that the leading coefficient of $f(x)$ is $ca_0 = (-1)^k \binom{d-1}{k}$. It follows that if $\beta < 0$ is a rational root of $f(x) - 1$, then we have

$$\beta = \frac{-1}{b} \qquad \text{with } b \in \mathbb{N} \text{ such that } b \mid \binom{d-1}{k}.$$

Similarly, assume that $\gamma > 1$ is a rational root of $f(x)$. We use the expression $f(x) = x^{d-k} \sum_{i=0}^{k} c_i (x-1)^i$ from Remark 4.8. Since $c_0 = 1$ and $c_k = \pm\binom{d-1}{k}$, we find

$$\gamma = 1 + \frac{1}{c} \qquad \text{with } c \in \mathbb{N} \text{ such that } c \mid \binom{d-1}{k}.$$

5. CONCLUSION

In this thesis, we classify and normalize the rational transformations of degree 2 using the behaviour of the ramified places in the corresponding rational function field extensions over the finite field $\mathbb{F}_q$. Then we investigate the explicit constructions of irreducible polynomials over $\mathbb{F}_q$ using Galois theory and some basic observations in group theory. This approach helps to better understand the iterative constructions and gives various generalisations of them. It also enables to determine the requirements put on the initial polynomials.

REFERENCES

1. Berlekamp, E. R., *Algebraic Coding Theory*, McGraw-Hill Book, New York, 1968.

2. Lidl, R. and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1987.

3. MacWilliams, F. and N. Sloane, *The Theory of Error-Correcting Codes*, Northholland Publishing Company, Amsterdam, New York, Oxford, 2nd edn., 1978.

4. Blake, I. F., G. Seroussi and N. P. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1999.

5. Chor, B. and R. Rivest, "A Knapsack-type Public Key Cryptosystem Based on Arithmetic in Finite Fields", *Transactions of Information Theory*, Vol. 34, pp. 901–909, 1988.

6. Koblitz, N., *Algebraic Aspects of Cryptography*, Springer, Berlin, 1998.

7. Calmet, J., "Algebraic Algorithms in GF(q)", *Discrete Mathematics*, Vol. 56, No. 2, pp. 101–109, 1985.

8. Capelli, A., "Sulla Rudittibilit a Delle Equazioni Algebriche I", *Società Nazionale di Scienze, Lettere ed Arti in Napoli*, Vol. 3, pp. 243–252, 1897.

9. Cohen, S., "On Irreducible Polynomials of Certain Types in Finite Fields", *Proceedings of the Cambridge Philosophical Society*, Vol. 66, pp. 335–344, 1969.

10. Meyn, H., "On the Construction of Irreducible Self-reciprocal Polynomials over Finite Fields", *Applicable Algebra in Engineering, Communication and Com-*

puting, Vol. 1, No. 1, pp. 43–53, 1990.

11. Jia, Y., S. Ling and C. Xing, "On Self-dual Cyclic Codes over Finite Fields", *Transactions on Information Theory*, Vol. 57, No. 4, pp. 2243–2251, 2011.

12. Xing, Y. and J. L. Massey, "The Condition for a Cyclic Code to Have a Complementary Dual", *Discrete Mathematics*, Vol. 126, pp. 391–393, 1994.

13. Hong, S. J. and D. C. Bossen, "On Some Properties of Self-reciprocal Polynomials", *Transactions on Information Theory*, Vol. 21, pp. 462–464, 1975.

14. Yucas, J. L. and G. Mullen, "Self-reciprocal Irreducible Polynomials over Finite Fields", *Designs, Codes and Cryptography*, Vol. 33, No. 3, pp. 275–281, 2004.

15. Massey, J. L., "Reversible codes", *Information and Control*, Vol. 7, No. 3, pp. 369–380, 1964.

16. Patel, A. M. and S. J. Hong, "Optimal Rectangular Code for High Density Magnetic Tapes", *IBM Journal of Research and Development*, Vol. 18, pp. 579–588, 1974.

17. Miller, R. L., "Necklaces, Symmetries and Self-Reciprocal Polynomials", *Discrete Mathematics*, Vol. 22, pp. 25–33, 1978.

18. Gilbert, E. N. and J. Riordan, "Symmetry Types of Periodic Sequences", *Illinois Journal of Mathematics*, Vol. 5, pp. 657–665, 1961.

19. Varshamov, R. R. and G. A. Garakov, "On the Theory of Self-dual Polynomials over a Galois Field", *Bulletin Mathematique de la Societe des Sciences Mathematiques de Roumanie*, Vol. 13, pp. 403–415, 1969.

20. Varshamov, R. R., "A General Method for Constructing Irreducible Polynomials over Galois Fields,", *Doklady Akademii Nauk SSSR*, Vol. 275, pp. 1041–1044,

1984.

21. Wiedemann, D., "An Iterated Quadratic Extension of $GF(2)$", *The Fibonacci Quarterly*, Vol. 26, pp. 290–295, 1988.

22. Kyuregyan, M. K., "Recurrent Methods for Constructing Irreducible Polynomials over $GF(2)$", *Finite Fields and Their Applications*, Vol. 8, No. 1, pp. 52–68, 2002.

23. Kyuregyan, M. K., "Recursive Constructions of N-polynomials over $GF(2^s)$", *Discrete Applied Mathematics, Combinatorial Algorithms, Optimization and Computer Science*, Vol. 156, No. 9, pp. 1554–1559, 2008.

24. Gao, S., *Normal Bases over Finite Fields*, Ph.D. Thesis, University of Waterloo, 1993.

25. Scheerhorn, A., "Iterated Constructions of Normal Bases over Finite Fields", *Finite Fields: Theory, Applications and Algorithms: American Mathematical Society*, pp. 309–325, 1994.

26. Schwartz, S., "Irreducible polynomials over finite fields with linearly independent roots", *Mathematica Slovaca*, Vol. 38, pp. 147–158, 1988.

27. Kyuregyan, M. K., "Iterated Construction of Irreducible Polynomials over Finite Fields with Linearly Independent Roots", *Finite Fields and Their Applications*, Vol. 10, No. 3, pp. 323–341, 2004.

28. Bassa, A. and R. Menares, "Galois Theory and Iterative Constructions of Irreducible Polynomials", In preparation, 2022.

29. Chapman, R., "Completely Normal Elements in Iterated Quadratic Extensions of Finite Fields", *Finite Fields and their Applications. Academic Press, Orlando*, Vol. 3, No. 1, pp. 1–10, 1997.

30. Kyuregyan, M. K., "Recurrent Methods for Constructing Irreducible Polynomials over $\mathbb{F}_q$ of Odd Characteristics, II", *Finite Fields and Their Applications*, Vol. 9, pp. 357–378, 2006.

31. Menezes, A. J., I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone and T. Yaghoobian, *Applications of Finite Fields*, Springer US, Boston, MA, 1993.

32. Cohen, S. D., "The Explicit Constructions of Irreducible Polynomials over Finite Fields", *Designs, Codes and Cryptography*, Vol. 2, No. 2, pp. 169–174, 1992.

33. McNay, G., *Topics in Finite Fields*, Ph.D. Thesis, University of Glasgow, 1995.

34. Meyn, H., "Explicit N-polynomials of 2-power Degree over Finite Fields, I", *Designs, Codes and Cryptography*, Vol. 6, No. 2, pp. 107–116, 1995.

35. Bassa, A. and R. Menares, "The R-transform as a Power Map and Its Generalisations to Higher Degree", ArXiv:1909.02608 [cs], 2019.

36. Stichtenoth, H., *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.

37. Jones, R. and N. Boston, "Settled Polynomials over Finite Fields", *Proceedings of the American Mathematical Society*, Vol. 140, No. 6, pp. 1849–1863, 2012.

38. Jones, R. and N. Boston, "Errata to "Settled Polynomials over Finite Fields", *Proceedings of the American Mathematical Society*, Vol. 148, pp. 913–914, 2020.

39. Anderson, J., I. Bouw, O. Ejder, N. Girgin, V. Karemaker and M. Manes, "Dynamical Belyi Maps", *Women in Numbers Europe II, Association for Women in Mathematics Series,Springer*, Vol. 11, pp. 57–82, 2018.

40. Aravena, A., “Iterated Constructions of Completely Normal Polynomials”, *Finite Fields Their Applications*, Vol. 68, p. 101755, 2020.

41. Kyuregyan, M. K., “Recurrent Methods for Constructing Irreducible Polynomials over $\mathbb{F}_q$ of Odd Characteristics”, *Finite Fields and Their Applications*, Vol. 9, pp. 39–58, 2003.

42. Kaplansky, I., *Fields and Rings, 2nd edition*, University of Chicago Press, Chicago, 1972.

43. Kappe, L. C. and B. Warren, “An Elementary Test for the Galois Group of a Quartic Polynomial”, *The American Mathematical Monthly*, Vol. 96, pp. 133–137, 1989.

44. Alizadeh, M. and S. Mehrabi, “Construction of Self-reciprocal Normal Polynomials over Finite Fields of Even Characteristic”, *Turkish Journal of Mathematics*, Vol. 39, No. 2, pp. 259–267, 2015.

45. Jungnickel, D., “Trace-orthogonal Normal Basis”, *Discrete Applied Mathematics*, Vol. 47, No. 3, pp. 233–249, 1993.

46. Völklein, H., *Groups as Galois groups*, Cambridge University Press, Cambridge, 1996.

47. Silverman, J. H., *Moduli Spaces and Arithmetic Dynamics*, American Mathematical Society, Rhode Island, 2012.

48. Eskin, M., *Stable Reduction of Three-point Covers*, Ph.D. Thesis, Ulm University, 2015.

49. Osserman, B., “Rational Functions with Given Ramification in Characteristic p”, *Compositio Mathematica*, Vol. 142, No. 2, pp. 433–450, 2006.

50. Silverman, J. H., *The Arithmetic of Dynamical Systems*, Graduate Texts in Mathematics, no. 241, Springers, New York, 2007.